

Ataques sobre una aplicación Web

Objetivos

Esta práctica le va a permitir conocer cómo se realizan algunos de los ataques más habituales sobre aplicaciones Web, para poner en práctica lo aprendido durante el curso y entender mejor cómo se deben desarrollar aplicaciones Web para evitar estos ataques.

1. Introducción

WebGoat es una aplicación web JavaEE deliberadamente insegura, mantenida por OWASP y diseñada para enseñar lecciones de seguridad en aplicaciones Web. En cada lección, los usuarios deben demostrar su entendimiento de los problemas de seguridad al explotar la vulnerabilidad real en la aplicación *WebGoat*. Por ejemplo, en una de las lecciones el usuario debe usar SQL injection para robar números de tarjeta de crédito ficticios. La aplicación es un ambiente realista de enseñanza, que proporciona a los usuarios pistas y código para explicar mejor la lección.

La seguridad en aplicaciones Web es difícil de aprender y poner en práctica. No mucha gente desarrolla aplicaciones Web completas, como tiendas electrónicas de libros o bancos en línea, que pueden ser usados para buscar vulnerabilidades. Además, los profesionales de seguridad frecuentemente necesitan probar herramientas contra una plataforma conocida por ser vulnerable para asegurarse que se desempeñan según se anuncian. Todo esto debe ocurrir en un ambiente seguro y legal. Incluso si sus intenciones son buenas, creemos que no debe intentar buscar vulnerabilidades sin permiso.

WebGoat está escrito en Java y por lo tanto se instala en cualquier plataforma con una máquina virtual de Java. Una vez instalado, el usuario puede revisar las lecciones y rastrear su progreso con el tablero electrónico.

Actualmente hay más de 30 lecciones, incluyendo las que lidian con los siguientes problemas:

- Secuencia de Comandos en Sitios Cruzados (Cross Site Scripting - XSS)
- Control de acceso
- Seguridad de hilos
- Manipulación de campos ocultos

- Manipulación de parámetros
- Testigos de sesión inseguros
- Inyección SQL
- Inyección de SQL con números
- Inyección de SQL con cadenas de caracteres
- Servicios Web
- Autenticación fallida
- Los peligros de los comentarios HTML

2. Instalación

1. Para instalar WebGoat, necesita tener instalada previamente en su máquina J2RE o cualquier otra versión de la Máquina Virtual Java o JDK, que puede encontrar en:

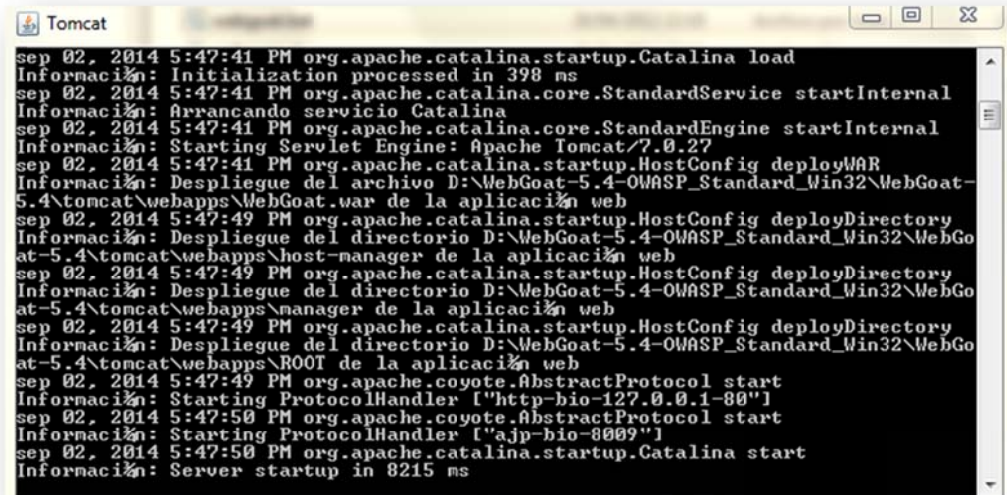
<http://www.oracle.com/technetwork/java/javase/downloads/index-isp-138363.html>

2. A continuación debe descargar WebGoat 5.4 desde:
http://code.google.com/p/webgoat/downloads/detail?name=WebGoat-5.4-OWASP_Standard_Win32.zip

3. Descomprimir la carpeta donde lo prefiera. Por ejemplo, en C:\

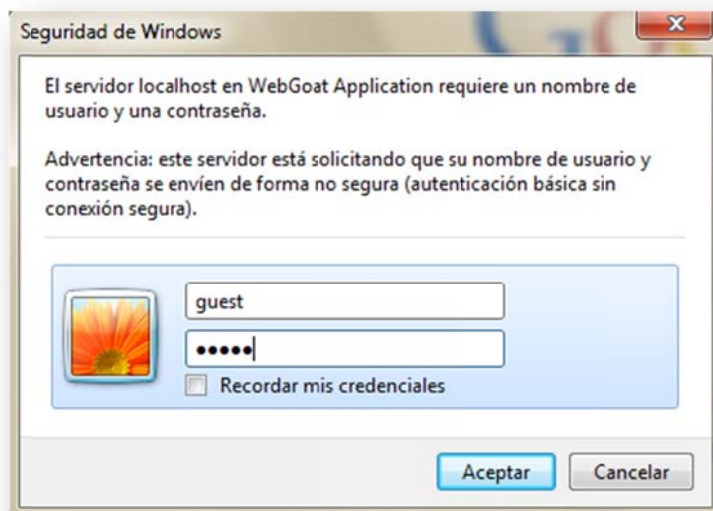
Con esto, en realidad ya está instalado. Lo único que le queda es ejecutarlo para poder empezar la práctica.

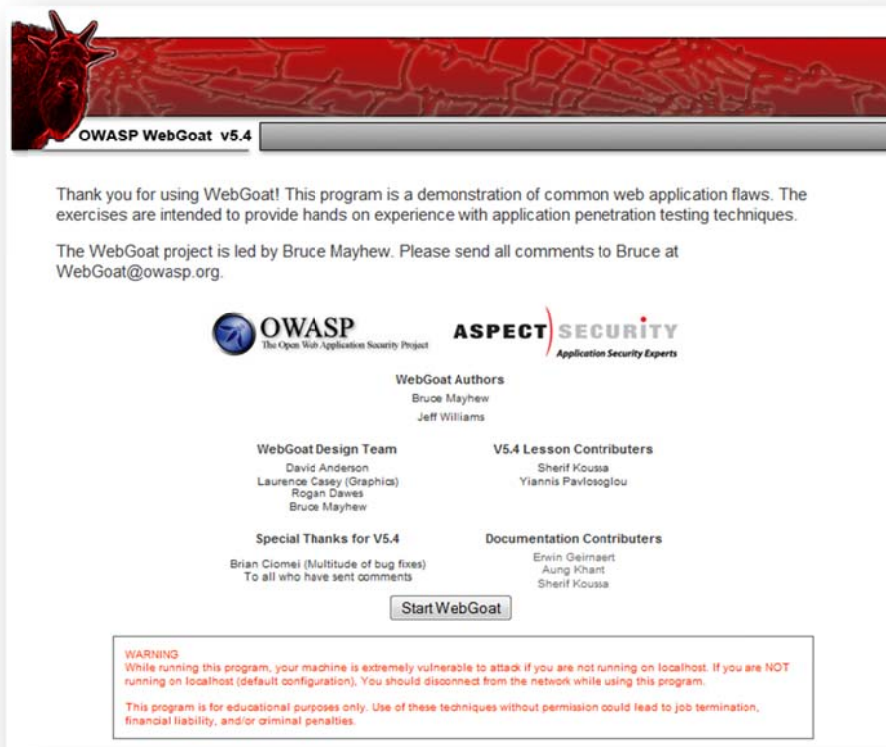
- a. Ejecutar el archivo **webgoat.bat** contenido dentro de la carpeta.
 - Si lo prefiere, puede ejecutar **webgoat_8080.bat**, para levantar el servicio del Tomcat que lleva integrado en el puerto 8080, pero tenga en cuenta que, a partir de ese momento todo lo demás deberá hacerlo con el puerto 8080. Utilice esta opción, sólo si en la máquina donde lo va a ejecutar ya tiene otro servidor web levantado en el puerto predeterminado (80) y pudieran colisionar.



```
Tomcat
sep 02, 2014 5:47:41 PM org.apache.catalina.startup.Catalina load
Información: Initialization processed in 398 ms
sep 02, 2014 5:47:41 PM org.apache.catalina.core.StandardService startInternal
Información: Arrancando servicio Catalina
sep 02, 2014 5:47:41 PM org.apache.catalina.core.StandardEngine startInternal
Información: Starting Servlet Engine: Apache Tomcat/7.0.27
sep 02, 2014 5:47:41 PM org.apache.catalina.startup.HostConfig deployWAR
Información: Despliegue del archivo D:\WebGoat-5.4-OWASP_Standard_Win32\WebGoat-5.4\tomcat\webapps\WebGoat.war de la aplicación web
sep 02, 2014 5:47:49 PM org.apache.catalina.startup.HostConfig deployDirectory
Información: Despliegue del directorio D:\WebGoat-5.4-OWASP_Standard_Win32\WebGoat-5.4\tomcat\webapps\host-manager de la aplicación web
sep 02, 2014 5:47:49 PM org.apache.catalina.startup.HostConfig deployDirectory
Información: Despliegue del directorio D:\WebGoat-5.4-OWASP_Standard_Win32\WebGoat-5.4\tomcat\webapps\manager de la aplicación web
sep 02, 2014 5:47:49 PM org.apache.catalina.startup.HostConfig deployDirectory
Información: Despliegue del directorio D:\WebGoat-5.4-OWASP_Standard_Win32\WebGoat-5.4\tomcat\webapps\ROOT de la aplicación web
sep 02, 2014 5:47:49 PM org.apache.coyote.AbstractProtocol start
Información: Starting ProtocolHandler ["http-bio-127.0.0.1-80"]
sep 02, 2014 5:47:50 PM org.apache.coyote.AbstractProtocol start
Información: Starting ProtocolHandler ["ajp-bio-8009"]
sep 02, 2014 5:47:50 PM org.apache.catalina.startup.Catalina start
Información: Server startup in 8215 ms
```

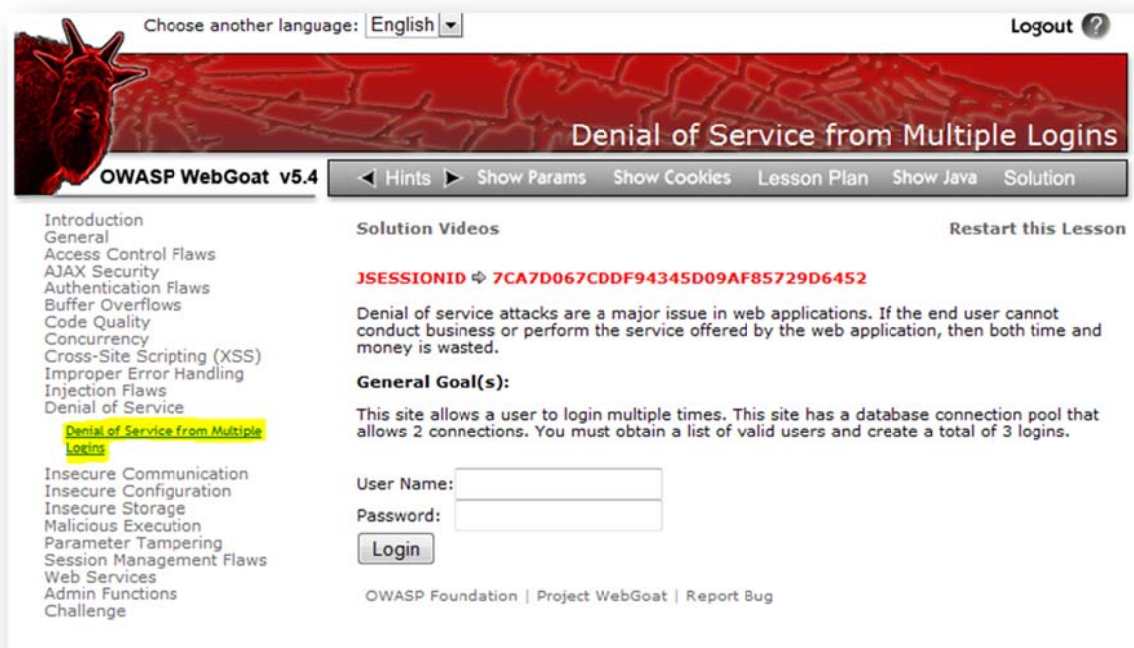
- b. Abrir un navegador web y escribir: <http://localhost/WebGoat/attack>
 - Si hubiera levantado el servicio del Tomcat en el puerto 8080, recuerde que ahora la URL será:
<http://8080/localhost/WebGoat/attack>
- c. Cuando le pida nombre de usuario y contraseña:
 - Usuario: **guest**
 - Contraseña: **guest**





3. Desarrollo

La práctica consiste en elegir una de todas las lecciones que propone WebGoat y llevarla a cabo.



Para ayudarse, tenga en cuenta que la herramienta le proporciona pistas (Hints), que le pueden ayudar a llevar a buen puerto el ataque. En última instancia, puede utilizar la última opción que le permite ver la solución, pero tenga en cuenta que ahí le cuentan cómo se hace, pero la práctica consiste en ponerlo en práctica y explicar en detalle cómo lo llevó a la práctica y qué efecto produjo.

El entregable será un documento explicativo en PDF con la extensión que considere necesaria (sin límite) donde indique qué realizó para conseguir que el ataque fuera fructífero, escribiendo todos los pasos que haya llevado a cabo y todos los detalles de cómo lo llevó a cabo. Y por último qué efecto produjo sobre la aplicación.