

W13D1 - Pratica (1)



Esercizio
Traccia

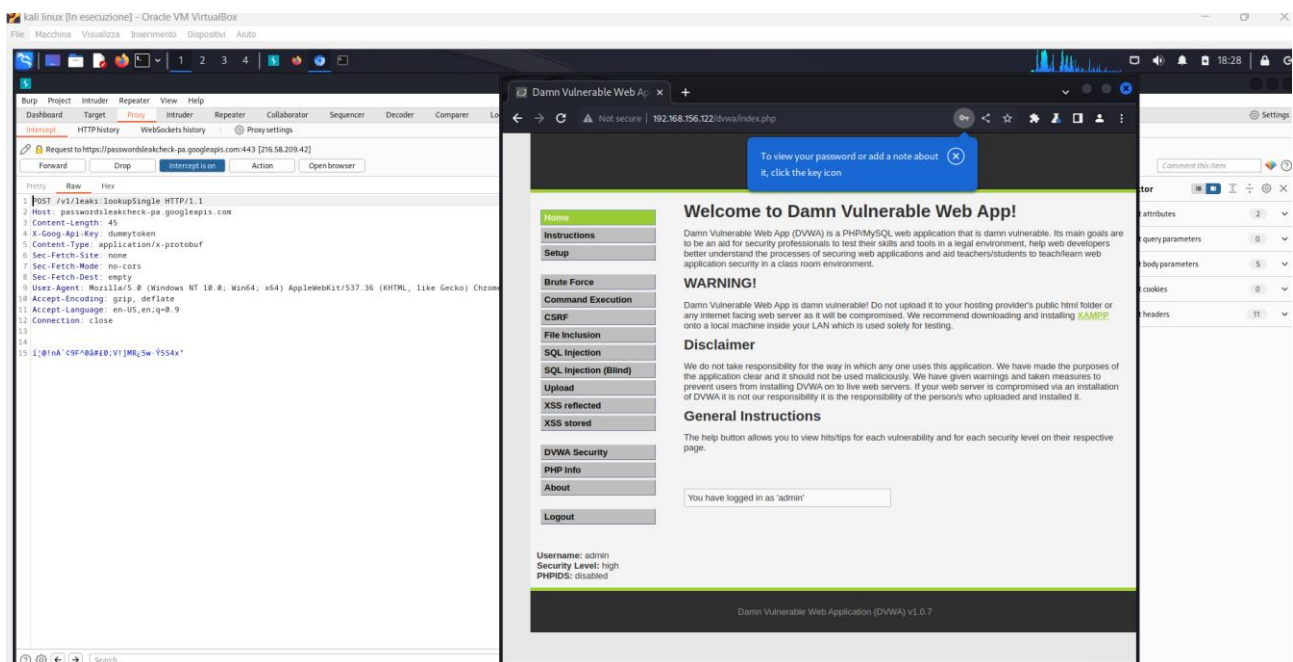
Nella lezione pratica di oggi vedremo come sfruttare un file upload sulla DVWA per caricare una semplice shell in PHP. **Monitoreremo tutti gli step con BurpSuite**

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**.



Damn Vulnerable Web Ap x

+

Not secure | 192.168.156.122/dvwa/vulnerabilities/upload/#

⏪ ⏩ ↺ ⚠️ ⚙️ ⭐ ⚙️ 🔒 🏠 👤 ⋮

DVWA

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: File Upload

Choose an image to upload:

Choose File No file chosen

Upload

../../../../hackable/uploads/shell.php succesfully uploaded!

More info

http://www.owasp.org/index.php/Unrestricted_File_Upload
<http://blogs.securiteam.com/index.php/archives/1268>
<http://www.acunetix.com/websecurity/upload-forms-threat.htm>

Username: admin

Security Level: low

PHPIDS: disabled

View Source View Help

Damn Vulnerable Web Application (DVWA) v1.0.7

