

G2

DIPLOMATURA EN SEGURIDAD DE
LA INFORMACIÓN 2021



PENETRATION TESTING

21/06/2021

Docentes: Federico Pacheco | Matias Sliafertis

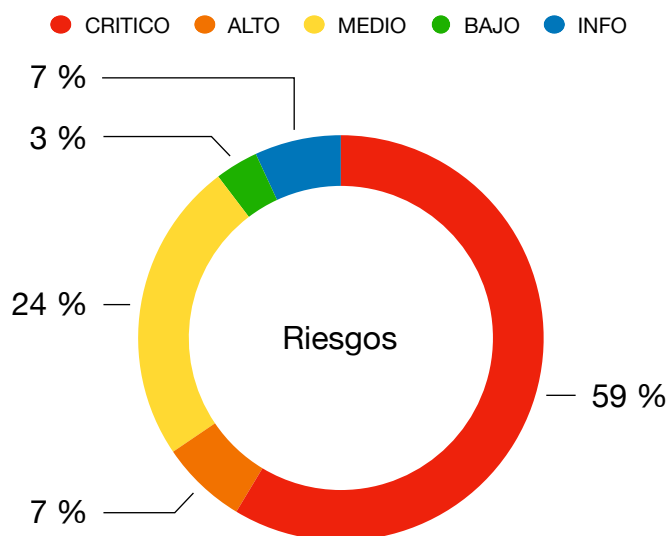
Alumnos: Eugenio Levalle | Federico Lo Cascio | Nestor Penayo | Lucas Baruffa | Carlos Benitez

Declaración de no divulgación: Toda la información obtenida durante la evaluación sobre los sistemas y activos de nuestros clientes, incluidos, entre otros, sus procedimientos y sistemas, se considera información privilegiada y no para divulgación pública. estrictamente confidencial. Esta información no será divulgada ni discutida con ningún tercero sin el consentimiento expreso por escrito del cliente. Estamos totalmente comprometidos a mantener el más alto nivel de estándares éticos en su práctica comercial.

Contenidos

1. Resumen ejecutivo	3
Introducción.....	3
Metodología	3
Alcance y objetivo.....	3
Recomendaciones.....	4
2. OSINT	5
3. Informe de evaluación.....	7
Hallazgos del proyecto.....	7
Tabla de hallazgos	7
Resultados técnicos	9
Fase de reconocimiento y explotación	9
4. Recomendaciones generales y hardening.....	30
5. Apendice A	35
6. Herramientas utilizadas.....	35
7. Creditos	36

1. RESUMEN EJECUTIVO



HALLAZGOS ENCONTRADOS

17 Critico
2 Alto
7 Medio
1 Bajo
2 Informativo

29 resultados totales

DÍAS

01/06/2021 -
14/06/2021
Active testing

21/06/2021
Entrega de informes

Introducción

██████████ es una empresa de ingeniería y construcciones que brinda, desde hace más de 40 años, soluciones integrales de alta calidad en obras civiles e industriales, de petróleo y gas, hidráulica, de infraestructura urbana y regional, portuarias y de protección costera, así como también obras viales y puentes.

██████████ Inc contrató a **G2** para evaluar la seguridad del host <http://██████████>. El siguiente informe detalla los hallazgos identificados durante el curso del compromiso, que comenzó el 01 de junio de 2021.

Metodología

G2 trata cada compromiso como una entidad fluida. Utilizamos una base estándar de herramientas y técnicas a partir de las cuales construimos nuestra propia metodología única. Nuestros 30 años de experiencia en seguridad de la información nos han enseñado que mezclar filosofías ofensivas y defensivas es la clave para enfrentar las amenazas. Durante esta evaluación, hemos empleado metodologías de prueba estándar (por ejemplo, recomendaciones de la guía de pruebas de OWASP), así como listas de verificación personalizadas para garantizar una cobertura completa de las vulnerabilidades.

Alcance y objetivo

El alcance de la prueba fue resaltar las vulnerabilidades que podrían ser utilizadas por un usuario malintencionado sin privilegios para subvertir el entorno, escalar privilegios y obtener acceso a información sensible. El proceso de prueba se llevó a cabo en fases para simular diferentes ataques y atacantes que podrían representar una amenaza para el negocio y la red de ██████████. El objetivo de las pruebas era analizar la lista de sistemas proporcionados, enumerar y explotar las vulnerabilidades de seguridad. Se identificaron tanto el alcance como el impacto de estas vulnerabilidades y los hallazgos se presentan dentro de los Resultados técnicos (*Página 9*). La explotación de las vulnerabilidades de seguridad por parte de un atacante puede exponer a una organización a una serie de riesgos relacionados con la TI.

Se descubrió que la confidencialidad de todos los datos almacenados en el entorno de [REDACTED] podrían verse comprometidos por un ataque.

Resumen de hallazgos

El servidor [REDACTED] se vio afectado por múltiples vulnerabilidades críticas y de alto riesgo que resultaron en el compromiso del usuario [REDACTED], comprometiendo sesiones de múltiples aplicaciones y de los servidores.

En el host [http://\[REDACTED\]](http://[REDACTED]) se encontró información sensible expuesta que comprometía la integridad del servidor.

Las vulnerabilidades identificadas deben volver a probarse al parchear para verificar la integridad de la corrección.

Recomendaciones

- Verificar que la información subida al servidor no contenga datos sensibles.
- Utilizar contraseñas robustas.
- Utilizar distintos nombres de usuarios y contraseñas para cada aplicación y/o servidor.
- Mantener actualizadas a fecha las aplicaciones y sistemas operativos.
- Hacer una buena gestión de privilegios de usuarios.

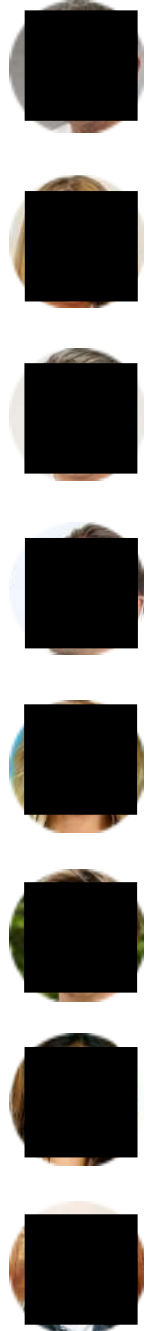
2. OSINT

OSINT son las siglas de Open Source Intelligence (Inteligencia de Fuentes Abiertas). Se trata de un conjunto de técnicas y herramientas utilizadas para recopilar información pública, correlacionar los datos y procesarlos.

• DESCRIPCIÓN:

Se realizó una recopilación de datos sobre empleados de la empresa [REDACTED] a partir de la información publica encontrada en la pagina web [http://\[REDACTED\]](http://[REDACTED]). Esto podría conllevar un riesgo por parte de ataques de ingeniería social hacia los empleados para comprometer a la empresa si es que no están los suficientemente capacitados sobre el tema.

- [REDACTED]
[https://www.linkedin.com/in/\[REDACTED\]](https://www.linkedin.com/in/[REDACTED])
- CEO at [REDACTED] S.A.
Buenos Aires, Provincia de Buenos Aires, Argentina
- [REDACTED]
[https://www.linkedin.com/in/\[REDACTED\]](https://www.linkedin.com/in/[REDACTED])
- Economista at [REDACTED] Argentina
Buenos Aires, Provincia de Buenos Aires, Argentina
- [REDACTED]
[https://www.linkedin.com/in/\[REDACTED\]](https://www.linkedin.com/in/[REDACTED])
- Abogado en [REDACTED] Argentina
Buenos Aires, Provincia de Buenos Aires, Argentina
- [REDACTED]
[https://www.linkedin.com/in/\[REDACTED\]](https://www.linkedin.com/in/[REDACTED])
- Chief Information Security Officer at [REDACTED] Argentina
Buenos Aires, Provincia de Buenos Aires, Argentina
- [REDACTED]
[https://www.linkedin.com/in/\[REDACTED\]](https://www.linkedin.com/in/[REDACTED])
- Analista de planificación financiera en [REDACTED] Argentina
Buenos Aires, Provincia de Buenos Aires, Argentina
- [REDACTED]
[https://www.linkedin.com/in/\[REDACTED\]](https://www.linkedin.com/in/[REDACTED])
- Full Stack Developer en [REDACTED] Argentina
Buenos Aires, Provincia de Buenos Aires, Argentina
- [REDACTED]
[https://www.linkedin.com/in/\[REDACTED\]](https://www.linkedin.com/in/[REDACTED])
- Analista de Cumplimiento en [REDACTED] Argentina
Buenos Aires, Provincia de Buenos Aires, Argentina
- [REDACTED]
[https://www.linkedin.com/in/\[REDACTED\]](https://www.linkedin.com/in/[REDACTED])
- Analista financiero en [REDACTED] Argentina
Buenos Aires, Provincia de Buenos Aires, Argentina



- [REDACTED]
[https://www.linkedin.com/company/\[REDACTED\]](https://www.linkedin.com/company/[REDACTED])
- Especialista en TI en [REDACTED] Argentina
Buenos Aires, Provincia de Buenos Aires, Argentina
- [REDACTED]
[https://www.linkedin.com/company/\[REDACTED\]](https://www.linkedin.com/company/[REDACTED])
- Analista financiero en [REDACTED] Argentina
Buenos Aires, Provincia de Buenos Aires, Argentina



3. INFORME DE EVALUACIÓN

Hallazgos del proyecto

La siguiente tabla enumera los hallazgos con su ID y gravedad asociados. La clasificación de gravedad se definen en el Apéndice A al final de este documento.

Tabla de hallazgos

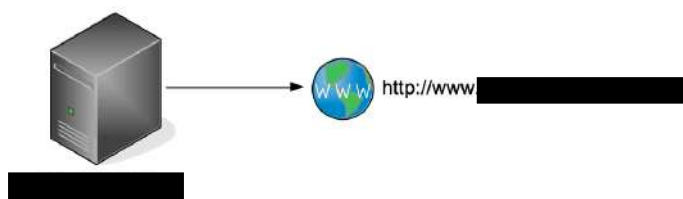
ID	Hallazgo	Riesgo
1	Información sensible expuesta	CRITICO
2	Sesión de SSH comprometida	CRITICO
3	Elevación de privilegios SSH	CRITICO
4	Slowloris DOS (Denial-of-Service)	CRITICO
5	Sesión de SSH comprometida	CRITICO
6	Elevación de privilegios SSH	CRITICO
7	Sesión de phpMyAdmin comprometida	CRITICO
8	Sesión de Wordpress comprometida	CRITICO
9	Sesión de vsFTPD comprometida	CRITICO
10	phpMyAdmin 4.x < 4.8.5 Multiples Vulnerabilidades (PMASA-2019-1) (PMASA-2019-2)	CRITICO
11	phpMyAdmin < 4.8.6 vulnerabilidad SQLi (PMASA-2019-3)	CRITICO
12	WordPress 4.5.x < 4.5.23 varias vulnerabilidades	CRITICO
13	Vulnerabilidad en ap_get_basic_auth_pw()	CRITICO
14	mod_ssl puede desreferenciar un puntero NULL	CRITICO
15	Vulnerabilidad en mod_mime	CRITICO
16	Ejecutar código arbitrario con los privilegios del proceso root	CRITICO
17	Error en el análisis de la lista de tokens	CRITICO
18	Reutilización de contraseñas	ALTO
19	phpMyAdmin 4.x < 4.9.4 / 5.x < 5.0.1 SQLi (PMASA-2020-1)	ALTO

20	Enumeración del usuario de WordPress	MEDIO
21	XSS en librería de Bootstrap	MEDIO
22	Biblioteca de jQuery vulnerable	MEDIO
23	Directorios webs navegables	MEDIO
24	Aplicación web potencialmente vulnerable a Clickjacking	MEDIO
25	phpMyAdmin 4.x < 4.9.0 CSRF (PMASA-2019-4)	MEDIO
26	Slowloris DOS attack	MEDIO
27	Divulgación de distribución de Apache Banner Linux	INFO
28	Software y tecnología de servidor encontrados	INFO
29	El servidor web transmite credenciales de texto sin cifrar	INFO

Resultados técnicos

Esta sección cubre las dos fases principales del compromiso; las fases de reconocimiento y explotación. Estas fases se dividen aún más en las técnicas de prueba utilizadas y las tecnologías que se descubrieron que revelaron información valiosa o condujeron a un compromiso total del host.

Fase de reconocimiento y explotación



• DESCRIPCIÓN:

Se realizó un escaneo de puertos con la herramienta Nmap para ubicar los servicios clave que se ejecutan en el host [http://\[REDACTED\]](http://[REDACTED]). A continuación se muestra el resultado del escaneo.

```
user@Fede-MacBook-Pro ~ % nmap -sV
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-06 20:13 -03
Nmap scan report for [REDACTED]
Host is up (0.17s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.18 ((Ubuntu))
8080/tcp   open  ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
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 58.14 seconds
user@Fede-MacBook-Pro ~ %
```

Puertos descubiertos

PUERTO	ESTADO	SERVICIO	APLICACIÓN/VERSIÓN
80/TCP	ABIERTO	HTTP	Apache https 2.4.18 (Ubuntu)
8080/TCP	ABIERTO	SSH	OpenSSH 7.2p2 Ubuntu

Información del dominio

Información de DNS	
HOST	DNS
http://[REDACTED]	ns1.uniregistry-dns.com 102701 IN A 54.197.228.206
	ns1.uniregistry-dns.net 163188 IN A 23.253.58.227
	ns2.uniregistry-dns.com 102701 IN A 162.242.150.89
	ns2.uniregistry-dns.net 163188 IN A 176.34.241.253

FECHAS IMPORTANTES:

Caducidad del registro: 2023-05-14 23:59:59 UTC

Actualizado: 2018-07-04 11:00:25 UTC

Creado: 2018-05-14 00:27:40 UTC

• RECOMENDACIÓN:

Comprobar que el host tenga activada la renovación automática del registro web para evitar la caducidad del mismo.

Enumeración

• DESCRIPCIÓN:

Se realizó una enumeración de directorios con la herramienta gobuster al host [http://\[REDACTED\]](http://[REDACTED])

```
wordlists — -zsh — 114x26
user@Fede-MacBook-Pro wordlists % gobuster dir -u http://[REDACTED] -t 100 -w directory-list-1.0.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://[REDACTED]
[+] Method:       GET
[+] Threads:      100
[+] Wordlist:      directory-list-1.0.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.1.0
[+] Timeout:      10s

2021/06/06 21:44:27 Starting gobuster in directory enumeration mode

/storage      (Status: 301) [Size: 326] [--> http://[REDACTED]]
/wordpress    (Status: 301) [Size: 328] [--> http://[REDACTED]]
/phpmyadmin    (Status: 301) [Size: 329] [--> http://[REDACTED]]
/wp-content    (Status: 301) [Size: 329] [--> http://[REDACTED]]
/wp-admin      (Status: 301) [Size: 327] [--> http://[REDACTED]]

2021/06/06 21:48:52 Finished
user@Fede-MacBook-Pro wordlists %
```

Directorios	URL
/storage	http://[REDACTED]
/wordpress	http://[REDACTED]

/phpmyadmin	http://[REDACTED]
/wp-content	http://[REDACTED]
/wp-admin	http://[REDACTED]

1. Información sensible expuesta

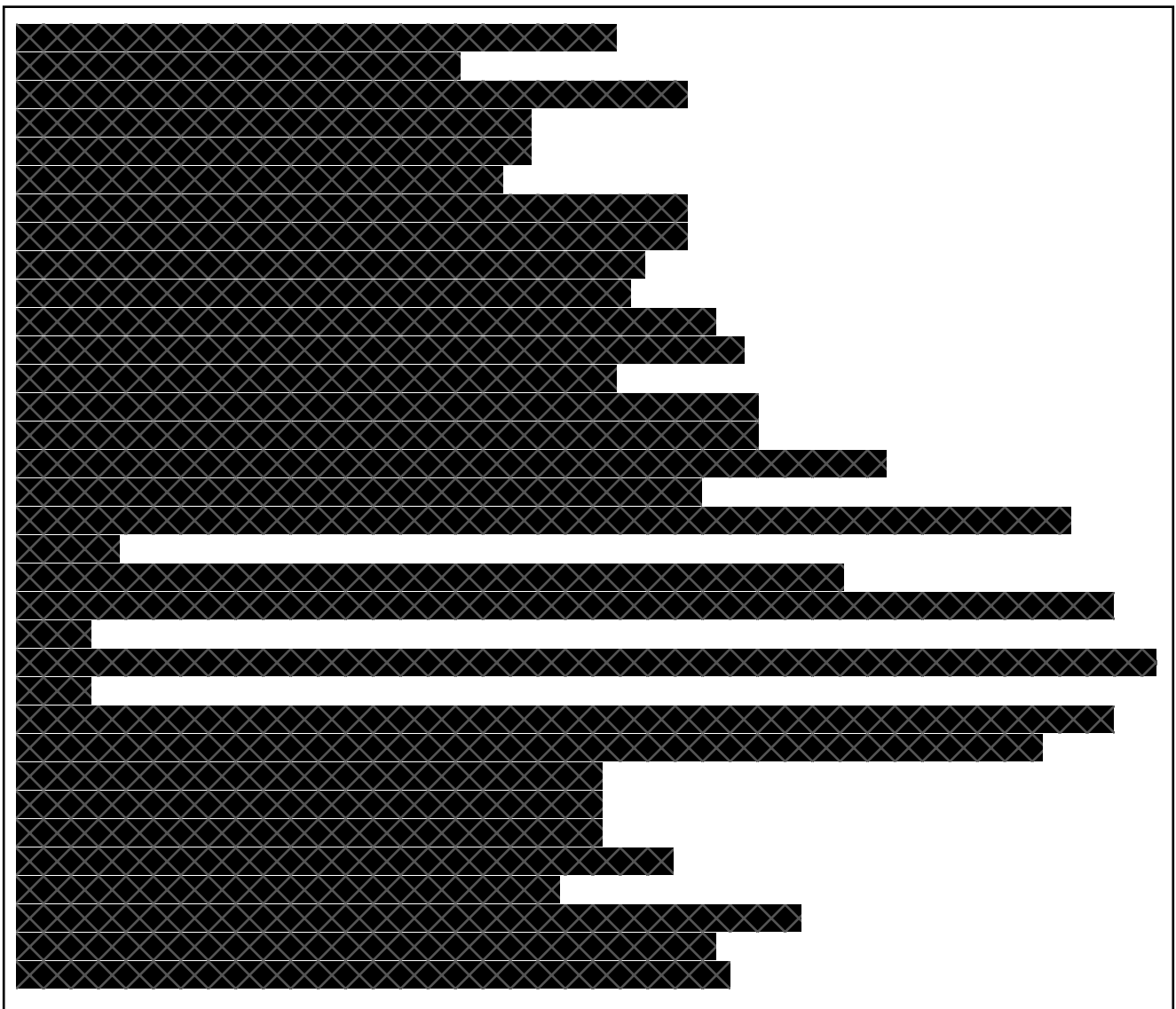
Riesgo: CRITICO

• DESCRIPCIÓN:

Dentro del directorio storage ([http://\[REDACTED\]](http://[REDACTED])) se encontraron multiples archivos exponiendo **información sensible** del servidor.

- I. Dentro del directorio '**storage**', se encontró el archivo '**Auditoria.zip**' protegido con la clave 'bridgedesign'. Dentro se encontró el archivo '192.241.151.12etc-passwd.txt' en el cual se **expone información** de los usuarios del sistema, y del usuario y contraseña cifrada en MD5 del usuario [REDACTED].
- II. Dentro del directorio '**storage**' se encontró el archivo 'Procedimientos tech.docx' en el cual **expone información** sensible sobre el servidor comprometiendo el usuario y contraseña del usuario [REDACTED].

I. **ARCHIVO:** '192.241.151.12ETC-PASSWD.TXT'



Usuario	Clave (MD5)	Clave descifrada
[REDACTED]	[REDACTED]	[REDACTED]

Decifrado en <https://hashes.com/>

II. **ARCHIVO:** ‘Procedimientos tech.docx’

La password por defecto para el usuario [REDACTED] en todos los servers será

Fragmento del archivo 'Procedimientos tech.docx'

2. Sesión de SSH comprometida

Riesgo: CRITICO

- DESCRIPCIÓN:

Se comprometió el inicio de sesión SSH en el host http://[REDACTED]
[REDACTED] con el usuario '[REDACTED]' y la contraseña '[REDACTED]'
obtenidas del los archivos '**192.241.151.12etc-passwd.txt**' y '**Procedimientos
tech.docx**'



```

user@Fede-MacBook-Pro ~ % ssh -p 8080
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-184-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

93 packages can be updated.
2 updates are security updates.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

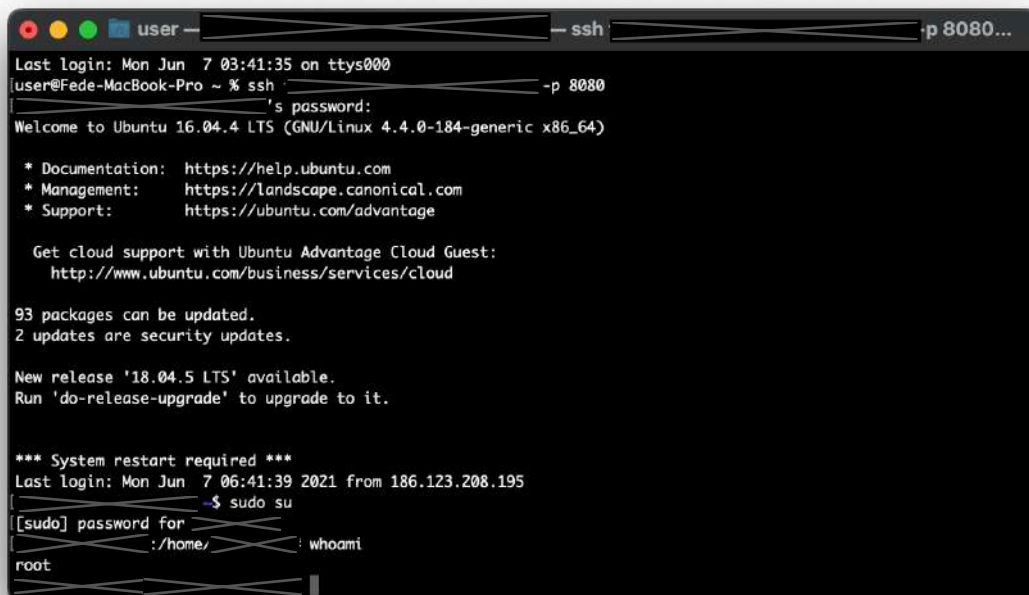
*** System restart required ***
Last login: Mon Jun  7 06:40:38 2021 from 186.123.208.195
~$ whoami
root
~$ uname -a
Linux FedoraSrv 4.4.0-184-generic #214-Ubuntu SMP Thu Jun 4 10:14:11 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
~$
```

3. Elevación de privilegios SSH

Riesgo: CRITICO

• DESCRIPCIÓN:

Se obtuvo privilegios de usuario root con el usuario [REDACTED] y la contraseña [REDACTED] en el servidor [REDACTED]



```
user@Fede-MacBook-Pro ~ % ssh [REDACTED] -p 8080
Last Login: Mon Jun 7 03:41:35 on ttys000
[REDACTED]'s password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-184-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

93 packages can be updated.
2 updates are security updates.

New release '18.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

*** System restart required ***
Last login: Mon Jun 7 06:41:39 2021 from 186.123.208.195
[REDACTED]~$ sudo su
[sudo] password for [REDACTED]:
[REDACTED]~#
```

• RECOMENDACIÓN:

Realizar una correcta gestión de privilegios de los usuarios del sistema.
Usar una contraseña distinta para privilegios de root.

4. Slowloris ataque de DOS (Denial-of-Service)

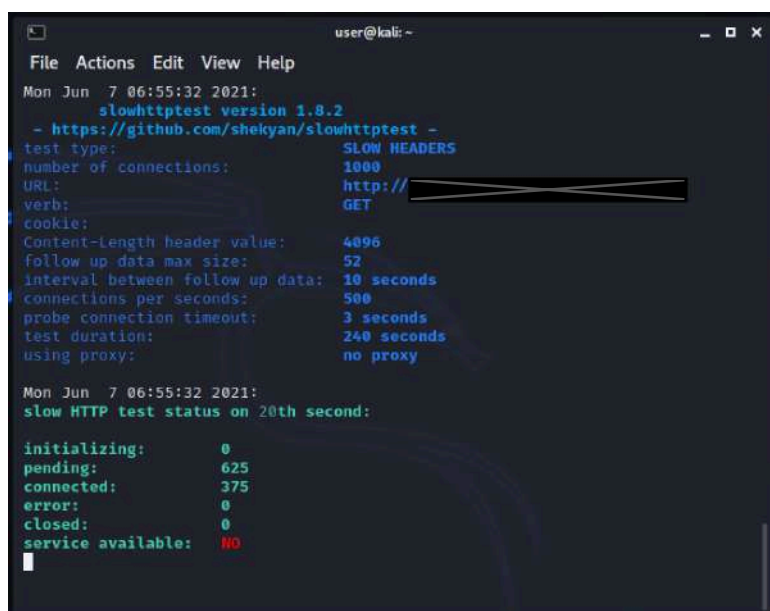
Riesgo: MEDIO

• DESCRIPCIÓN:

Slowloris intenta mantener abiertas muchas conexiones con el servidor web de destino y mantenerlas abiertas el mayor tiempo posible. Lo logra abriendo conexiones al servidor web de destino y enviando una solicitud parcial. Al hacerlo, priva de los recursos del servidor http, lo que provoca la denegación de servicio.

• RECOMENDACIÓN:

Implementar mod_antiloris (https://github.com/Deltik/mod_antiloris) en el servidor Apache.



```
user@kali: ~
File Actions Edit View Help
Mon Jun 7 06:55:32 2021:
slowhttptest version 1.8.2
- https://github.com/shekyaan/slowhttptest -
test type: SLOW HEADERS
number of connections: 1000
URL: http://[REDACTED]
verb: GET
cookie:
Content-Length header value: 4096
follow up data max size: 52
interval between follow up data: 10 seconds
connections per seconds: 500
probe connection timeout: 3 seconds
test duration: 240 seconds
using proxy: no proxy

Mon Jun 7 06:55:32 2021:
slow HTTP test status on 20th second:

initializing: 0
pending: 625
connected: 375
error: 0
closed: 0
service available: NO
```

SlowHTTPTest



• DESCRIPCIÓN:

Se realizó un escaneo de puertos con la herramienta Nmap para ubicar los servicios clave que se ejecutan en el host XXXXXXXXXX. A continuación se muestra el resultado del escaneo.

```

user -p 8080 - 114x26
FedoraSsrv:~$ nmap -sV
Starting Nmap 7.01 ( https://nmap.org ) at 2021-06-07 07:15 UTC
Nmap scan report for 
Host is up (0.0050s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
25/tcp    filtered smtp
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
3306/tcp  open  mysql    MySQL 5.7.26-0ubuntu0.16.04.1
Service Info: OSs: Unix, 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 9.16 seconds
FedoraSsrv:~$
  
```

PUERTO	ESTADO	SERVICIO	VERSION
21/TCP	ABIERTO	FTP	vsftpd 3.0.3
22/TCP	ABIERTO	SSH	OpenSSH 7.2p2 (ubuntu 2.8)
80/TCP	ABIERTO	HTTP	Apache https 2.4.18 (Ubuntu)
3306/TCP	ABIERTO	MySQL	MySQL 5.7.26-Ubuntu 16.04.1
25/TCP	FILTRADO	smtp	

5. Sesión de SSH comprometida

Riesgo: CRITICO

• DESCRIPCIÓN:

Se comprometió el inicio de sesión SSH en el host [REDACTED] con el usuario [REDACTED] y la contraseña [REDACTED] obtenidas de los archivos '192.241.151.12etc-passwd.txt' y 'Procedimientos tech.docx'



```
user — 114x26
[REDACTED]:~$ whoami
[REDACTED]:v
[REDACTED]@gentooserver:~$ uname -a
Linux gentooserver 4.4.0-138-generic #164-Ubuntu SMP Tue Oct 2 17:16:02 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
[REDACTED]@gentooserver:~$
```

• RECOMENDACIÓN:

No re utilizar contraseñas.

Utilizar contraseñas y nombres de usuarios diferentes para cada servidor.

6. Elevación de privilegios SSH

Riesgo: CRITICO

DESCRIPCIÓN:

Se obtuvo privilegios de usuario root con el usuario [REDACTED] en el servidor [REDACTED]

```
user — -p 808...
[REDACTED]@gentooserver:~$ sudo su
[sudo] password for [REDACTED]:
root@gentooserver:~/home/[REDACTED]#
```

- **RECOMENDACIÓN:**

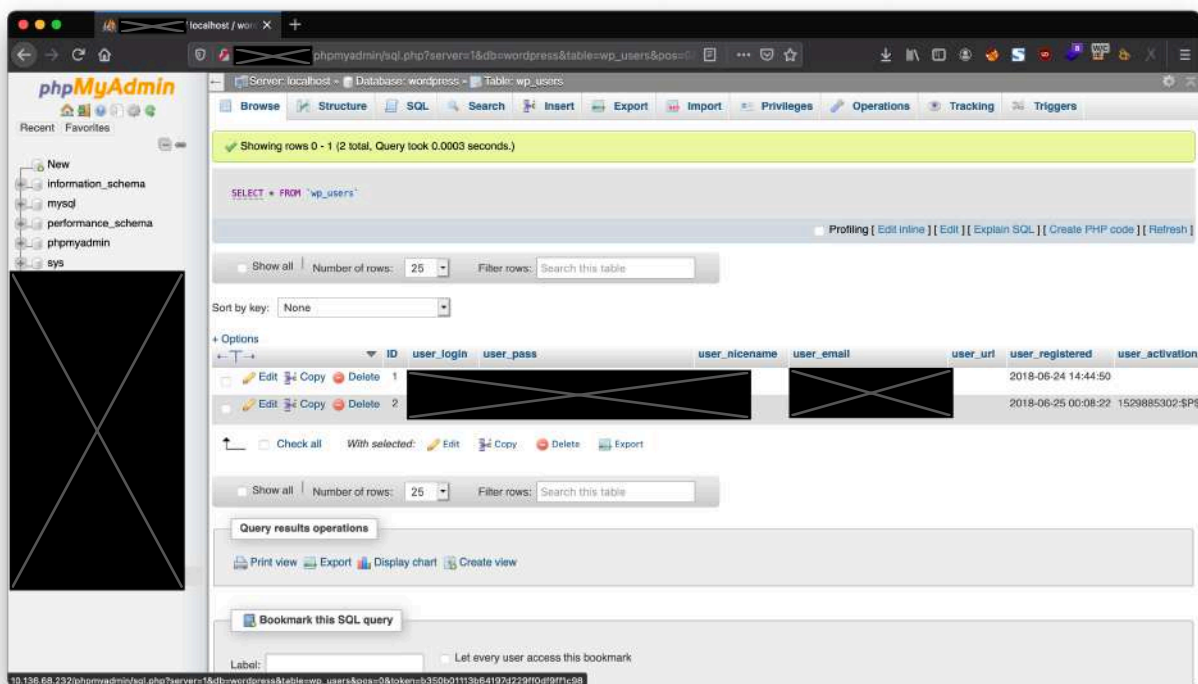
Realizar una correcta gestión de privilegios de los usuarios del sistema.
Usar una contraseña distinta para privilegios de root.

7. Sesión de phpMyAdmin comprometida

Riesgo: CRITICO

- **DESCRIPCIÓN:**

- Se obtuvo acceso a las **bases de datos** de phpMyAdmin del servidor [REDACTED] con el usuario [REDACTED] y contraseña [REDACTED] obtenidas del archivo **config-db.php** alojado en **'/etc/phpmyadmin/config-db.php'** en el servidor [REDACTED]
- Se obtuvo información sensible de usuarios y contraseñas de la base de datos 'wordpress'



- **RECOMENDACIÓN:**

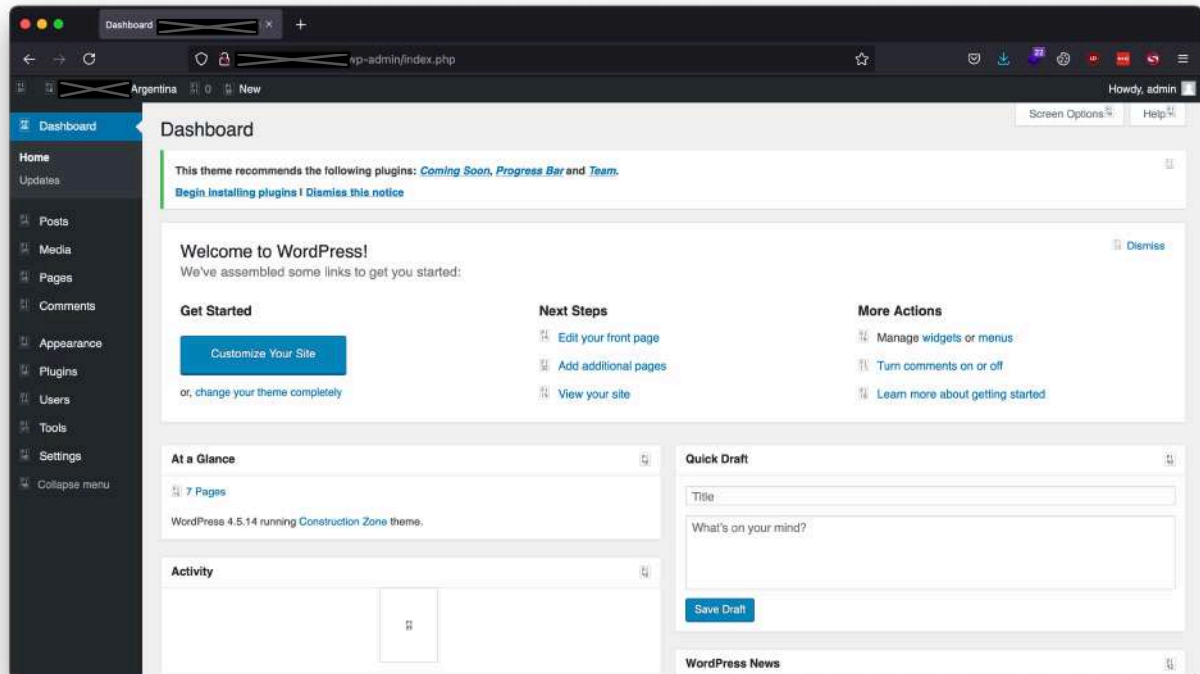
Utilizar contraseñas más seguras, que no tengan un parecido con otras del sistema.

8. Sesión de WordPress comprometida

Riesgo: CRITICO

• DESCRIPCIÓN:

Mediante fuerza bruta manual, se obtuvo acceso al panel de control de Wordpress ([http://\[REDACTED\]wp-admin/](http://[REDACTED]wp-admin/))



USUARIO	CONTRASEÑA
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

• RECOMENDACIÓN:

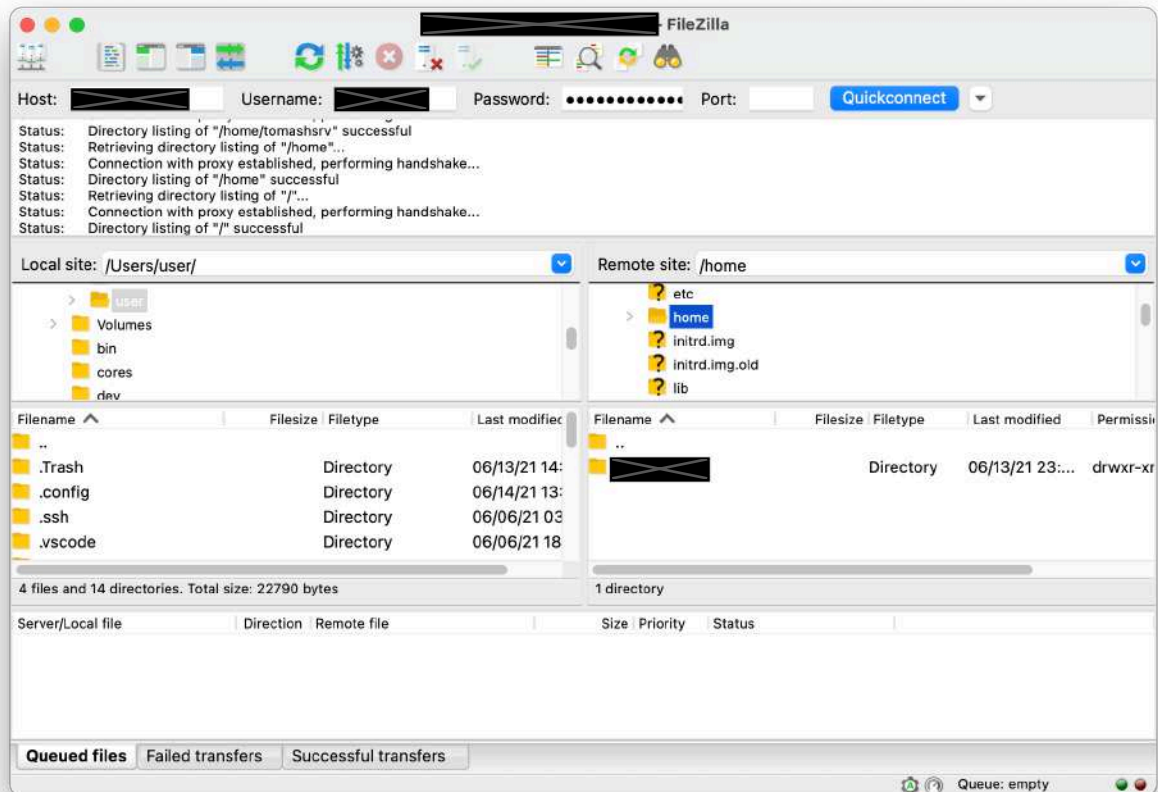
Utilizar contraseñas más seguras, que no tengan un parecido con otras del sistema.
Utilizar contraseñas distintas para cada usuario.

9. Sesión de vsFTPD comprometida

Riesgo: CRITICO

• DESCRIPCIÓN:

Se logró comprometer el inicio de sesión FTP en el servidor [REDACTED] con el usuario [REDACTED] y la contraseña [REDACTED] obtenidas de los archivos '192.241.151.12etc-passwd.txt' y 'Procedimientos tech.docx'



• RECOMENDACIÓN:

No re utilizar contraseñas.

Utilizar contraseñas y nombres de usuarios diferentes para cada servicio.

10. phpMyAdmin 4.x < 4.8.5 Múltiples Vulnerabilidades (PMASA-2019-1) (PMASA-2019-2)

Riesgo	CRITICO
Aplicación	phpMyAdmin
Descripción	<p>Según su número de versión autoinformado, la aplicación phpMyAdmin alojada en el servidor web remoto es 4.x anterior a 4.8.5. Por lo tanto, se ve afectado por al menos una de las siguientes vulnerabilidades:</p> <ul style="list-style-type: none">- Existe una vulnerabilidad de inyección SQL (SQLi) en phpMyAdmin debido a una validación incorrecta de la entrada proporcionada por el usuario. Un atacante remoto no autenticado puede aprovechar esto para inyectar o manipular consultas SQL en la base de datos de back-end, lo que resulta en la divulgación o manipulación de datos arbitrarios (CVE- 2019-6798).- Existe una vulnerabilidad de lectura de archivo arbitrario en phpMyAdmin cuando la opción de configuración AllowArbitraryServer está establecida en true. Un atacante remoto no autenticado puede aprovechar esto, a través de un servidor MySQL falso, para leer archivos arbitrarios y revelar información confidencial (CVE-2019-6799). https://www.phpmyadmin.net/security/PMASA-2019-1/ https://www.phpmyadmin.net/security/PMASA-2019-2/
Solución	Actualice a phpMyAdmin versión 4.8.5 o posterior. Alternativamente, aplique los parches a los que se hace referencia en los avisos de proveedores.
CVSS v3.0 Base Score	9.8
CVE	CVE-2019-6798, CVE-2019-6799
Versión instalada	4.5.4.1deb2ubuntu2.1
Versión parcheada	4.8.5

11. phpMyAdmin < 4.8.6 vulnerabilidad SQLi (PMASA-2019-3)

Riesgo	CRITICO
Aplicación	phpMyAdmin
Descripción	Según su número de versión autoinformado, la aplicación phpMyAdmin alojada en el servidor web remoto es anterior a 4.8.6. Por lo tanto, se ve afectado por una vulnerabilidad de inyección SQL (SQLi) que existe en la función del diseñador de phpMyAdmin. Un atacante remoto no autenticado puede aprovechar esto para inyectar o manipular consultas SQL en la base de datos de back-end, lo que resulta en la divulgación o manipulación de datos arbitrarios.
Solución	Actualice a phpMyAdmin versión 4.8.5 o posterior. Alternativamente, aplique los parches a los que se hace referencia en los avisos de proveedores.
CVSS v3.0 Base Score	9.8
CVE	CVE-2019-11768
Versión instalada	4.5.4.1deb2ubuntu2.1
Versión parcheada	4.8.5

12. WordPress 4.5.x < 4.5.23 varias vulnerabilidades

Riesgo	CRITICO
Aplicación	Wordpress
Descripción	Según su número de versión autoinformado, la aplicación phpMyAdmin alojada en el servidor web remoto es anterior a 4.8.6. Por lo tanto, se ve afectado por una vulnerabilidad de inyección SQL (SQLi) que existe en la función del diseñador de phpMyAdmin. Un atacante remoto no autenticado puede aprovechar esto para inyectar o manipular consultas SQL en la base de datos de back-end, lo que resulta en la divulgación o manipulación de datos arbitrarios.
Solución	Actualice a la versión 4.5.23 de WordPress o la más reciente.
CVSS v3.0 Base Score	9.8
CVE	CVE-2020-28035, CVE-2020-28036, CVE-2020-28039, CVE-2020-28032, CVE-2020-28033, CVE-2020-28040, CVE-2020-28037, CVE-2020-28038, CVE-2020-28034
Versión instalada	4.5.14

Versión parcheada	4.5.23
-------------------	--------

13. Vulnerabilidad en ap_get_basic_auth_pw()

Riesgo	CRITICO
Aplicación	Apache
Descripción	En Apache httpd 2.2.x antes de 2.2.33 y 2.4.x antes de 2.4.26, el uso de ap_get_basic_auth_pw () por módulos de terceros fuera de la fase de autenticación puede llevar a que se omitan los requisitos de autenticación.
Solución	Actualice a la ultima version de Apache.
CVSS v3.0 Base Score	9.8
CVE	CVE-2017-3167
Versión instalada	2.14.18

14. mod_ssl puede desreferenciar un puntero NULL

Riesgo	CRITICO
Aplicación	Apache
Descripción	En Apache httpd 2.2.x antes de 2.2.33 y 2.4.x antes de 2.4.26, mod_ssl puede eliminar la referencia a un puntero NULL cuando los módulos de terceros llaman a ap_hook_process_connection () durante una solicitud HTTP a un puerto HTTPS.
Solución	Actualice a la ultima version de Apache.
CVSS v3.0 Base Score	9.8
CVE	CVE-2017-3169
Versión instalada	2.4.18

15. Vulnerabilidad en mod_mime

Riesgo	CRITICO
Aplicación	Apache
Descripción	En Apache httpd 2.2.x antes de 2.2.33 y 2.4.x antes de 2.4.26, mod_mime puede leer un byte más allá del final de un búfer al enviar un encabezado de respuesta de Content-Type malicioso.
Solución	Actualice a la última versión de Apache.
CVSS v3.0 Base Score	9.8
CVE	CVE-2017-7679
Versión instalada	2.14.18

16. Ejecutar código arbitrario con los privilegios del proceso root

Riesgo	CRITICO
Aplicación	Apache
Descripción	En Apache httpd 2.2.x antes de 2.2.33 y 2.4.x antes de 2.4.26, mod_mime puede leer un byte más allá del final de un búfer al enviar un encabezado de respuesta de Content-Type malicioso. En las versiones 2.4.17 a 2.4.38 de Apache HTTP Server 2.4, con evento MPM, worker o prefork, el código que se ejecuta en procesos o subprocesos secundarios con menos privilegios (incluidos los scripts ejecutados por un intérprete de scripts en proceso) podría ejecutar código arbitrario con los privilegios del proceso padre (normalmente root) manipulando el marcador. Los sistemas que no son Unix no se ven afectados.
Solución	Actualice a la última versión de Apache.
CVSS v3.0 Base Score	5.0
CVE	CVE-2019-0211
Versión instalada	2.14.18

17. Error en el análisis de la lista de tokens

Riesgo	CRITICO
Aplicación	Apache
Descripción	Los cambios de análisis estricto de HTTP agregados en Apache httpd 2.2.32 y 2.4.24 introdujeron un error en el análisis de la lista de tokens, que permite que <code>ap_find_token()</code> busque más allá del final de su cadena de entrada. Al crear maliciosamente una secuencia de encabezados de solicitud, un atacante puede causar un error de segmentación o forzar a <code>ap_find_token()</code> a devolver un valor incorrecto.
Solución	Actualice a la última versión de Apache.
CVSS v3.0 Base Score	9.8
CVE	CVE-2017-7668
Versión instalada	2.14.18



18. Reutilización de contraseñas

Riesgo	ALTO
Descripción	<p>La reutilización de contraseñas en general es una práctica que debería desalentarse y evitarse en la medida de lo posible.</p> <p>En este caso, el impacto de la vulnerabilidad se ve amplificado por el hecho de que un atacante externo comprometió indirectamente un conjunto de aplicaciones del servidor interno.</p>
Solución	Actualice las políticas de administración de contraseñas para hacer cumplir el uso de contraseñas sólidas y únicas para todos los servicios dispares. Se debe fomentar el uso de administradores de contraseñas para permitir que se utilicen contraseñas únicas en los distintos sistemas más fácilmente.

19. phpMyAdmin 4.x < 4.9.4 / 5.x < 5.0.1 SQLi (PMASA-2020-1)

Riesgo	ALTO
Aplicación	phpMyAdmin
Descripción	Según su número de versión autoinformado, la aplicación phpMyAdmin alojada en el servidor web remoto es 4.x anterior a 4.9.4, o 5.x anterior a 5.0.1. Por lo tanto, se ve afectado por una vulnerabilidad de inyección SQL (SQLi) en la página de cuentas de usuario. Un atacante remoto autenticado puede explotar esto, inyectando SQL personalizado en lugar de su propio nombre de usuario, para inyectar o manipular consultas SQL en la base de datos back-end, lo que resulta en la divulgación o manipulación de datos arbitrarios. https://www.phpmyadmin.net/security/PMASA-2020-1/
Solución	Actualice a phpMyAdmin versión 4.9.4, 5.0.1 o posterior. Alternativamente, aplique los parches a los que se hace referencia en los avisos de proveedores.
CVSS v3.0 Base Score	8.8
CVE	CVE-2020-5504
Versión instalada	4.5.4.1deb2ubuntu2.1
Versión parcheada	4.9.4

20. Enumeración del usuario de WordPress

Riesgo	MEDIO
Aplicación	WordPress
Descripción	La versión de WordPress alojada en el servidor web remoto se ve afectada por una vulnerabilidad de enumeración de usuarios. Un atacante remoto no autenticado puede explotar esto para aprender los nombres de los usuarios válidos de WordPress. Esta información podría usarse para montar más ataques.
Solución	Actualice a la última versión de Wordpress
CVSS v3.0 Base Score	5.0
Enumeración de usuarios	
	

21. XSS en librería de Bootstrap

Riesgo	MEDIO
Aplicación	Bootstrap
Descripción	La biblioteca identificada de bootstrap, versión 3.3.6 es vulnerable a ataques XSS
Solución	Actualice a la última versión de bootstrap.
CVSS v3.0 Base Score	6.1
CVE	CVE-2019-8331 CVE-2018-14041 CVE-2018-14040 CVE-2018-14042
Versión instalada	3.3.6
Versión parcheada	4.3.1

22. Biblioteca de jQuery vulnerable

Riesgo	MEDIO
Aplicación	jQuery
Descripción	La biblioteca identificada de jquery, versión 1.12.4 es vulnerable. En versiones de jQuery mayores o iguales a 1.0.3 y anteriores a 3.5.0, pasar HTML que contiene elementos <option> de fuentes no confiables, incluso después de sanitizarlos, a uno de los métodos de manipulación DOM de jQuery (es decir, .html (), .append () y otros) puede que ejecute código que no es de confianza. Este problema está parcheado en jQuery 3.5.0.
Solución	Actualice a la última versión de jquery.
CVSS v3.0 Base Score	6.1
CVE	CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358
Versión instalada	1.12.14
Versión parcheada	3.5.0

23. Directorios webs navegables

Riesgo	MEDIO
Aplicación	Apache
Descripción	Asegúrese de que los directorios navegables no filtren información confidencial ni den acceso a recursos sensibles. Además, use restricciones de acceso o desactive la indexación de directorios para cualquiera que lo haga.

24. Aplicación web potencialmente vulnerable a Clickjacking

Riesgo	MEDIO
Descripción	<p>El servidor web remoto no establece un encabezado de respuesta X-Frame-Options o un encabezado de respuesta Content-Security-Policy 'frame-ancestors' en todas las respuestas de contenido. Potencialmente, esto podría exponer el sitio a un clickjacking o un ataque de reparación de la interfaz de usuario, en el que un atacante puede engañar a un usuario para que haga clic en un área de la página vulnerable que es diferente de lo que el usuario percibe que es la página. Esto puede resultar en que un usuario realice transacciones fraudulentas o maliciosas.</p> <p>http://www.nessus.org/u?399b1f56 https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet https://en.wikipedia.org/wiki/Clickjacking</p>
Solución	Devuelva el encabezado HTTP X-Frame-Options o Content-Security-Policy (con la directiva 'frame-ancestors') con la respuesta de la página. Esto evita que otro sitio represente el contenido de la página cuando se utilizan las etiquetas HTML de marco o iframe.
CVSS v2.0 Base Score	4.3
CWE	693
Versión instalada	3.3.6
Versión parcheada	4.3.1

25. phpMyAdmin 4.x < 4.9.0 CSRF (PMASA-2019-4)

Riesgo	MEDIO
Aplicación	phpMyAdmin
Descripción	Según su número de versión autoinformado, la aplicación phpMyAdmin alojada en el servidor web remoto es 4.x anterior a 4.9.0. Por lo tanto, se ve afectado por una vulnerabilidad de falsificación de solicitudes entre sitios (XSRF). Un atacante remoto puede aprovechar esto engañando a un usuario para que visite una página web especialmente diseñada, lo que le permite revelar información confidencial, hacerse pasar por la identidad del usuario o inyectar contenido malicioso en el navegador web de la víctima.
Solución	Actualice a phpMyAdmin versión 4.9.0 o posterior. Alternativamente, aplique los parches a los que se hace referencia en los avisos de proveedores.
CVSS v3.0 Base Score	6.5
CVE	CVE-2019-12616
Versión instalada	4.5.4.1deb2ubuntu2.1
Versión parcheada	4.9.0

26. Slowloris DOS attack

Riesgo	MEDIO
Aplicación	Apache
Descripción	Slowloris intenta mantener abiertas muchas conexiones con el servidor web de destino y mantenerlas abiertas el mayor tiempo posible. Lo logra abriendo conexiones al servidor web de destino y enviando una solicitud parcial. Al hacerlo, priva de los recursos del servidor http, lo que provoca la denegación de servicio.
Solución	Implementar mod_antiloris (https://github.com/Deltik/mod_antiloris)
CVSS v2.0 Base Score	5.0
CVE	<u>CVE-2007-6750</u>

27. Divulgación de distribución de Apache Banner Linux

Riesgo	INFO
Aplicación	Apache
Descripción	El nombre de la distribución de Linux que se ejecuta en el host remoto se encontró en el banner del servidor web.
Solución	Si no desea mostrar esta información, edite 'httpd.conf' y configure la directiva 'ServerTokens Prod' y reinicie Apache.
CVSS v2.0 Base Score	2.6
XREF	CWE:522 CWE:523 CWE:718 CWE:724 CWE:928 CWE:930

28. Software y tecnología de servidor encontrados

Riesgo	INFO
Aplicación	Apache
Descripción	Un atacante podría utilizar esta información para montar ataques específicos contra el tipo y la versión de software identificados.
Solución	<p>Si no desea mostrar esta información, edite 'httpd.conf' y configure la directiva 'ServerTokens Prod' y reinicie Apache.</p> <p>Más información sobre este problema: https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server</p>
XREF	CWE:522 CWE:523 CWE:718 CWE:724 CWE:928 CWE:930

29. El servidor web transmite credenciales de texto sin cifrar

Riesgo	BAJO
Descripción	<p>El servidor web remoto contiene varios campos de formulario HTML que contienen una entrada de tipo "contraseña" que transmite su información a un servidor web remoto en texto sin cifrar.</p> <p>Un atacante que espía el tráfico entre el navegador web y el servidor puede obtener inicios de sesión y contraseñas de usuarios válidos.</p> <p>Asegúrese de que todos los formularios sensibles transmitan contenido a través de HTTPS.</p>

Solución	
CVSS v2.0 Base Score	2.6
XREF	CWE:522 CWE:523 CWE:718 CWE:724 CWE:928 CWE:930

4. Recomendaciones generales y hardening



1. SSL y cifrado de base de datos

1. Como primera medida del sitio se recomienda montarlo en el puerto 443 y aplicarle un certificado SSL.
2. La Base de datos actualmente no esta cifrada. Se recomienda implementar un cifrado.

```

@gentooserver:~$ sudo mysql -u root -p -h 127.0.0.1
Enter password:
ERROR 1045 (28000): Access denied for user 'root'@'localhost' (using password: YES)
@gentooserver:~$ sudo mysql -u wordpress -p -h 127.0.0.1
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 577673
Server version: 5.7.26-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> SHOW VARIABLES LIKE '%ssl%';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| have_openssl  | DISABLED |
| have_ssl      | DISABLED |
| ssl_ca        |          |
| ssl_capath    |          |
| ssl_cert      |          |
| ssl_cipher    |          |
| ssl_crl       |          |
| ssl_crlpath   |          |
| ssl_key       |          |
+-----+-----+
9 rows in set (0.00 sec)

mysql>

```

```
mysql> \s

mysql Ver 14.14 Distrib 5.7.26, for Linux (x86_64) using EditLine wrapper

Connection id:          577673
Current database:
Current user:           wordpress@localhost
SSL:                    Not in use
Current pager:          stdout
Using outfile:          ''
Using delimiter:        ;
Server version:         5.7.26-0ubuntu0.16.04.1 (Ubuntu)
Protocol version:       10
Connection:             127.0.0.1 via TCP/IP
Server characterset:    latin1
Db characterset:        latin1
Client characterset:    utf8
Conn. characterset:     utf8
TCP port:               3306
Uptime:                 5 days 12 hours 30 min 29 sec

Threads: 1  Questions: 6919826  Slow queries: 0  Opens: 967  Flush tables: 1  Open tables: 411  Q
ueries per second avg: 14.506

mysql> █
```

2. Ocultar la versión y el sistema operativo de Apache

De forma predeterminada, la versión de apache y el sistema operativo se muestran en los encabezados de respuesta. Esto puede llevar a un problema de seguridad ya que expone los detalles a un atacante.

Para ocultar esos detalles, agregar las dos líneas en el archivo de configuración de apache **/etc/apache2/conf-enabled/security.conf**

```
SERVERSIGNATURE OFF
SERVETOKENS PROD
```

3. Deshabilitar la lista de directorios y FollowSymLinks

De forma predeterminada, la lista de directorios para todos los archivos en el directorio raíz web está habilitada. Además, Apache está configurado por defecto para seguir enlaces simbólicos, lo cual no es recomendable.

Para deshabilitarlos, editar el archivo de configuración **/etc/apache2/apache2.conf** colocando “-” antes de cada directiva de etiqueta en la línea Options Indexes FollowSymLinks para convertirse en Options -Indexes -FollowSymLinks como se muestra a continuación:

```
<DIRECTORY /VAR/WWW/>
OPTIONS -INDEXES -FOLLOWSYMLINKS
ALLOWOVERRIDE NONE
REQUIRE ALL GRANTED
</DIRECTORY>
```

4. Actualizar WordPress

Aunque WordPress es muy seguro, siempre se puede mejorar y por eso hay actualizaciones de la versión de software. En cuanto se detecta el más mínimo problema en la seguridad se corrige y se lanza una actualización.

Esto quiere decir que la versión más segura de WordPress es la última disponible. Por eso es muy importante mantener actualizado WordPress en todo momento.

Desde la versión 3.7 se puede configurar WordPress para que se actualice de manera automática.

5. Asegurar wp-admin

Para acceder a la administración de WordPress lo hacemos a través de wp-admin, por lo que es uno de los archivos más susceptibles a ataques.

De hecho, el codex de WordPress indica que la gran mayoría de los ataques en WordPress se producen de dos formas:

- Por medio de exploit específico para vulnerabilidades conocidas en plugins y themes antiguos. Por eso es tan importante estar actualizado.

Acceder al blog por medio de un ataque de fuerza bruta en wp-admin.

Esto se puede evitar con la mayoría de los plugins de seguridad que tenemos disponibles en

WordPress, como **Wordfence Security, WP Limit Login Attempts, Limit Login Attempts**, etc...

Básicamente, estos plugins banean cualquier ip que intenta acceder a wp-admin de manera repetida y equivocadamente. Una forma muy efectiva de evitar los ataques de fuerza bruta.

6. Asegurar wp-config.php

Una de las formas más habituales y efectivas que tenemos de proteger el archivo **wp-config.php** es añadiendo estas líneas de código en el archivo **.htaccess**.

Denegar el acceso al archivo **wp-config.php**

```
<FILES WP-CONFIG.PHP>  
ORDER ALLOW,DENY  
DENY FROM ALL  
</FILES>
```

7. Copias de Seguridad

Se recomienda mantener copias de seguridad y conocer el estado de la instalación de WordPress en intervalos regulares. Tener un plan para hacer una copia de seguridad y así recuperar la instalación en caso de una catástrofe, sin mayores inconvenientes.

8. Política de contraseñas

1. **No repetir.** Las contraseñas deben ser únicas, así que debemos utilizar claves diferentes para cada uno de los servicios en los que estemos dados de alta. De lo contrario, el robo de la clave de un servicio permitiría el acceso al resto.
2. **Elegir una combinación robusta.** Siempre debemos elegir una contraseña con un mínimo de ocho caracteres y que a ser posible combine mayúsculas, minúsculas, números y símbolos. Un truco para memorizar contraseñas complejas consiste en recurrir a poemas, letras de canciones o alguna otra frase que nos resulte familiar y que incluya algún número. A partir de ahí, podemos construir una contraseña robusta si empleamos solo las iniciales de cada palabra y los dígitos, comenzando en mayúscula y terminando con algún símbolo, como %. Por ejemplo, si tomamos como referencia la oración "El 7 de septiembre es nuestro aniversario", nuestra clave sería E7dsena%.

3. **Utilizar gestores de contraseñas.** En el caso de que cueste recordar cada una de las 'passwords' utilizadas para los distintos servicios (correo electrónico, redes sociales, mensajería instantánea, foros, etc.), es posible utilizar un gestor de contraseñas, es decir, una aplicación que guarda las credenciales de manera segura y las protege con una clave de acceso maestra. Aunque antes de usar este tipo de programas se debe tener en cuenta lo siguiente:
 - La clave maestra debe ser muy segura y robusta, ya que nos da acceso al resto de contraseñas.
 - Se deben realizar copias de seguridad del fichero de claves, para evitar perder las contraseñas almacenadas.
4. **Evitar la simplicidad.** Se desaconseja utilizar palabras comunes en cualquier idioma, nombres propios, lugares, números de teléfono, números consecutivos (como el famoso 123456), teclas consecutivas de un teclado (el también conocido 'qwerty') y fechas de nacimiento, así como combinaciones excesivamente cortas de alguno de los anteriores elementos, como "Manuel1974".
5. **No utilizar cualquier variación** de nombres, fechas de nacimiento, etc...
6. **Nunca usar una contraseña corta.**
7. Si es posible usar autenticación de **múltiples factores**.

9. Desactivar o deshabilitar el usuario root

Deshabilitar root en linux Ahora sí nos ponemos manos a la obra. Como es necesario tener privilegios para desactivar la cuenta root, tendrás que ejecutar este primer comando desde un terminal:

```
sudo -s
```

Esto permite ejecutar comandos al usuario más o menos como si fuese root. Ahora ejecuta el comando `passwd` sobre la cuenta de root para deshabilitar la contraseña y que no se pueda conectar.

```
passwd -l root
```

Esta es una forma bastante efectiva de asegurar la cuenta de root, pero aun así no es la única forma de mejorar la seguridad. Codificar y configurar en su cuenta una contraseña que no se puede usar es también muy efectivo:

```
usermode -p '!' root
```

Cómo habilitar la cuenta de root de nuevo

Porque no solo de bloquear se trata, sino de poder recuperarla en caso necesario vamos a ver como se hace. Solo necesitarás un usuario con permisos root como antes con `sudo -s`. Ahora escribes este comando para configurar la contraseña de nuevo:

```
passwd root
```

Y cuando te pregunte dos veces la contraseña, solo tienes que ponerla.

Este método sirve para que el usuario root no sea capaz de acceder incluso si conociese la contraseña original (ya que la hemos invalidado). El caso, es que otros usuarios en el archivo `sudoers` pueden tener los mismos permisos que este, y por eso es necesario poner una contraseña segura, para que no pueda filtrarse.

10. Dar permisos a un usuario para que únicamente pueda usar los comandos que nosotros queramos

De forma fácil podemos limitar los permisos que damos a un usuario.

A modo de ejemplo podemos introducir el siguiente comando en el fichero /etc/sudoers:

```
usrUTN ALL=(root:root) /usr/bin/passwd *, !/usr/bin/passwd root
```

Con este comando damos permiso al usuario usrUTN para que en el cualquier equipo pueda cambiar la contraseña de cualquier usuario exceptuando la contraseña del usuario root.

Nota: Mediante el operador * indicamos que el usuario usrUTN podrá cambiar la contraseña de todos los usuarios. Con el operador ! Forzamos que el usuario usrUTN no pueda cambiar la contraseña del usuario root.

11. Dar permisos para que únicamente los usuarios de un grupo puedan utilizar iptables

Por ejemplo: Si únicamente quiero que los usuarios del grupo usrUTN puedan utilizar iptables introduciré la siguiente línea dentro del fichero /etc/sudoers:

```
%usrUTN ALL=(root:root) /sbin/iptables
```

Una vez introducidos los cambios tan solo tenemos que guardarlos y cerrar el editor de textos.

12. Asegurar conexión SSH

Cambiar los parámetros

Utilizar el siguiente comando:

```
vi /etc/ssh/sshd_config
```

Modificar los siguientes parámetros:

-LoginGraceTime: Es el tiempo que posee cada usuario en colocar los datos de acceso o intentarlo en varias ocasiones si ingresa mal los datos. Este punto es muy importante porque por default, esta configurado en 2 minutos tiempo suficiente para que un script haga cientos de intentos de login. Para un usuario normal bastan 10 o 20 segundos para poder loguearse.

- PermitRootLogin: Este interesante punto es el que SIEMPRE tendremos que modificar para tener nuestro sistema seguro, todos los servers linux y unix usan al usuario root como administrador del sistema, es decir que el usuario default con más privilegios se llama "root" en consecuencia es el usuario más atacado y forzado. Por eso mismo es altamente recomendable usar cualquier usuario para ingresar al SSH, negando el login directo al Root y manejandose con la escala de privilegios que da el su o sudo.

- MaxAuthTries: Este valor es el que nos da la cantidad de logins incorrectos que podemos tener antes de cerrar la pantalla de login, normalmente y por default este valor es 6 pero lo recomendable es dejarlo en 2 para así evitar el intento masivo de login.

- MaxStartups: Indica la cantidad de ssh que se pueden abrir por IP, este valor por default es de 100 lo cual permitirá abrir 100 conexiones hacia nuestro servidor desde una misma IP. Este valor es muy exagerado, pasándolo a 3 o 5 es más que suficiente.

- AllowUsers: Si solo usamos un par de usuarios el ssh lo mejor es limitar el acceso a dichos users y tener una tabla de accesos. Por ejemplo:

```
AllowUsers soyadmin
```

```
AllowUsers quemiras
```

```
AllowUsers otromas
```

En este ejemplo estamos otorgando permisos de acceso a estos 3 usuarios.

5. APÉNDICE A - CRITERIO DE VULNERABILIDAD CLASIFICACIÓN

A continuación se muestran los criterios de calificación de riesgo utilizados para clasificar las vulnerabilidades discutidas en este informe:

Serveridad	Descripción
CRITICO	Dirige el compromiso del sistema y de datos. Puede ser explotado por un atacante sin habilidades utilizando herramientas disponibles públicamente. Debe ser abordado de inmediato.
ALTO	Por lo general, lleva a comprometer el sistema y los datos que maneja.
MEDIO	No conduce al compromiso inmediato del sistema, pero cuando se encadena con otros problemas puede conllevar graves riesgos de seguridad.
BAJO	No plantea un riesgo inmediato e incluso cuando esté encadenado con otras vulnerabilidades es menos probable que cause un impacto grave.
INFO	No plantea un riesgo de inmediato, pero puede dar información valiosa para un atacante.

6. Herramientas utilizadas



A continuación se muestran las herramientas que se utilizaron para llevar a cabo el Pentest:

Nessus - <https://www.tenable.com/products/nessus>

Nmap - <https://nmap.org/>

Gobuster - <https://github.com/OJ/gobuster>

SlowHTTPTest - <https://github.com/shekya/slowhttpstest>

HASH MD5 - <http://hashes.com>

Pentest-Tools - <https://pentest-tools.com/website-vulnerability-scanning/website-scanner>

WPscan - <https://wpscan.com/wordpress-security-scanner>