

WEB2S SECURITY

Reporte de pentesting y comprobación de vulnerabilidades, utilizando
Metaexploitable2 y Kali Linux.

Web2S Security

Febrero 2024

versión 1.0

Realizado por: Miguel Ángel Fernández Parejo

mafparejo@proton.me

mdr716@gmail.com

mafparejo@gmail.com

CONTENIDO

- 1 Autoría del documento y derechos de copyright.
- 2 Ámbito y alcance de la auditoría.
- 3 Resumen.
- 4 Posibles soluciones a la falta de seguridad.

1 AUTORÍA DEL DOCUMENTO Y DERECHOS DE COPYRIGHT

El presente documento ha sido realizado por Web2S Security, y está protegido con derechos de autor *copyright*, está prohibida su copia parcial o totalmente, así como su distribución fuera del ámbito de Web2S Security y de su cliente Oblibion, S.A. Contiene información sensible estando prohibida su divulgación por cualquier medio digital o físico.

CLIENTE: Oblibion, S.A.

PROYECTO: Seguridad y pentesting.

CLASIFICACIÓN: Confidencial

AUTOR: Miguel Ángel Fernández Parejo

2 ÁMBITO Y ALCANCE DE LA AUDITORÍA

La auditoría se ha realizado en Metasploitable2 y Kali Linux, utilizando la herramienta Nmap, se han recuperado los siguientes datos:

Escaneando la IP de Meta `http://192.168.0.14` con nmap lanza estos resultados:

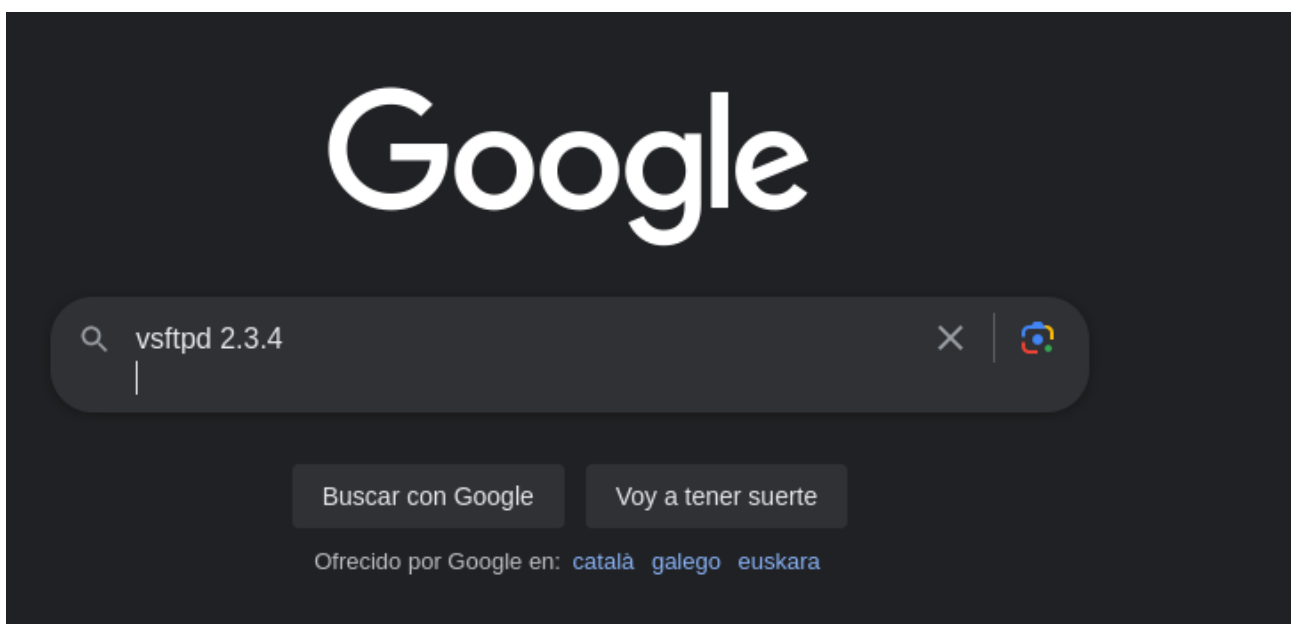
```
(kali@kali)-[~]
$ nmap 192.168.0.14 -p- --open -A -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-16 02:26 EST
Nmap scan report for 192.168.0.14
Host is up (0.00080s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|_STAT:
|_FTP server status:
|_   Connected to 192.168.0.12
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
53/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_   bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind      2 (RPC #100000)
|_rpcinfo:
|_   program version  port/proto  service
|_   100000  2              111/tcp    rpcbind
|_   100000  2              111/udp    rpcbind
|_   100003  2,3,4          2049/tcp   nfs
|_   100003  2,3,4          2049/udp   nfs
|_   100005  1,2,3          38155/tcp  mountd
|_   100005  1,2,3          42756/udp  mountd
|_   100021  1,3,4          51296/udp  nlockmgr
|_   100021  1,3,4          57482/tcp  nlockmgr
|_   100024  1              41517/udp  status
|_   100024  1              42354/tcp  status
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
|_version: v
|_server: irc.Metasploitable.LAN
|_version: Unreal3.2.8.1. irc.Metasploitable.LAN
|_uptime: 0 days, 0:05:24
|_source ident: nmap
|_source host: DF56A143.F8D9233E.FFFA6D49.IP
|_error: Closing Link: kvpxkzvou[192.168.0.12] (Quit: kvpxkzvou)
8009/tcp  open  Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
8787/tcp  open  drb          Ruby DRB RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbi)
38155/tcp open  mountd       1-3 (RPC #100005)
42354/tcp open  status       1 (RPC #100024)
54609/tcp open  java-rmi     GNU Classpath gmrregistry
57482/tcp open  nlockmgr     1-4 (RPC #100021)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

|_   41517  1              41517/udp  status
|_   100024  1              41517/udp  status
|_   100024  1              42354/tcp  status
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
```

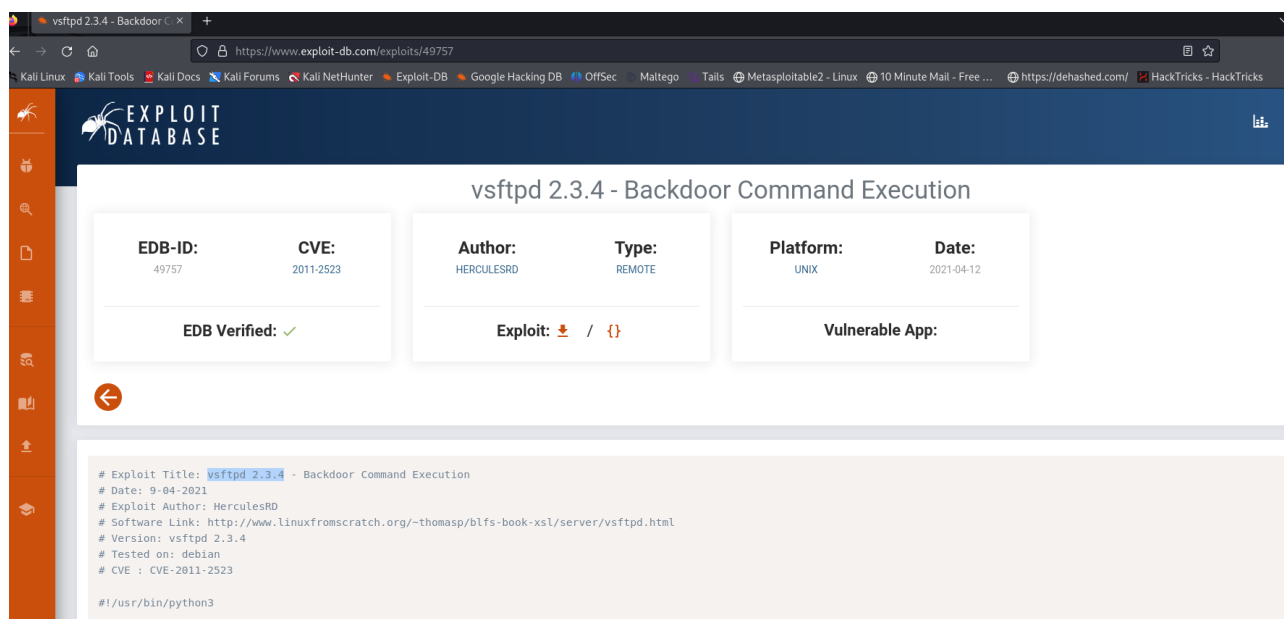
```
File Actions Edit View Help
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rshd
513/tcp open login? Netkit rshd
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 9
| Capabilities flags: 43564
| Some Capabilities: SwitchToSSLAfterHandshake, Support41Auth, SupportsTransactions, LongColumnFlag, SupportsCompression, ConnectWithDatabase, Speaks41ProtocolNew
| Status: Autocommit
| Salt: 24Lb)ANDI%vHD2yrQ-H)
3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu0804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
| ssl-date: 2024-02-16T08:52:30+00:00; +3s from scanner time.
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
| VNC Authentication (2)
6000/tcp open X11 (access denied)
6667/tcp open irc UnrealIRCd (Admin email admin@Metasploitable.LAN)
| irc-info:
| users: 1
| servers: 1
| lusers: 1
| lservers: 0
| server: irc.Metasploitable.LAN
| version: Unreal3.2.8.1. irc.Metasploitable.LAN
| uptime: 0 days, 0:05:00
| channel ident: nman
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
39688/tcp open java-rmi GNU Classpath grmiregistry
41800/tcp open nlockmgr 1-4 (RPC #100021)
47986/tcp open status 1 (RPC #100024)
53781/tcp open mountd 1-3 (RPC #100005)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Vamos a ir buscando vulnerabilidades a través de los puertos abiertos, con sus versiones, para ello copiamos por ej. el primero y vamos buscar en Google, las vulnerabilidades:

vsftpd 2.3.4



En la web exploit-db.com encontramos este exploit que se lanza en python3:



The screenshot shows the Exploit-DB website interface. The main title is "vsftpd 2.3.4 - Backdoor Command Execution". Below the title, there are three boxes containing metadata:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49757	2011-2523	HERCULESRD	REMOTE	UNIX	2021-04-12

Below these boxes, there are three sections:

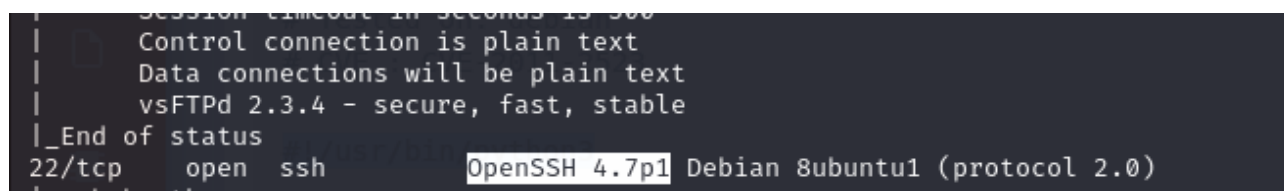
- EDB Verified:** ✓
- Exploit:** Download icon / Copy icon
- Vulnerable App:**

Below these sections, there is a code block containing the exploit details:

```
# Exploit Title: vsftpd 2.3.4 - Backdoor Command Execution
# Date: 9-04-2021
# Exploit Author: HerculesRD
# Software Link: http://www.linuxfromscratch.org/~thomasp/blfs-book-xsl/server/vsftpd.html
# Version: vsftpd 2.3.4
# Tested on: debian
# CVE : CVE-2011-2523

#!/usr/bin/python3
```

Siguiente servicio/puerto OpenSSH 4.7.p1:



```
Session timeout in seconds is 300
Control connection is plain text
Data connections will be plain text
vsFTPD 2.3.4 - secure, fast, stable
_End of status
22/tcp open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
Last hostkey:
```

Buscamos en Google algún exploit, en cvedetails.com encontramos muchas vulnerabilidades:

Openbsd Openssh version: X +

https://www.cvedetails.com/vulnerability-list/vendor_id-97/product_id-585/version_id-430455/Openbsd-Openssh-4.7p1.html?page=1&order=1&trc=31&sha=a0f995a88b5436a219ecc740747b1

Documentation CVE id, product, vendor... Search Log in

Openbsd » Openssh » 4.7p1 : Security Vulnerabilities, CVEs,

cpe:2.3:a:openbsd:openssh:4.7p1:*:*:*:*:*

Published in: 2024 January February

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By: Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

31 vulnerabilities found

1 2 Copy

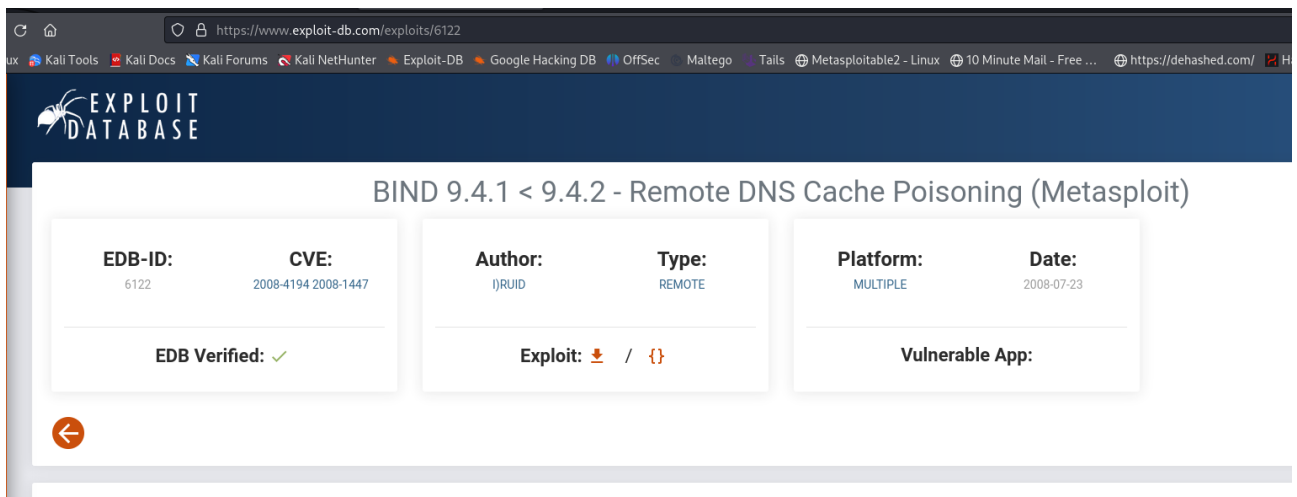
CVE	Description	Max CVSS	Published	Updated	EPSS
CVE-2023-51385	In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.	6.5	2023-12-18	2024-01-05	0.19%
CVE-2023-51384	In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.	5.5	2023-12-18	2024-01-05	0.05%
CVE-2023-48795	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP),	5.9	2023-12-18	2024-01-29	69.44%
CVE-2023-38408		9.8	2023-07-20		

El OpenSSH 4.7.p1 al ser una versión antigua se aconseja actualización de este servicio.

Buscamos en Google vulnerabilidades para el servicio ISC BIND 9.4.2

```
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPE
53/tcp open domain ISC BIND 9.4.2
|_dns-nsid:
```

En exploit-db.com, nos dice que tiene un envenenamiento de caché remoto por DNS:

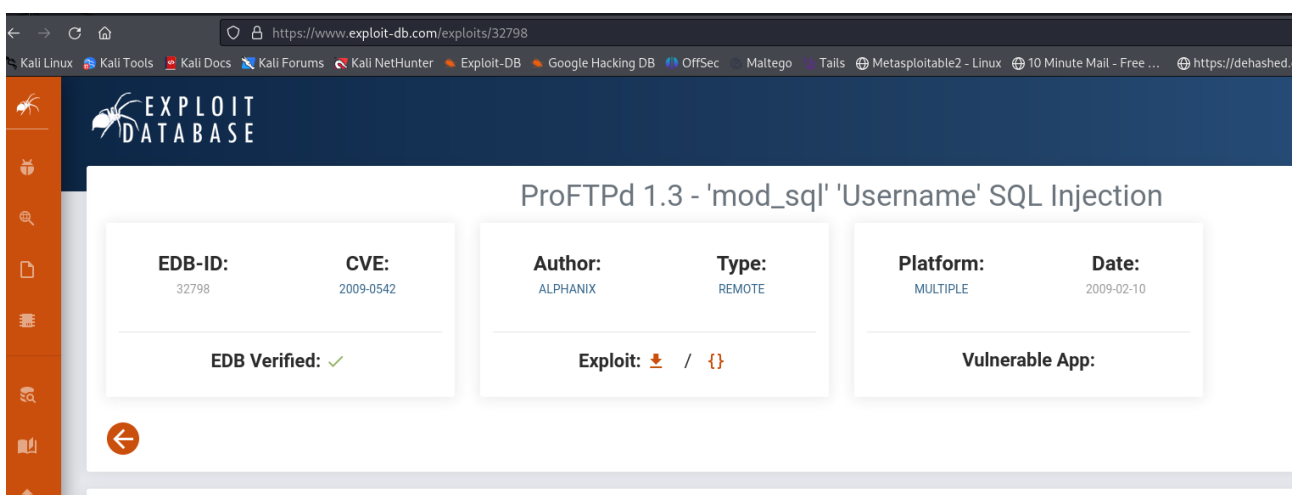


Este servicio tiene una versión de la cual se descubrió un exploit público de 2008 y se aconseja actualizar la versión.

Veo el servicio ProFTPD 1.3.1

```
1099/tcp open  java-rmi      GNU Classpath grmregistry
1524/tcp open  bindshell     Metasploitable root shell
2049/tcp open  nfs          2-4 (RPC #100003) allow an
2121/tcp open  ftp          ProFTPD 1.3.1 location; other
3306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
mysql-info:
```

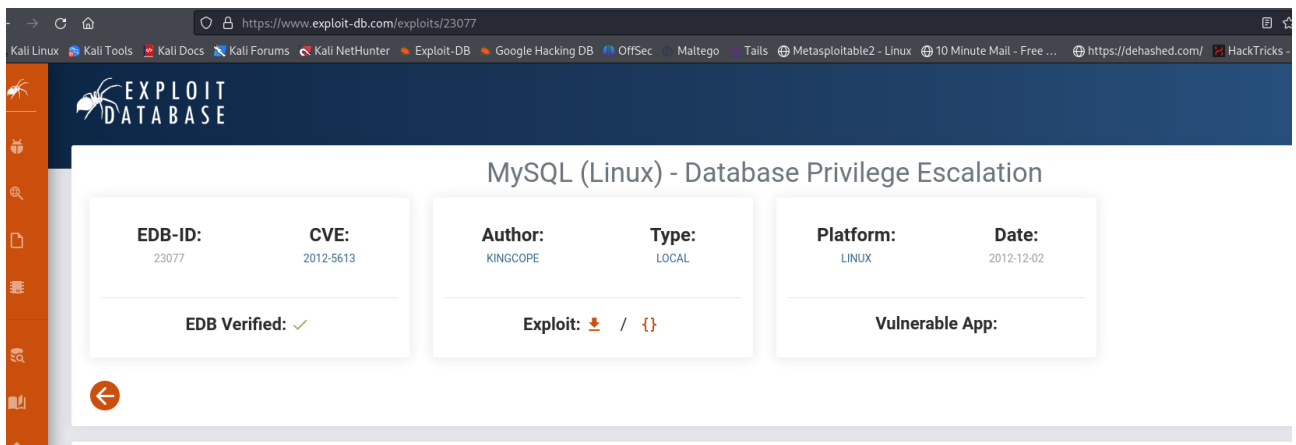
Buscamos en google y encontramos:



pasa lo mismo que el anterior, tiene una vulnerabilidad descubierta en

2009, se aconseja al cliente actualizar el servicio.

El servicio MySQL 5.0.51a-3ubuntu5, buscamos y nos da esta vulnerabilidad, que es una escalada de privilegios del año 2012:



The screenshot shows a web browser window with the URL <https://www.exploit-db.com/exploits/23077>. The page title is "MySQL (Linux) - Database Privilege Escalation". The page contains the following information:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
23077	2012-5613	KINGCOPE	LOCAL	LINUX	2012-12-02

Below the table, there are three sections:

- EDB Verified:** ✓
- Exploit:** 📄 / {}
- Vulnerable App:**

Se aconseja actualizar el servicio.

```
(kali@kali)-[~]
$ dirb http://192.168.0.14 | Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking D

DIRB v2.22
By The Dark Raver

START_TIME: Fri Feb 16 04:15:21 2024
URL_BASE: http://192.168.0.14/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.0.14/ ---
+ http://192.168.0.14/cgi-bin/ (CODE:403|SIZE:293)
=> DIRECTORY: http://192.168.0.14/dav/
+ http://192.168.0.14/index (CODE:200|SIZE:891)
+ http://192.168.0.14/index.php (CODE:200|SIZE:891)
+ http://192.168.0.14/phpinfo (CODE:200|SIZE:48062)
+ http://192.168.0.14/phpinfo.php (CODE:200|SIZE:48074)
=> DIRECTORY: http://192.168.0.14/phpMyAdmin/
+ http://192.168.0.14/server-status (CODE:403|SIZE:298)
=> DIRECTORY: http://192.168.0.14/test/
=> DIRECTORY: http://192.168.0.14/twiki/

--- Entering directory: http://192.168.0.14/dav/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.0.14/phpMyAdmin/ ---
+ http://192.168.0.14/phpMyAdmin/calendar (CODE:200|SIZE:4145)
+ http://192.168.0.14/phpMyAdmin/changelog (CODE:200|SIZE:74593)
+ http://192.168.0.14/phpMyAdmin/ChangeLog (CODE:200|SIZE:40540)
=> DIRECTORY: http://192.168.0.14/phpMyAdmin/contrib/
+ http://192.168.0.14/phpMyAdmin/docs (CODE:200|SIZE:4583)
+ http://192.168.0.14/phpMyAdmin/error (CODE:200|SIZE:1063)
+ http://192.168.0.14/phpMyAdmin/export (CODE:200|SIZE:4145)
+ http://192.168.0.14/phpMyAdmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.0.14/phpMyAdmin/import (CODE:200|SIZE:4145)
+ http://192.168.0.14/phpMyAdmin/index (CODE:200|SIZE:4145)
+ http://192.168.0.14/phpMyAdmin/index.php (CODE:200|SIZE:4145)
=> DIRECTORY: http://192.168.0.14/phpMyAdmin/js/
=> DIRECTORY: http://192.168.0.14/phpMyAdmin/lang/
=> DIRECTORY: http://192.168.0.14/phpMyAdmin/libraries/
+ http://192.168.0.14/phpMyAdmin/license (CODE:200|SIZE:18011)
+ http://192.168.0.14/phpMyAdmin/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.0.14/phpMyAdmin/main (CODE:200|SIZE:4227)
+ http://192.168.0.14/phpMyAdmin/navigation (CODE:200|SIZE:4145)
+ http://192.168.0.14/phpMyAdmin/phpinfo (CODE:200|SIZE:0)
+ http://192.168.0.14/phpMyAdmin/phpinfo.php (CODE:200|SIZE:0)
```

puertos abiertos: 8080, 9090 y 42525


```

(kali@kali)-[~]
$ sudo nmap -O 127.0.0.1
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-06 11:05 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00012s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
8080/tcp  open  http-proxy
9090/tcp  open  zeus-admin
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds

```

la aplicación WebGoat está creada en java 21.0.1

```

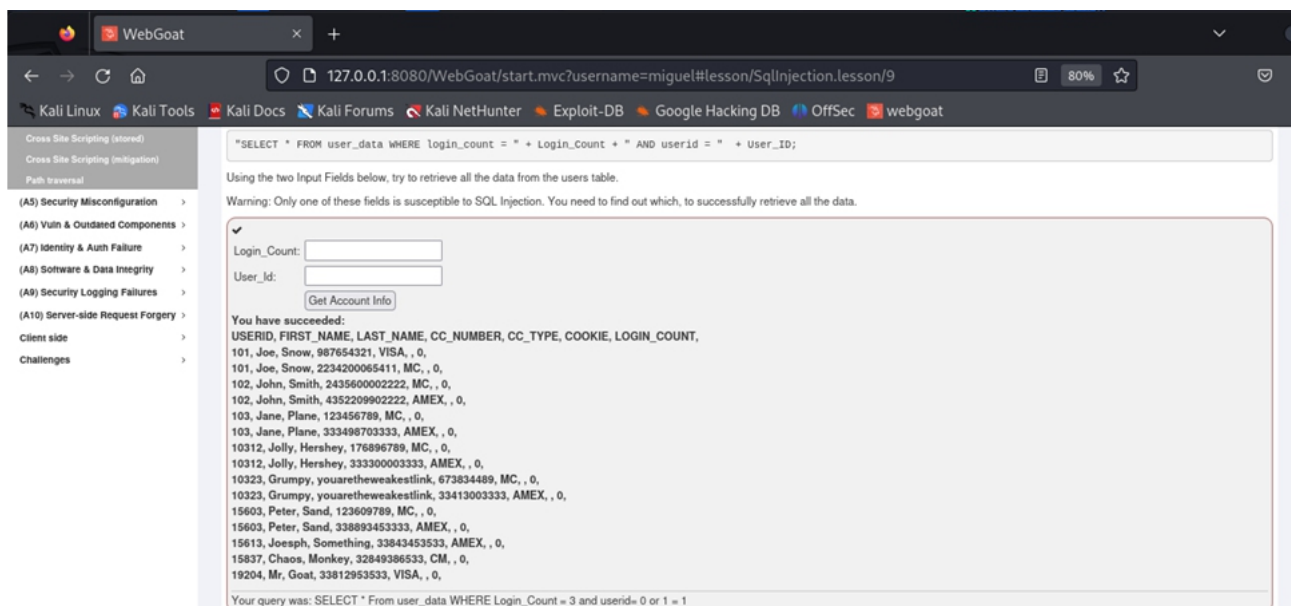
(kali@kali)-[/home/kali]
PS> sudo docker run -it -p 127.0.0.1:8080:8080 -p 127.0.0.1:9090:9090 -e TZ=Europe/Berlin webgoat/webgoat
[sudo] password for kali:
2023-12-07T15:36:32.956+01:00 INFO 1 --- [ main] org.owasp.webgoat.server.StartWebGoat : Starting StartWebGoat v2023.8 using Java 21.0.1 with PID 1
me/webgoat/webgoat.jar started by webgoat in /home/webgoat)

```

La auditoría ha encontrado las siguientes vulnerabilidades:

A3 Injection - SQL Injection (intro) - Apartado 10

Esta se basa en la inyección de código SQL, es decir, introducir caracteres de este lenguaje de consulta, para cada petición al servidor, que permite obtener datos como usuarios y sus tarjetas de crédito, incluso podría descargar toda la base de datos:



A3 Injection - SQL Injection (intro) - Apartado 11

En esta ocasión, mediante el campo Employee Name, podemos obtener información confidencial de usuarios y también podemos descargar la base de datos:

127.0.0.1:8080/WebGoat/start.mvc?username=miguel#lesson/SqlInjection.lesson/10

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec webgoat

(A9) Security Logging Failures >
(A10) Server-side Request Forgery >
Client side >
Challenges >

own SQL after that.

It is your turn!

You are an employee named John **Smith** working for a big company. The company has an internal system that allows all employees to see data such as the department they work in and their salary.

The system requires the employees to use a unique *authentication TAN* to view their data.
Your current TAN is **3SL99A**.

Since you always have the urge to be the most highly paid employee, you want to exploit the system so that instead of viewing your own info to *take a look at the data of all your colleagues* to check their current salaries.

Use the form below and try to retrieve all employee data from the **employees** table. You should not need to know any specific names or other information you need.
You already found out that the query performing your request looks like this:

```
"SELECT * FROM employees WHERE last_name = '' + name + '' AND auth_tan = '' + auth_tan + ''";
```

Employee Name:

Authentication TAN:

No employee found with matching last name. Or maybe your authentication TAN is incorrect?

A3 Injection - Cross Site Scripting - Apartado - Apartado 7

Se ha podido encontrar esta vulnerabilidad, que se basa en la inyección de código JavaScript en el campo de entrada “Enter your credit card number”:

Archivo Máquina Ver Entrada Dispositivos Ayuda

WebGoat

127.0.0.1:8080/WebGoat/start.mvc?username=miguel#lesson/CrossSiteScripting.lesson/6

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec webgoat

Cross Site Scripting (stored)
Cross Site Scripting (mitigation)
Path traversal

(A5) Security Misconfiguration >
(A6) Vuln & Outdated Components >
(A7) Identity & Auth Failure >
(A8) Software & Data Integrity >
(A9) Security Logging Failures >
(A10) Server-side Request Forgery >
Client side >
Challenges >

It is always a good practice to validate all input on the server side. XSS can occur when unvalidated user input gets used in an HTTP response. In a reflected XSS attack, an attacker can craft a URL with the attack script and post it to another website, email it, or otherwise get a victim to click on it.

An easy way to find out if a field is vulnerable to an XSS attack is to use the `alert()` or `console.log()` methods. Use one of them to find out which field is vulnerable.

Shopping Cart

Shopping Cart Items -- To Buy Now	Price	Quantity	Total
Studio RTA - Laptop/Desk/Chair with Tilting Surface, Chrome	69.99	1	\$0.00
Dynex - Traditional	27.99	1	\$0.00
Hewlett-Packard	1599.99	1	\$0.00
3 - Year Performance	299.99	1	\$0.00

Enter your credit card number:

Enter your three digit access code:

Congratulations, but alerts are not very impressive are they? Let's continue to the next assignment.

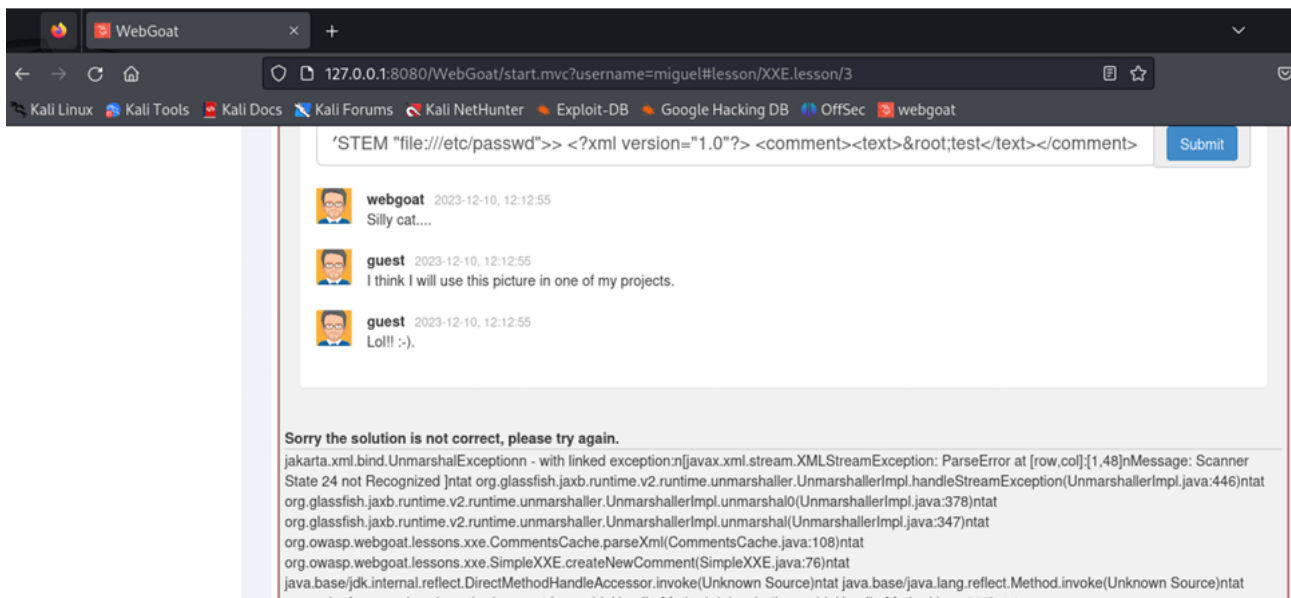
Thank you for shopping at WebGoat.
Your support is appreciated

We have charged credit card:4128 3214 0002 1999

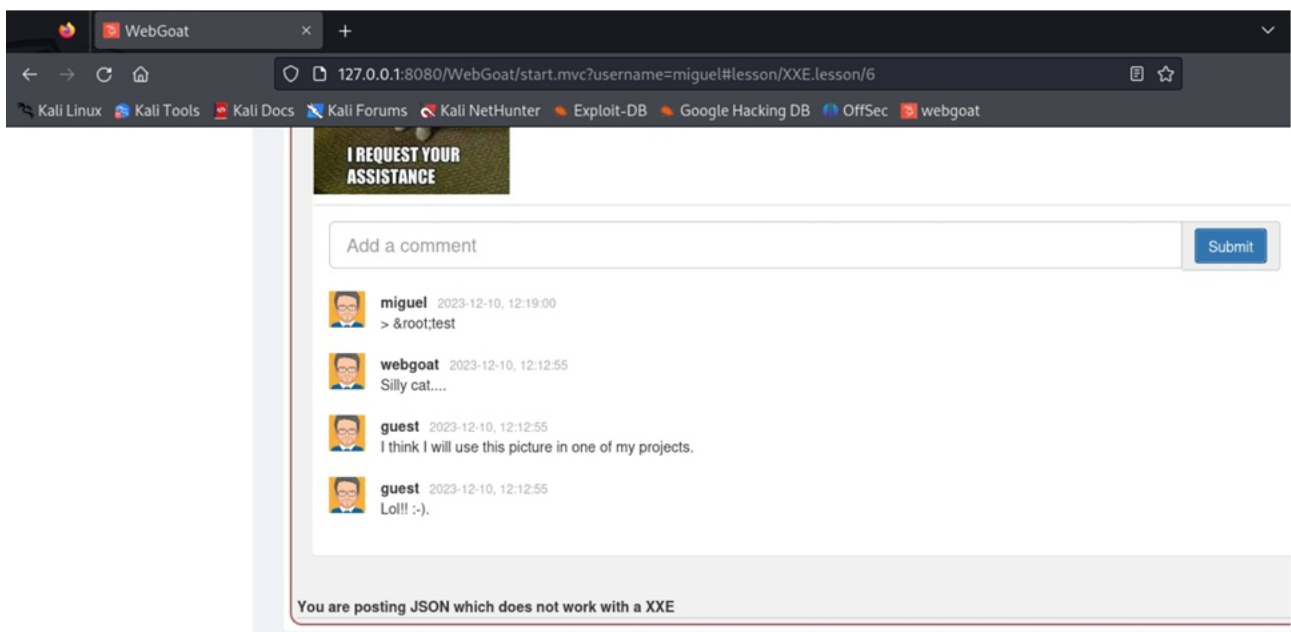
\$1997.96

A5 Security Misconfiguration - Apartado 4

Esta trata de la falta de seguridad adecuada en cualquier parte de la aplicación o permisos configurados incorrectamente:

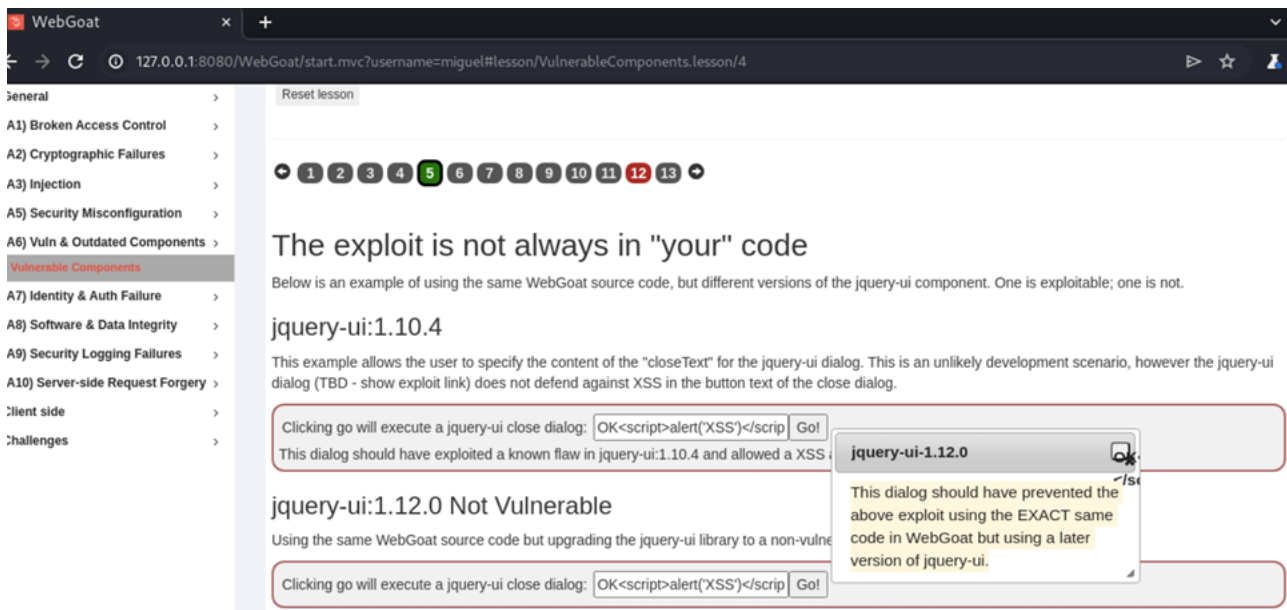


A5 Security Misconfiguration - Apartado 7



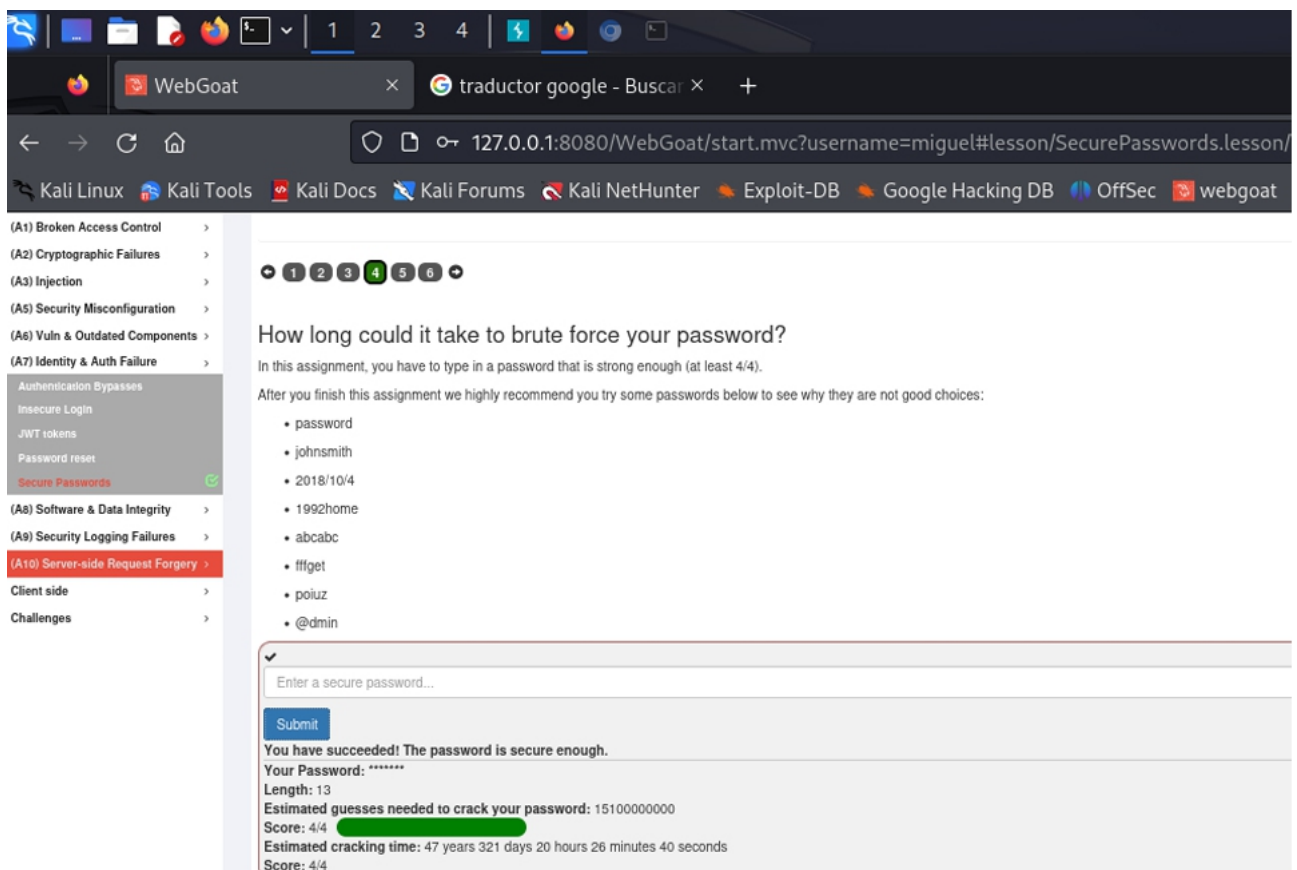
A6 Vuln & outdated Components - Apartado 5

Vulnerabilidad basada en software desactualizado; versiones obsoletas y sin posibilidad de soporte, de tal manera que no puedan ser actualizadas con parches de seguridad:



A7 Identity & Auth Failure - Secure Passwords Apartado 4

Fallos en la parte de autenticación e identificación de la aplicación, ofreciendo un ataque por ejemplo, de fuerza bruta:



3 RESUMEN

Se han encontrado numerosos fallos de seguridad o vulnerabilidades de varios tipos como: inyección SQL, inyección de XSS (código javascript), fallos de software obsoleto o desactualizado sin posibilidad de soporte, fallos de configuración de permisos, así como de autenticación e identificación.

4 POSIBLES SOLUCIONES A LA FALTA DE SEGURIDAD

Se recomienda introducir framework como Spring Security [Spring Security](#) (lenguaje Java) para aumentar la seguridad en la autenticación e identificación de usuarios de la aplicación, ORM 's como Hibernate [Hibernate. Everything data](#) o MyBatis [MyBatis \(github.com\)](#) para el control de las consultas SQL.

También se recomienda revisar la configuración de la aplicación y su actualización.