

Web Security Activity: Part 1 (Lab Setup)

Description:

WebGoat is a deliberately insecure web application maintained by [OWASP](#) and it is designed to teach web application security lessons. This program is a demonstration of common server-side application flaws. The WebGoat exercises are intended to be used by people to learn about application security and penetration testing techniques.

*WARNING 1: While running this program your machine will be **extremely vulnerable to attack**. You **should disconnect from the Internet** while using this program. WebGoat's default configuration binds to localhost to minimize the exposure.*

WARNING 2: This program is for educational purposes only. If you attempt these techniques without authorization, you are very likely to get caught. If you are caught engaging in unauthorized hacking, most companies will fire you. Claiming that you were doing security research will not work as that is the first thing that all hackers claim.

Prerequisite: Java 11 and above

To check whether java is installed or not:

Open terminal/Command Prompt→ type “`java -version`”→ You will see the java version.

If you do not have Java 11, download it from this site:

<https://www.oracle.com/technetwork/java/javase/downloads/jdk11-downloads-5066655.html>

Lab Setup

1. Navigate to the following link and download ‘**webgoat-server-8.0.0.M25.jar**’
<https://github.com/WebGoat/WebGoat/releases>

Do not download the M26 version.

2. In a Terminal/Command Prompt window, navigate to the directory where you saved the above JAR file:
You can use `cd file_path/file_name` to navigate to the location of file (generally the downloaded file goes into download folder but you can place it in the desired location).
Hint: type the command: ‘`cd Downloads`’
3. Now execute the following command:

Web-Based Application Design and Development (ITIS 3135)

```
java -jar webgoat-server-8.0.0.VERSION.jar
```

The “VERSION” should be replaced with the correct version name (M25)->

Example: `java -jar webgoat-server-8.0.0.M25.jar`

It should take 10-20 seconds for the server to be up and running.

```
C:\Windows\System32\cmd.exe - java -jar webgoat-server-8.0.0.M25.jar
lic java.lang.Object org.springframework.boot.actuate.endpoint.mvc.EndpointMvcAdapter.invoke()
2019-09-24 10:27:13.429 INFO 19648 --- [main] o.s.b.a.e.mvc.EndpointHandlerMapping : Mapped "[[/{autoconf
ig || /autoconfig.json}],methods=[GET],produces=[application/vnd.spring-boot.actuator.v1+json || application/json]]" onto
public java.lang.Object org.springframework.boot.actuate.endpoint.mvc.EndpointMvcAdapter.invoke()
2019-09-24 10:27:13.430 INFO 19648 --- [main] o.s.s.web.DefaultSecurityFilterChain : Creating filter cha
in: org.springframework.boot.actuate.autoconfigure.ManagementWebSecurityAutoConfiguration$LazyEndpointPathRequestMatcher
@519eable, [org.springframework.security.web.context.request.async.WebAsyncManagerIntegrationFilter@7d2a4598, org.spring
framework.security.web.context.SecurityContextPersistenceFilter@5fa9971f, org.springframework.security.web.header.Header
WriterFilter@64df8422, org.springframework.web.filter.CorsFilter@65880400, org.springframework.security.web.authenticati
on.logout.LogoutFilter@556944cd, org.springframework.security.web.authentication.www.BasicAuthenticationFilter@40071890,
org.springframework.security.web.savedrequest.RequestCacheAwareFilter@70a24463, org.springframework.security.web.servle
tapi.SecurityContextHolderAwareRequestFilter@684430c1, org.springframework.security.web.authentication.AnonymousAuthenti
cationFilter@415419a4, org.springframework.security.web.session.SessionManagementFilter@2b30b627, org.springframework.se
curity.web.access.ExceptionTranslationFilter@1107c465, org.springframework.security.web.access.intercept.FilterSecurityI
nterceptor@3c2f310c]
2019-09-24 10:27:13.568 INFO 19648 --- [main] s.w.s.m.m.a.RequestMappingHandlerAdapter : Looking for @Contro
llerAdvice: org.springframework.boot.context.embedded.AnnotationConfigEmbeddedWebApplicationContext@313ac989: startup da
te [Tue Sep 24 10:27:00 EDT 2019]; root of context hierarchy
2019-09-24 10:27:14.114 INFO 19648 --- [main] o.s.j.e.a.AnnotationMBeanExporter : Registering beans f
or JMX exposure on startup
2019-09-24 10:27:14.126 INFO 19648 --- [main] o.s.c.support.DefaultLifecycleProcessor : Starting beans in p
hase 0
2019-09-24 10:27:14.229 INFO 19648 --- [main] s.b.c.e.t.TomcatEmbeddedServletContainer : Tomcat started on p
ort(s): 8080 (http)
2019-09-24 10:27:14.234 INFO 19648 --- [main] org.owasp.webgoat.StartWebGoat : Started StartWebGoa
t in 14.944 seconds (JVM running for 16.67)
```

Troubleshoot:

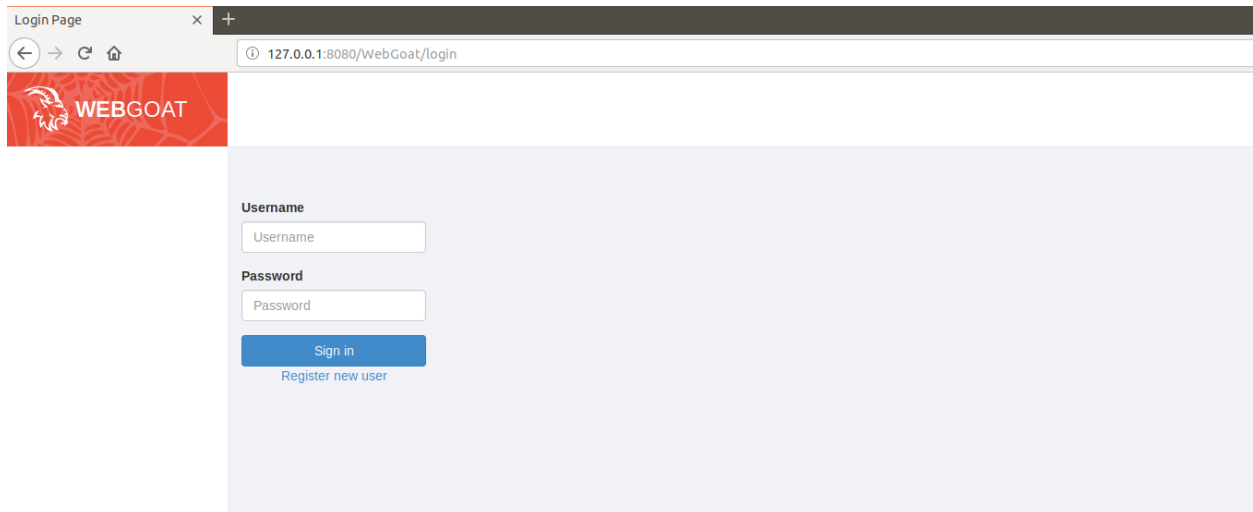
- If you are getting the "UnsupportedClassVersionError" while trying to start the webgoat server, then you have to set the path variable.

Go to systems->advanced system settings->Environment Variable->Click on Path under System variables-> click edit->new->add the path- path of the Java until the bin folder (example-for me it was C:\Program Files\Java\jdk-11.0.5\bin)->ok

- After setting the path variable, then command prompt (cmd) needs to be closed and opened again.
- Try to run the webgoat server now. It should work.
- If again you are getting an error, you can again check the path variable. Sometimes a path with oracle gets added, which needs to be deleted.

Web-Based Application Design and Development (ITIS 3135)

- Once installed connect to <http://localhost:8080/WebGoat> using your browser. You should see the following screen:



- Now you can click on 'Register new user' and create a new user that you will use for this lab.
- SUBMISSION:** Take a screenshot (**Screenshot 1**) of WebGoat "home page" page on your browser with a notepad containing your student name and ID number visible. Add it in a word document, called **YourLastName_WebSecurityActivity.docx**. **After you complete part 2, you will upload this document on Canvas individually. (10 points)**