Shell.php

Preparazione dell'Ambiente:

- Configurate la macchina virtuale Metasploitable.
- Configurate la macchina virtuale Kali Linux. Verificate la connessione tra le due macchine con un semplice ping.

Caricamento della Shell PHP:

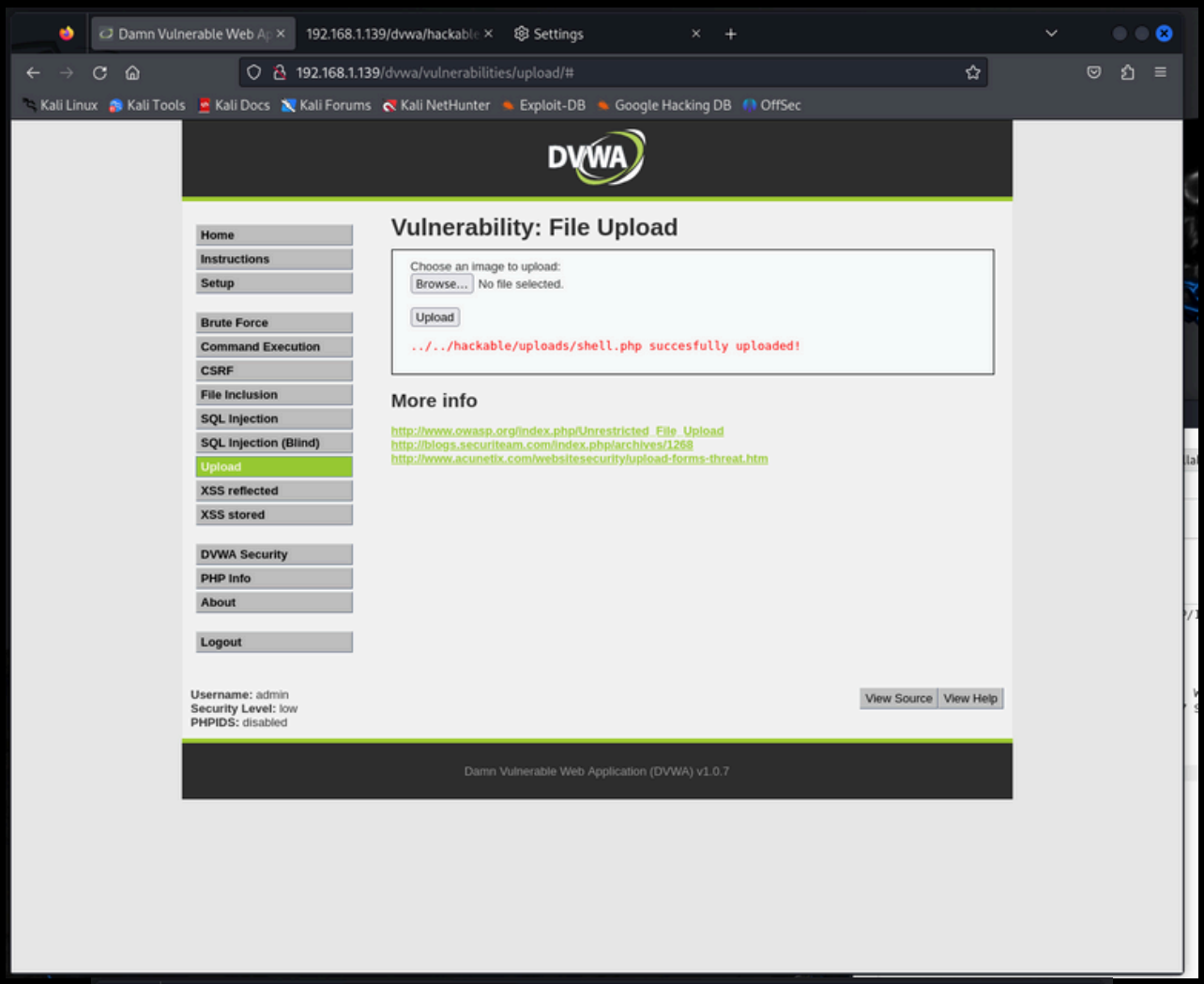
- Accedete alla DVWA sulla macchina Metasploitable tramite il browser della Kali Linux.
- Navigare alla sezione File Upload della DVWA.
- Create una semplice shell PHP (ad esempio, shell.php) e caricatela attraverso il modulo di upload.
- Verificate che il file sia stato caricato con successo.

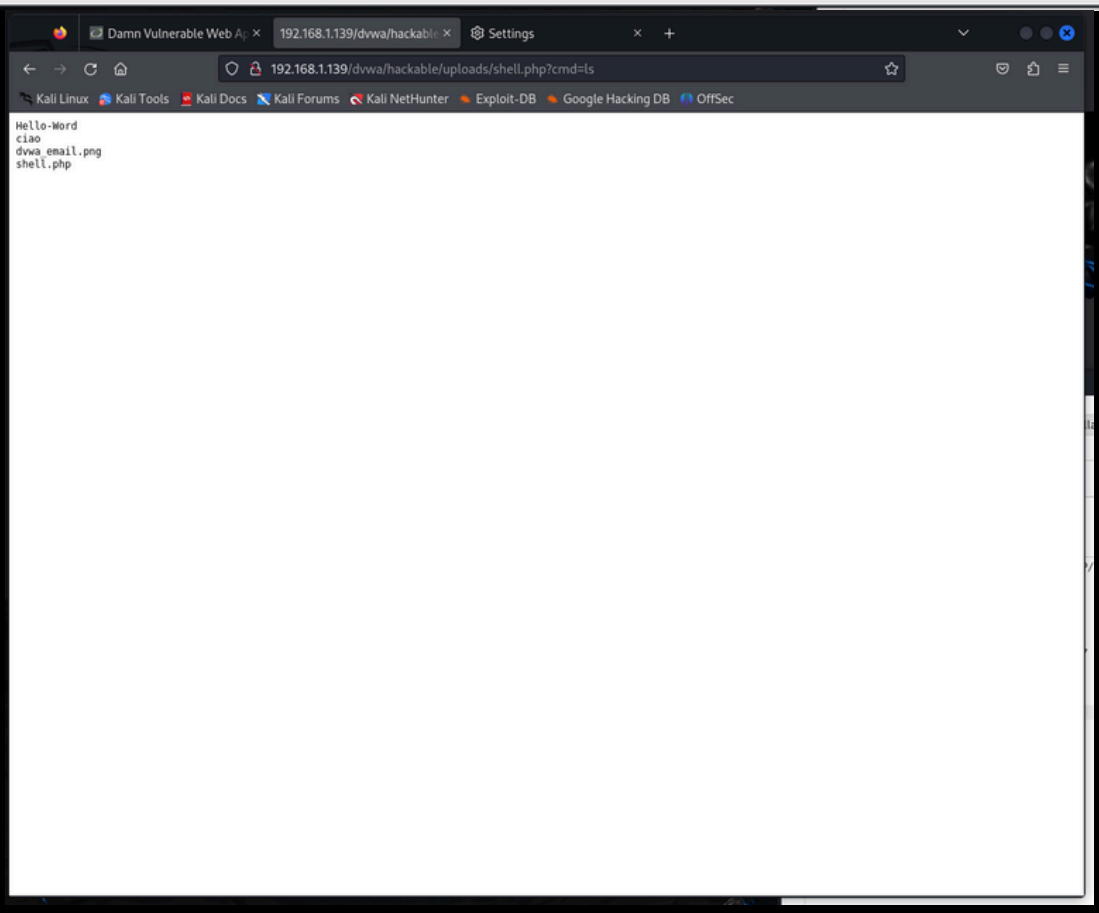
Esecuzione della Shell PHP:

- Accedete alla shell caricata tramite il browser.
- Utilizzate la shell per eseguire comandi da remoto sulla macchina Metasploitable.

Intercettazione e Analisi con BurpSuite:

- Avviate BurpSuite e configurate il browser per utilizzare Burp come proxy. Intercettate le richieste HTTP/HTTPS effettuate durante il processo di upload e di esecuzione della shell.
- Analizzate le richieste e le risposte per comprendere il funzionamento e individuare eventuali vulnerabilità.


Damn Vulnerable Web Ap
192.168.1.139/dvwa/hackable
Settings
192.168.1.139/dvwa/vulnerabilities/upload/#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
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:
Browse...
No file selected.
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/websitesecurity/upload-forms-threat.htm
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help
Damn Vulnerable Web Application (DVWA) v1.0.7


Damn Vulnerable Web Ap
192.168.1.139/dvwa/hackable
Settings
192.168.1.139/dvwa/hackable/uploads/shell.php?cmd=ls
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Hello-Word
ciao
dvwa_email.png
shell.php

Relazione

L'esercizio svolto in Burp Suite serve a testare una vulnerabilità nota come iniezione di comandi. Questa vulnerabilità permette a un eventuale attaccante di eseguire comandi di sistema su un server tramite parametri di input. Modificando la risposta per mostrare un messaggio personalizzato (come "Ciao" o "Hello World", nel nostro caso), ho simulato la possibilità di intercettare e manipolare i dati tra il server e il client. Questo esercizio aiuta a comprendere come alterare le risposte per simulare possibili attacchi o per ottenere informazioni sensibili.

Daniel_Gabriel_Costeanu