

WICOS SECURITY

Reporte de seguridad y comprobación de vulnerabilidades, utilizando técnicas y herramientas de *ethical hacking* en la aplicación web Webgoat.

Wicos 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 Wicos Security, y está protegido con derechos de autor *copyright*, está prohibida su copia parcial o totalmente, así como su distribución fuera del ámbito de Wicos Security y de su cliente Omnya, S.A. Contiene información sensible estando prohibida su divulgación por cualquier medio digital o físico.

CLIENTE: Omnya, 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 Kali Linux, utilizando la herramienta Nmap, se han recuperado los siguientes datos sobre puertos, SO y lenguaje utilizado:

Escaneando la IP http://127.0.0.1 con nmap lanza estos resultados:

```
(kali@kali)-[~]  
$ nmap -p- 127.0.0.1  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-06 10:47 EST  
Nmap scan report for localhost (127.0.0.1)  
Host is up (0.00022s latency).  
Not shown: 65532 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
8080/tcp  open  http-proxy  
9090/tcp  open  zeus-admin  
42525/tcp open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 4.46 seconds
```

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

```

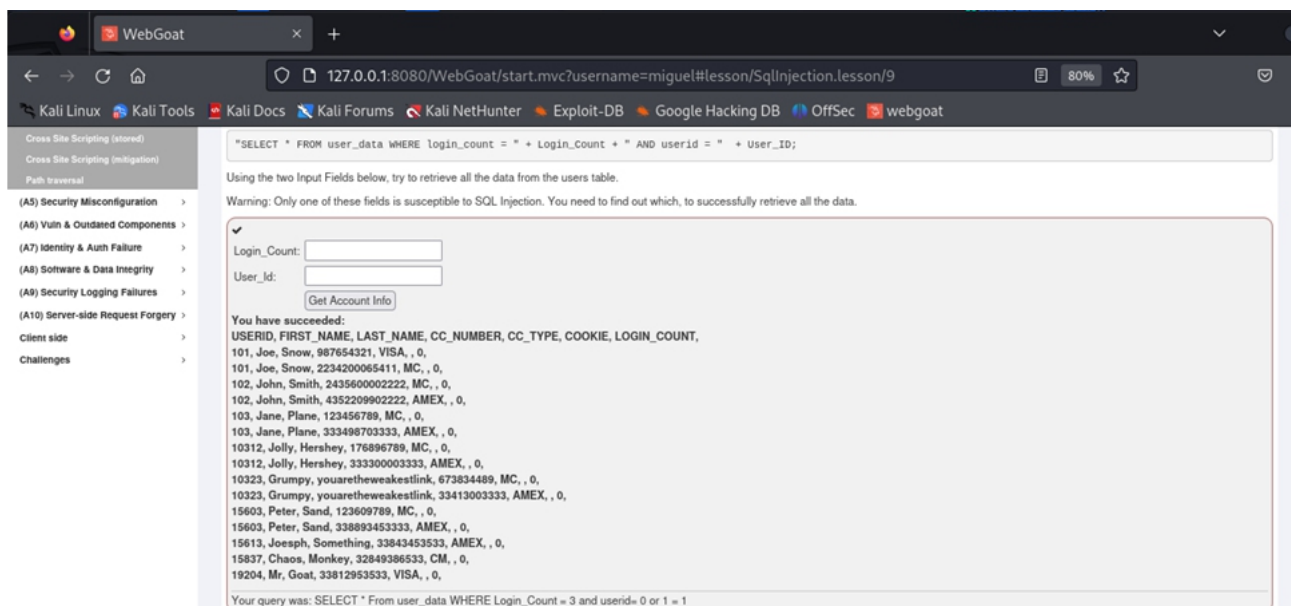
(kali@kali)-[/home/kali]
PS> sudo docker run -it -p 127.0.0.1:8080:8080 -p 127.0.0.1:9090:9090 -e TZ=Europe/Berlin webgoat/webgoat
[sudo] password for kali:
2023-12-07T15:36:32.956+01:00 INFO 1 --- [           main] org.owasp.webgoat.server.StartWebGoat : Starting StartWebGoat v2023.8 using Java 21.0.1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

```

La auditoría ha encontrado las siguientes vulnerabilidades:

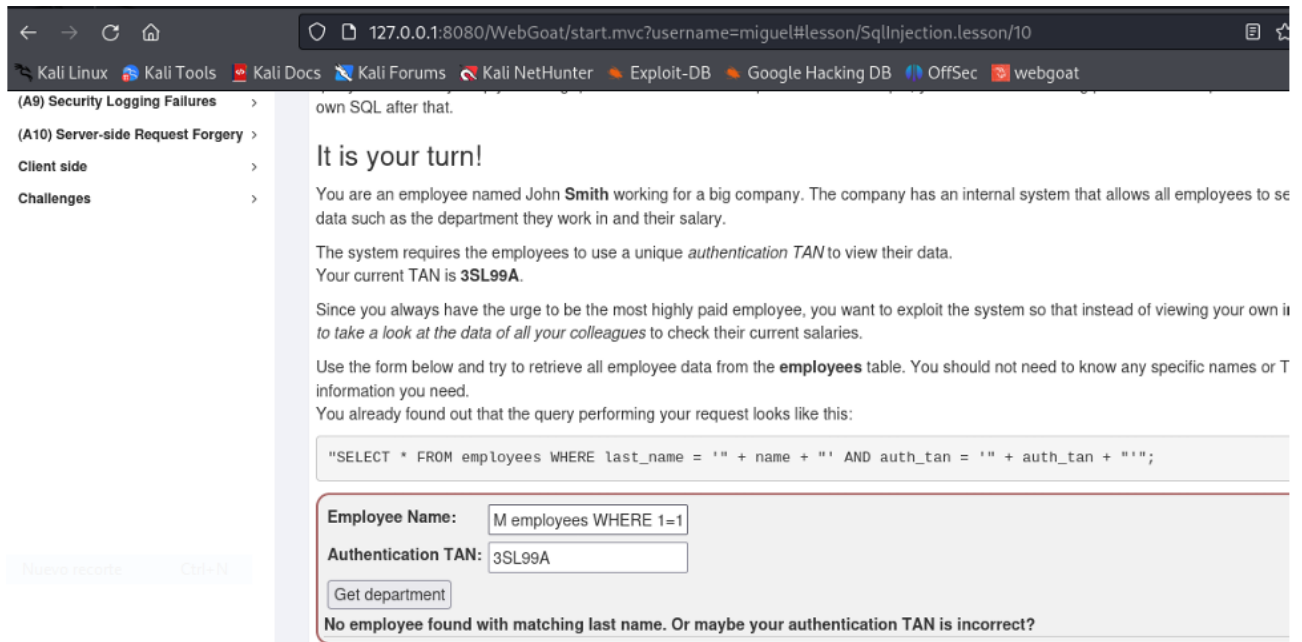
A3 Injection - SQL Injection (intro) - Apartado 10

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

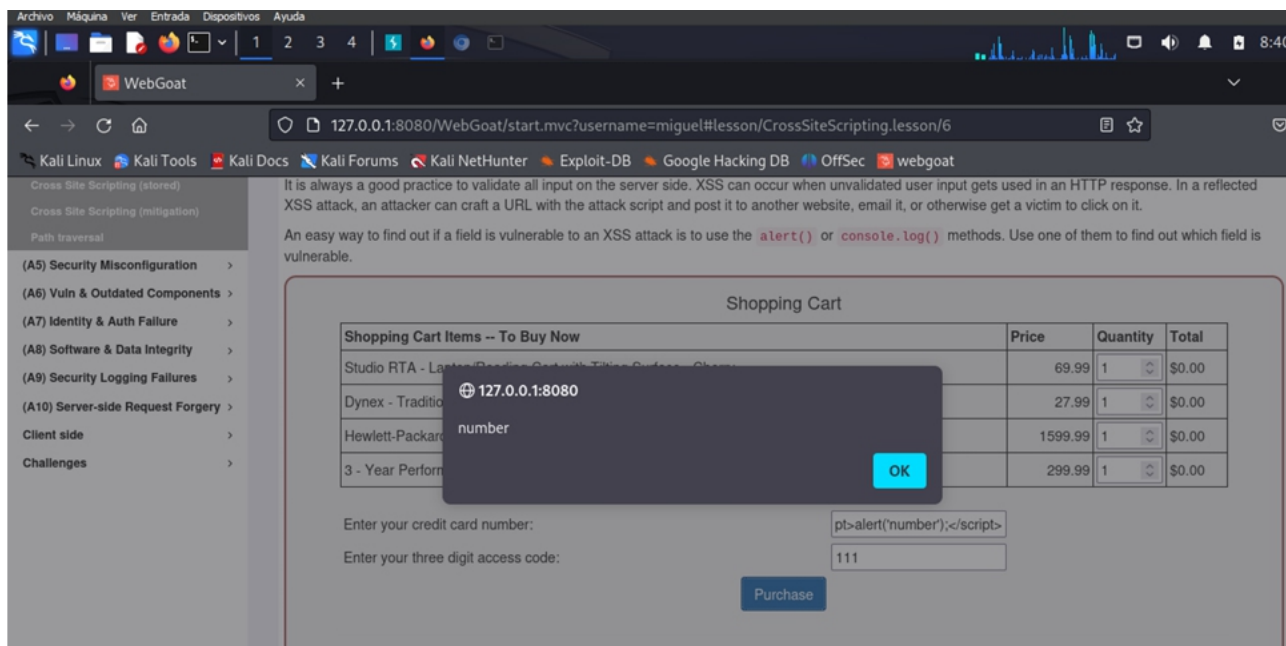
En esta ocasión, mediante el campo Employee Name, podemos obtener información confidencial de usuarios y también podemos descargar la base de datos:



A3 Injection - Cross Site Scripting - Apartado - Apartado 7

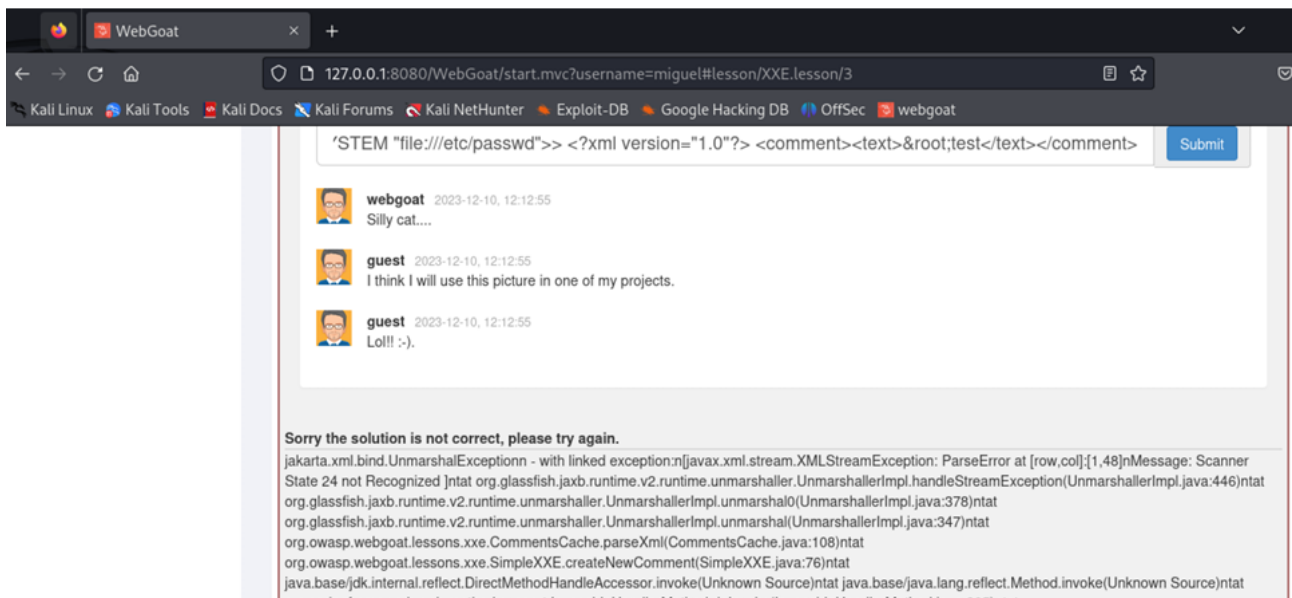
Se ha podido encontrar esta vulnerabilidad, que se basa en la inyección de

código JavaScript en el campo de entrada “Enter your credit card number”:

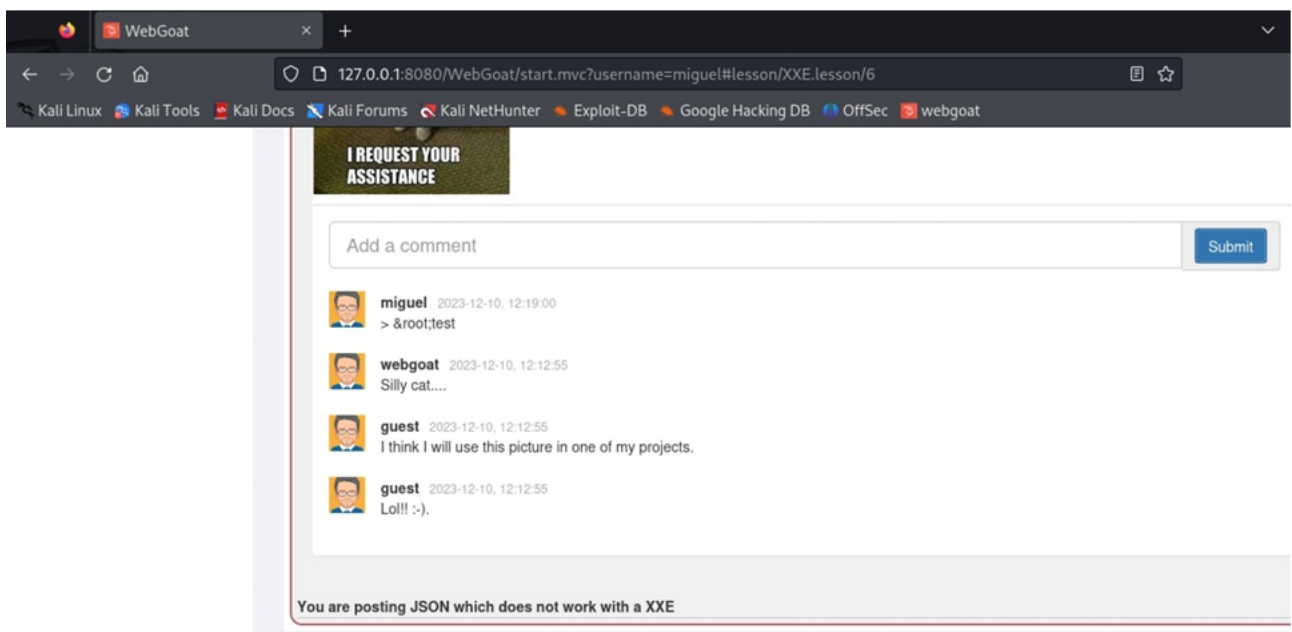


A5 Security Misconfiguration - Apartado 4

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

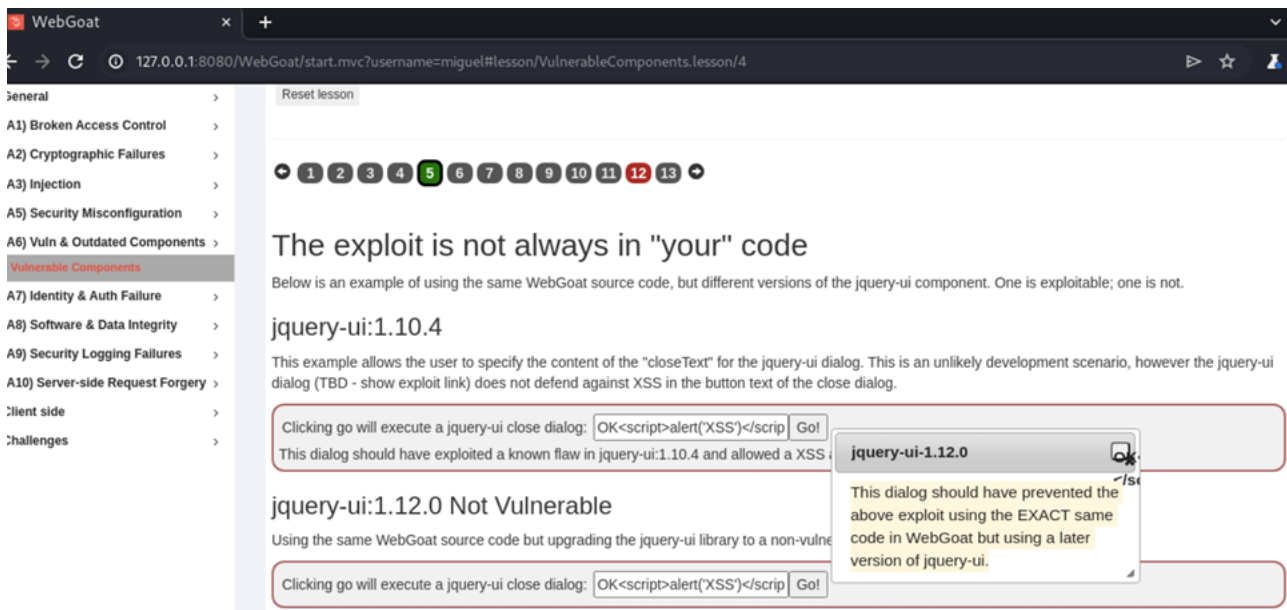


A5 Security Misconfiguration - Apartado 7



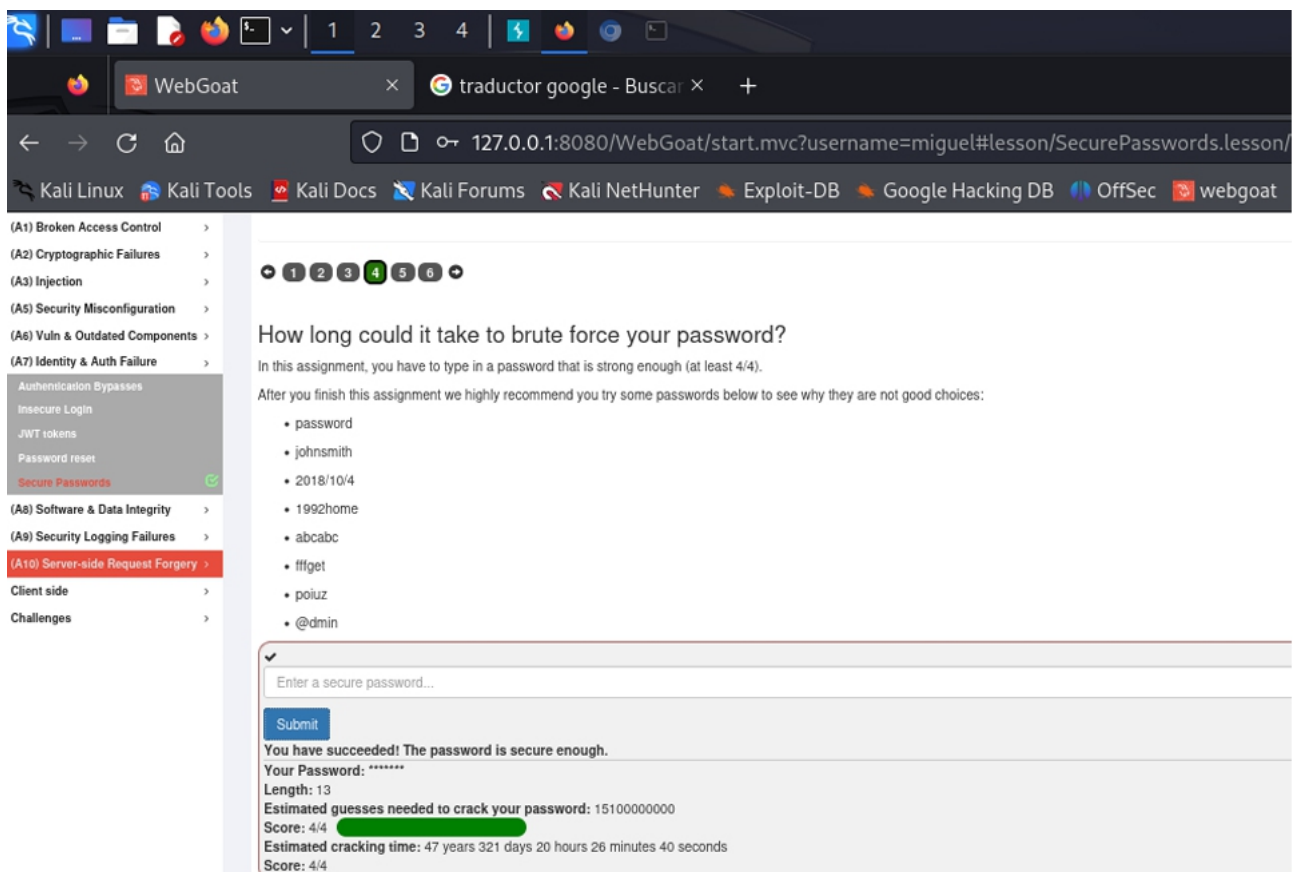
A6 Vuln & outdated Components - Apartado 5

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.