

Desarrollo Seguro de Aplicaciones Web con OWASP

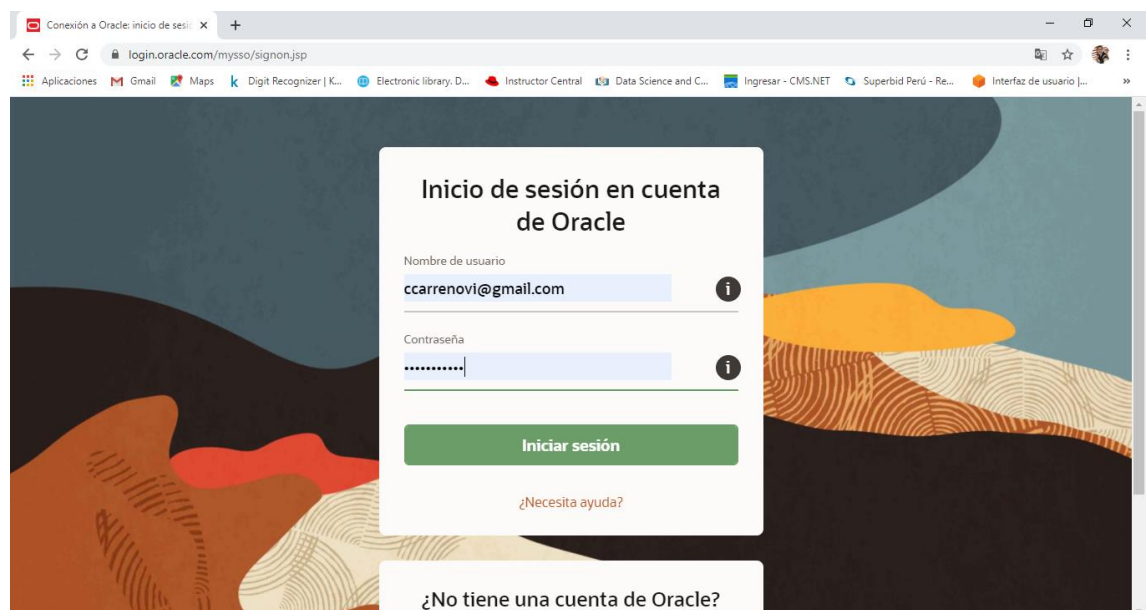
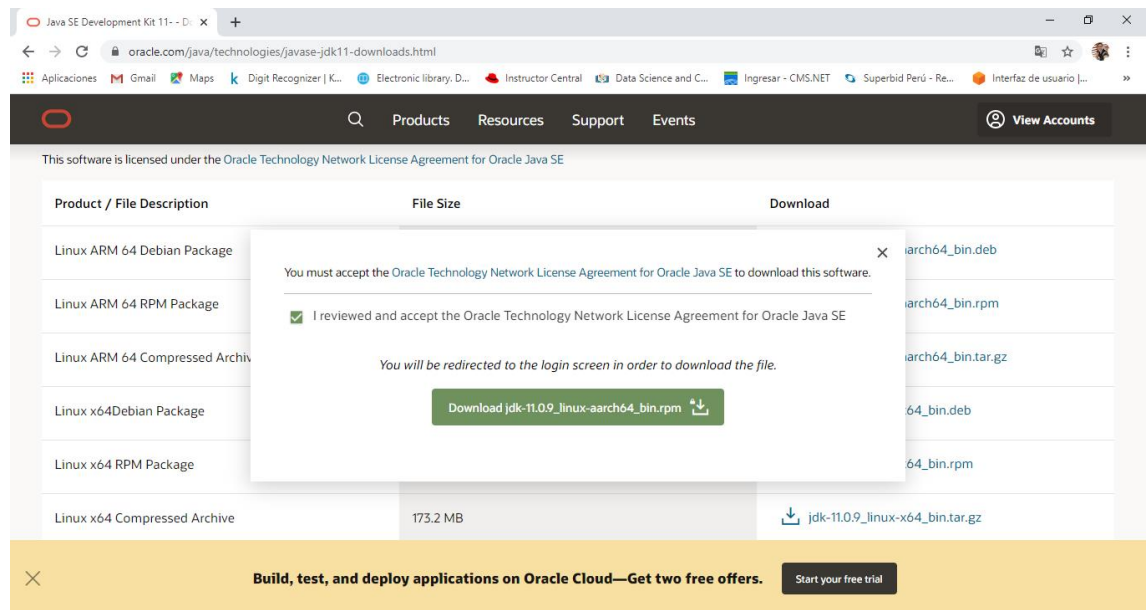
Lab: Authentication Broken

Objetivo

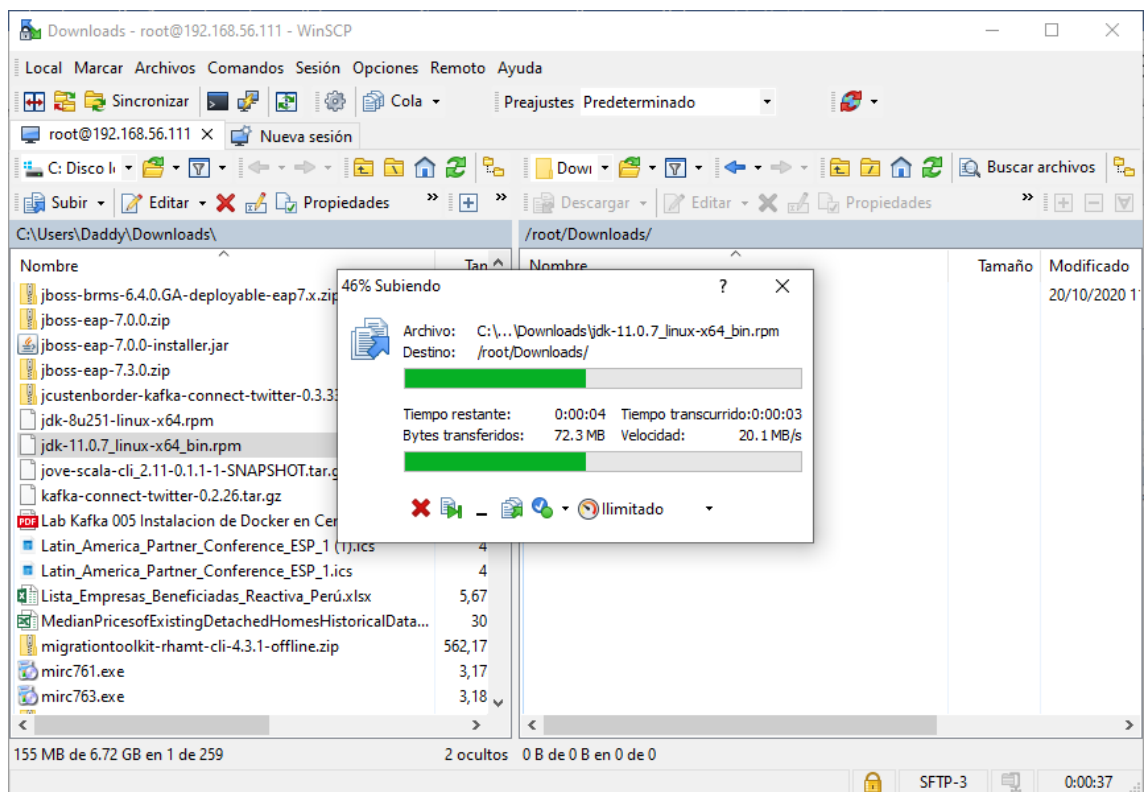
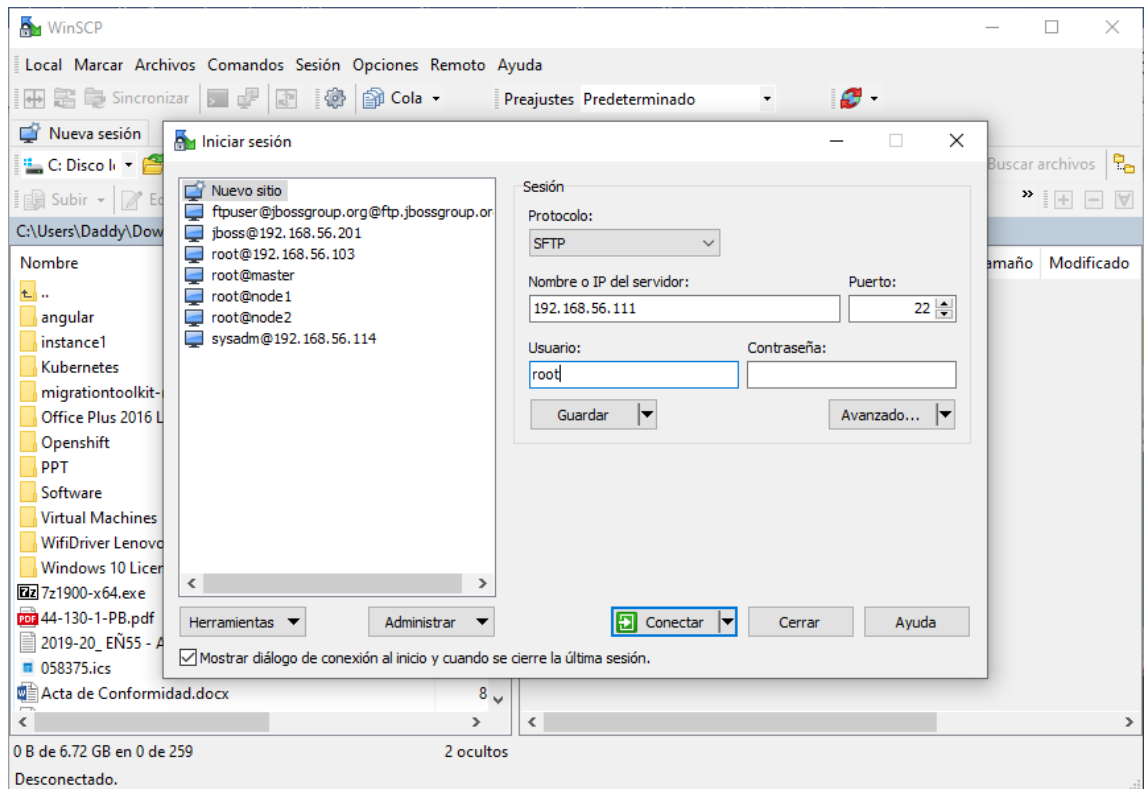
- Revisar el vector de ataque Authentication Bypass

Procedimiento

1. Instalar Java 11 en Centos 7



Copia el archivo **jdk-11.0.7_linux-x64_bin.rpm** a la máquina virtual con Centos 7 usando WinSCP



Instala el rpm

```
root@buggy:~/Downloads
[root@buggy Downloads]# pwd
/root/Downloads
[root@buggy Downloads]# ls
jdk-11.0.7_linux-x64_bin.rpm
[root@buggy Downloads]# rpm -ivh jdk-11.0.7_linux-x64_bin.rpm
warning: jdk-11.0.7_linux-x64_bin.rpm: Header V3 RSA/SHA256 Signature, key ID ec
551f03: NOKEY
Preparing... ##### [100%]
Updating / installing...
 1:jdk-11.0.7-2000:11.0.7-ga ##### [100%]
[root@buggy Downloads]#
```

Usa alternatives para configura ha java 11 por defecto para el sistema.

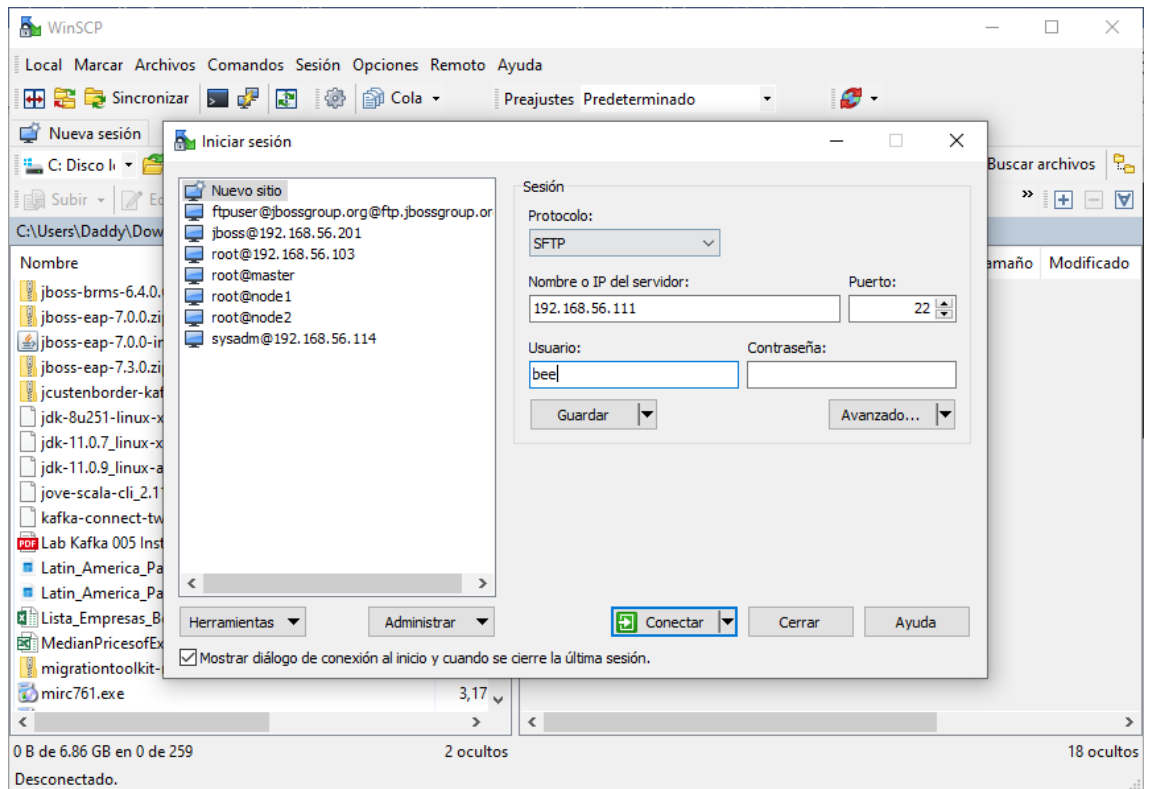
```
root@buggy:~/Downloads
Updating / installing...
 1:jdk-11.0.7-2000:11.0.7-ga ##### [100%]
[root@buggy Downloads]# alternatives --config java

There are 2 programs which provide 'java'.

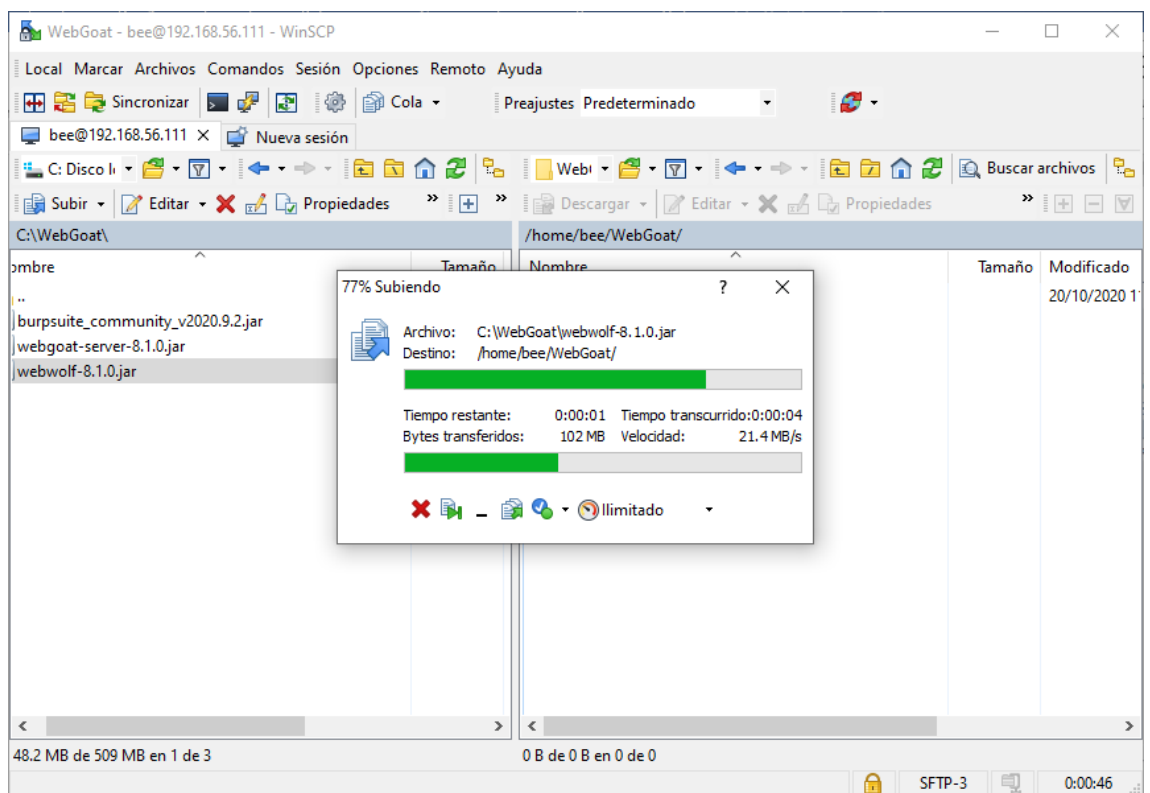
   Selection    Command
-----
      1          java-1.8.0-openjdk.x86_64 (/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.161-2.b14
.el7.x86_64/jre/bin/java)
*+ 2            /usr/java/jdk-11.0.7/bin/java

Enter to keep the current selection[+], or type selection number: 2
[root@buggy Downloads]# java -version
java version "11.0.7" 2020-04-14 LTS
Java(TM) SE Runtime Environment 18.9 (build 11.0.7+8-LTS)
Java HotSpot(TM) 64-Bit Server VM 18.9 (build 11.0.7+8-LTS, mixed mode)
[root@buggy Downloads]#
```

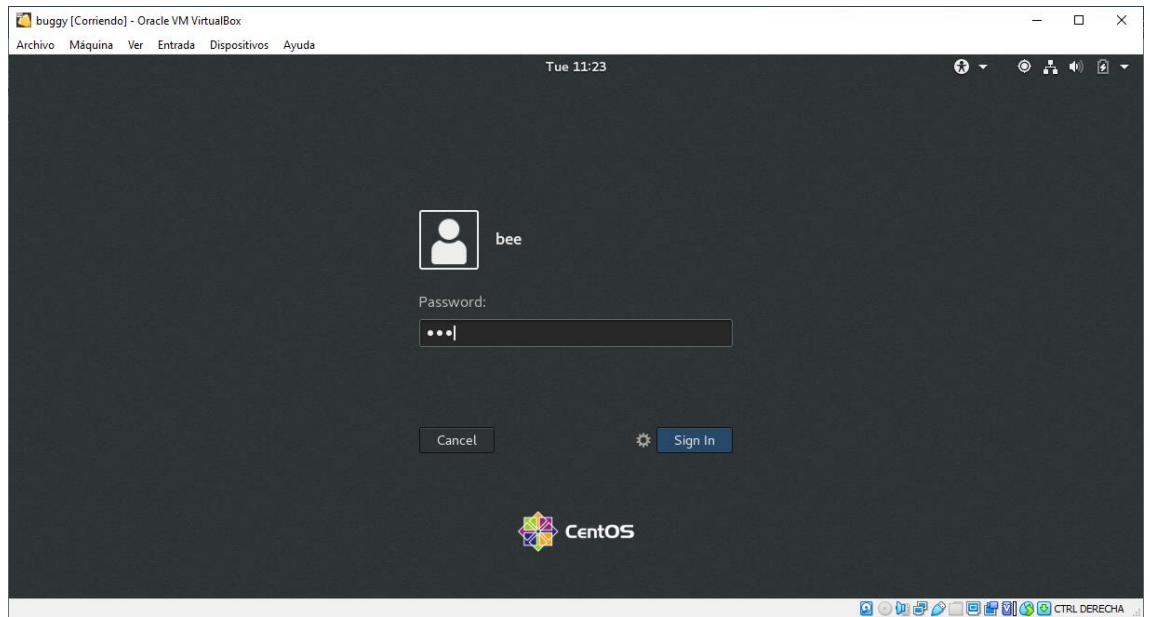
2. Ingresa con bee y copia los archivos *.jar de las aplicaciones WebGoat y WebWolf



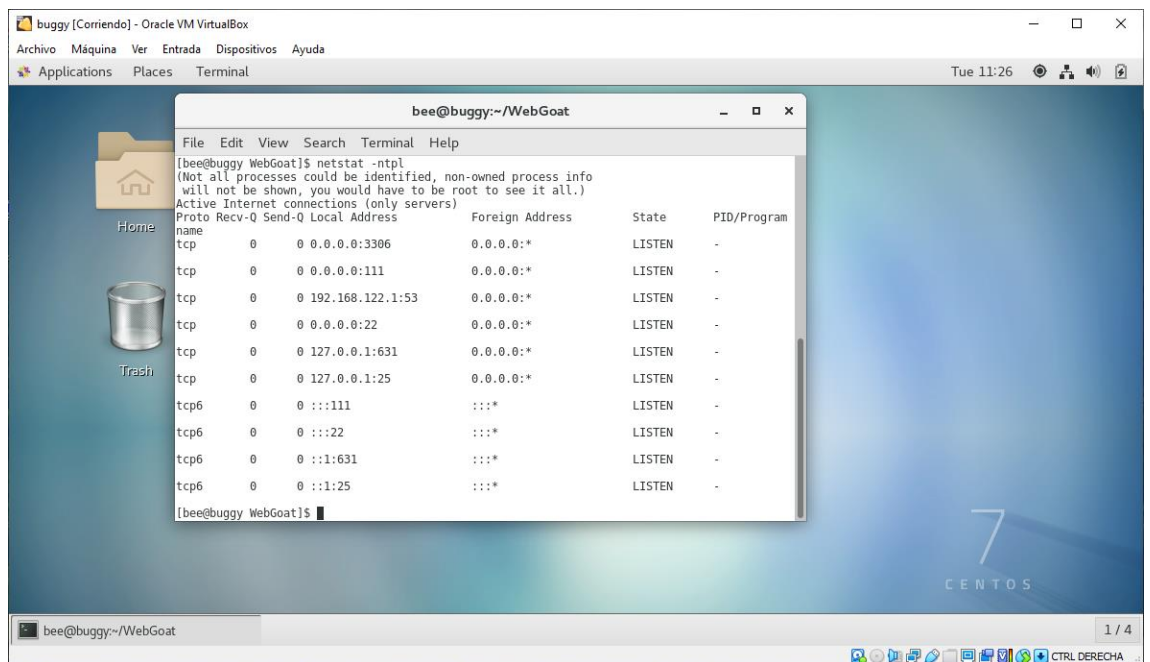
Copia los archivos WebGoat



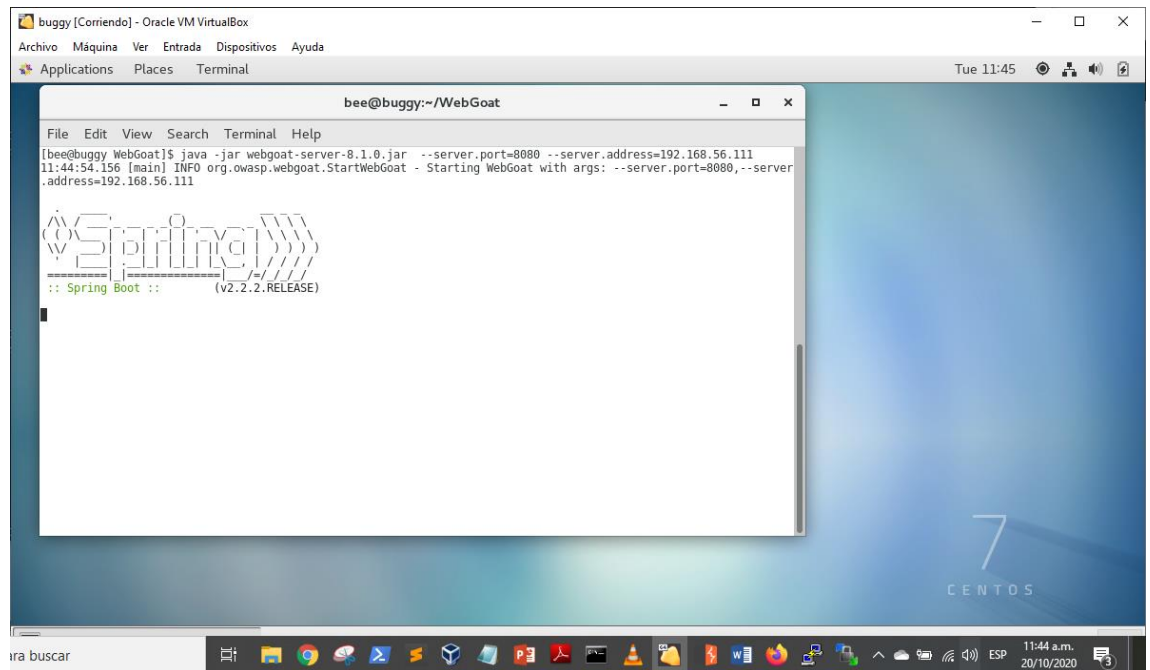
3. Ingresa con el usuario bee clave box a la maquina virtual



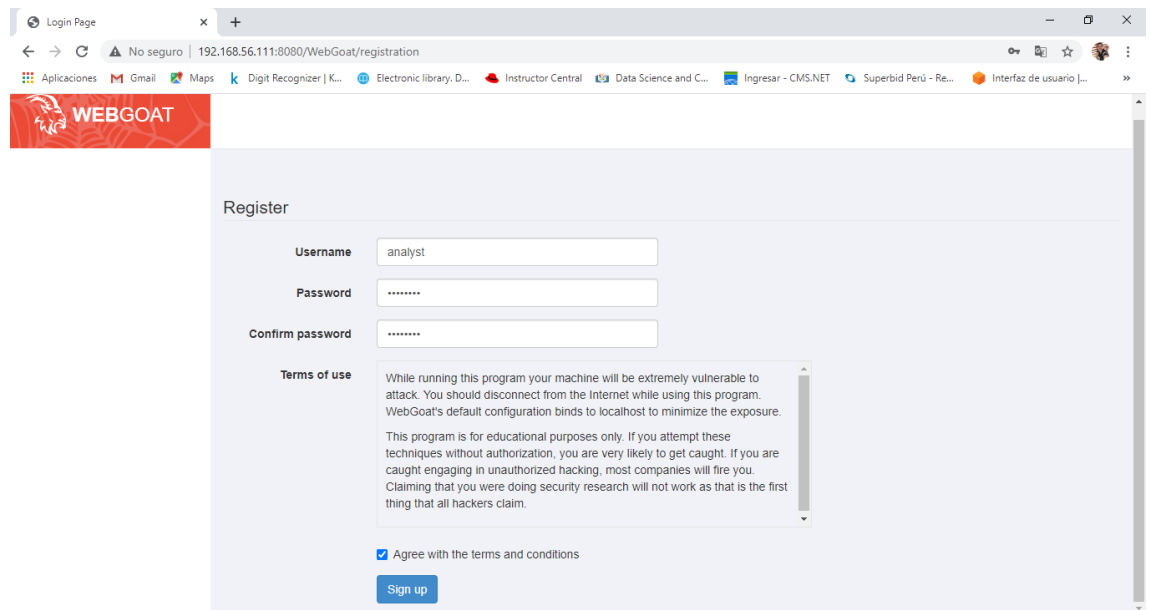
Abre un terminal y verifica que el puerto 8080 este libre



4. Inicia WebGoat



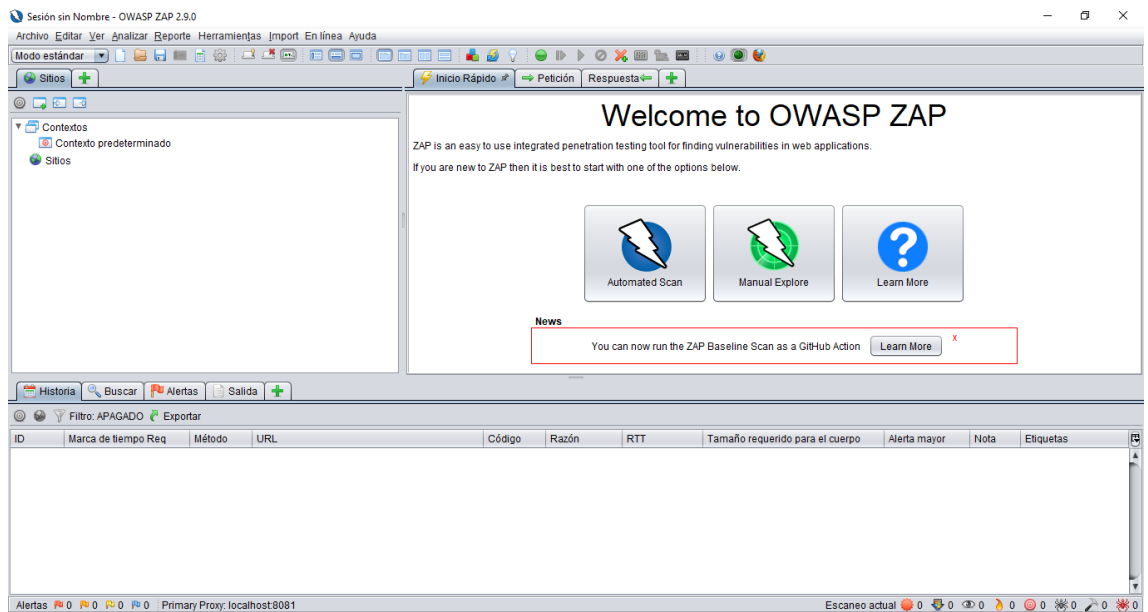
5. Crea el usuario **analyst** con clave **password** en la aplicación WebGoat



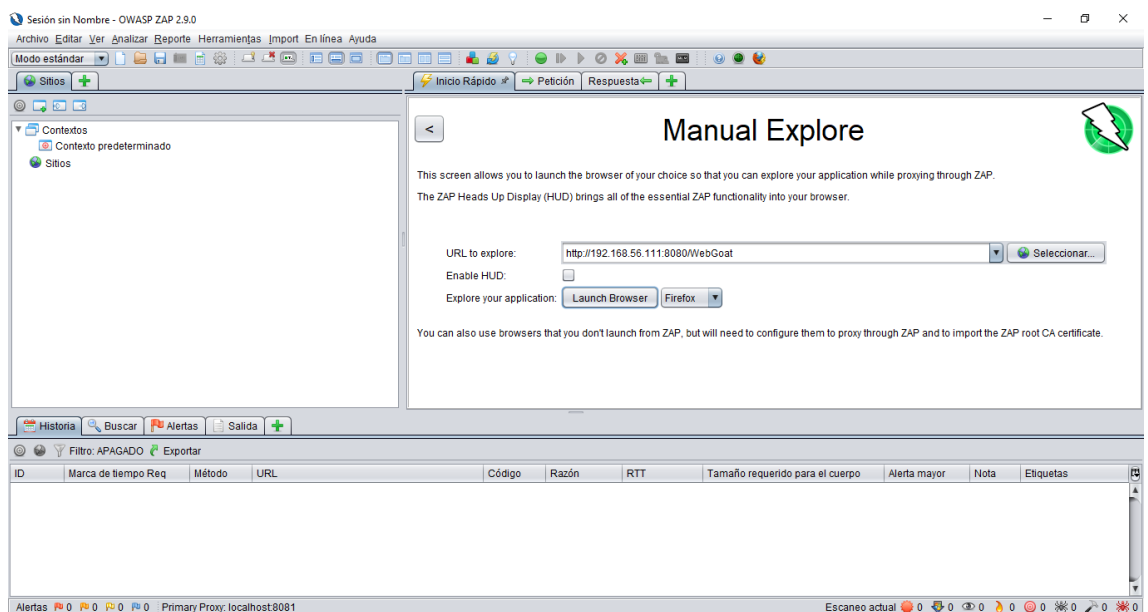
6. Verifica que los puertos este ocupados por las aplicaciones.

```
root@buggy:~/Downloads
[root@buggy Downloads]# netstat -ntpl
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      1317/mysqld
tcp        0      0 0.0.0.0:1111           0.0.0.0:*               LISTEN      691/rpcbind
tcp        0      0 192.168.122.1:53       0.0.0.0:*               LISTEN      1664/dnsmasq
tcp        0      0 0.0.0.0:22             0.0.0.0:*               LISTEN      1049/sshd
tcp        0      0 127.0.0.1:631          0.0.0.0:*               LISTEN      1053/cupsd
tcp        0      0 127.0.0.1:25           0.0.0.0:*               LISTEN      1382/master
tcp6       0      0 192.168.56.111:9001    :::*                   LISTEN      7668/java
tcp6       0      0 :::1111                :::*                   LISTEN      691/rpcbind
tcp6       0      0 192.168.56.111:8080    :::*                   LISTEN      7668/java
tcp6       0      0 :::22                  :::*                   LISTEN      1049/sshd
tcp6       0      0 :::1631                :::*                   LISTEN      1053/cupsd
tcp6       0      0 :::125                 :::*                   LISTEN      1382/master
[root@buggy Downloads]#
```

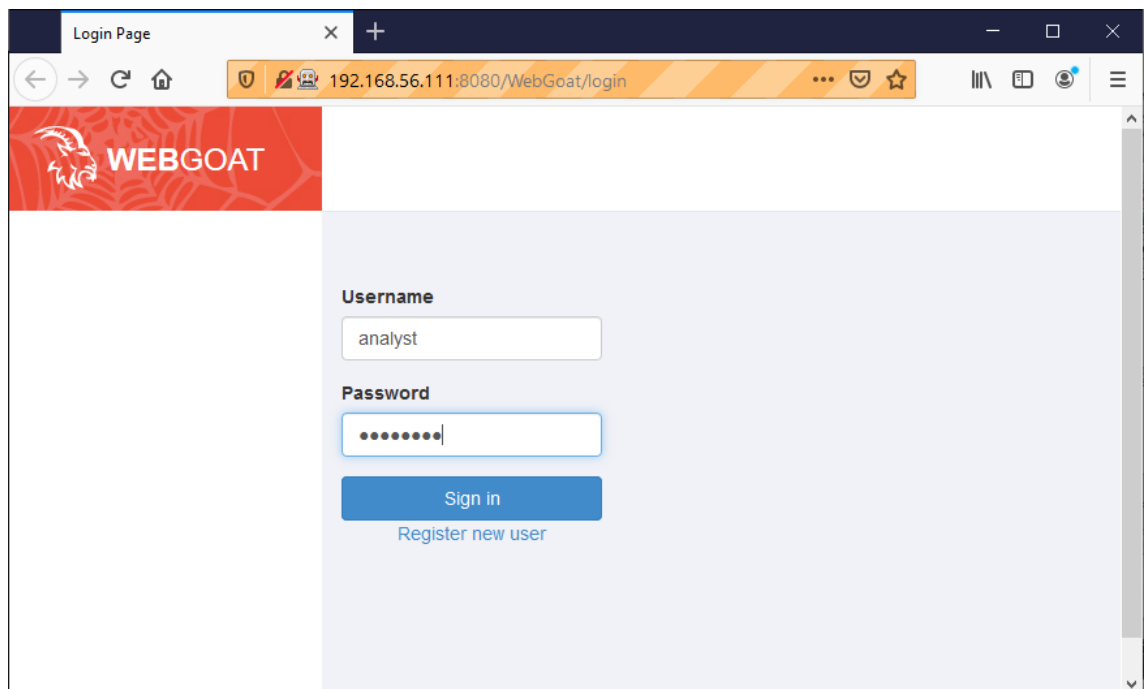
7. Instala OWASP Zap e inicialó.



8. Haz una exploración manual de la url <http://192.168.56.111:8080/WebGoat>



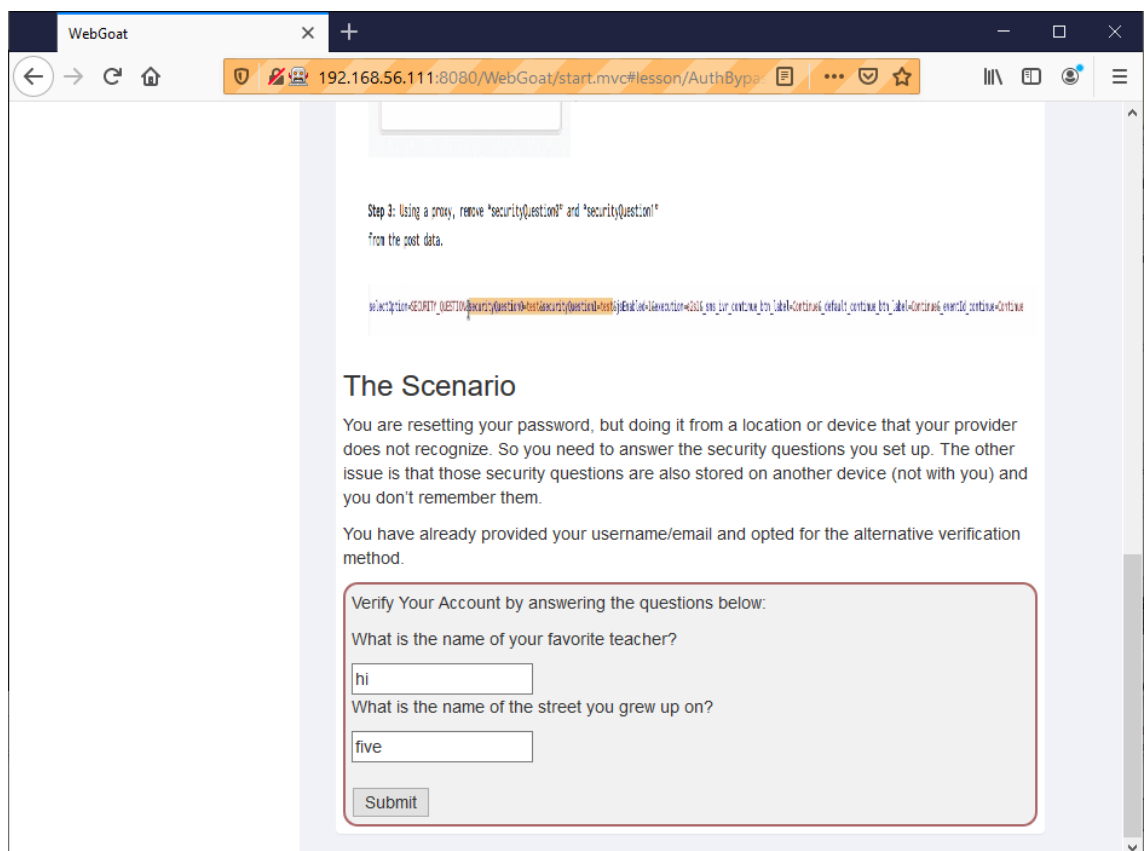
Haz clic en Launch Browser. Inicia sesión con el usuario analyst



The screenshot shows a web browser window with the title "Login Page". The address bar displays "192.168.56.111:8080/WebGoat/login". The page features the WebGoat logo on the left. On the right, there is a login form with the following elements:

- Username:** A text input field containing the text "analyst".
- Password:** A password input field with masked characters (dots).
- Sign in:** A blue button.
- Register new user:** A link below the "Sign in" button.

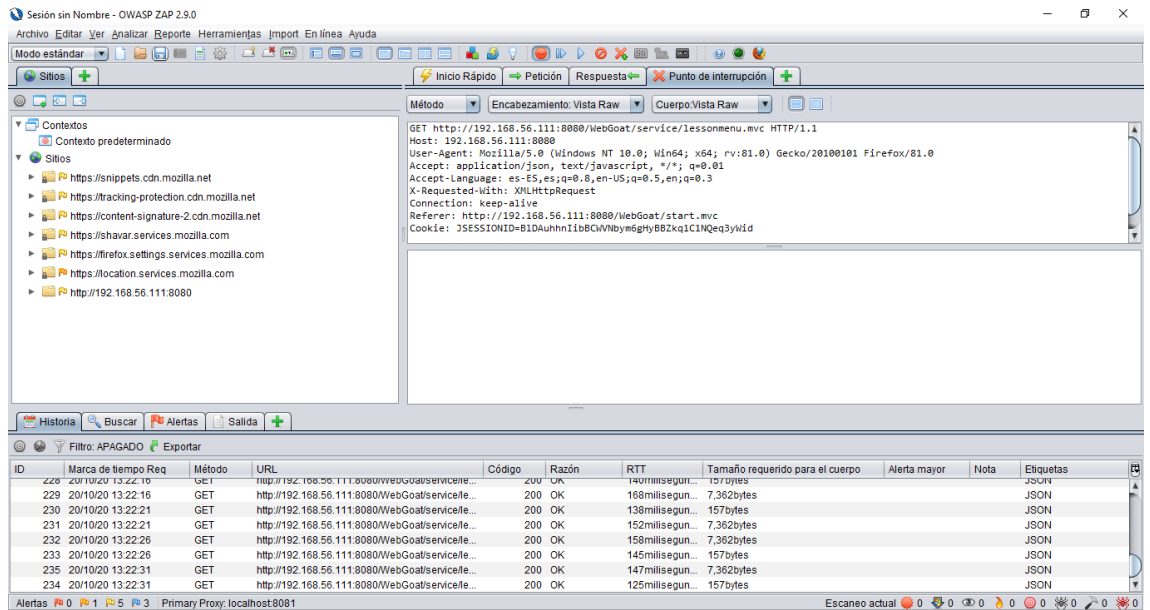
Dirigite a la sesión de Authentication Bypasses



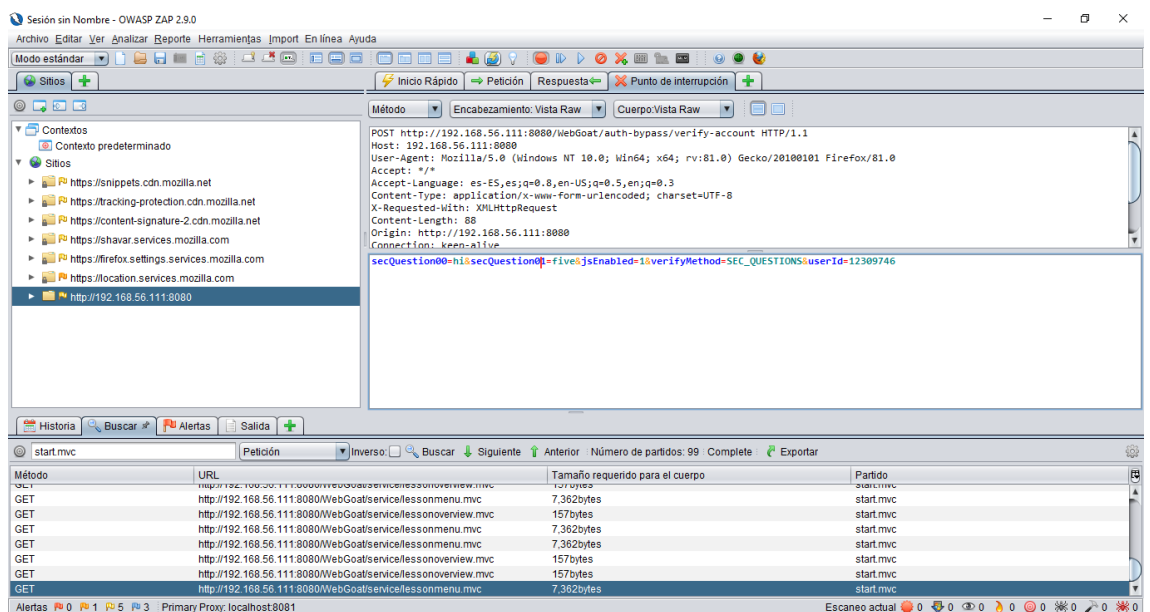
The screenshot shows a web browser window with the title "WebGoat". The address bar displays "192.168.56.111:8080/WebGoat/start.mvc#lesson/AuthBypa". The page content includes:

- Step 3:** Using a proxy, remove "securityQuestion?" and "securityQuestion" from the post data.
- The Scenario:** A text block explaining a password reset scenario where security questions are stored on a different device.
- Verify Your Account:** A section with the instruction "Verify Your Account by answering the questions below:" and two questions:
 - "What is the name of your favorite teacher?" with an input field containing "hi".
 - "What is the name of the street you grew up on?" with an input field containing "five".
- Submit:** A button at the bottom of the verification section.

Antes hacer clic en **Submit**, agrega una interrupción.



Ejecuta un step y captura el cuerpo de la petición en OWASP Zap



Modifica el cuerpo original a:

secQuestion00=hi&secQuestion01=five&jsEnabled=1&verifyMethod=SEC Questions&userId=12309746

- Ejecuta un step en OWASP Zap y verifica que en la sesión en Firefox la Autenticacion es exitosa.

