



# Security Engineering

## Lecture 14 – Web Application Hacking Lab Federica Paci

- **How to create the virtual environment**
- **Hacking Exercises**
  - SQL Injection
  - Broken Authentication
  - Forced Browsing
  - XSS
    - Phishing with XSS
    - Stored
    - Reflected
  - CSRF

- **Proxy: OWASP ZAP**
- **Browser: Firefox**
- **Vulnerable Web Application: OWASP WebGoat**
- **Runtime Environment: JAVA 7**
- **Virtual Machine: Oracle VirtualBox**

- **Download Virtual Box from**
  - <https://www.virtualbox.org/wiki/Downloads>
- **Download Ubuntu.ova**
  - [192.168.131.7/~sweng000/](http://192.168.131.7/~sweng000/)
- **Run Virtual Box and Import Ubuntu.ova**
  - Go to File → Import Appliance in the menu bar
  - Click the Open Appliance button to select Ubuntu.ova file
  - Click Import
  - If the import succeeds, you should see the Ubuntu Virtual Machine in your list
  - Go Devices → Network → Disconnect Network Adapter

- **Right Click on Ubuntu in the left pane of the Oracle VM VirtualBox Manager App and hit “Start”**
- **Virtual Machine Password**
  - **securityvm**

# Run OWASP ZAP



- **Open a Terminal**
- **Type**
  - `cd Documents/WebApp/ZAP_2.3.1`
  - `sudo ./zap.sh`

# Run OWASP ZAP



File View Analyse Report Tools Online Help

File mode [Icons]

Scripts [Quick Start] [Request] [Response] [Break] [Script Console]

## 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 given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack:

Progress: Not started

For a more in depth test you should explore your application using your browser or automated regression tests while proxying through

If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:

Configure your browser:

Spider Forced Browse Fuzzer Params Http Sessions Zest Results Clients WebSockets AJAX Spider Out

History Search Break Points Alerts Active Scan

Filter: OFF

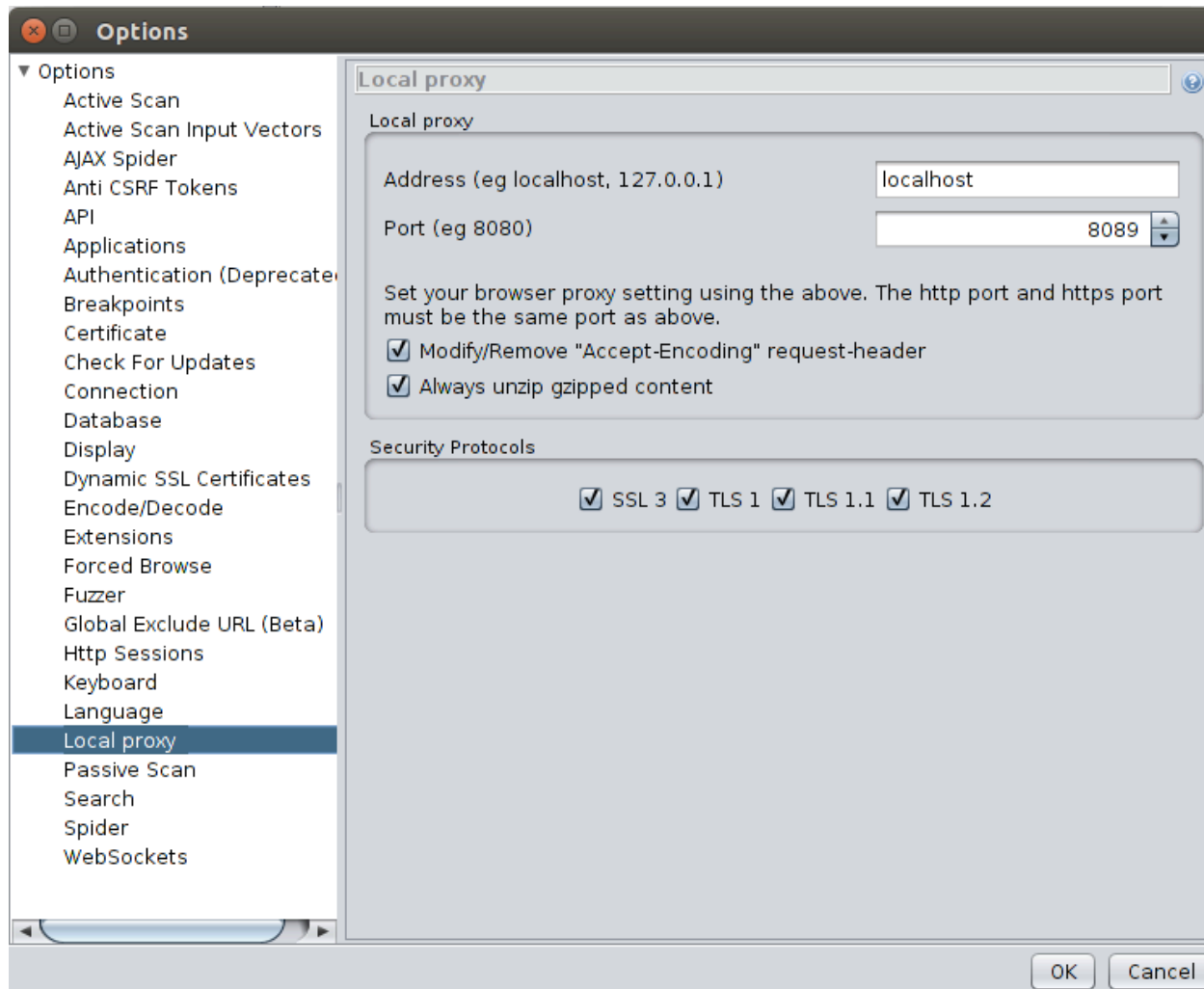
Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
----------------	--------	-----	------	--------	-----	-----------------	---------------	------	------

Current Scans [Icons]

# Configure ZAP



- Go to Tools → Option → Local Proxy

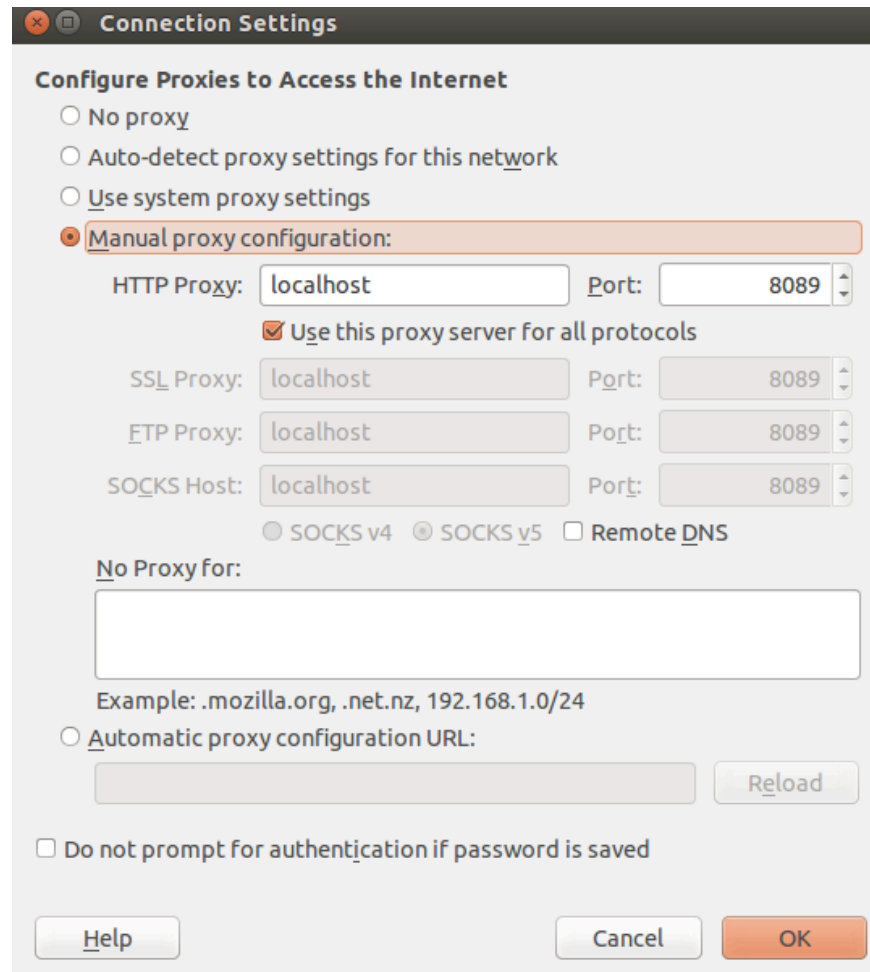




# Configure ZAP as a Proxy



- Open Firefox
- Go to Preferences → Advanced → Network → Settings



The screenshot shows the 'Connection Settings' dialog box in Firefox. The title bar reads 'Connection Settings'. The main heading is 'Configure Proxies to Access the Internet'. There are four radio button options: 'No proxy', 'Auto-detect proxy settings for this network', 'Use system proxy settings', and 'Manual proxy configuration:'. The 'Manual proxy configuration:' option is selected and highlighted. Below this, there are four rows of proxy settings, each with a text input field for the host and a spin button for the port. The first row is for 'HTTP Proxy', with 'localhost' in the host field and '8089' in the port field. Below this row is a checked checkbox labeled 'Use this proxy server for all protocols'. The second row is for 'SSL Proxy', with 'localhost' and '8089'. The third row is for 'FTP Proxy', with 'localhost' and '8089'. The fourth row is for 'SOCKS Host', with 'localhost' and '8089'. Below these rows are three radio button options: 'SOCKS v4', 'SOCKS v5' (which is selected), and 'Remote DNS'. There is a section titled 'No Proxy for:' with a large empty text input field. Below this field is an example: 'Example: .mozilla.org, .net.nz, 192.168.1.0/24'. There is a radio button option for 'Automatic proxy configuration URL:' with an empty text input field and a 'Reload' button. At the bottom, there is a checkbox for 'Do not prompt for authentication if password is saved'. The dialog box has three buttons at the bottom: 'Help', 'Cancel', and 'OK'.

# Run WebGoat



- **Open a Second Tab**
- **Type**
  - `cd Documents/WebApp`
- **Type**
  - `java -jar WebGoat-6.0.1-war-exec.jar`
- **Open Mozilla Firefox**
- **Type**
  - `localhost:8080/WebGoat`

# Run WebGoat

A screenshot of a web browser window. The address bar shows 'localhost:8080/WebGoat/login.mvc'. The page has a red header with 'WEBGOAT' and a main heading 'Please login'. There are two input fields: 'Username' with 'guest' and 'Password' with '.....'. A red 'Sign in' button is below. A table lists built-in accounts: Webgoat User (guest/guest) and Webgoat Admin (webgoat/webgoat).

age x +

localhost:8080/WebGoat/login.mvc

Google

**WEBGOAT**

## Please login

**Username**

**Password**

**Sign in**

The following accounts are built into Webgoat

Account	User	Password
Webgoat User	guest	guest
Webgoat Admin	webgoat	webgoat