

A photograph of a large, modern building with a grid of windows, identified as Red River College. The building has a glass facade and a sign on top. To the right, a portion of an older, more ornate building is visible. The image has a sepia or brownish tint.

RED RIVER COLLEGE

OWASP: WebGoat/WebWolf

BUHLER LIBRARY

OWASP

- Open Web Application Security Project
- www.owasp.org
- Not for profit organization focused on helping individuals and organizations on understanding, developing, acquiring, running, and maintaining web applications that can be trusted
- Focused on web, but applies elsewhere

Java

- If java is missing, don't download the most recent version of the runtime environment, it is incompatible
- Download Java SDK from this link:
- <https://www.oracle.com/technetwork/java/javase/downloads/index.html>
- May require modification of your path

download Java 17 SDK Windows x64 Installer

ORACLE

Products Industries Resources Customers Partners Developers Company



View Accounts



Contact Sales

Java downloads

Tools and resources

Java archive

JDK Development Kit 17.0.10 downloads

JDK 17 binaries are free to use in production and free to redistribute, at no cost, under the [Oracle No-Fee Terms and Conditions](#) (NFTC).

JDK 17 will receive updates under the NFTC, until September 2024. Subsequent JDK 17 updates will be licensed under the [Java SE OTN License](#) (OTN) and production use beyond the [limited free grants](#) of the OTN license will [require a fee](#).

Linux macOS **Windows**

Product/file description	File size	Download
x64 Compressed Archive	172.47 MB	https://download.oracle.com/java/17/latest/jdk-17_windows-x64_bin.zip (sha256)
x64 Installer	153.55 MB	https://download.oracle.com/java/17/latest/jdk-17_windows-x64_bin.exe (sha256)
x64 MSI Installer	152.34 MB	https://download.oracle.com/java/17/latest/jdk-17_windows-x64_bin.msi (sha256)

Documentation Download

Cut and paste in Software Folder



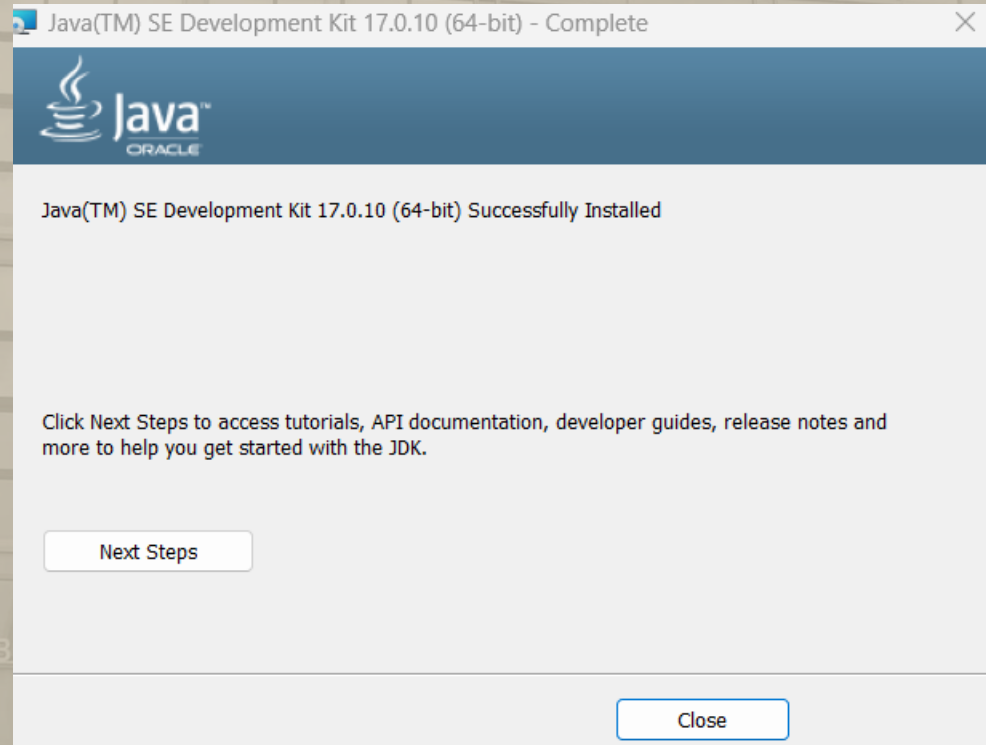
jdk-17_windows-x64_bin

Install Java





RED RIVER COLLEGE



JDK 17 Documentation

- <https://docs.oracle.com/en/java/javase/17/index.html>

WebGoat

- Up to version 8.2.2
- <https://github.com/WebGoat/WebGoat/releases>
- Requires Java to run
 - Open command prompt, type:
java -version
- ➔ • Runs on port 8080 by default

v8.2.2

Version 8.2.2

New functionality





- Docker image now supports nginx when browsing to <http://localhost> a landing page is shown.

Bug fixes

- [#1039 jwt-7-Code review](#)
- [#1031 SQL Injection \(intro\) 5: Data Control Language \(DCL\) the wiki's solution is not correct](#)
- [#1027 Webgoat 8.2.1 Vulnerable_Components_12 Shows internal server error](#)

Assets

4

 webgoat-server-8.2.2.jar	91.9 MB	Sep 5, 2021
 webwolf-8.2.2.jar	51.3 MB	Sep 5, 2021
 Source code (zip)		Sep 5, 2021
 Source code (tar.gz)		Sep 5, 2021

Cut and paste in Software Folder

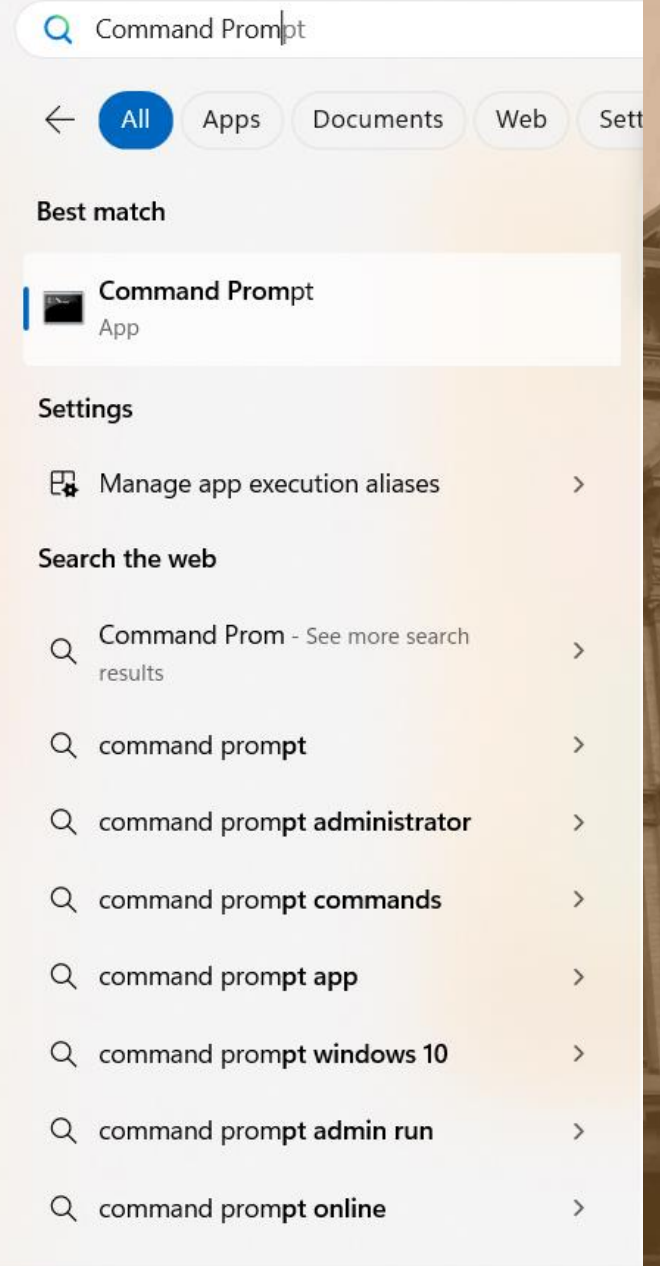


webwolf-8.2.2



webgoat-server-8.2.2

Command Prompt



Search



RED RIVER COLLEGE

Command Prompt



Microsoft Windows [Version 10.0.22621.3155]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mgghanbari>

RED RIVER COLLEGE



Administrator: Windows Powe ×



Windows PowerShell

Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

```
PS C:\Users\mganbari> java -version
java version "17.0.10" 2024-01-16 LTS
Java(TM) SE Runtime Environment (build 17.0.10+11-LTS-240)
Java HotSpot(TM) 64-Bit Server VM (build 17.0.10+11-LTS-240, mixed mode, sharing)
PS C:\Users\mganbari>
```



WebGoat

- Will run on our host environment

WebWolf

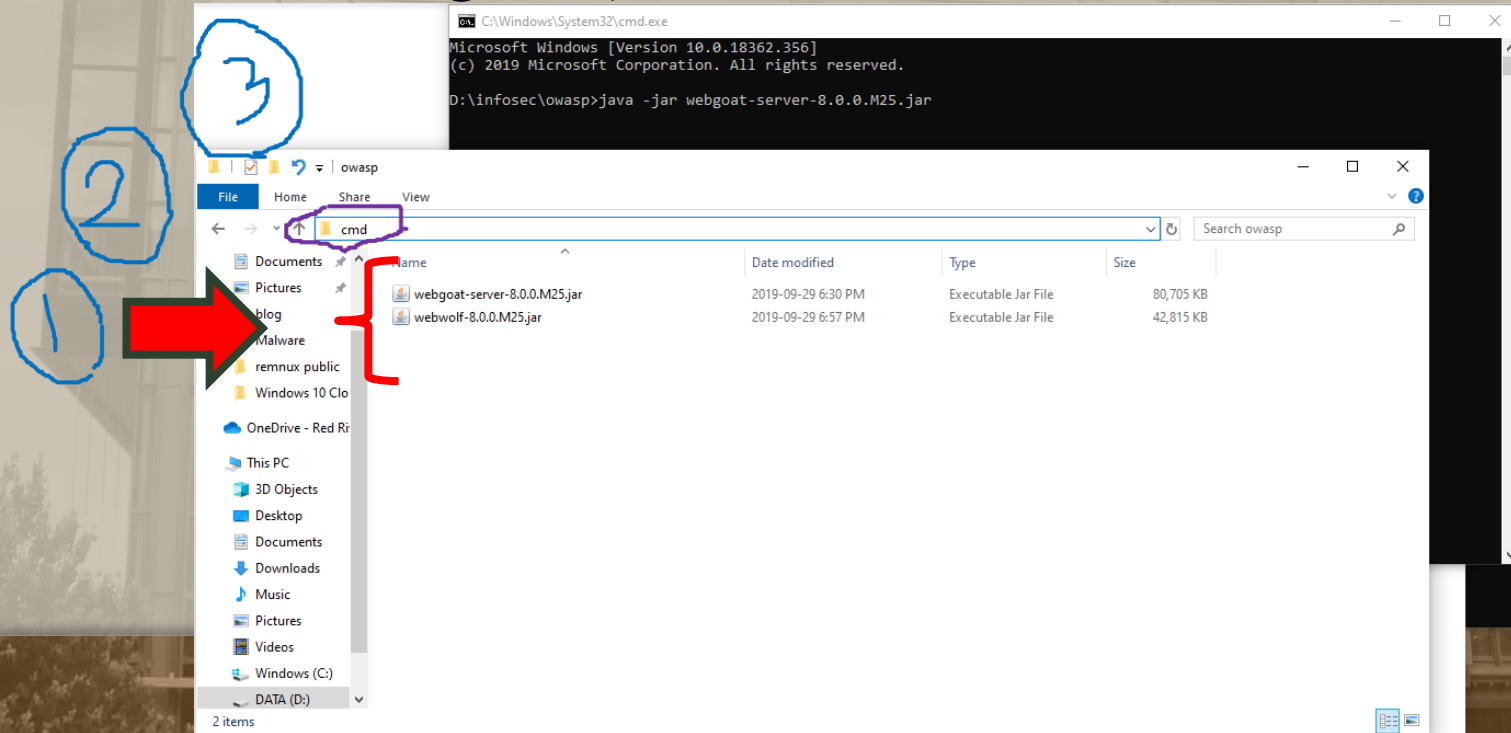
- Creates an **interface** that allows WebGoat to do things like make server requests and send email
- Downloaded from the same page as WebGoat
- ➔ • Runs on port 9090 by default

Zap

- Gives us a simple proxy to analyze data as it leaves from and returns to the browser
- Useful for manipulating form data, headers, and other web data
- More simple version to implement and use than Burpe Suite (comprehensive web application security testing platform)
- Simple installer (checks for java)

WebGoat

- Once downloaded, move both jar files to a dedicated folder (such as c:\webgoat or d:\webgoat)



WebGoat

- Once downloaded, move both jar files to a dedicated folder (such as c:\webgoat or d:\webgoat)

```
cd C:\Users\mgghanbari\RRC Courses\Winter 2024\Web Security\Softwares
```

➔ Executing is done by calling java:
java -jar webgoat-*version*.jar

```
java -jar webgoat-server-8.2.2.jar
```

- If there are errors, it will report them

➔ Can try different ports:
java -jar webgoat-ver#.jar --server.port 8081


```
C:\Users\mgghanbari>cd C:\Users\mgghanbari\RRC Courses\Winter 2024\Web Security\Softwares
```

```
C:\Users\mghanbari\RRC Courses\Winter 2024\Web Security\Softwares>java -jar webgoat-server-8.2.2.jar
13:33:20.851 [main] INFO org.owasp.webgoat.StartWebGoat - Starting WebGoat with args:
```

21

RED RIVER COLLEGE

```
Command Prompt - java -jar x + v
Microsoft Windows [Version 10.0.22621.3155]
(c) Microsoft Corporation. All rights reserved.

C:\Users\mgghanbari>java -version
java version "17.0.10" 2024-01-16 LTS
Java(TM) SE Runtime Environment (build 17.0.10+11-LTS-240)
Java HotSpot(TM) 64-Bit Server VM (build 17.0.10+11-LTS-240, mixed mode, sharing)

C:\Users\mgghanbari>java -jar webgoat-version.jar
Error: Unable to access jarfile webgoat-version.jar

C:\Users\mgghanbari>cd C:\Users\mgghanbari\RRC Courses\Winter 2024\Web Security\Softwares

C:\Users\mgghanbari\RRC Courses\Winter 2024\Web Security\Softwares>java -jar webgoat-version.jar
Error: Unable to access jarfile webgoat-version.jar

C:\Users\mgghanbari\RRC Courses\Winter 2024\Web Security\Softwares>java -jar webgoat-server-8.2.2.jar
13:33:20.851 [main] INFO org.owasp.webgoat.StartWebGoat - Starting WebGoat with args:

  /\ /-----\
  ( )\-----\
  \V /-----\
  ' |-----\
  =====|_=====
  :: Spring Boot ::                (v2.4.3)

2024-03-11 13:33:22.882 INFO 2972 --- [main] org.owasp.webgoat.StartWebGoat : Starting StartWebGoat v8.2.2 using Java 17.0.10 on ITSM1
059085 with PID 2972 (C:\Users\mgghanbari\RRC Courses\Winter 2024\Web Security\Softwares\webgoat-server-8.2.2.jar started by mgghanbari in C:\Users\mgghanbari\RRC Courses\Winter 2024\Web Security\Softwares)
2024-03-11 13:33:22.893 DEBUG 2972 --- [main] org.owasp.webgoat.StartWebGoat : Running with Spring Boot v2.4.3, Spring v5.3.4
2024-03-11 13:33:22.893 INFO 2972 --- [main] org.owasp.webgoat.StartWebGoat : No active profile set, falling back to default profiles: default
2024-03-11 13:33:27.547 INFO 2972 --- [main] .s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Spring Data JPA repositories in DEFAULT mode.
2024-03-11 13:33:27.845 INFO 2972 --- [main] .s.d.r.c.RepositoryConfigurationDelegate : Finished Spring Data repository scanning in 282 ms. Found 2 JPA repository interfaces.
2024-03-11 13:33:29.642 WARN 2972 --- [main] io.undertow.websockets.jsr : UT026010: Buffer pool was not set on WebSocketDeploymentInfo, the default pool will be used
2024-03-11 13:33:29.705 INFO 2972 --- [main] io.undertow.servlet : Initializing Spring embedded WebApplicationContext
2024-03-11 13:33:29.705 INFO 2972 --- [main] w.s.c.ServletWebServerApplicationContext : Root WebApplicationContext: initialization completed in
```

Initial Startup

- Initial startup can take some time
- Looking for something like the following:

```
C:\Windows\System32\cmd.exe - "c:\Program Files\Java\jdk-12.0.1\bin\java.exe" -jar webgoat-server-8.0.0.M25.jar

on.logout.LogoutFilter@2093bb6c, org.springframework.security.web.authentication.www.BasicAuthenticationFilter@3a42145,
org.springframework.security.web.savedrequest.RequestCacheAwareFilter@193d7ac7, org.springframework.security.web.servlet
api.SecurityContextHolderAwareRequestFilter@7d0333c8, org.springframework.security.web.authentication.AnonymousAuthentic
ationFilter@f0d01c9, org.springframework.security.web.session.SessionManagementFilter@5e976553, org.springframework.secu
rity.web.access.ExceptionTranslationFilter@c8531b9, org.springframework.security.web.access.intercept.FilterSecurityInte
rceptor@7eb774c3]
2019-09-30 08:02:35.546 INFO 15548 --- [          main] s.w.s.m.m.a.RequestMappingHandlerAdapter : Looking for @Contro
llerAdvice: org.springframework.boot.context.embedded.AnnotationConfigEmbeddedWebApplicationContext@6ec8211c: startup da
te [Mon Sep 30 08:02:26 CDT 2019]; root of context hierarchy
2019-09-30 08:02:36.047 INFO 15548 --- [          main] o.s.j.e.a.AnnotationMBeanExporter      : Registering beans f
or JMX exposure on startup
2019-09-30 08:02:36.063 INFO 15548 --- [          main] o.s.c.support.DefaultLifecycleProcessor : Starting beans in p
hase 0
2019-09-30 08:02:36.132 INFO 15548 --- [          main] s.b.c.e.t.TomcatEmbeddedServletContainer : Tomcat started on p
ort(s): 8080 (http)
2019-09-30 08:02:36.148 INFO 15548 --- [          main] org.owasp.webgoat.StartWebGoat      : Started StartWebGoa
t in 10.354 seconds (JVM running for 12.889)
```


RED RIVER COLLEGE

```
h context path '/WebGoat'  
INFO 13964 --- [          main] org.owasp.webgoat.StartWebGoat      : Started Sta  
running for 20.652)
```



BUHLER LIBRARY


Login

- Once WebGoat is set up, you want to log in to the web interface
- Open Firefox (preferred) and browse to:
<http://localhost:8080/WebGoat>
- You will need to create an account

RED RIVER COLLEGE

Browser window: Login Page

Address bar: localhost:8080/WebGoat/login

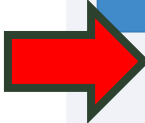
 **WEBGOAT**

Username

Password

[Sign in](#)

[Register new user](#)



Create Account

Username:

Password:

Register

Username

Password

size must be between 6 and 10

Confirm password

size must be between 6 and 10

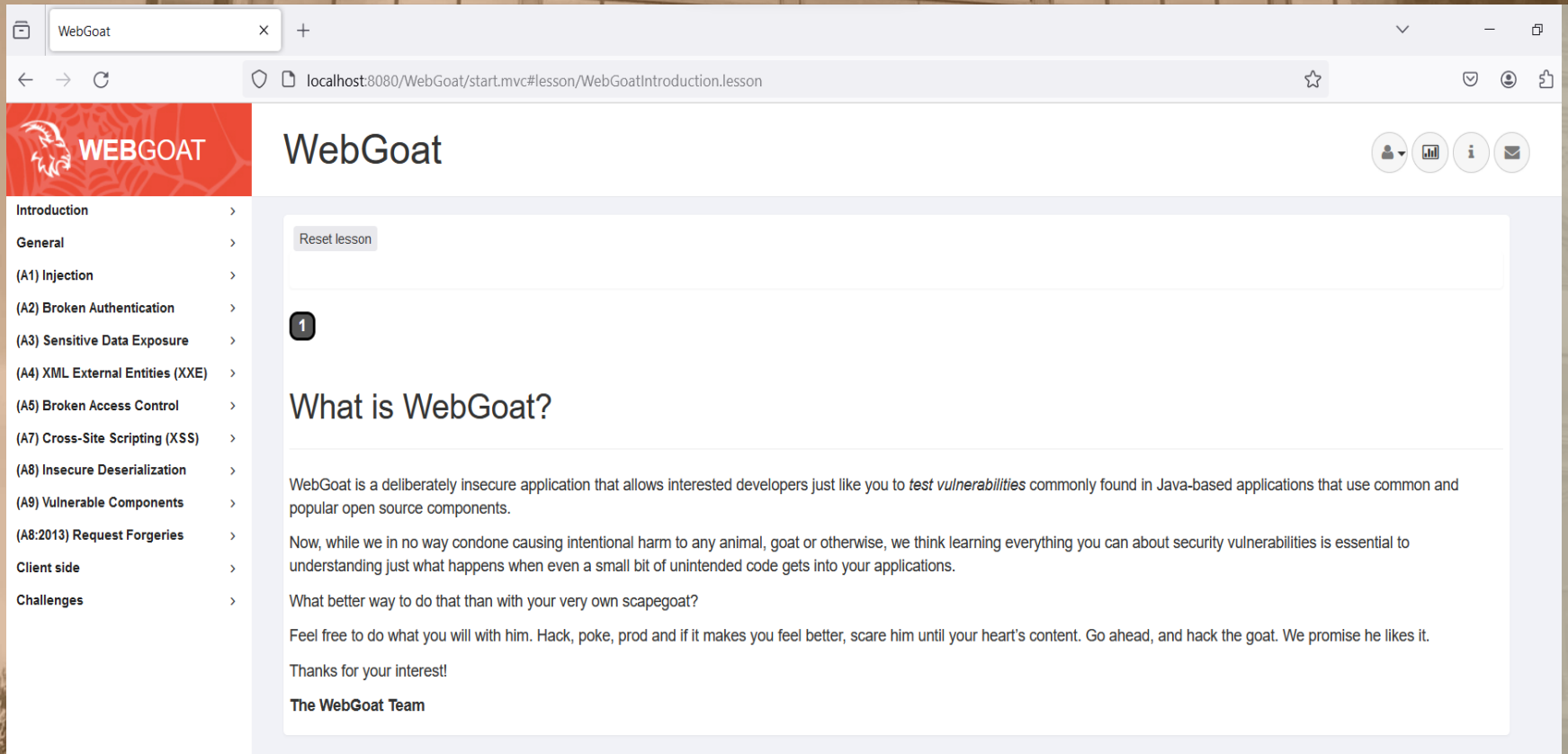
Terms of use

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.

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.


☒ Agree with the terms and conditions

Sign up



WebGoat

localhost:8080/WebGoat/start.mvc#lesson/WebGoatIntroduction.lesson

 **WEBGOAT**

WebGoat

- Introduction >
- General >
- (A1) Injection >
- (A2) Broken Authentication >
- (A3) Sensitive Data Exposure >
- (A4) XML External Entities (XXE) >
- (A5) Broken Access Control >
- (A7) Cross-Site Scripting (XSS) >
- (A8) Insecure Deserialization >
- (A9) Vulnerable Components >
- (A8:2013) Request Forgeries >
- Client side >
- Challenges >

Reset lesson

1 What is WebGoat?

WebGoat is a deliberately insecure application that allows interested developers just like you to *test vulnerabilities* commonly found in Java-based applications that use common and popular open source components.

Now, while we in no way condone causing intentional harm to any animal, goat or otherwise, we think learning everything you can about security vulnerabilities is essential to understanding just what happens when even a small bit of unintended code gets into your applications.

What better way to do that than with your very own scapegoat?

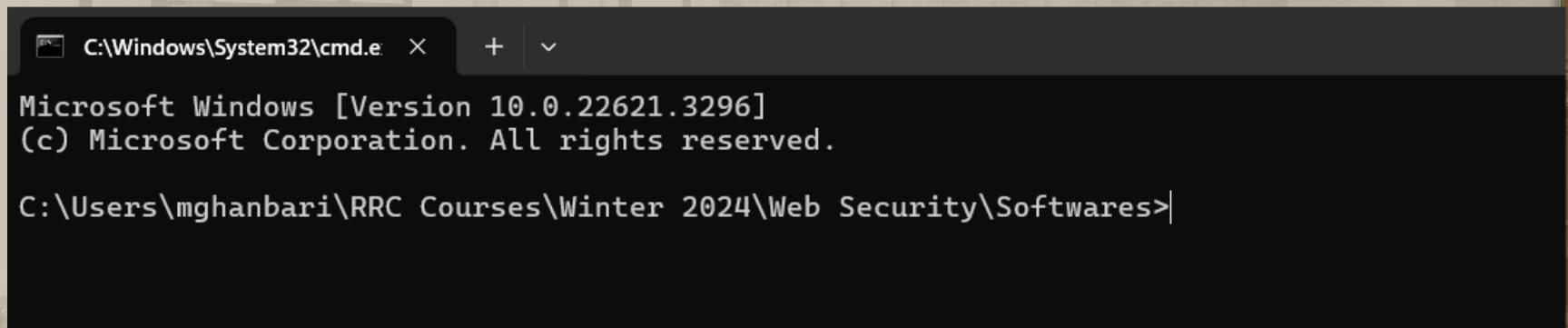
Feel free to do what you will with him. Hack, poke, prod and if it makes you feel better, scare him until your heart's content. Go ahead, and hack the goat. We promise he likes it.

Thanks for your interest!

The WebGoat Team

WebWolf

- Once you have an account, you can open a new command prompt and **start WebWolf**



```
C:\Windows\System32\cmd.e  ×  +  ▾  
Microsoft Windows [Version 10.0.22621.3296]  
(c) Microsoft Corporation. All rights reserved.  
C:\Users\mghanbari\RRC Courses\Winter 2024\Web Security\Softwares>
```

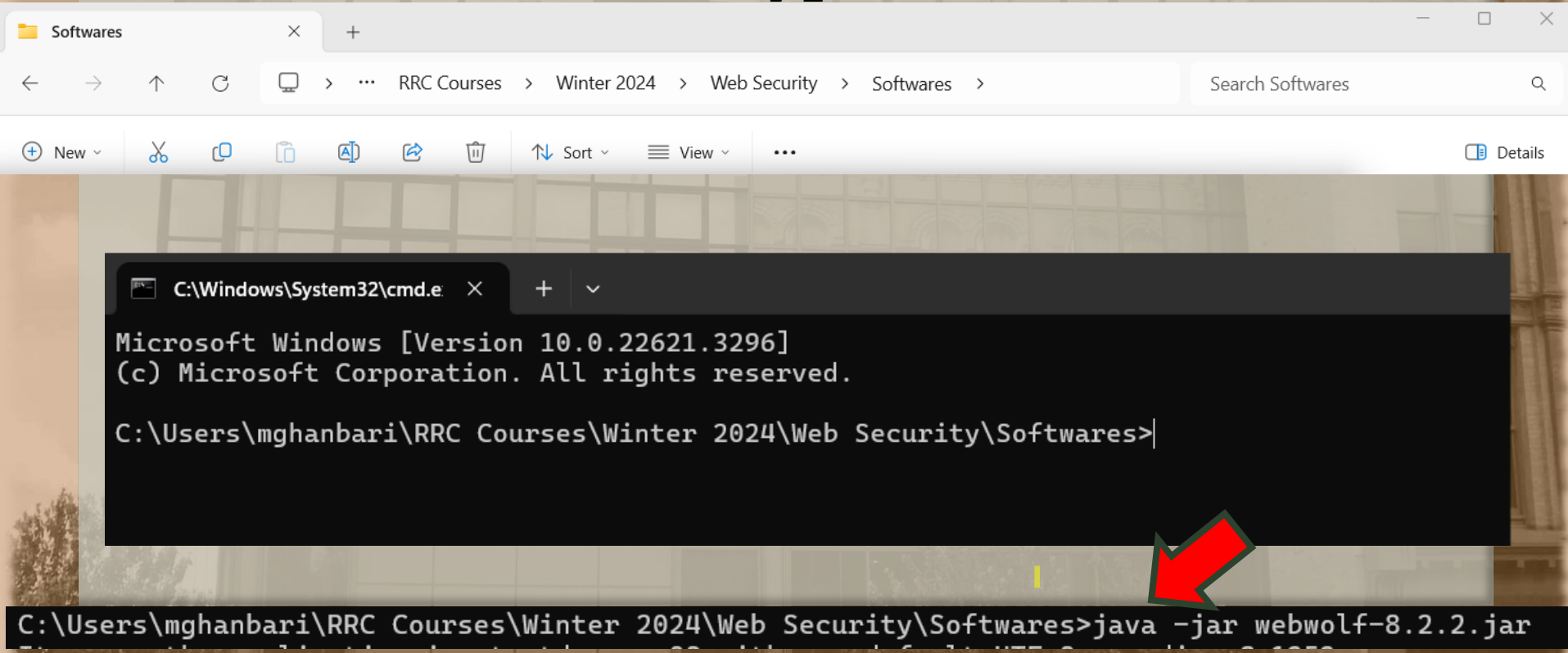
WebWolf

- Once you have an account, you can open a new command prompt and **start WebWolf**

```
java -jar webwolf-8.2.2.jar
```

WebWolf


- In the address area of the folder that webwolf file exist, type cmd and hit enter




If You Have an Error

```
C:\Users\mganbari\RRC Courses\Winter 2024\Web Security\Softwares>java -jar webwolf-8.2.2.jar
```

It seems the application is started on a OS with non default UTF-8 encoding: Cp1252
Please add: -Dfile.encoding=UTF-8



```
C:\Users\mganbari\RRC Courses\Winter 2024\Web Security\Softwares>java -Dfile.encoding=UTF-8 -jar webwolf-8.2.2.jar
```



If you have an error:

Initial Startup

- Initial startup can take some time
- Looking for something like the following:

```
security.web.authentication.UsernamePasswordAuthenticationFilter@22a736d7, org.springframework.security.web.savedrequest
.RequestCacheAwareFilter@35d5ac51, org.springframework.security.web.servletapi.SecurityContextHolderAwareRequestFilter@3
0364216, org.springframework.security.web.authentication.AnonymousAuthenticationFilter@4649d70a, org.springframework.sec
urity.web.session.SessionManagementFilter@546e61d5, org.springframework.security.web.access.ExceptionTranslationFilter@6
944e53e, org.springframework.security.web.access.intercept.FilterSecurityInterceptor@210308d5]
2025-02-12 11:12:23.412 INFO 15848 --- [main] o.s.s.concurrent.ThreadPoolTaskExecutor : Initializing Execut
orService 'applicationTaskExecutor'
2025-02-12 11:12:24.119 INFO 15848 --- [main] o.s.b.a.e.web.EndpointLinksResolver : Exposing 2 endpoint
(s) beneath base path '/actuator'
2025-02-12 11:12:24.198 INFO 15848 --- [main] io.undertow : starting server: Un
dertow - 2.2.4.Final
2025-02-12 11:12:24.229 INFO 15848 --- [main] org.xnio : XNIO version 3.8.0.
Final
2025-02-12 11:12:24.264 INFO 15848 --- [main] org.xnio.nio : XNIO NIO Implementa
tion Version 3.8.0.Final
2025-02-12 11:12:24.554 INFO 15848 --- [main] org.jboss.threads : JBoss Threads versi
on 3.1.0.Final
2025-02-12 11:12:24.628 INFO 15848 --- [main] o.s.b.w.e.undertow.UndertowWebServer : Undertow started on
port(s) 9090 (http)
2025-02-12 11:12:24.644 INFO 15848 --- [main] org.owasp.webwolf.WebWolf : Started WebWolf in
12.376 seconds (JVM running for 13.266)
```

RED RIVER COLLEGE

INFO 15848 --- [
ng for 13.266)

main] org.owasp.webwolf.WebWolf

: Started WebWo



BUHLER LIBRARY

WebWolf

- You can open a new tab, and go to:
<http://localhost:9090/WebWolf>
- You would log in with the same
user/password you created for WebGoat

RED RIVER COLLEGE

WebGoat



WebWolf



localhost:9090/login

WebWolf

Home

Files

Mailbox

Incoming requests

JWT

Sign in

Sign In



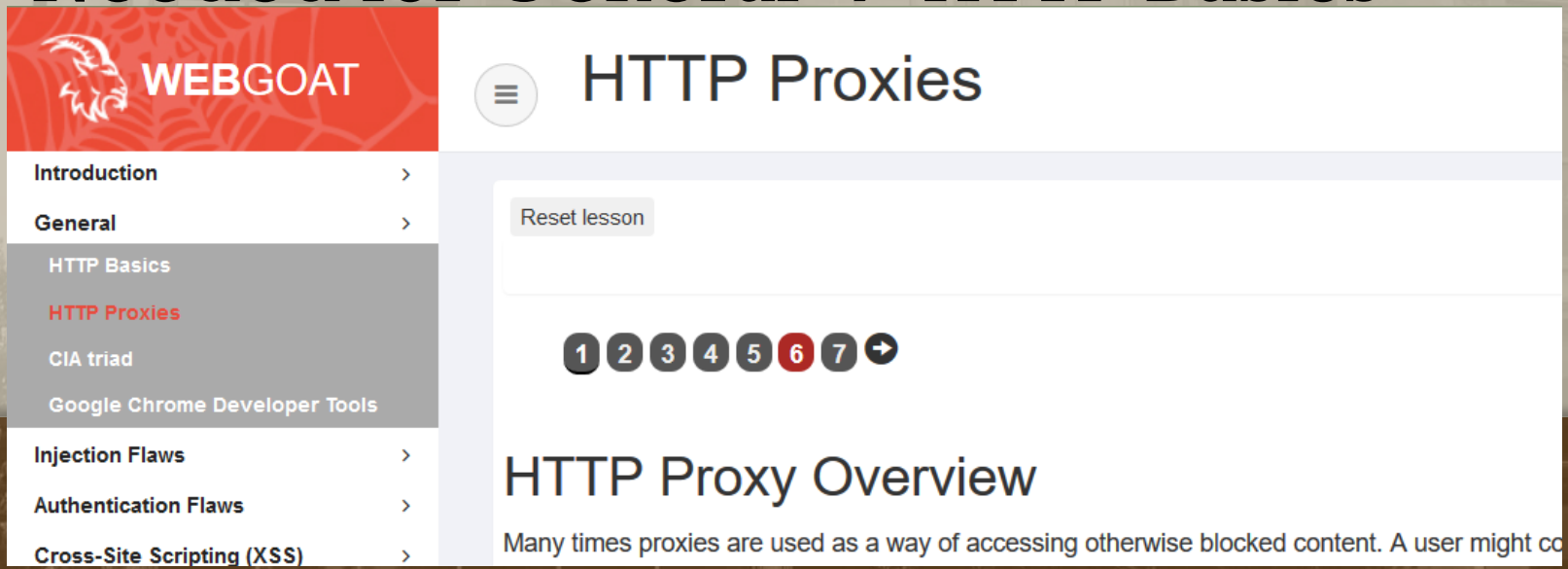


WebWolf

Some challenges requires to have a local web server running. WebWolf is for you the attacker it helps you while solving some of the assignments and challenges within WebGoat. An assignment might for example require you to serve a file or connect back to your own environment or to receive an e-mail. In order to not let you run WebGoat open and connected to the internet we provided these tools in this application, called WebWolf.

Zap

- Once you have set up WebGoat and WebWolf, you will eventually need to set up Zap. You can see the instructions under General → HTTP Proxies
- Needed for General → HTTP Basics



The screenshot displays the WebGoat application interface. On the left is a red sidebar with the WebGoat logo and a navigation menu. The menu items are: Introduction, General, HTTP Basics, HTTP Proxies (highlighted in red), CIA triad, Google Chrome Developer Tools, Injection Flaws, Authentication Flaws, and Cross-Site Scripting (XSS). The main content area has a white header with a hamburger menu icon and the title 'HTTP Proxies'. Below the header is a 'Reset lesson' button. A progress bar shows seven steps, with the sixth step highlighted in red. The main heading is 'HTTP Proxy Overview', followed by the text: 'Many times proxies are used as a way of accessing otherwise blocked content. A user might co'.

WEBGOAT

- Introduction >
- General >
- HTTP Basics
- HTTP Proxies**
- CIA triad
- Google Chrome Developer Tools
- Injection Flaws >
- Authentication Flaws >
- Cross-Site Scripting (XSS) >

HTTP Proxies

Reset lesson

1 2 3 4 5 6 7 →

HTTP Proxy Overview

Many times proxies are used as a way of accessing otherwise blocked content. A user might co



HTTP Proxies



- Introduction
- General >
- HTTP Basics
- HTTP Proxies**
- Developer Tools
- CIA Triad
- Crypto Basics
- Writing new lesson



Reset lesson



What's a HTTP Proxy

A proxy is some forwarder application that connects your http client to backend resources. HTTP clients can be browsers, or applications like curl, SOAP UI, Postman, etc. Usually these proxies are used for routing and getting access to internet when there is no direct connection to internet from the client itself. HTTP proxies are therefore also ideal when you are testing your application. You can always use the proxy log records to see what was actually sent from client to server. So you can check the request and response headers and the XML, JSON or other payload.

HTTP Proxies receive requests from a client and relay them. They also typically record them. They act as a man-in-the-middle. It even works fine with or without HTTPS as long as your client or browser trusts the certificate of the HTTP Proxy.

ZAP Proxy Capabilities

With ZAP you can record traffic, inspect traffic, modify requests and response from and to your browser, and get reports on a range of known vulnerabilities that are detected by ZAP through the inspection of the traffic. The passive and active reporting on

- 
- The background of the slide is a photograph of the Red River College Buhler Library. The building is a multi-story structure with a large glass facade and a sign that reads "RED RIVER COLLEGE" at the top. The text "BUHLER LIBRARY" is visible on the lower part of the building. The image is slightly faded and has a warm, orange-brown tint.
- Google “zaproxy download”
 - <https://www.zaproxy.org/download/>

RED RIVER COLLEGE



install4j Wizard



Zed Attack Proxy is preparing the install4j Wizard which will guide you through the rest of the setup process.



Cancel

BUHLER LIBRARY



Setup - Zed Attack Proxy 2.14.0



Welcome to the Zed Attack Proxy Setup Wizard

This will install Zed Attack Proxy on your computer. The wizard will lead you step by step through the installation.

Click Next to continue, or Cancel to exit Setup.

Next >

Cancel



Setup - Zed Attack Proxy 2.14.0



License Agreement

Please read the following important information before continuing.



Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

Apache License
Version 2.0, January 2004
<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.



I accept the agreement



I do not accept the agreement

install4j

< Back

Next >

Cancel



Setup - Zed Attack Proxy 2.14.0



Select Installation Type

Which type of installation should be performed?



Select the type of installation that you want to perform. Click Next when you are ready to continue.

- ☒ Standard installation
☐ Custom installation

install4j

< Back

Next >

Cancel



Setup - Zed Attack Proxy 2.14.0



Ready to Install

Setup is now ready to being installing Zed Attack Proxy on your computer.



Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:

C:\Program Files\ZAP\Zed Attack Proxy

Start Menu folder:

ZAP\Zed Attack Proxy

Additional tasks:

Additional icons:

Create a desktop icon

Check for Updates:

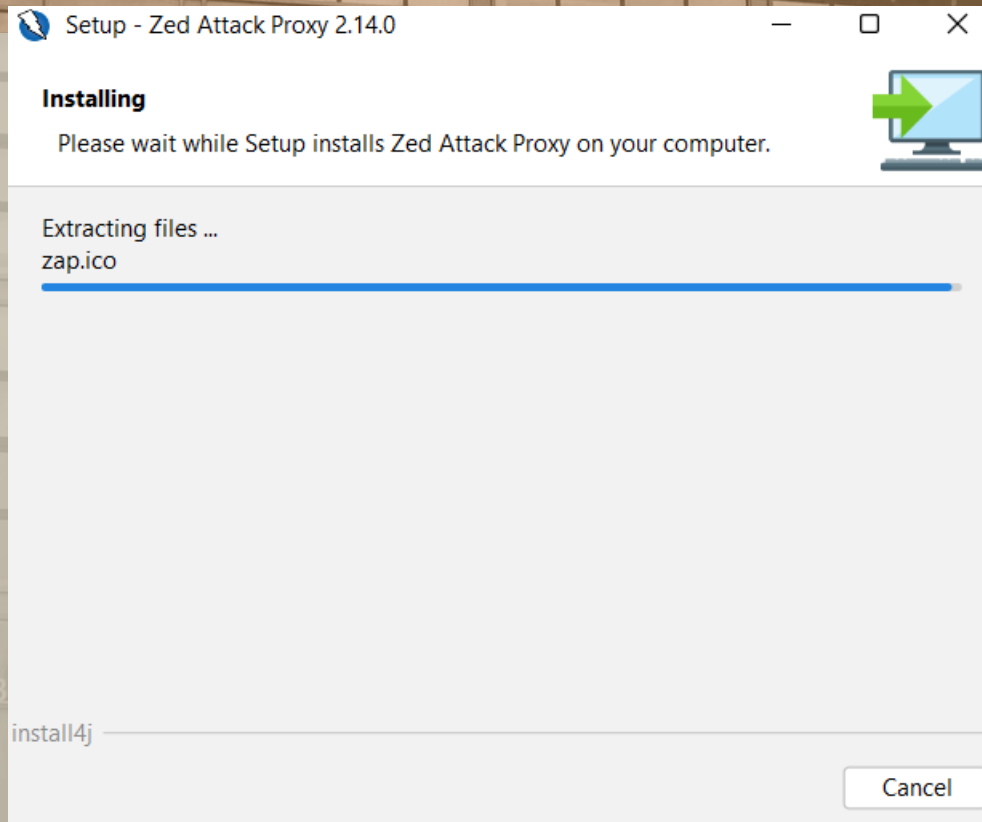
Check for updates on startup: Yes

install4j

< Back

Install

Cancel





Setup - Zed Attack Proxy 2.14.0



Completing the Zed Attack Proxy Setup Wizard

Setup has finished installing Zed Attack Proxy on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

Finish

Search for apps, settings, and documents

ZAP

Recent



ZAP 2.14.0



Command Prompt



Sublime Text 3



PuTTY



java



WinSCP



putty

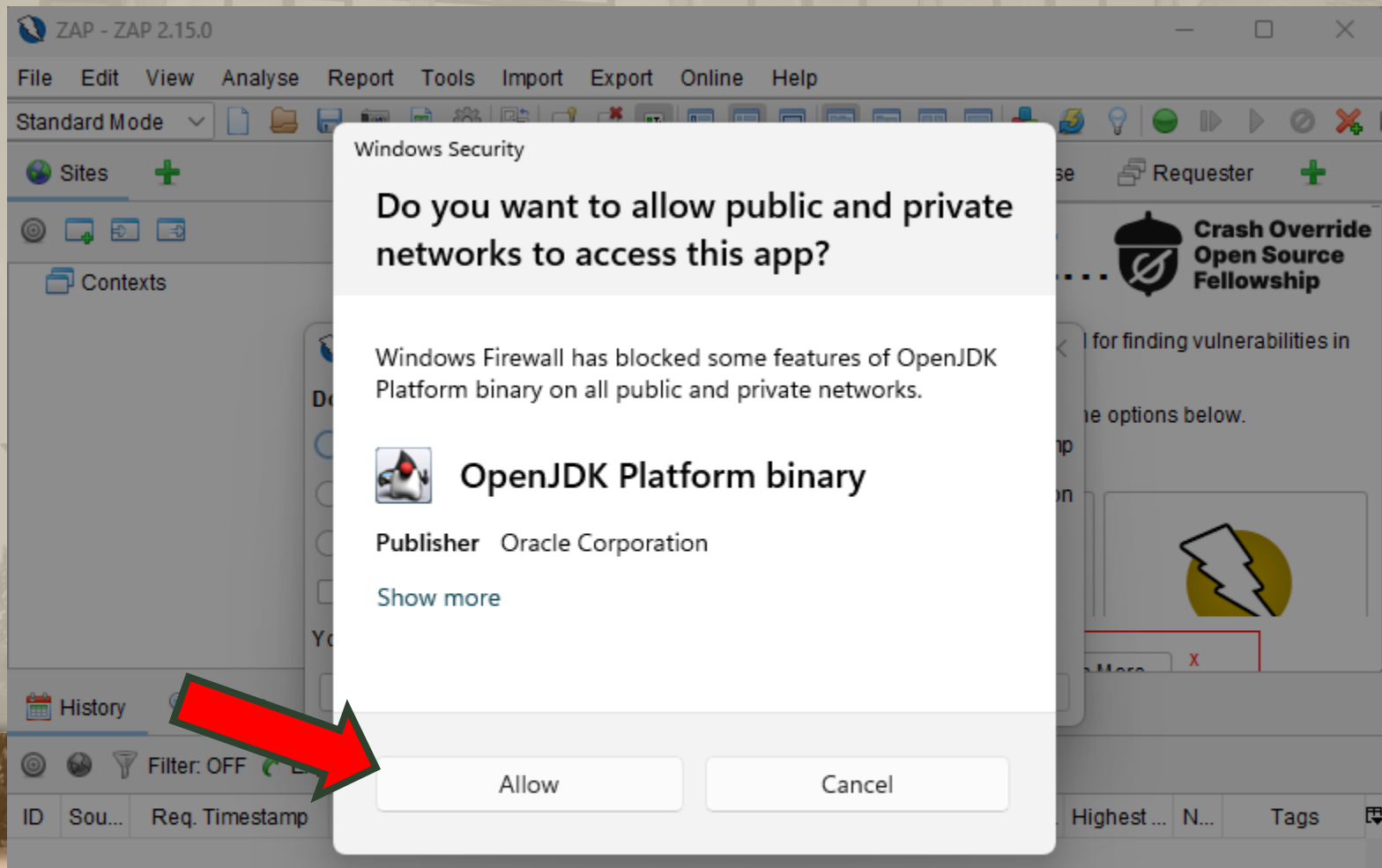


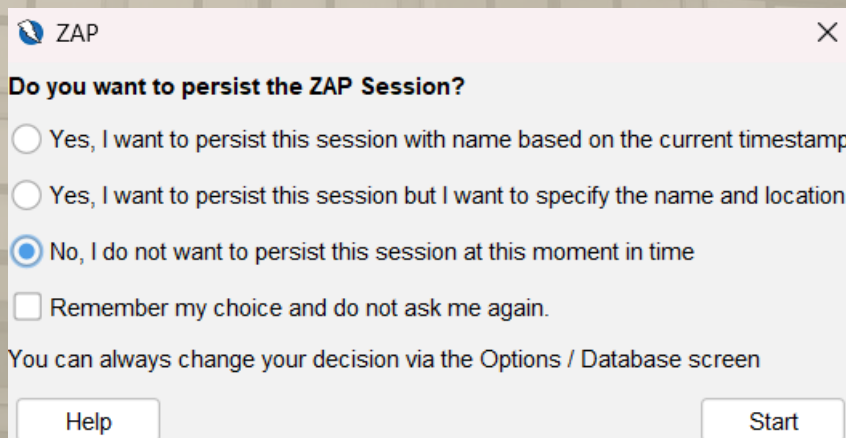
Search




RED RIVER COLLEGE

- Do you want,java access to this file: Allow



A screenshot of a ZAP (Zed Attack Proxy) dialog box overlaid on a background image of a building. The dialog box has a title bar with the ZAP logo and a close button. It contains a question about persisting the session, three radio button options, a checkbox for remembering the choice, and a note about changing the decision later. There are 'Help' and 'Start' buttons at the bottom.

 ZAP ×

Do you want to persist the ZAP Session?

☐ Yes, I want to persist this session with name based on the current timestamp

☐ Yes, I want to persist this session but I want to specify the name and location

☒ No, I do not want to persist this session at this moment in time

☐ Remember my choice and do not ask me again.

You can always change your decision via the Options / Database screen

Help Start

Error Starting Main Proxy



Unable to use the port 8080. Try:

8081



Yes

No

Welcome to ZAP



ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
If you are new to ZAP then it is best to start with one of the options below.



Automated Scan



Manual Explore



Support



Learn More

News

BIG ZAP funding announcement!

Learn More

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
----	--------	----------------	--------	-----	------	--------	-----	-----------------	---------------	------	------

HTTP Proxies

Reset lesson



report
card

What's a HTTP Proxy

A proxy is some forwarder application that connects your http client to backend resources. HTTP clients can be browsers, or applications like curl, SOAP UI, Postman, etc. Usually these proxies are used for routing and getting access to internet when there is no direct connection to internet from the client itself. HTTP proxies are therefore also ideal when you are testing your application. You can always use the proxy log records to see what was actually sent from client to server. So you can check the request and response headers and the XML, JSON or other payload.

HTTP Proxies receive requests from a client and relay them. They also typically record them. They act as a man-in-the-middle. It even works fine with or without HTTPS as long as your client or browser trusts the certificate of the HTTP Proxy.

ZAP Proxy Capabilities

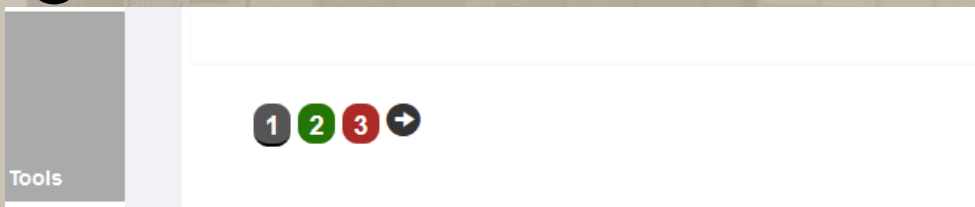
With ZAP you can record traffic, inspect traffic, modify requests and response from and to your browser, and get reports on a range of known vulnerabilities that are detected by ZAP through the inspection of the traffic. The passive and active reporting on

OWASP Compitency

- - General (should be the same) HTTP Basics, and HTTP Proxies
- - (A1) Injection - SQL Injection (Intro)
- - (A2) Broken Authentication - Authentication Bypasses - JWT Tokens
- - (A5) Broken Access Control
 - Insecure direct object References
 - Missing Function Level Access Control
- - (A7) Cross Site Scripting (XSS) - Cross Site Scripting

Report Card

- When you shut down WebGoat, it will track your progress
- As you progress, cookie crumbs that have activities assigned turn from red to green:



- You can also check out your report card:

