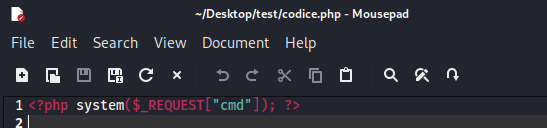
S6/L2

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.

Come primo passaggio, su kali, scriviamo un file di testo con codice php:



Abbiamo quindi un blocco di codice PHP.

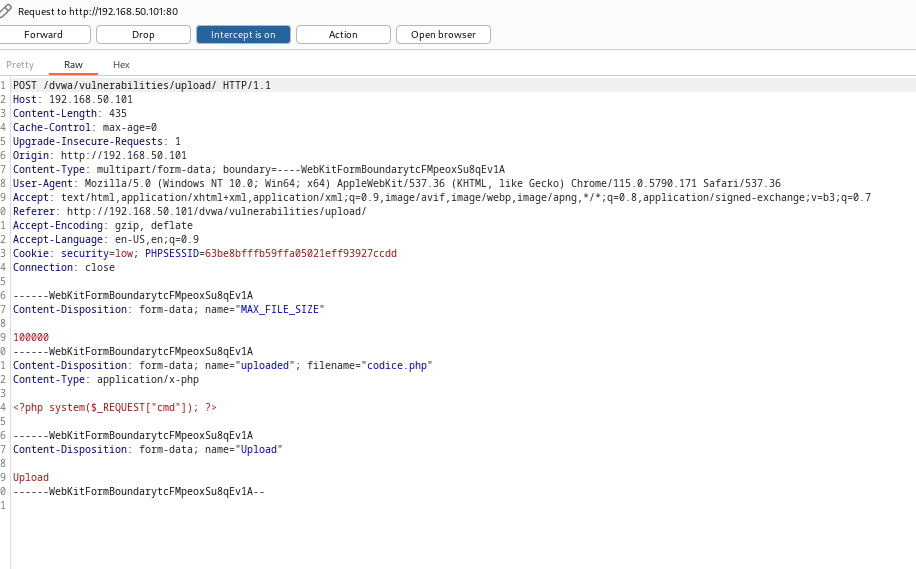
System($\_REQUEST[“cmd”]); il comando system è utilizzato per eseguire un comando del sistema operativo. La sua variabile in questo caso è Request[“cmd”]. $\_Request contiene dati inviati a uno script attraverso le richieste HTTP, come i parametri di una richiesta GET o POST.

Il codice tuttavia consente a chiunque di eseguire comandi del sistema sul server attraverso la richiesta HTTP inserendo il comando desiderato come parametro "cmd”.

Questo è un grave rischio per la sicurezza perché un utente malintenzionato potrebbe sfruttare questa vulnerabilità per eseguire comandi dannosi sul server, compromettendo la sicurezza del sistema.

Accediamo poi alla DVWA da Kali, tenendo aperta una sessione di BurpSuite per intercettare ogni richiesta e analizzare il contenuto. Impostiamo la security level della DVWA a “low” ed andiamo sulla scheda “upload” per mettere in pratica l’exploit. Carichiamo il nostro file.php e nel frattempo vediamo tutte le intercettazioni con burpsuite. Vediamo in questo caso che il metodo abilitato è “post” il quale invia i dati all’interno del corpo della richiesta http, è spesso utilizzato per inviare i dati da un modulo HTML a uno script lato server.

Per cui dato per conoscenza che il software DVWA presenta delle vulnerabilità su upload, lo sfrutto con uno script PHP, in questo modo aggiungo una funzione che mi abilita i comandi CMD.



Dopo aver cliccato su “forward” apro un’altra pagina e vado a scrivere sull’url:

192.168.50.101/dvwa/hackable/uploads/codice.php

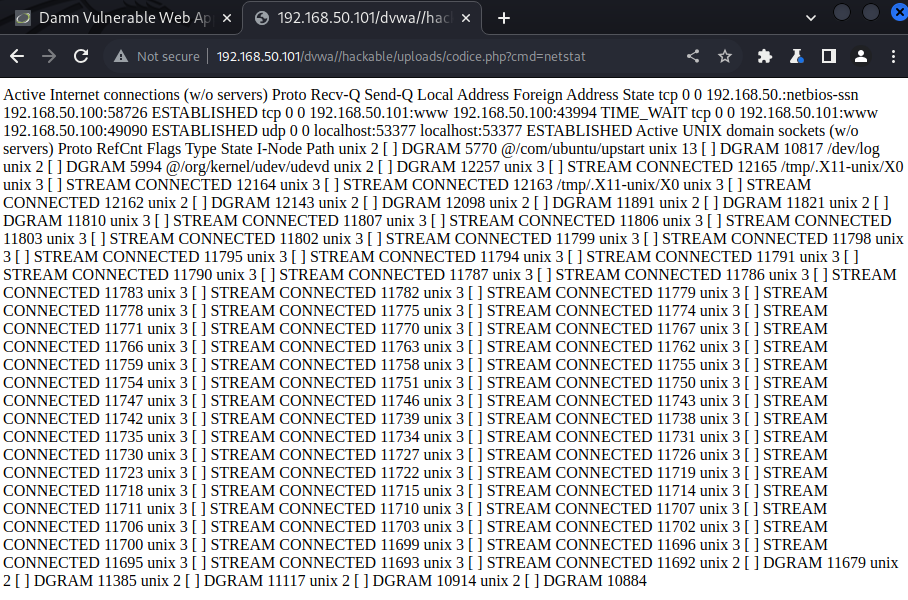
Andiamo adesso ad inserire un argomento che corrisponderà al comando da eseguire.

Aggiungiamo ?cmd = seguito dai comandi che vogliamo dare. (Questo codice PHP non presenta un’interfaccia grafica).

Abbiamo inserito dapprima il comando “netstat”, il cui suo utilizzo principale è quello di monitorare le attività di rete su un sistema.

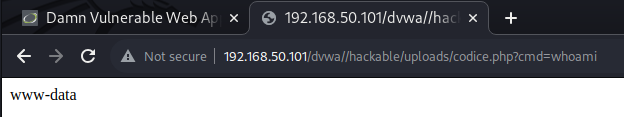


Vediamo che il metodo http è di tipo GET, spesso utilizzato quando si inviano dati attraverso l’URL, in modo che i parametri di query vengano inclusi direttamente nell’URL della richiesta; infatti quando un browser invia la richiesta GET sta chiedendo al server di restituire una rappresentazione della risorsa richiesta.

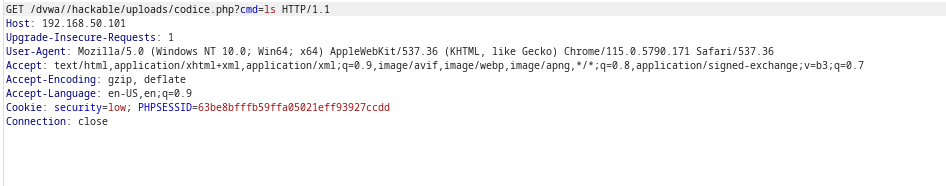


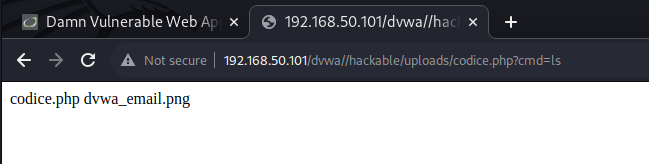
Di seguito invece abbiamo inserito il comando “whoami”, il sistema restituirà il nome dell'utente associato al processo in esecuzione. Questo può essere utile in script di shell o comandi per determinare il contesto dell'utente, e può essere utile anche per scopi diagnostici o nel controllo degli accessi.





Infine per esempio, scriviamo il comando ls:





In questo caso ci viene restituita la lista dei file, significa quindi che la richiesta LS è stata eseguita dalla shell.