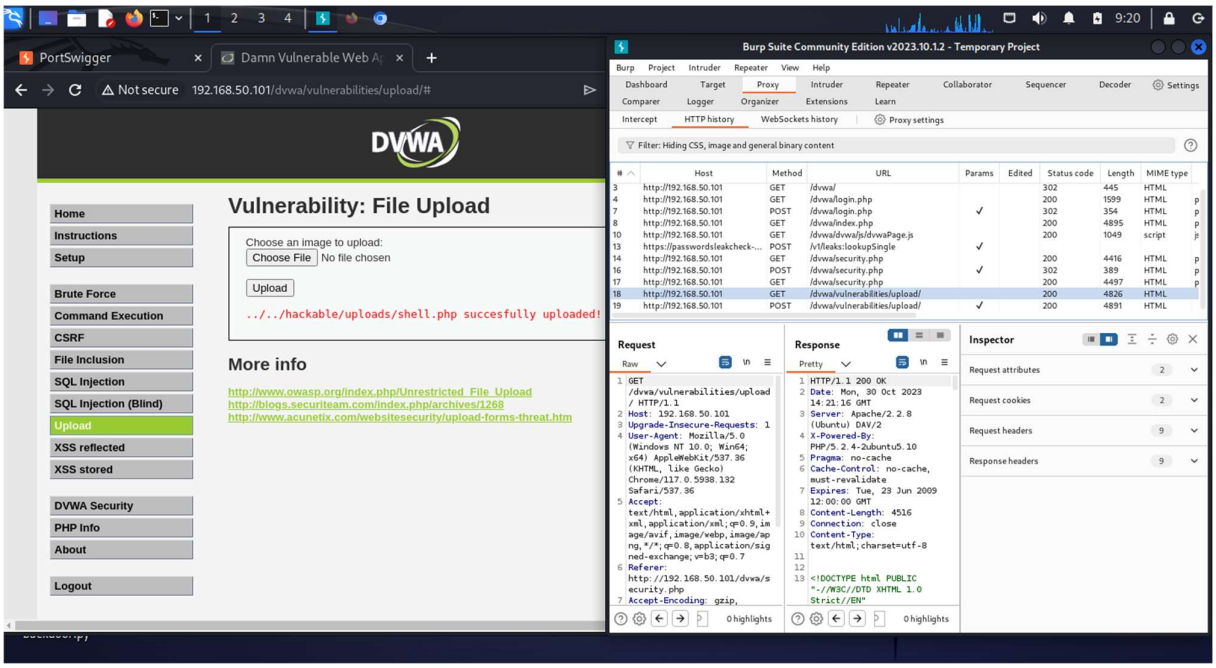
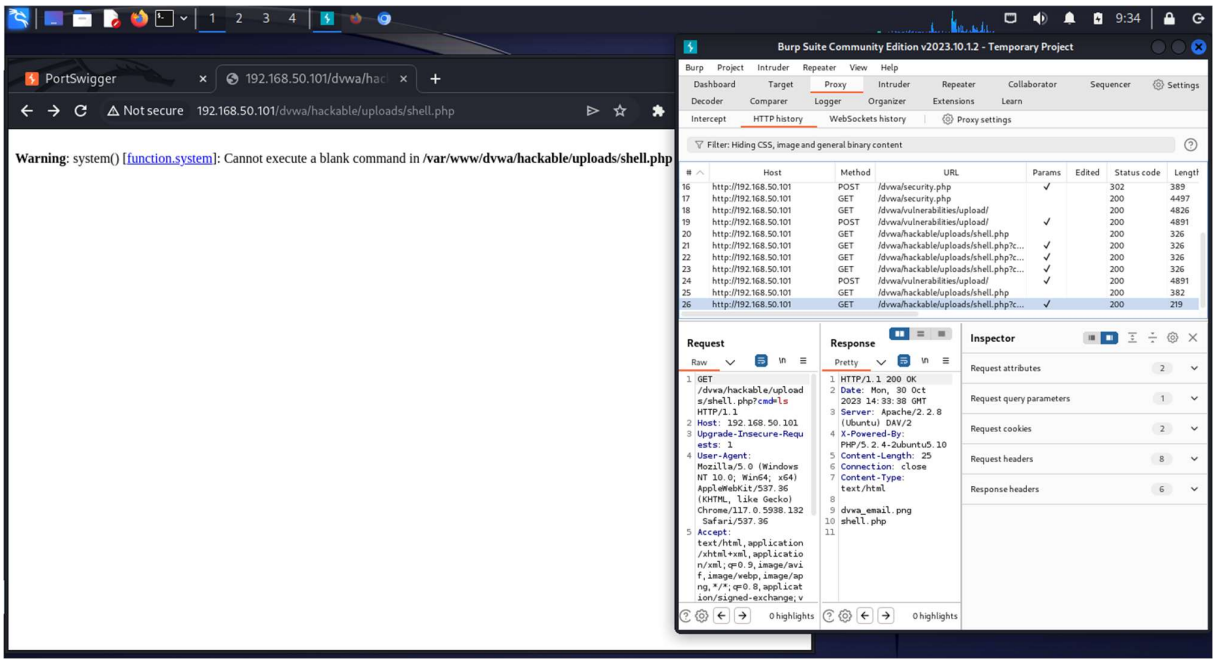
ESERCIZIO S6/L1

Lo scopo dell'esercizio di oggi è quello di 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.

Il primo passaggio che sono andata a fare è stato quello di aprire Burp Suite su Kali per intercettare le varie richieste. Ho aperto la pagina di DVWA, ho cliccato sulla sezione upload e ho caricato il file con la shell in PHP.



Successivamente ho copiato nell'URL quello che mi ha dato caricando il file, e ho visto che mi dava un errore.



Inserendo la voce “cmd=ls”, l’errore non è più apparso. Si è aperta la pagina dove ho visto le cartelle e in questo modo ho preso il comando della macchina.