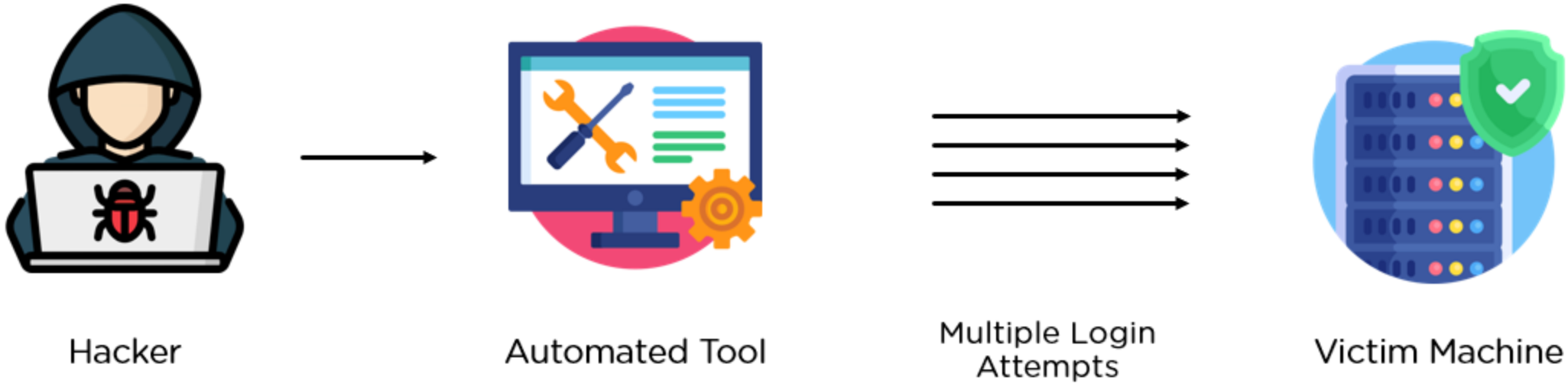
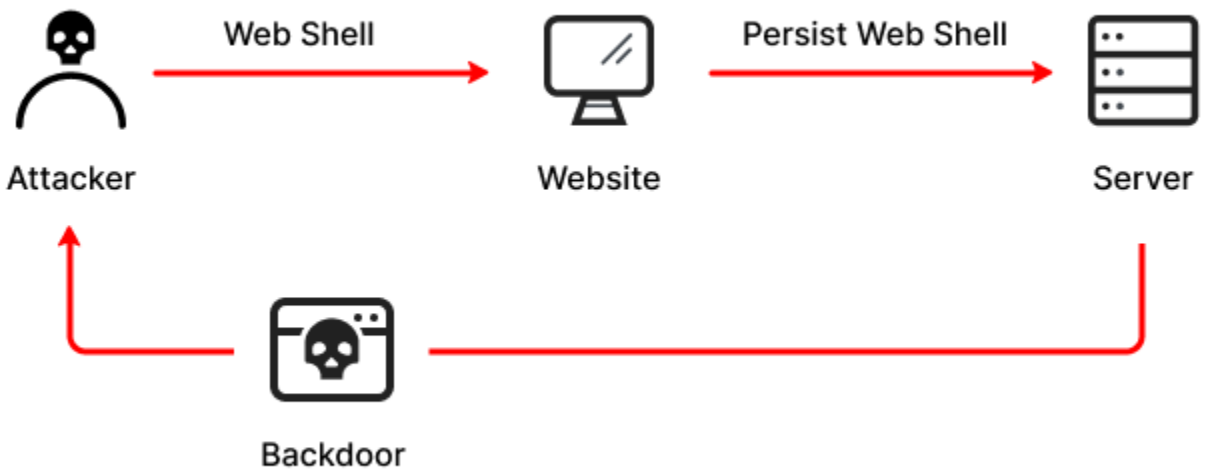
Getting Started with OWASP Zed Attack Proxy (ZAP) for Web Application Penetration Testing

INSTALLING AND SETTING UP YOUR ZAP ENVIRONMENT

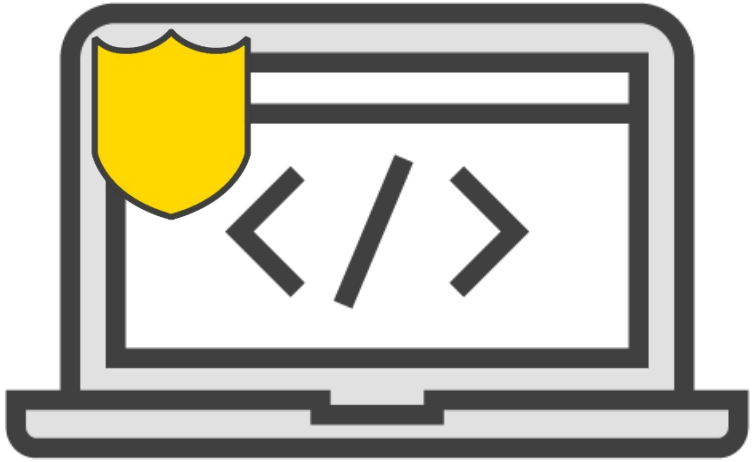

Hacker
Automated Tool
Multiple Login Attempts
Victim Machine


Web Shell
Persist Web Shell
Attacker
Website
Server
Backdoor

Open Web Application Security Project (OWASP)

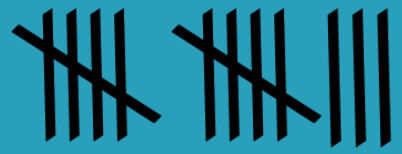
OWASP

Open Web Application Security Project




OWASP
Open Web Application
Security Project

CheatSheets 

Code 

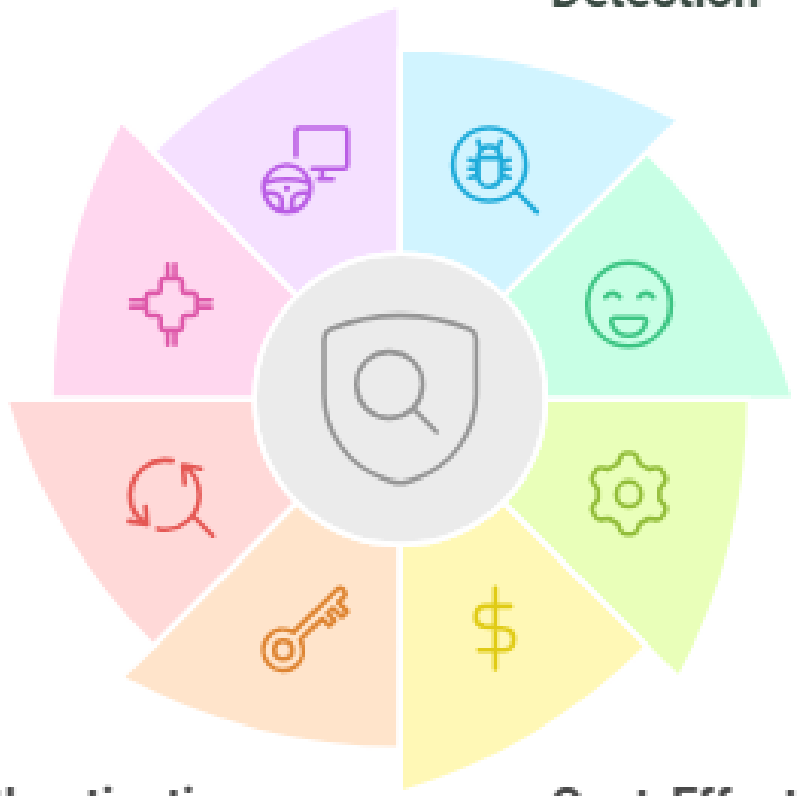
Documents 

Contests 

Research 

Tools 

Key Benefits of OWASP ZAP



Comprehensive Vulnerability Detection

Ease of Use

Integration with DevSecOps Pipelines

Cost-Effective

Authentication Testing

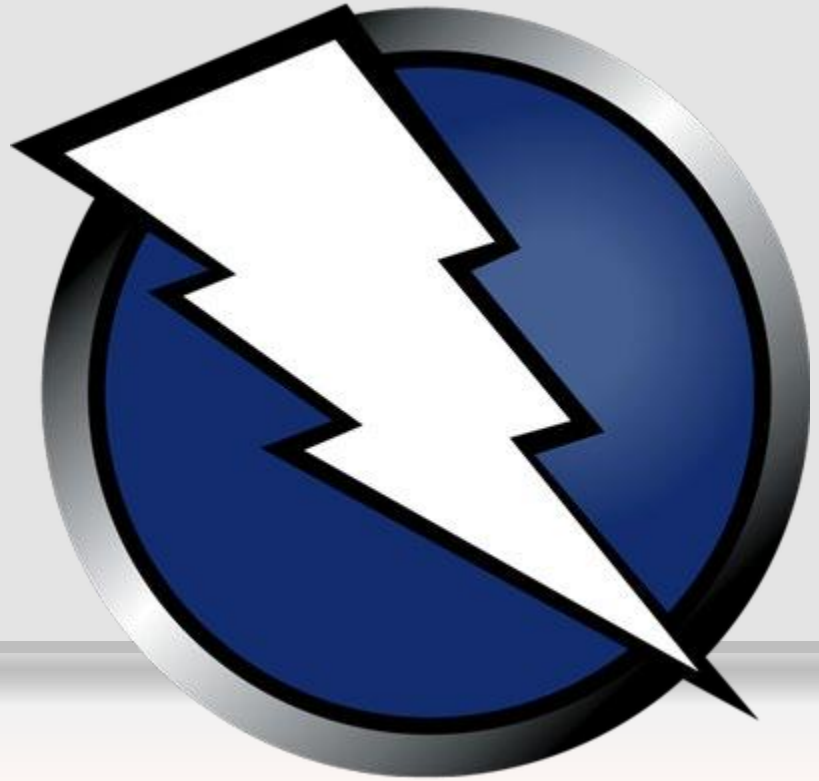
Cross-Platform Compatibility

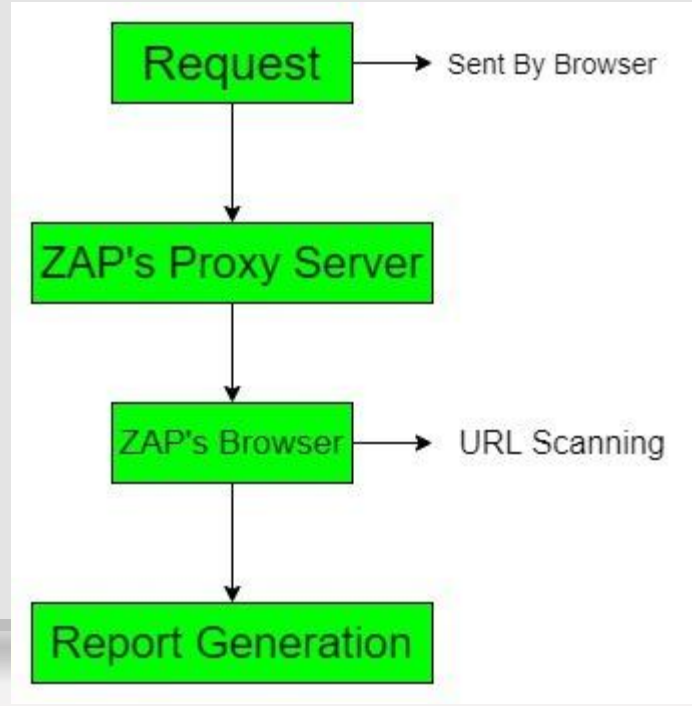
Real-Time Traffic Interception

Real-World Testing Scenarios

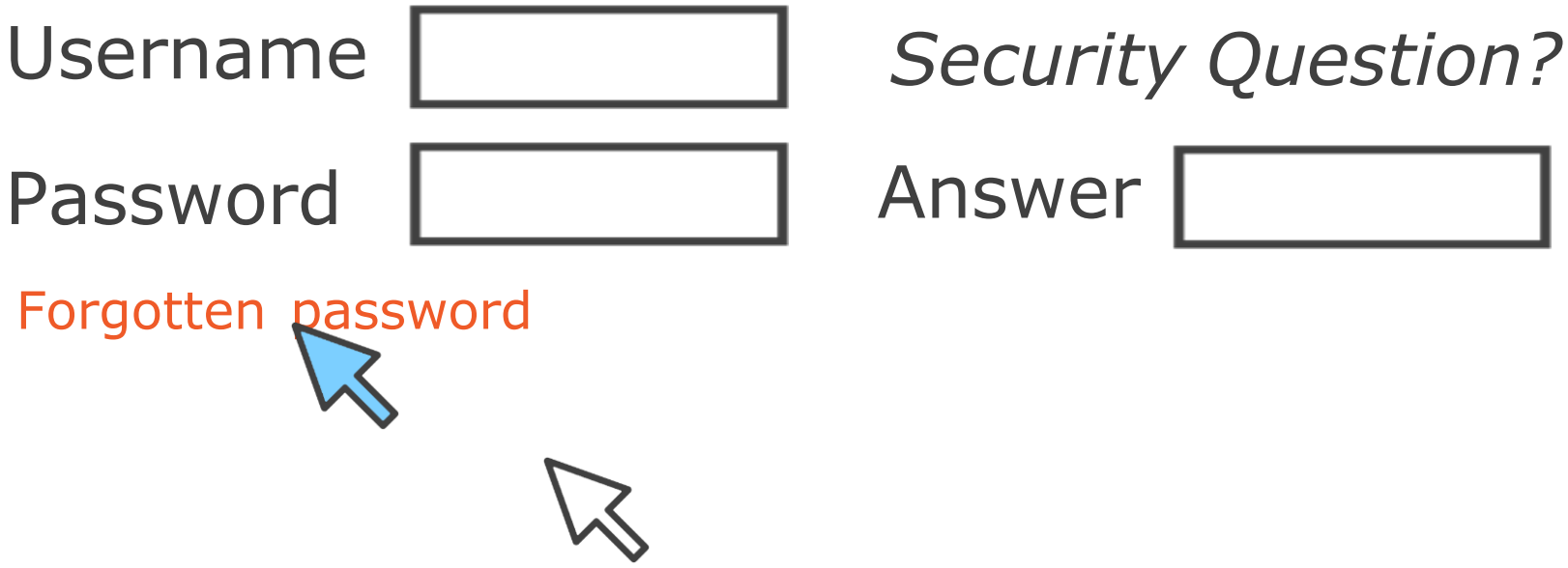
https://qaontop.com/how-to-perform-api-security-testing-with-owasp-zap/

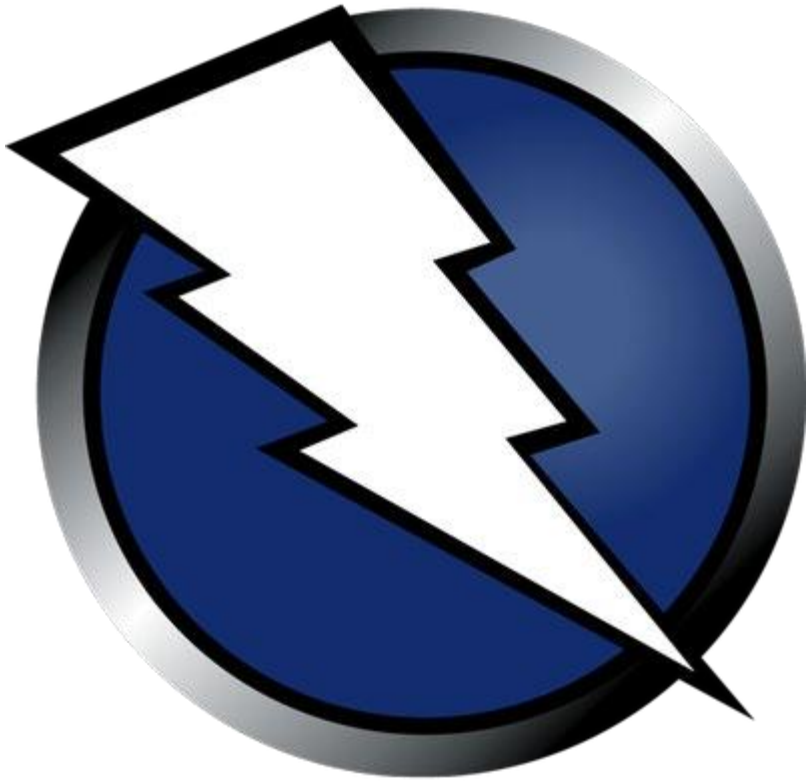
Zed Attack Proxy





Logic Flaws


Username
Password
Forgotten password
Security Question?
Answer
"values": {
"id": "198832",
"security question": "Wh
"security answer": "Nort
"email address": "mike@
}

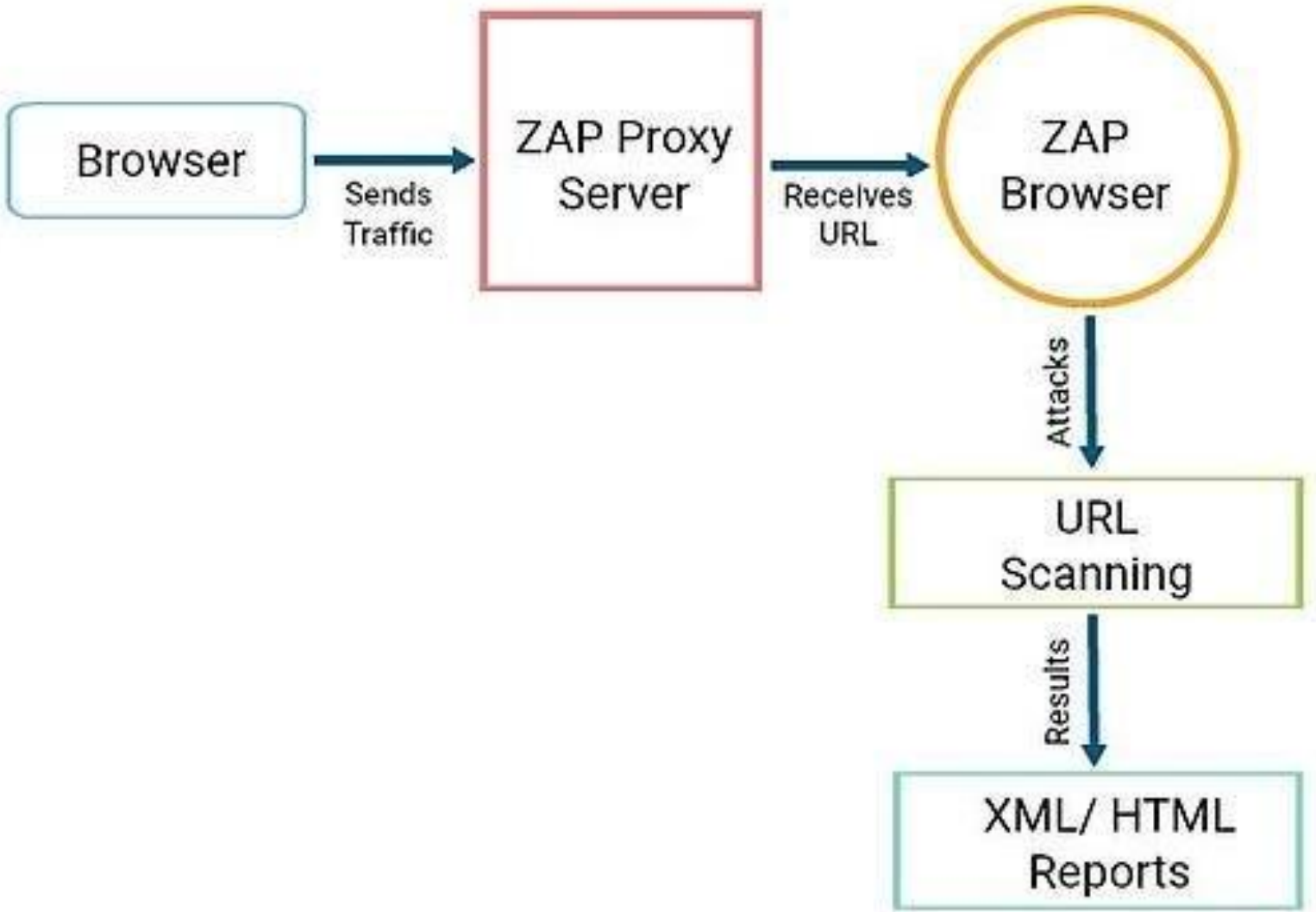


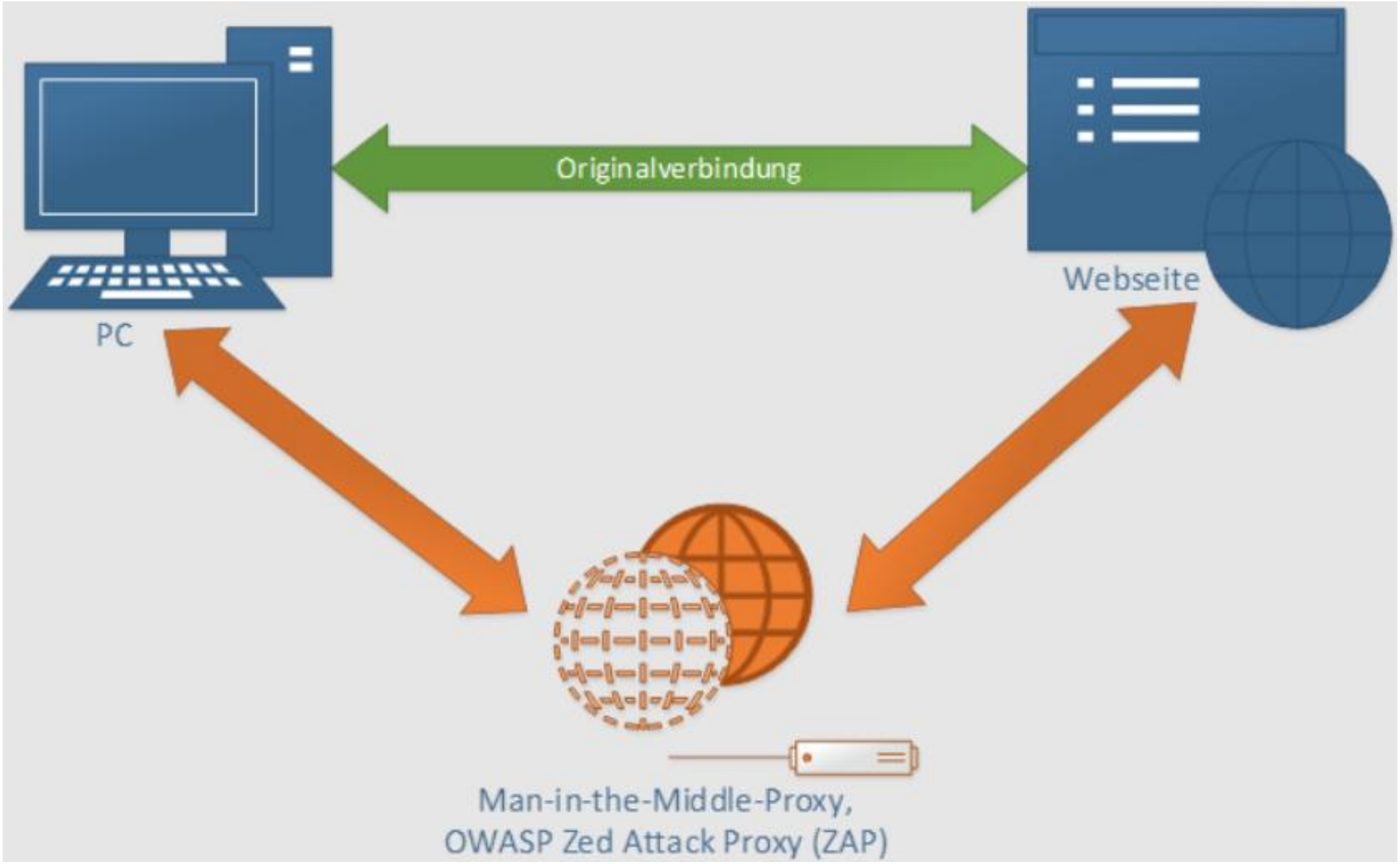
Project Leader

Simon Bennetts @psiinon

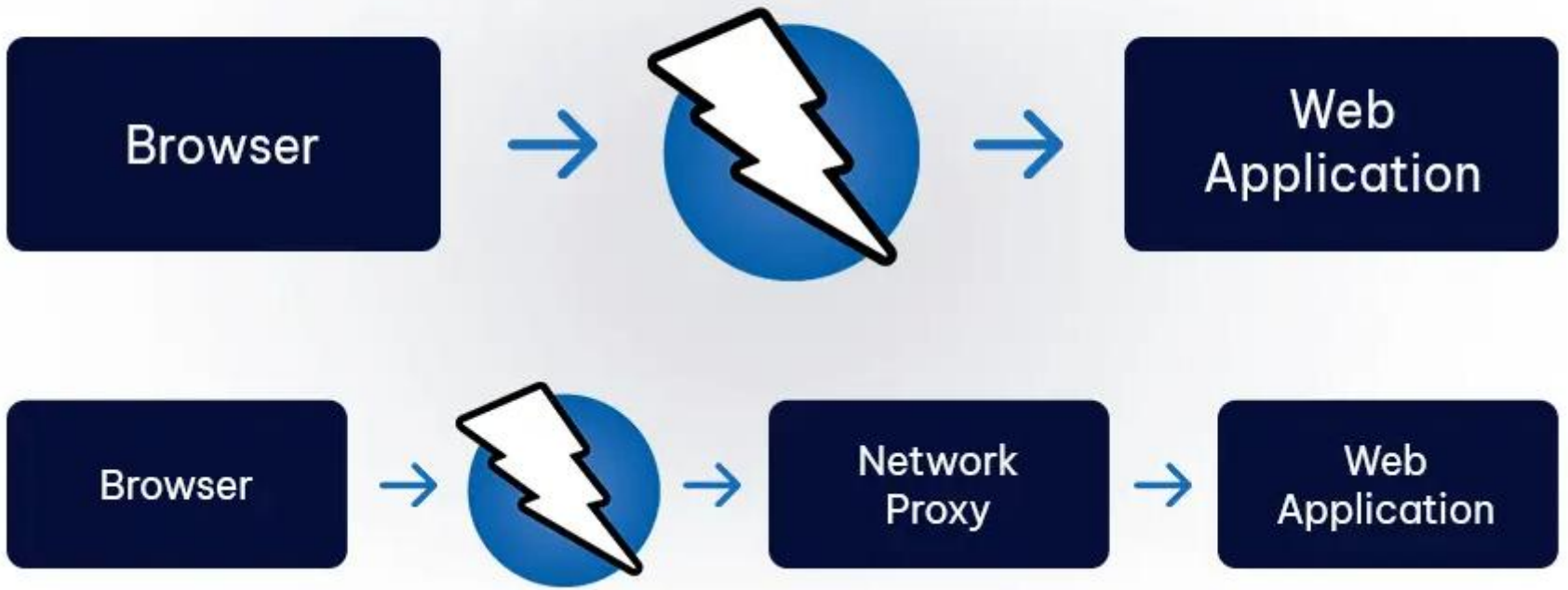
Downloads

- https://java.com *(7 or higher, not required for Mac)*
- https://www.zaproxy.org/download/


Browser
Sends Traffic
ZAP Proxy Server
Receives URL
ZAP Browser
Attacks
URL Scanning
Results
XML/ HTML Reports


Originalverbindung
PC
Webseite
Man-in-the-Middle-Proxy,
OWASP Zed Attack Proxy (ZAP)

ZAP Tool Guide



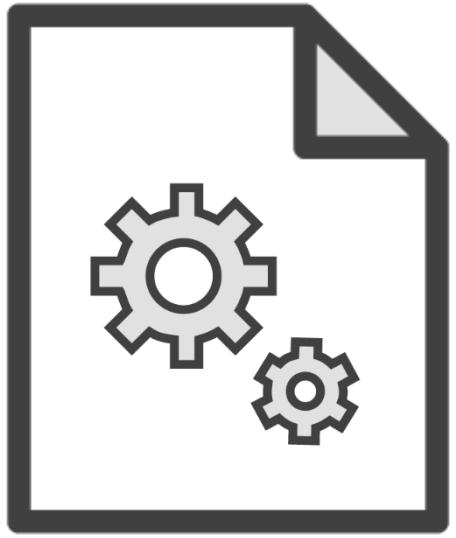
ZAP User Interface

Launching the Application

Application
.exe

Java
.jar

Shell Script
Linux: .sh

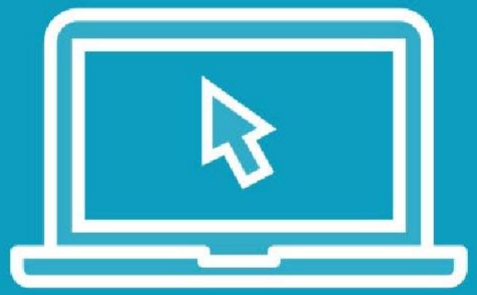


Batch File
.bat

Command Line Options

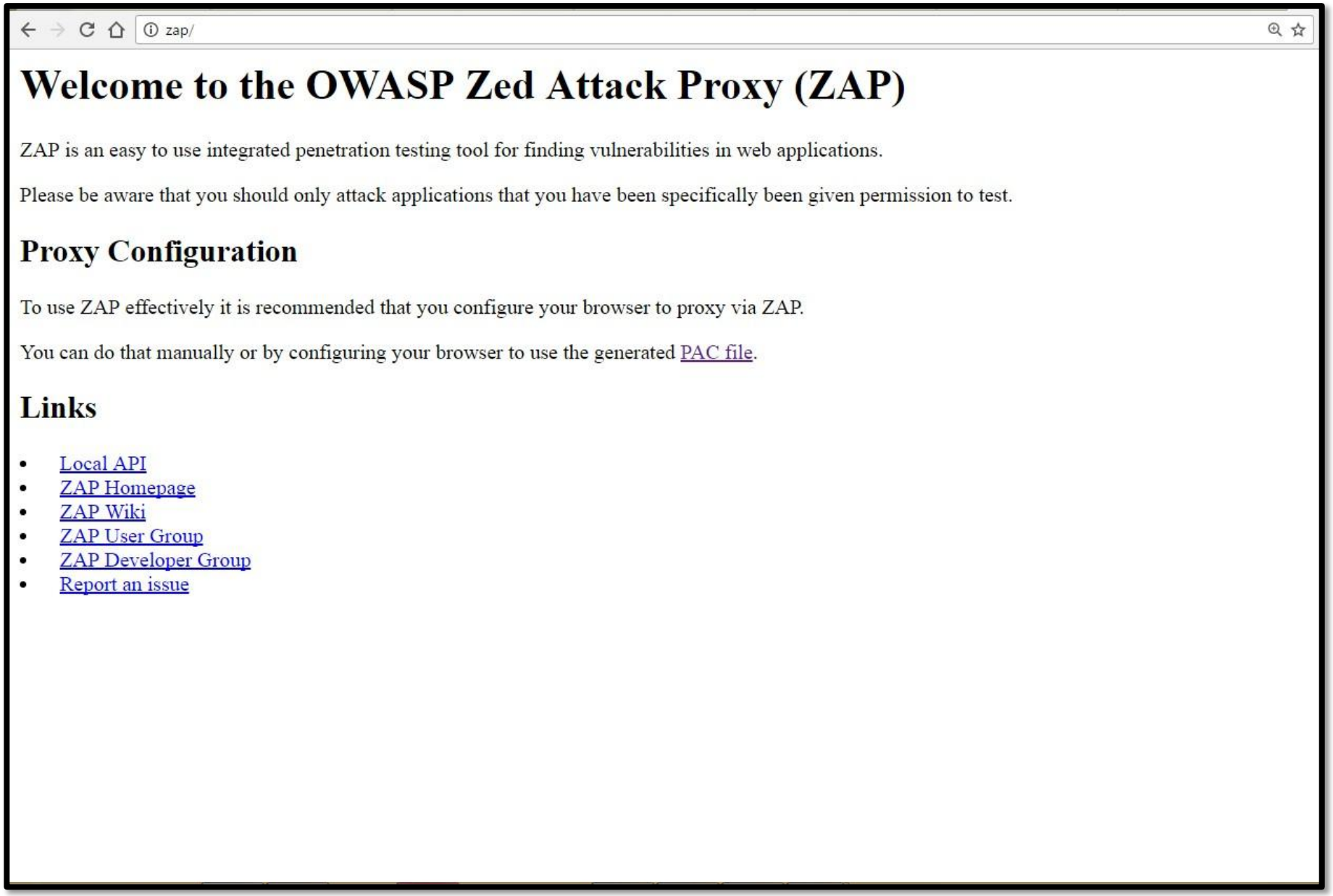
-config	Overrides specified key=value in config file
-daemon	Start in ‘daemon’ mode
-host	Override host used
-port	Override port used
-newsession	Create newsession at a given location
-session	Open given session

Demo



Walkthrough of ZAP UI

http://zap


zap/
Welcome to the OWASP Zed Attack Proxy (ZAP)
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
Proxy Configuration
To use ZAP effectively it is recommended that you configure your browser to proxy via ZAP.
You can do that manually or by configuring your browser to use the generated PAC file.
Links
Local API
ZAP Homepage
ZAP Wiki
ZAP User Group
ZAP Developer Group
Report an issue

Review

Persistent Session

- Yes > save for later
- No > temporary work. Delete on exit

Tree Window

- Set the context
- Target the scope

Workspace Window

- Request
- Response
- Scripts

Review

Information Window

- History
- Tool details

Toolbar

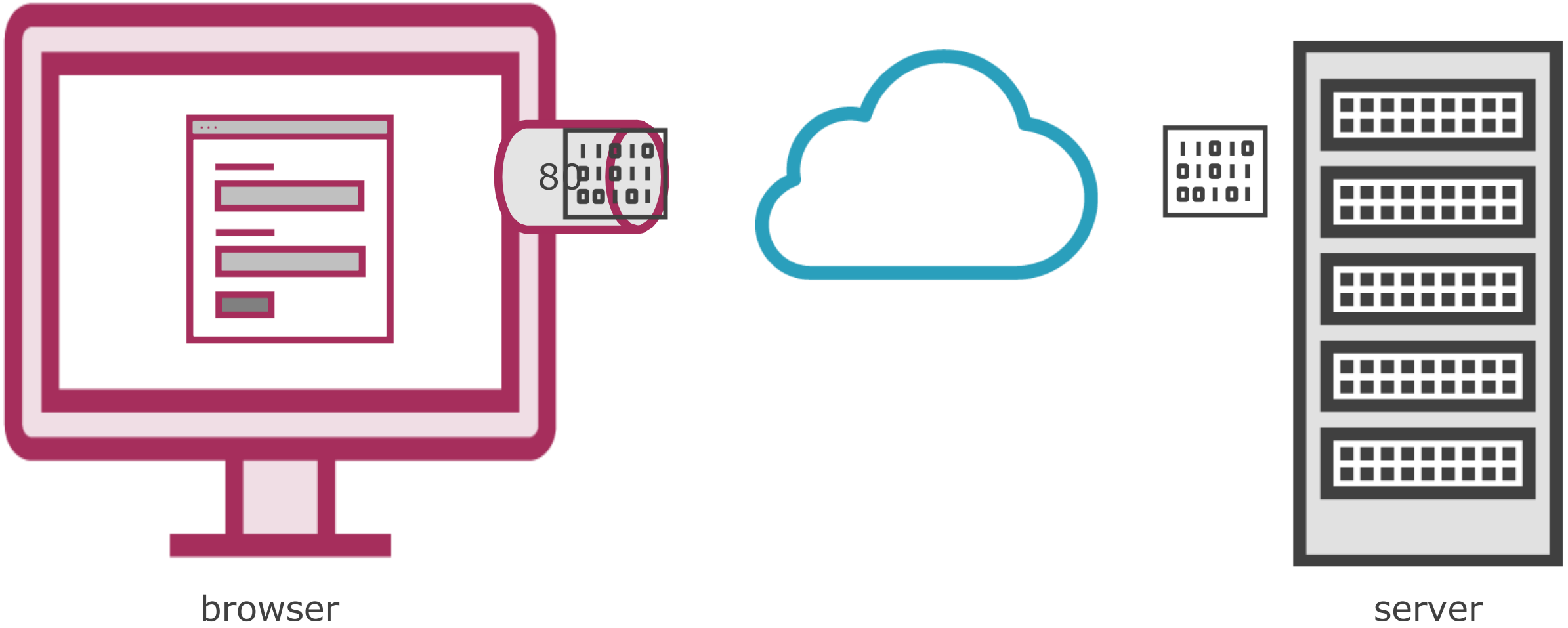
- Mode
- Break Point Advancement

Proxy Setup

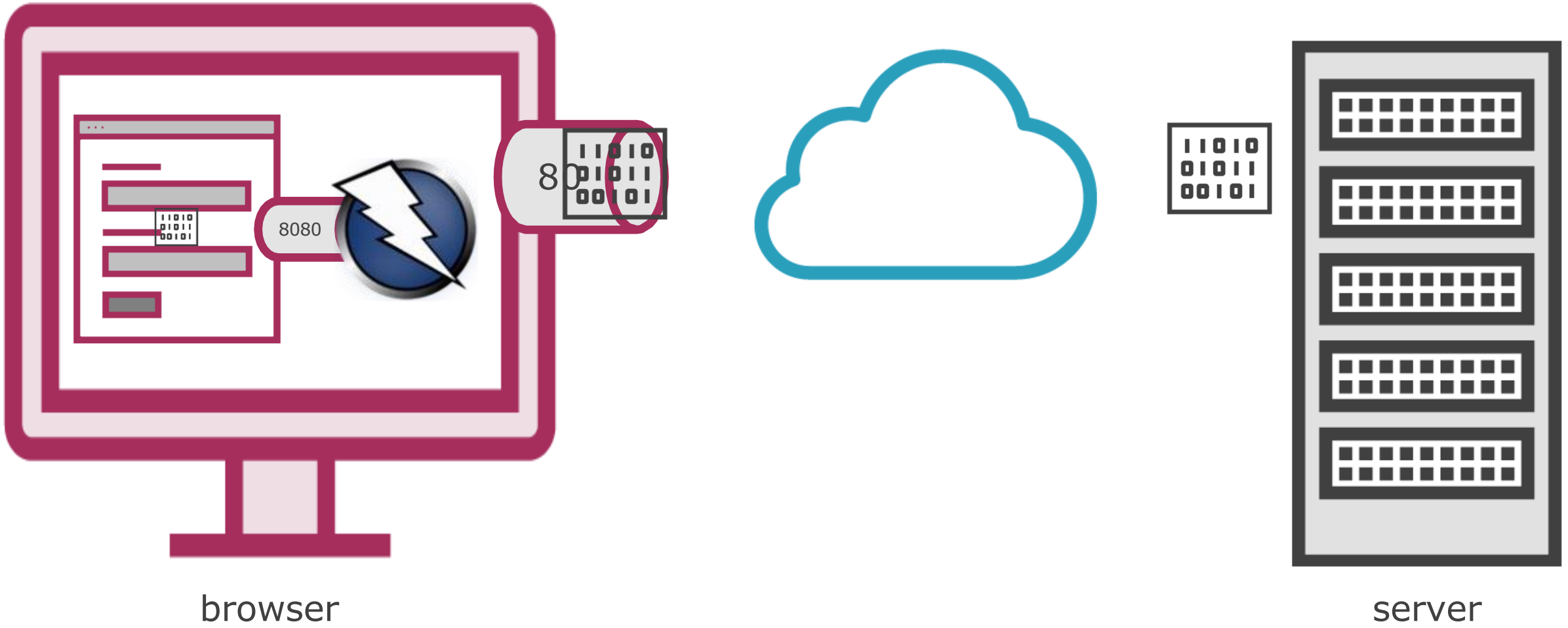
Proxy

Authority or power to act on behalf of or substitute for another.

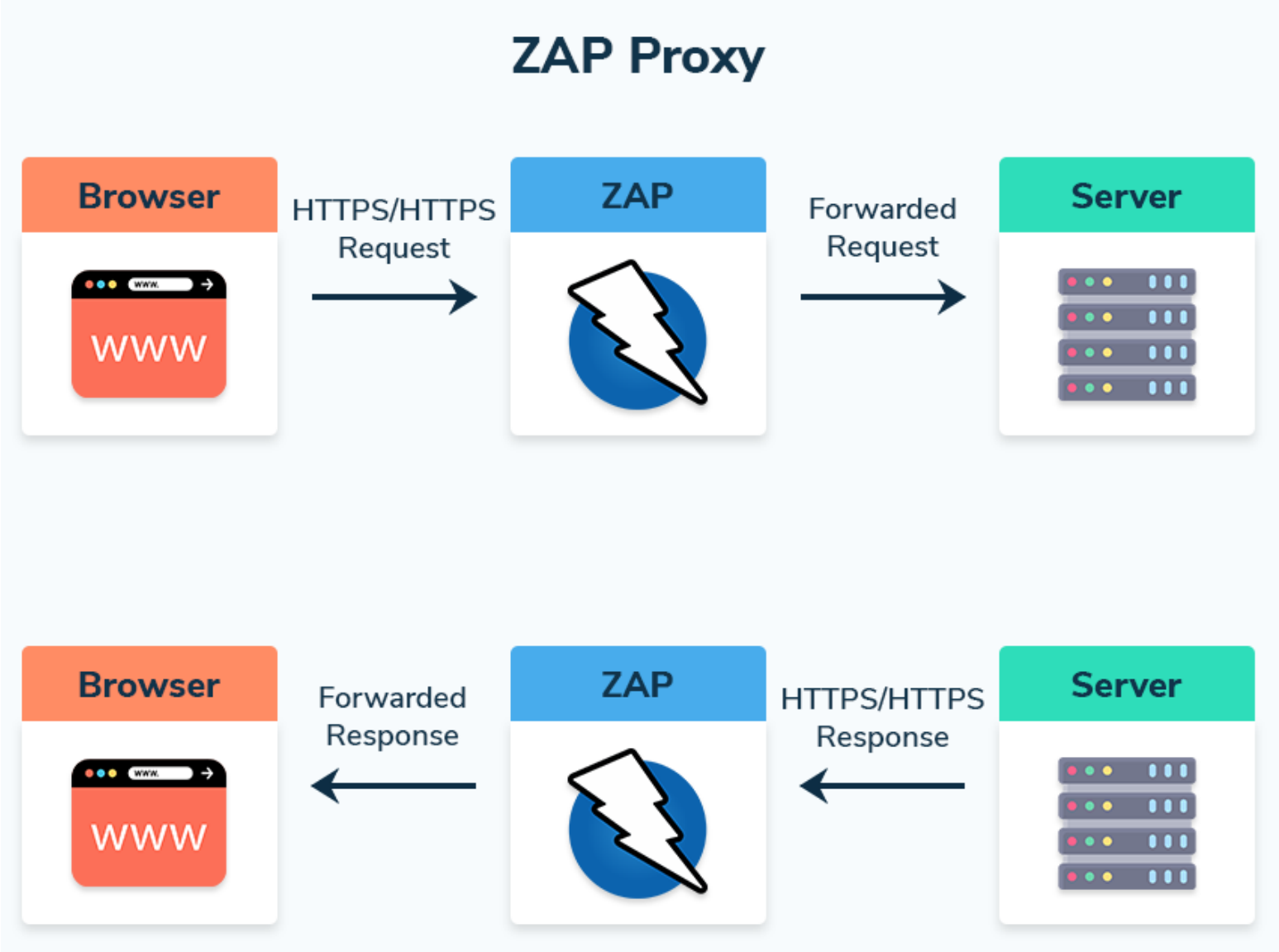
Proxy Web Traffic Through ZAP



Proxy Web Traffic Through ZAP



Proxy Web Traffic Through ZAP



Manual Proxy Configurations

- Menu > settings
- Search Settings
- “Proxy”
- Open proxy settings

- Menu > settings
- Advanced
- System

- Menu > options
- Network Settings
- *Settings…* button

Manual Proxy Configurations

Localhost // 127.0.0.1

Port: 8080 *(or port of choice)*

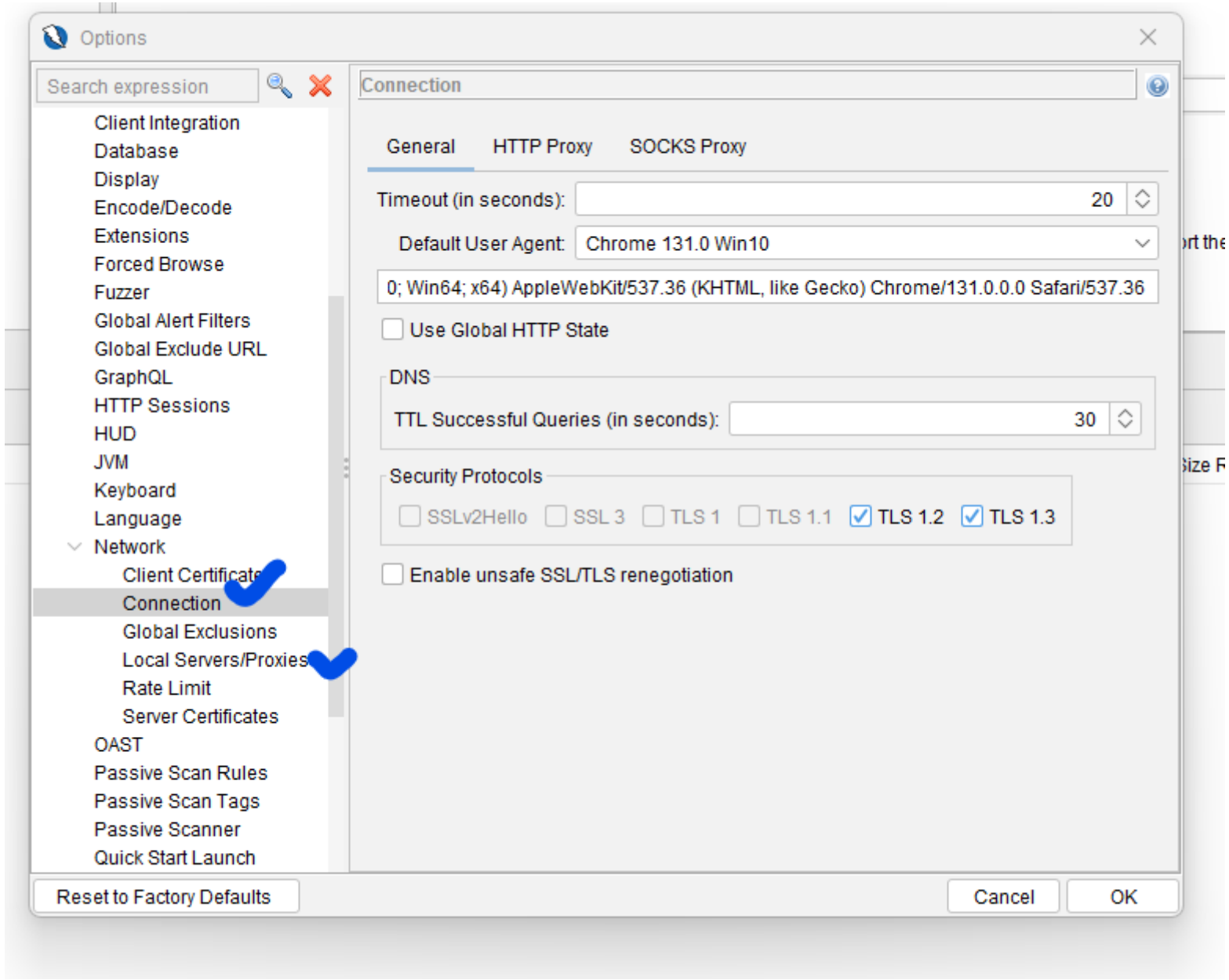
FoxyProxy Basic

FireFox

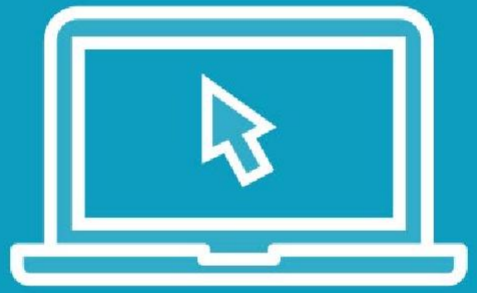
- Menu > Add-ons
- Search ‘FoxyProxy’

Chrome

- Google.com/chrome
- Click ‘Extensions’
- Search ‘FoxyProxy’


Options
Search expression
Client Integration
Database
Display
Encode/Decode
Extensions
Forced Browse
Fuzzer
Global Alert Filters
Global Exclude URL
GraphQL
HTTP Sessions
HUD
JVM
Keyboard
Language
Network
Client Certificate
Connection
Global Exclusions
Local Servers/Proxies
Rate Limit
Server Certificates
OAST
Passive Scan Rules
Passive Scan Tags
Passive Scanner
Quick Start Launch
Connection
General
HTTP Proxy
SOCKS Proxy
Timeout (in seconds):
20
Default User Agent:
Chrome 131.0 Win10
0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Use Global HTTP State
DNS
TTL Successful Queries (in seconds):
30
Security Protocols
SSLv2Hello
SSL 3
TLS 1
TLS 1.1
TLS 1.2
TLS 1.3
Enable unsafe SSL/TLS renegotiation
Reset to Factory Defaults
Cancel
OK

Demo



Complete proxy setup inside of ZAP

Reminder

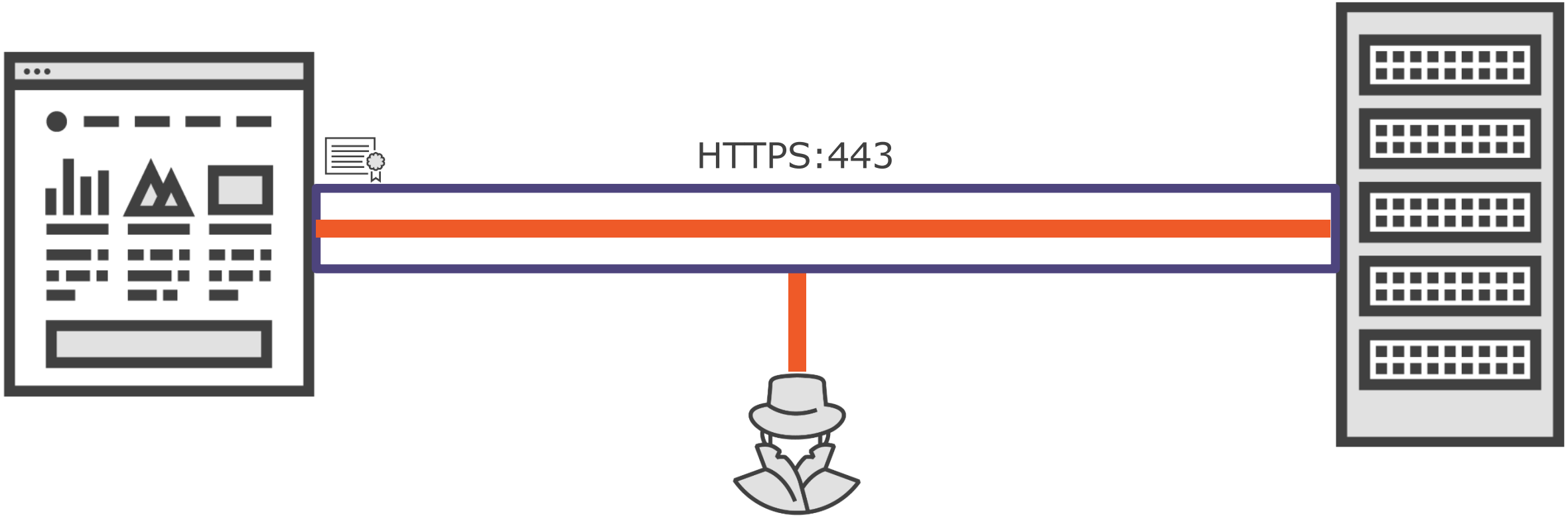
At this point, you should see browser traffic in ZAP. You can turn it off for now

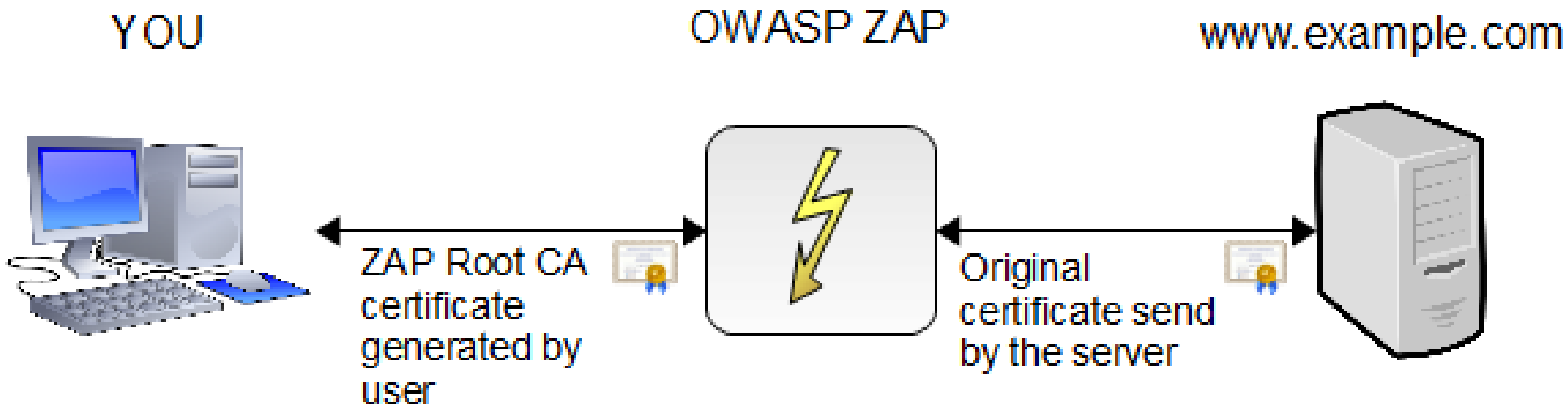
Only turn on your proxy service when you are ready to attack

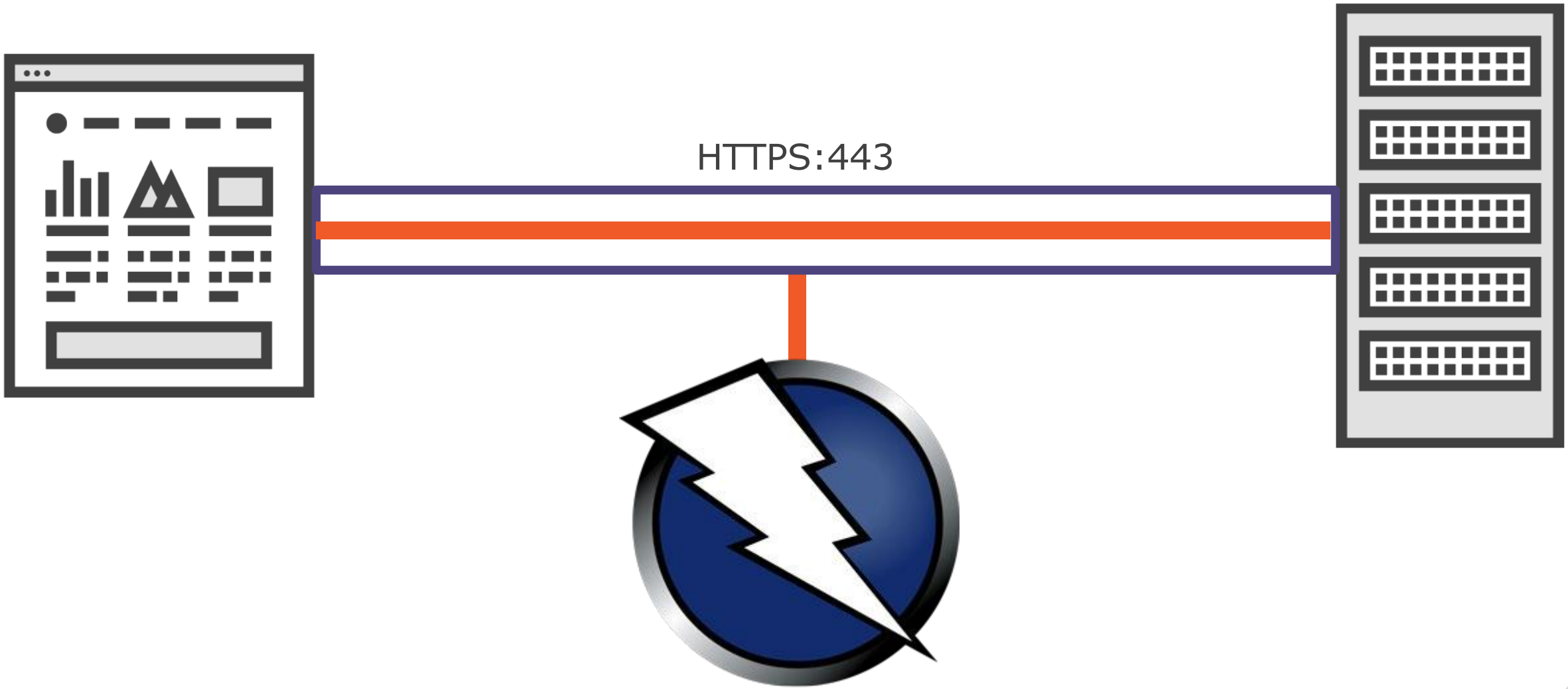
If you receive browser page errors after turning on the proxy service:

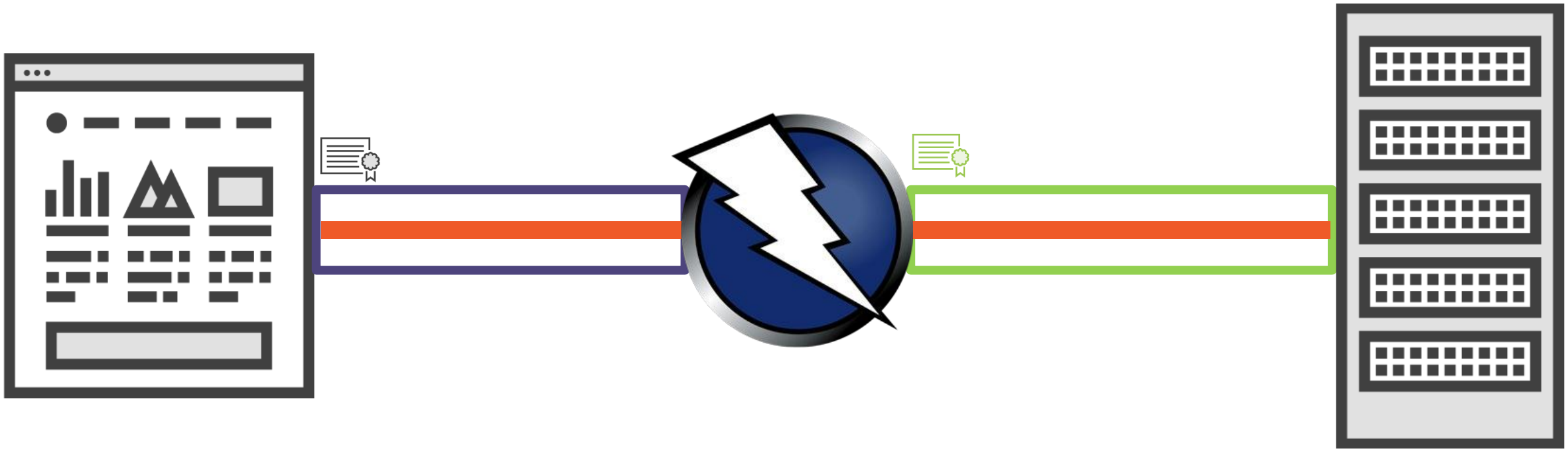
- Check to make sure ZAP is running
- If it is, make sure the ports are right
  - Check ZAP options
  - Check browser proxy options
- If accessing an https page, you may need to load the ZAP certificate

Browser Certificate

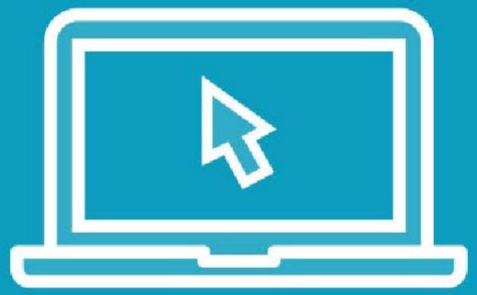

HTTPS:443


YOU
OWASP ZAP
www.example.com
ZAP Root CA certificate generated by user
Original certificate send by the server


HTTPS:443

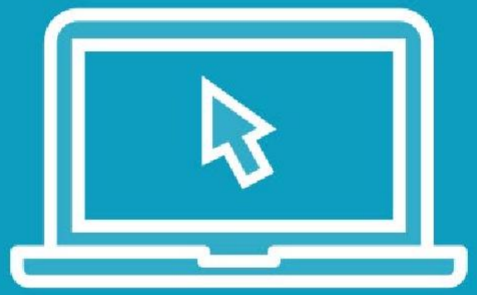

Hello!
0101011
1101010
Hello!
0111100
001010
Hello!

Demo



1. Open ZAP > Tools > Options
2. Select Dynamic SSL Certificates in menu
3. Click Generate button
4. Click Save button (remember location)
5. Navigate to certificate file
6. Right Click > Install Certificate
7. Next
8. Check “Place all certificates in the following store”
9. Browse > Trusted Root Certification Authorities > Ok
10. Next > Finish

Demo



Firefox Users…

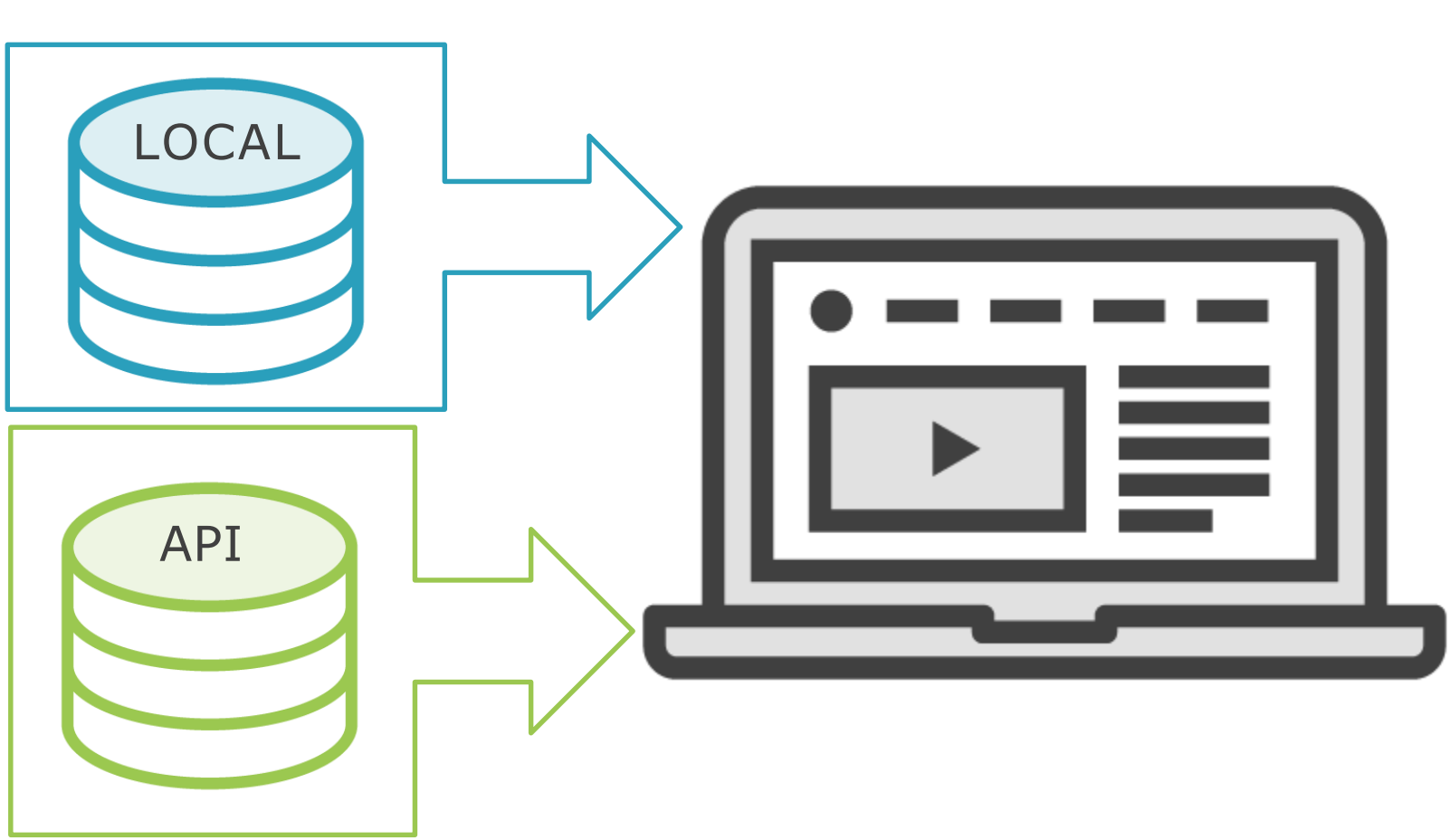
1. Click Menu Bars
2. Click Options
3. Click Privacy & Security in menu
4. Scroll down to Certificates section
5. Click View Certificates button
6. Click Import button
7. Navigate to certificate and select it
8. Check box to Trust this CA to identify websites
9. Click OK

Setting Up a Legal Target

Important Note

By law, you are only permitted to pentest, hack, assess web applications you own or have permission to test.

Context is Important



local

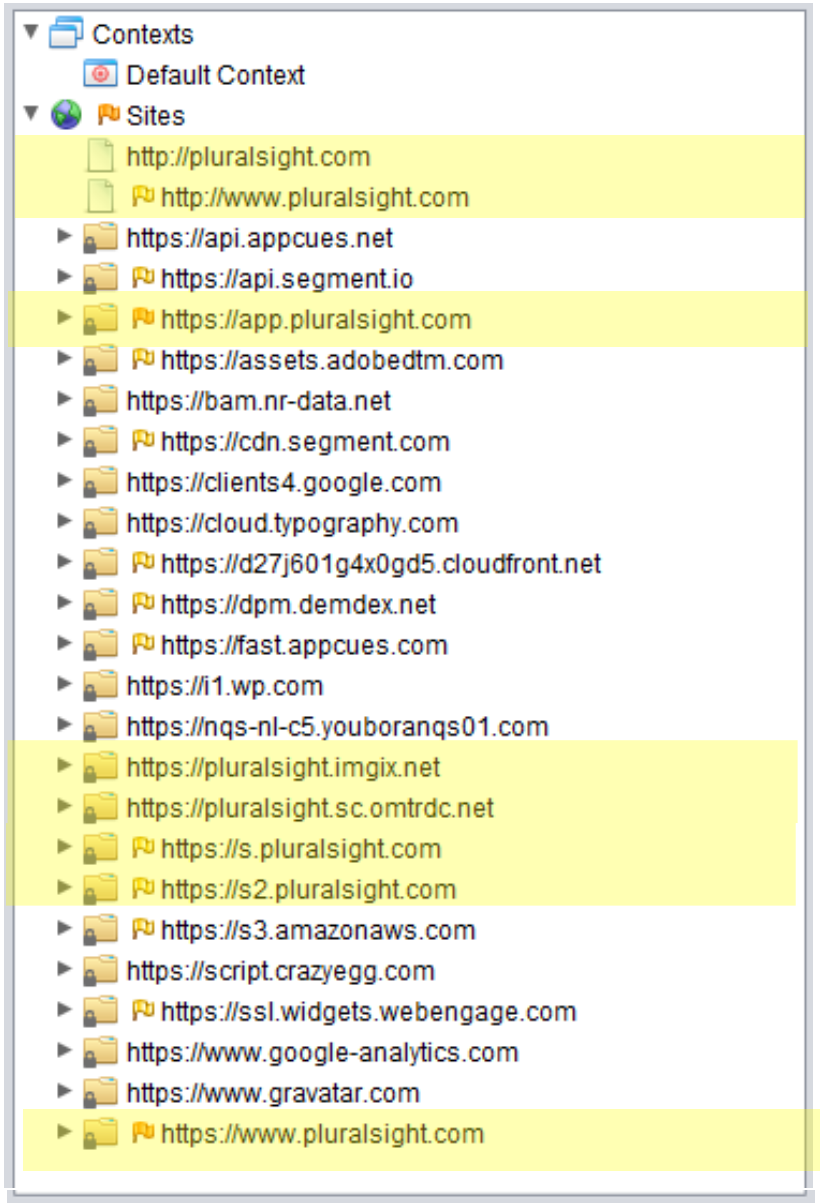
local

XYZ.com

youtube

API

Context Is Important



OWASP BWA (Broken Web Applications) is a pre-built virtual machine that bundles many *intentionally vulnerable* web apps (e.g., DVWA, WebGoat, Mutillidae, bWAPP, etc.) so you can safely practice web-app security testing and tool usage in an isolated lab. You import the VM (OVA) into VirtualBox/VMware, boot it, and browse to the hosted apps to learn and experiment.

Key points

•**Purpose:** Hands-on training for web security—manual testing, scanner/tool evaluation, and attack observation—without building each lab from scratch.

•**Distribution:** Downloadable OVA/VM images (most used release is 1.2) hosted on SourceForge.

Status: It's an **older project** (latest published VM from 2015) and is largely **not actively maintained**, but still useful for practice. **Login tip:** On first boot, typical console creds are `root` / `owaspbwa` (then access the apps via the VM's IP in your browser).

VirtualBox

Download

https://www.virtualbox.org/wiki/Downloads

OWASP BWA *(Broken Web Application)*

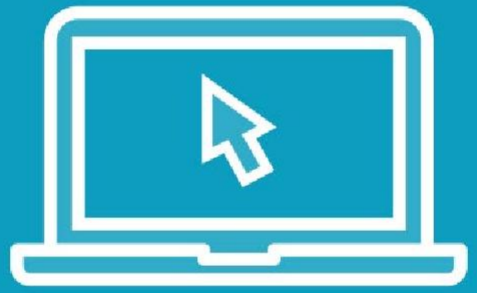
Website

https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project
https://www.vulnhub.com/entry/owasp-broken-web-applications-project-12,46/

Download

https://sourceforge.net/projects/owaspbwa/files/

Demo



Launching OWASP BWA

Introduction to

- bWAPP
- Security Shepherd

OWASP Juice Shop vs WebGoat

OWASP Juice Shop is a deliberately insecure, modern web app (Node.js/Express + Angular) packed with vulnerabilities across the OWASP Top 10 and beyond. It's used for hands-on security training, awareness demos, CTFs, and as a target for tools like OWASP ZAP.

What makes it great

Huge challenge set with built-in **scoreboard** showing categories, difficulty, and progress.

CTF-ready: run instances per participant, use a central score server, and generate flags with juice-shop-ctf-cli.

Actively maintained with frequent releases (e.g., v18.0.0 in 2025)

OWASP WebGoat is an intentionally vulnerable, Java/Spring web app maintained by OWASP for learning and practicing web-application security. It ships with guided lessons and challenges that mirror real-world flaws (OWASP Top 10 and more).

What's inside

WebGoat: the main training app with hands-on labs and a built-in progress/lesson flow.

WebWolf: a companion "attacker's helper" app used by some labs (e.g., receiving emails, hosting files) so attack traffic stays in your lab environment. Many lessons don't need it; enable it when a lab calls for it.

Summary

OWASP

ZAP UI

Setting up the browser to talk to ZAP through proxy settings

Browser Certificate

Legal concerns

Setting up a lawful target