W13D2

ATTACCO DELLA DVWA

La traccia

Nella lezione pratica di oggi vedremo come sfruttare un file upload sulla DVWA per caricare una semplice shell in PHP. **Monitoreremo tutti gli step con BurpSuite**

Traccia:

Configurate il vostro laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicuratevi che ci sia comunicazione tra le due macchine.

Lo scopo dell'esercizio di oggi è sfruttare la vulnerabilità di «file upload» presente sulla DVWA per prendere controllo della macchina ed eseguire dei comandi da remoto tramite una shell in PHP.

Inoltre, per familiarizzare sempre di più con gli strumenti utilizzati dagli Hacker Etici, vi chiediamo **di intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite**.

La consegna

1. Codice php
2. Risultato del caricamento (screenshot del browser)
3. Intercettazioni (screenshot di burpsuite)
4. Risultato delle varie richieste
5. Eventuali altre scoperte della macchina interna
6. BONUS: usare una shell php più sofisticata

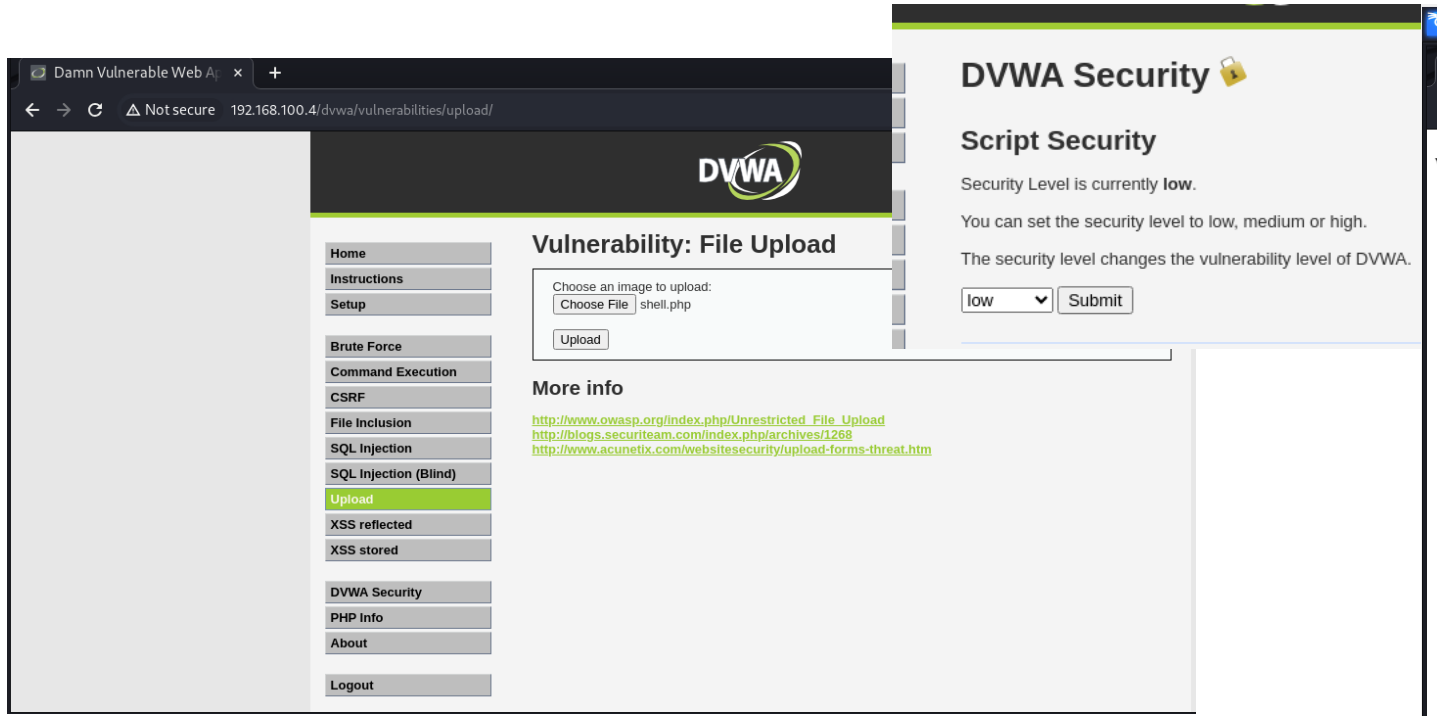
Creazione dello shellcode

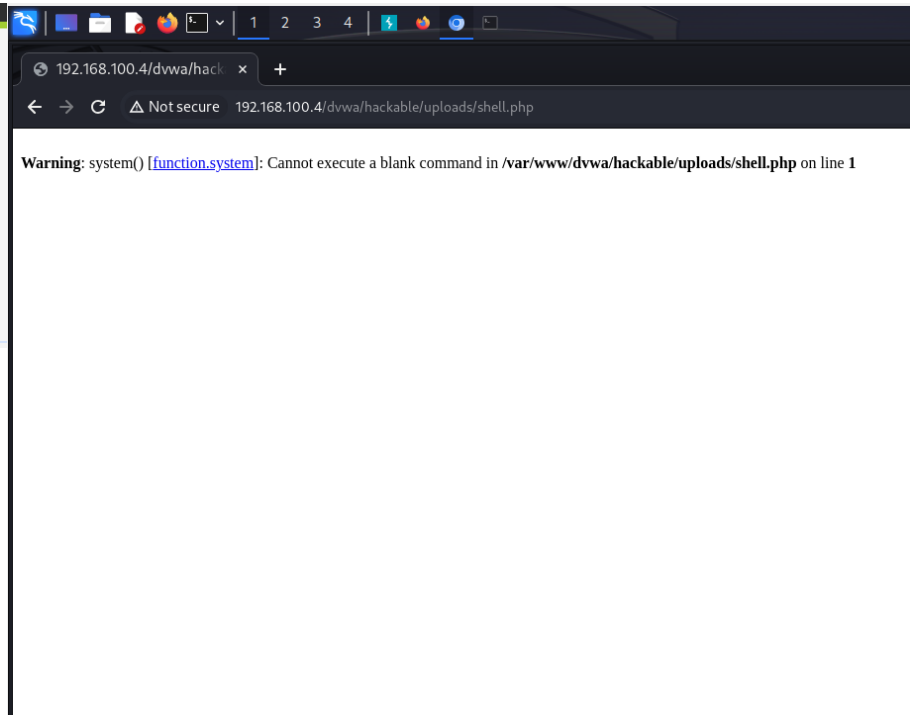
Creo innanzitutto lo shellcode da caricare sulla webapp.

```
┌──(kali㉿kali)-[~]
└─$ cat shell.php
<?php system($_REQUEST["cmd"]); ?>
```

Creazione dello shellcode ed avvio sul server

Carico lo shellcode su DVWA e provo ad avviare lo shellcode sul server.





Intercettazione e richiesta

Intercetto la richiesta che posso modificare in un secondo momento e reinoltrare col tasto forward