

OWASP:
WebGoat/WebWolf



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

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

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

WebGoat

- Will run on our host environment, but can be run in Debian
 - Bugs around host address
--server.address=<ip_addr>
 - If you choose, upload and run from /var/www/html

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

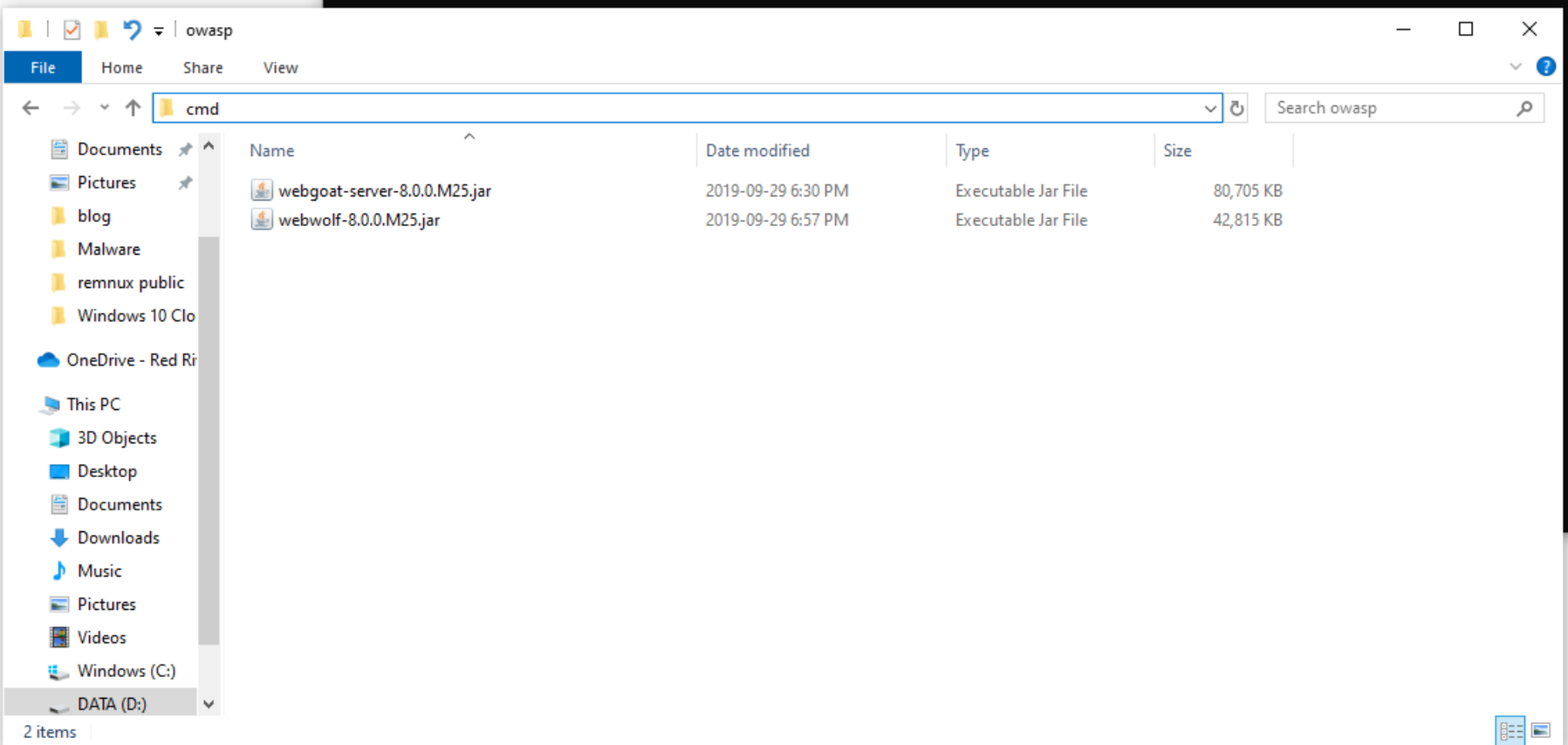
- Gives us a simple proxy to analyze data as it leaves from and returns to the browser
- Useful for manipulating form data, headers, and other web data
- More simple version to implement and use than Burpe Suite
- Simple installer (checks for java)

WebGoat

- Once downloaded, move both jar files to a dedicated folder (such as c:\webgoat or d:\webgoat)
- Executing is done by calling java:
`java -jar webgoat-version.jar`
- If there are errors, it will report them
- Can try different ports:
`java -jar webgoat-ver#.jar --server.port 8081`

WebGoat

```
C:\Windows\System32\cmd.exe  
Microsoft Windows [Version 10.0.18362.356]  
(c) 2019 Microsoft Corporation. All rights reserved.  
D:\infosec\owasp>java -jar webgoat-server-8.0.0.M25.jar
```



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)
```

Login

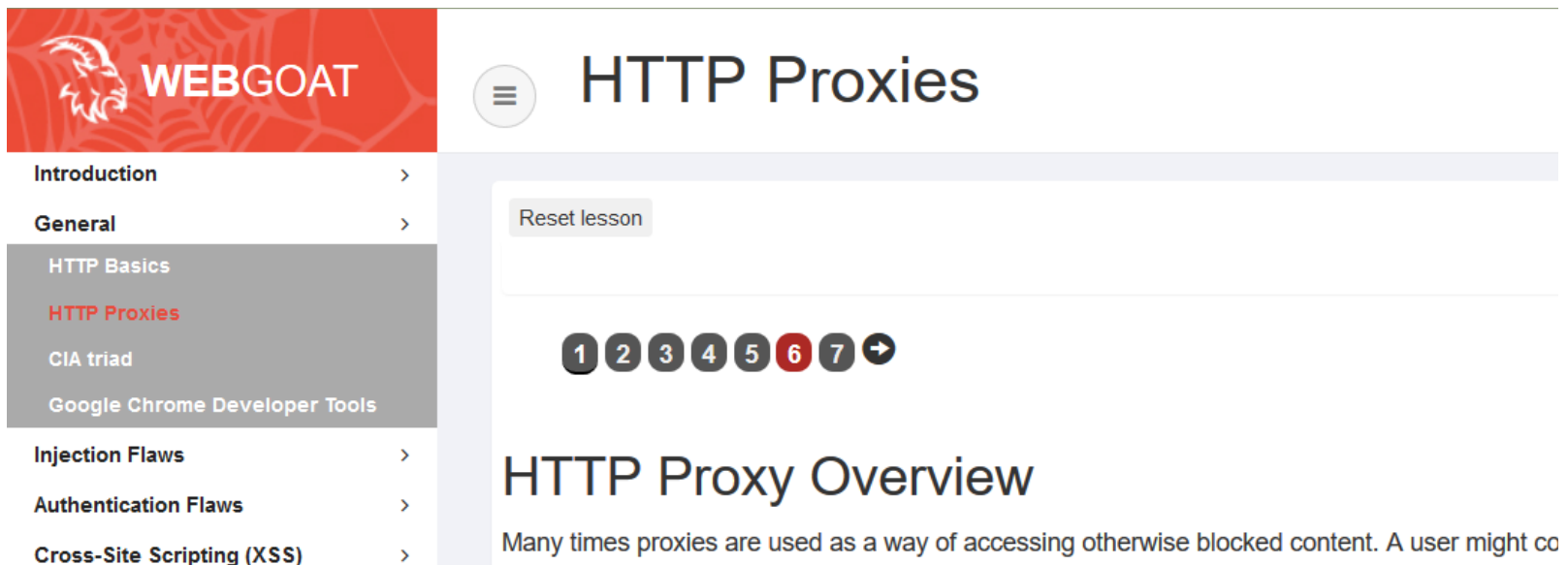
- Once WebGoat is set up, you want to log in to the web interface
- Open Firefox (preferred) and browse to:
<http://localhost:8080/WebGoat>
- You will need to create an account

WebWolf

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

Zap

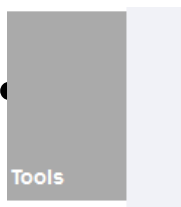
- Once you have set up WebGoat and WebWolf, you will eventually need to set up Zap. You can see the instructions under General → HTTP Proxies
- Needed for General → HTTP Basics



The screenshot displays the WebGoat application interface. On the left is a red sidebar with the WebGoat logo and a list of navigation items: 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 light blue box containing a 'Reset lesson' button. Underneath this is a progress indicator consisting of seven numbered circles (1-7) and a right arrow; the sixth circle is highlighted in red. The main heading 'HTTP Proxy Overview' is displayed in a large font, followed by a paragraph of introductory text: 'Many times proxies are used as a way of accessing otherwise blocked content. A user might co'.

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:



Report card:

