

EXPLOIT FILE UPLOAD

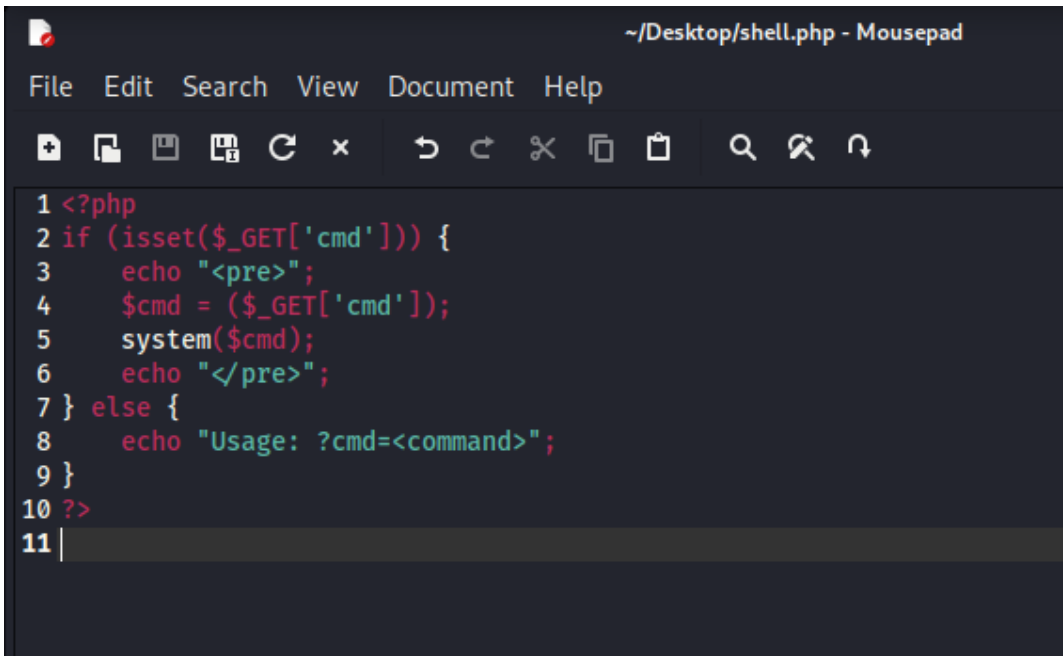
In questo esercizio, ho esplorato la vulnerabilità di file upload presente nella DVWA (Damn Vulnerable Web Application) per ottenere il controllo remoto su una macchina bersaglio, nel mio caso Metasploitable. Utilizzando strumenti come Burp Suite e PHP, sono riuscito a caricare una shell e a eseguire comandi da remoto.

Configurazione del Laboratorio

Per prima cosa, ho configurato l'ambiente virtuale assicurandomi che la macchina Metasploitable fosse raggiungibile dalla macchina Kali Linux. Ho testato la comunicazione tra le due macchine, confermando che fosse bidirezionale (esito positivo).

Procedura Eseguita

1. **Accesso a DVWA:** Ho aperto il browser e inserito l'IP della macchina Metasploitable per accedere all'interfaccia di DVWA, utilizzando le credenziali fornite.
2. **Impostazione della Sicurezza:** Ho abbassato il livello di sicurezza di DVWA a "low" per permettere l'esecuzione di comandi arbitrari tramite la shell.
3. **Caricamento della Shell in PHP:** Ho creato un file PHP per l'esecuzione di comandi. Il codice PHP utilizzato è il seguente:

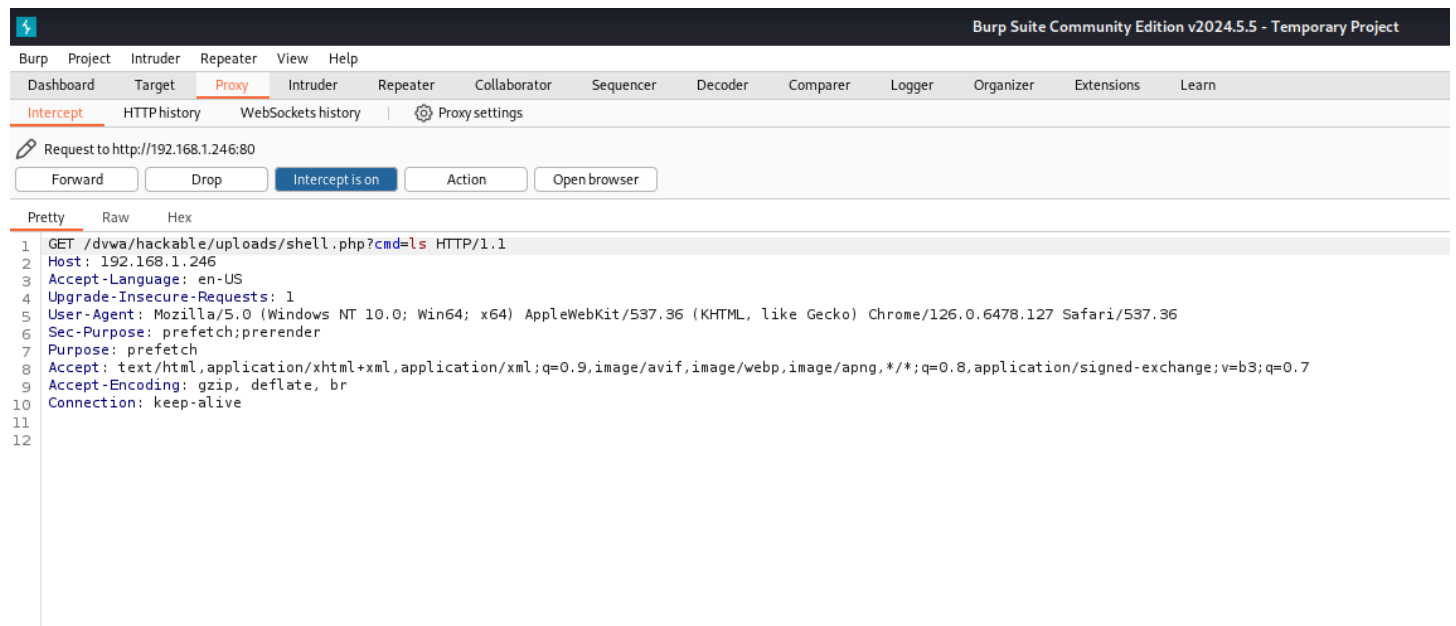
A screenshot of a text editor window titled '~/.Desktop/shell.php - Mousepad'. The window has a menu bar with 'File', 'Edit', 'Search', 'View', 'Document', and 'Help'. Below the menu bar is a toolbar with various icons for file operations. The main text area contains the following PHP code:

```
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 |
```

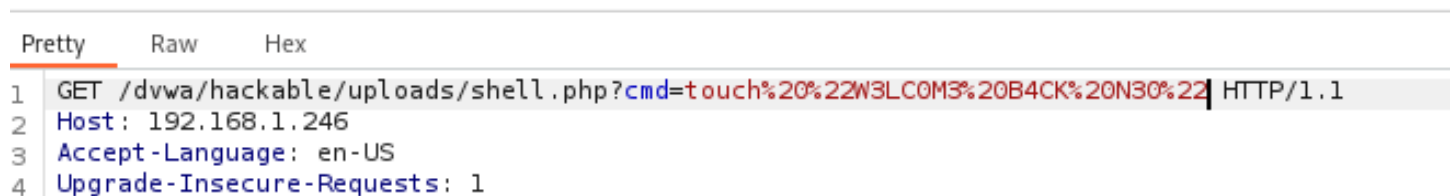
Caricamento del File: Ho caricato la shell PHP attraverso l'interfaccia di upload della DVWA.



Intercettazione della Richiesta GET: Utilizzando Burp Suite, ho intercettato la richiesta GET relativa al caricamento e all'esecuzione del comando.



Modifica della Richiesta: Ho modificato la richiesta GET per creare un file chiamato "W3LC0M3 B4CK N30" utilizzando il comando touch ed anche per un file chiamato ciao:



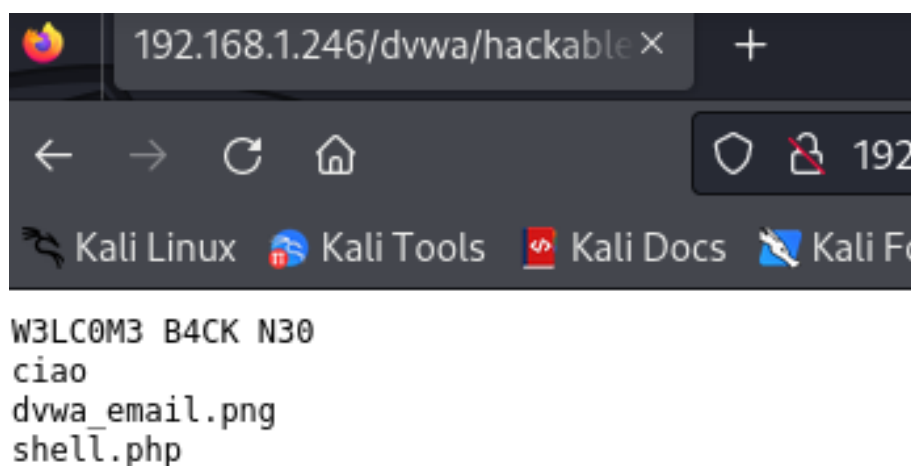
I caratteri di formattazione utilizzati nel nome del file "W3LC0M3 B4CK N30" servono a mascherare il testo per evitare rilevamenti e garantire che il nome del file sia accettato dal sistema durante il caricamento.

Dopo aver inoltrato la richiesta, ho verificato la risposta del server e ho visualizzato che il file era stato creato.

Verifica dell'Aggiunta del File: Ho eseguito un ulteriore comando per elencare i file nella directory di upload utilizzando `cmd=ls`, che ha confermato la presenza del file creato.

Risultato delle richieste:

- Risposta alla richiesta `cmd=touch` indicava che il file era stato creato correttamente.
- Risultato della richiesta `cmd=ls` mostrava il file **"W3LC0M3 B4CK N30"** presente nella directory.



Attraverso questa attività, ho acquisito una comprensione pratica delle vulnerabilità di file upload e delle tecniche utilizzate dagli hacker etici per ottenere accesso non autorizzato. La familiarizzazione con strumenti come Burp Suite è stata cruciale per l'intercettazione e l'analisi delle richieste HTTP/HTTPS.

Mattia Montis