Web Application Penetration Testing with Burp Suite

SETTING UP YOUR BURP SUITE ENVIRONMENT

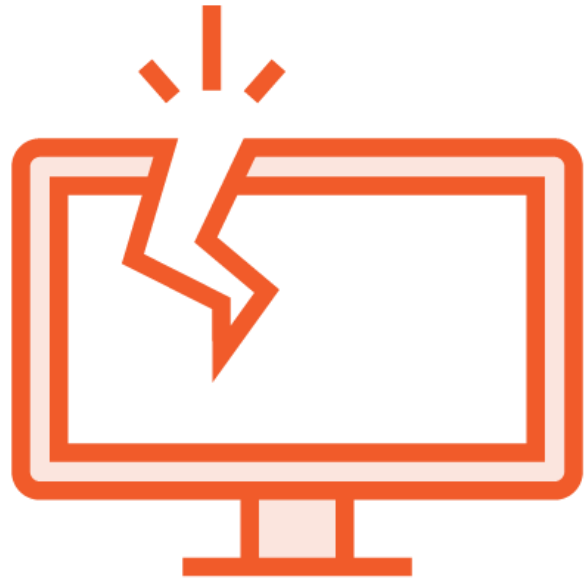
Sunny Wear
SECURITY ARCHITECT AND PENETRATION TESTER
@SunnyWear www.sunnywear.org

Why a Proxy Service

Intercepting Proxy

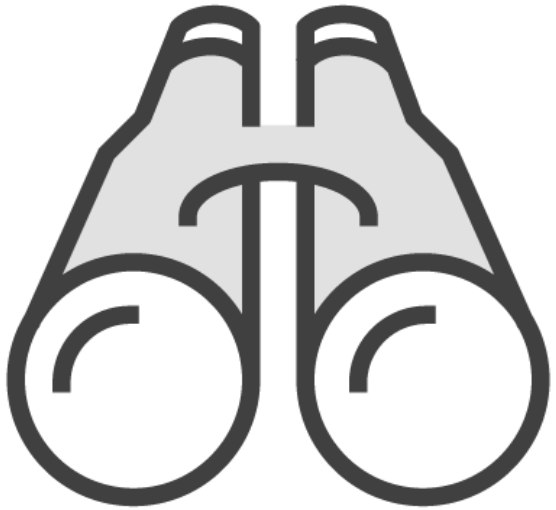
Penetration Testers

Web Traffic



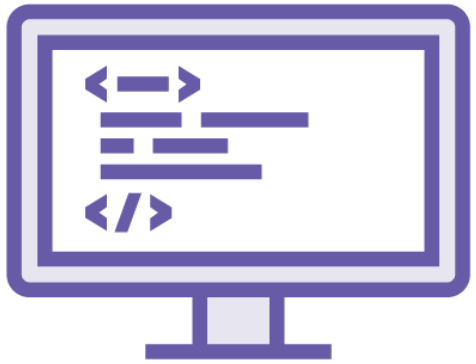
Manipulate

Objective



Observe Behavior

Proxy Traffic Through



Browser
Browses the web application with local proxy setting to 127.0.0.1 port 8080

Burp Suite Proxy
HTTP and HTTPS traffic flows through

Web Application
This is your target

Need a Legal Target

Priya Pentester

Image yourself here

Target Web Application

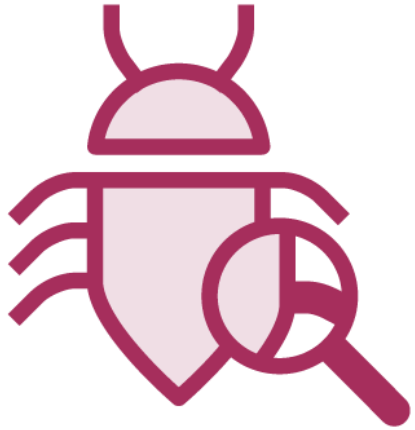
Intentionally vulnerable web application called DVWA

DVWA

An intentional vulnerable web application

http://www.dvwa.co.uk/

Demo



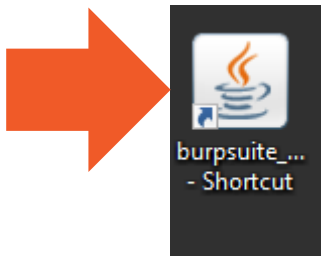
Launching Burp Suite Against Your Target

Burp Suite Product Options

Free	Professional
Most functionality tabs are enabled	All functionality tabs are enabled
Intruder functionality is throttled	No forced throttling
Payloads not available	Portswigger Payloads
Some plugins not available	Supports all plugins

Options for Burp Launch

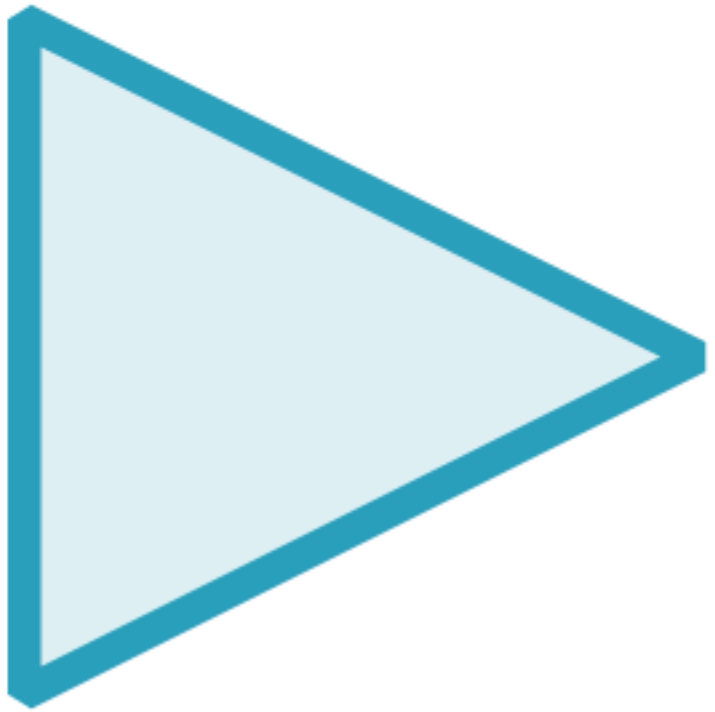
Double-click



Command line

```
c:\BurpSuite>java -jar -Xmx2g burpsuite_pro_v1.7.04.jar
```

Splash Screen



Proxy HTTP Traffic Through Burp

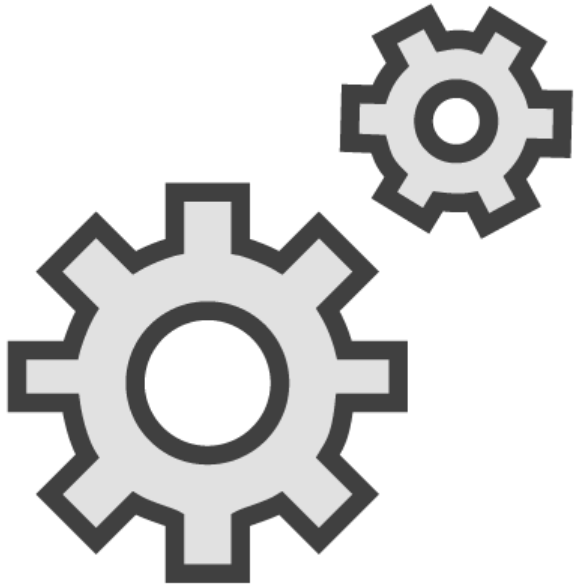
Browser
Firefox's local proxy setting to 127.0.0.1 Port 8080

Burp Suite Proxy
HTTP and HTTPS traffic flows through

Web Application
This is your Target

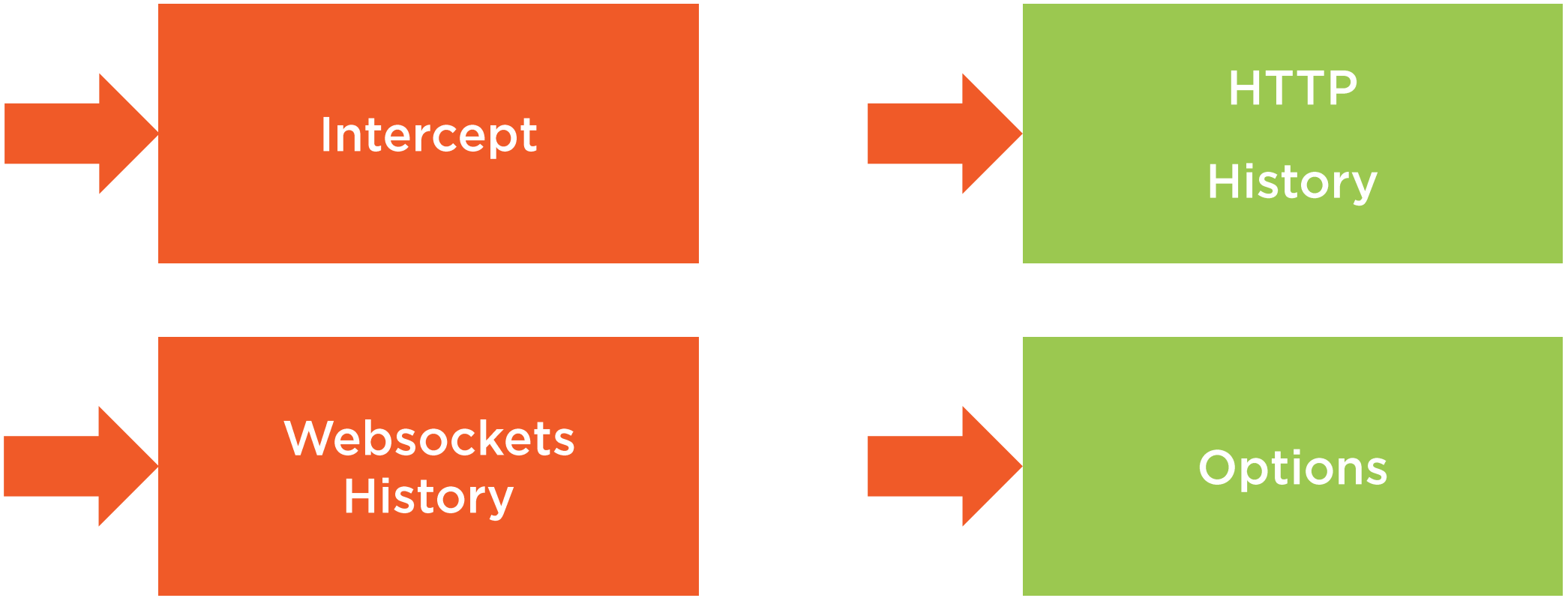
DVWA

Demo



Configuring Burp Proxy

Proxy “tabs”



Intercept Button

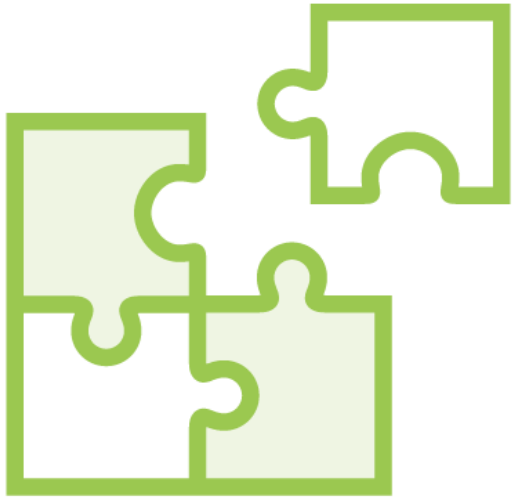
On / Off

Message Editor

Raw

Params

Headers



Hex

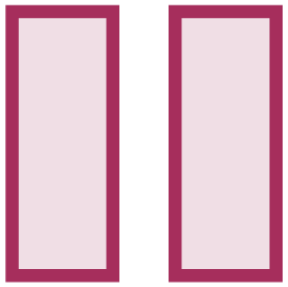
HTTP History

Historical Table

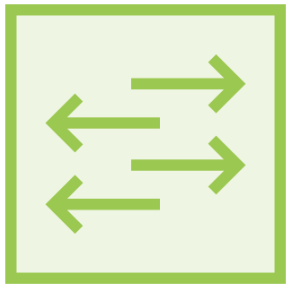
- Host, URL, Content-Length
- Sortable columns
- Non-editable

Proxy Options

Proxy Listeners



Intercept Client Requests



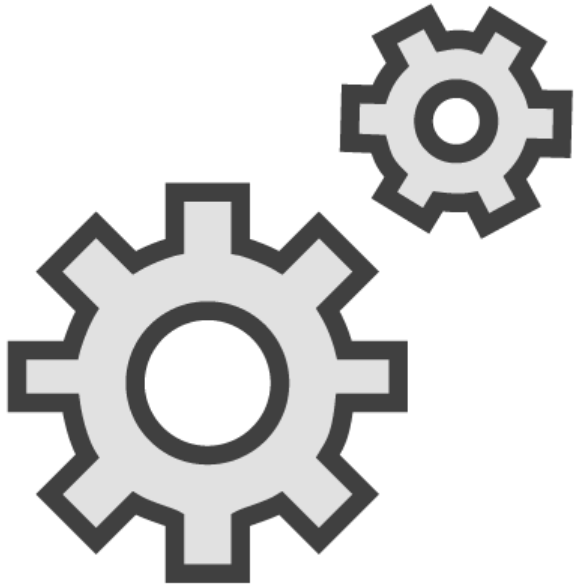
Intercept Server Responses

Response Modification

Match and Replace

SSL Pass Through

Demo



Trusting Portswigger in Your Browser

HTTPS

Encryption

Eavesdropping

Burp to Target

SSL/TLS Handshake

Trust Portswigger

Certificate Authority (CA)

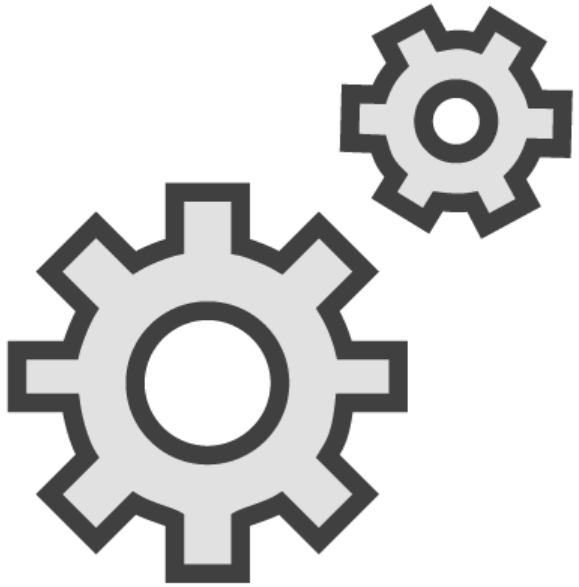
Browser Trust

Your Browser

Portswigger Certificate

Private Key

Demo



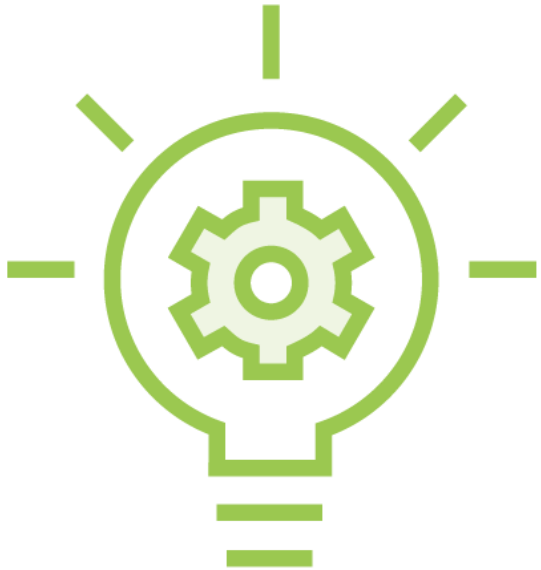
Setting up Your Configuration File

Configuration Option Levels

User-level

Project-level

Demo



Setting up Your Project File

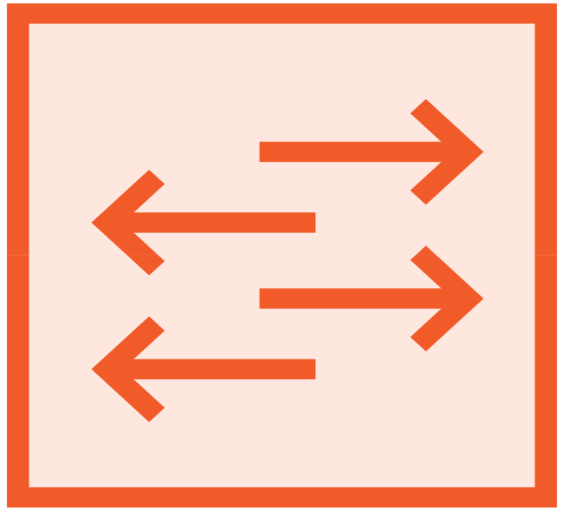
Project Files

Data

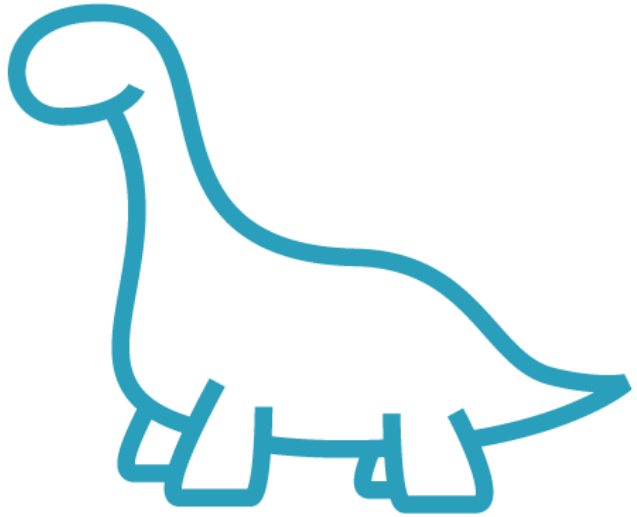
Configuration

Session State Files

Scope and content



Replacement

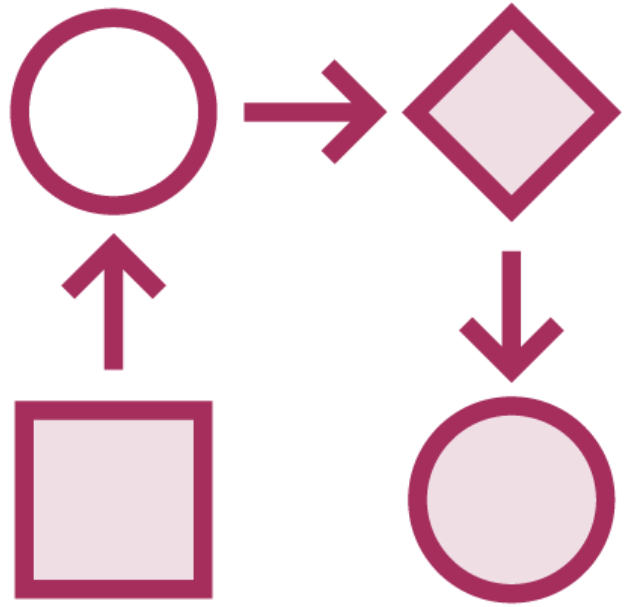


Deprecated

Session State vs Project Files

Session State	Project
Target Scope(s)	Target Scope(s)
Discovered Content	Discovered Content
Extenders	Extenders
Custom Proxy Settings	Custom Proxy Settings
Custom User Option Settings	Custom User Option Settings
	Automatic Saves
	Faster reload
	Scanner’s issue activity log

Demo



Summary

Environment and Configurations

Discovery and Attack