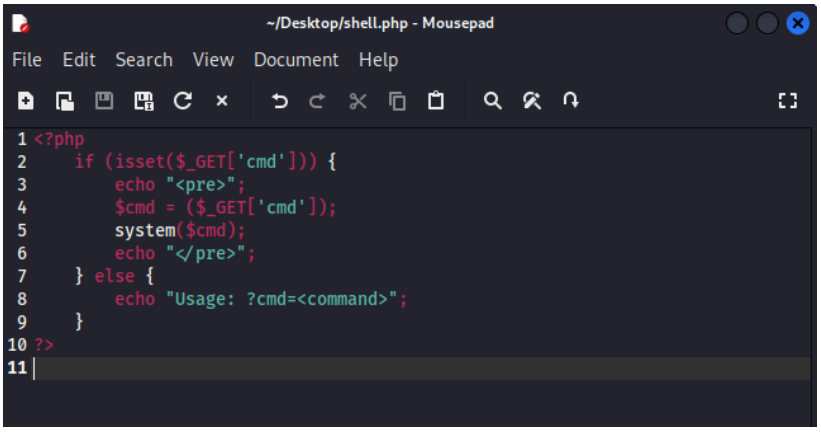
EXPLOIT FILE UPLOAD

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

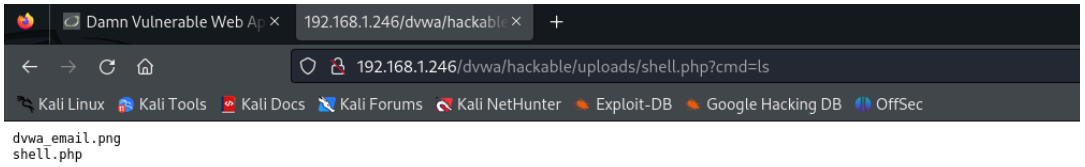
1. Configurazione del Laboratorio:
    - ○ Configurate il vostro ambiente virtuale in modo che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux.
    - ○ Assicuratevi che ci sia comunicazione bidirezionale tra le due macchine.
2. Esercizio Pratico:
    - ○ Sfruttate la vulnerabilità di file upload presente sulla DVWA Damn Vulnerable Web Application) per ottenere il controllo remoto della macchina bersaglio.
    - ○ Caricate una semplice shell in PHP attraverso l'interfaccia di upload della DVWA.
    - ○ Utilizzate la shell per eseguire comandi da remoto sulla macchina Metasploitable.
3. Monitoraggio con BurpSuite:
    - ○ Intercettate e analizzate ogni richiesta HTTP/HTTPS verso la DVWA utilizzando BurpSuite.
    - ○ Familiarizzate con gli strumenti e le tecniche utilizzate dagli Hacker Etici per monitorare e analizzare il traffico web.

Svolgimento:
Lo scopo dell'esercizio è quello di riuscire a modificare la macchina Metasploitable2 tramite la realizzazione di una shell che ne consenta l'accesso.
Il primo passo, come indicato dalla traccia, è stato quello di verificare che le macchine Kali e Metasploitable 2 comunicassero correttamente tramite ping.
Una volta appurato ciò sono andata a realizzare il primo step, ovvero la realizzazione della shell.

Shell
Ho realizzato un file shell semplice in estensione .php, di seguito il programma realizzato e salvato sulla macchina Kali Linux.



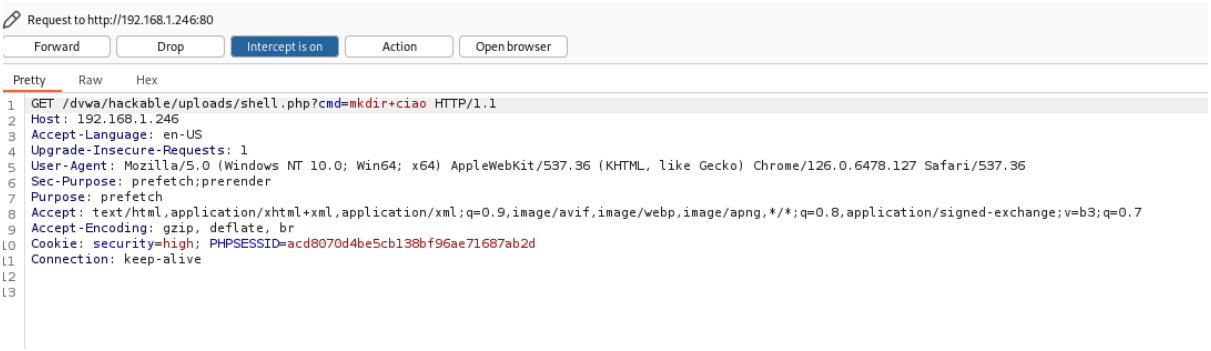
Impostazione DVWA
Il passo successivo fondamentale per il completamento dell'esercizio è quello di impostare la DVWA della macchina Metasploitable2. Andremo ad inserire la shell appena creata tramite upload. Il risultato che otterremo sarà il seguente.



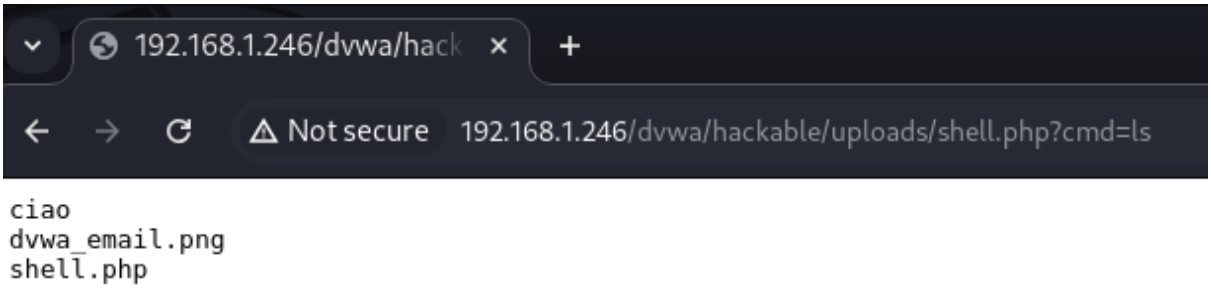
Intercettazione su BurpSuite
Per vedere cosa accade dietro alle quinte siamo andati ad avviare il tutto tramite BurpSuite che ci mostrerà il comando GET, ovvero quello che ci consente di andare a modificare la macchina Metasploitable2.

Modifica tramite Burpsuite
Grazie alla shell installata potremo andare a modificare facilmente la composizione della macchina Metasploitabile.
Come si può notare dalla riga GET, ciò che visualizzeremo a schermo non è altro che una lista. Per andare a modificare, per esempio, possiamo andare a creare nuovi file o directory, per poi visualizzarli direttamente sul browser.

Ipoteticamente ho creato una nuova directory sostituendo ls con mkdir+ciao, per fare un esempio.
Di seguito mostrerò come.



Il risultato a schermo sarà quella di visualizzare la lista rinnovata con la nuova Directory appena creata.



Conclusioni
Con questo procedimento ho fatto in modo da entrare, grazie ad una shell, all'interno della macchina Metasploitable2. Tramite questo procedimento potremo accedere liberamente alla macchina, ed è uno dei possibili attacchi ai verbi HTTP e ne sfrutta le vulnerabilità, in questo caso abbiamo sfruttato il verbo GET che viene utilizzato per la richiesta di una risorsa. I verbi, nella maggior parte dei casi, sono considerati delle vulnerabilità, soprattutto quelli come PUT e DELETE che consentono la modifica o la cancellazione di intere parti di codice.