UNIVERSITY OF TRENTO

Security Engineering

Lecture 14 – Web Application Hacking Lab

Federica Paci

Lecture Outline

UNIVERSITY OF TRENTO

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

Software

UNIVERSITY OF TRENTO

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

Setup Virtual Environment

UNIVERSITY OF TRENTO

- **Download Virtual Box from**
  - https://www.virtualbox.org/wiki/Downloads
- **Download Ubuntu.ova**
  - 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

Run Virtual Machine

UNIVERSITY OF TRENTO

- **Right Click on Ubuntu in the left pane of the Oracle VM VirtualBox Manager App and hit "Start"**

- **Virtual Machine Password**
  - securityvm

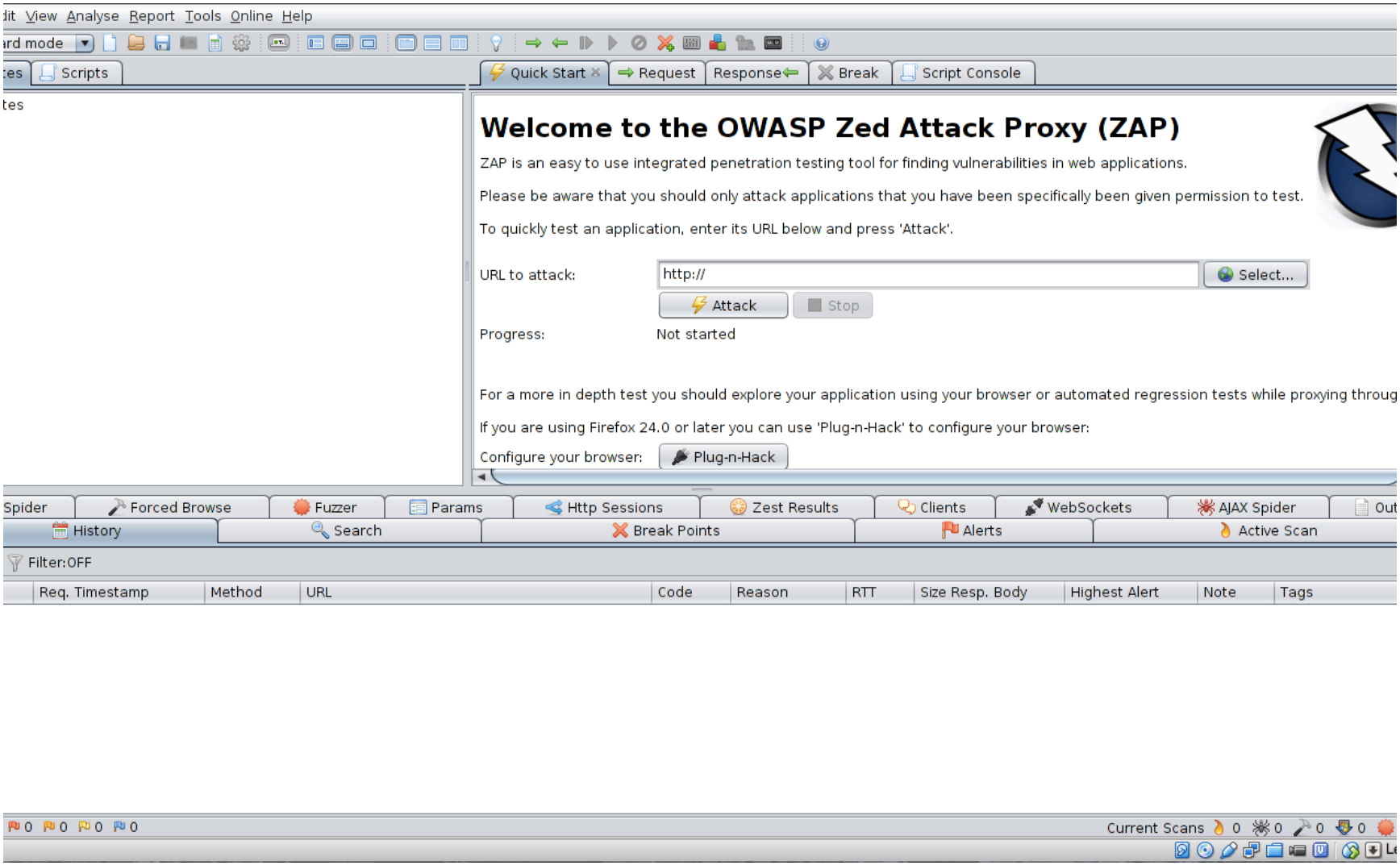
Run OWASP ZAP

UNIVERSITY OF TRENTO

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

Run OWASP ZAP

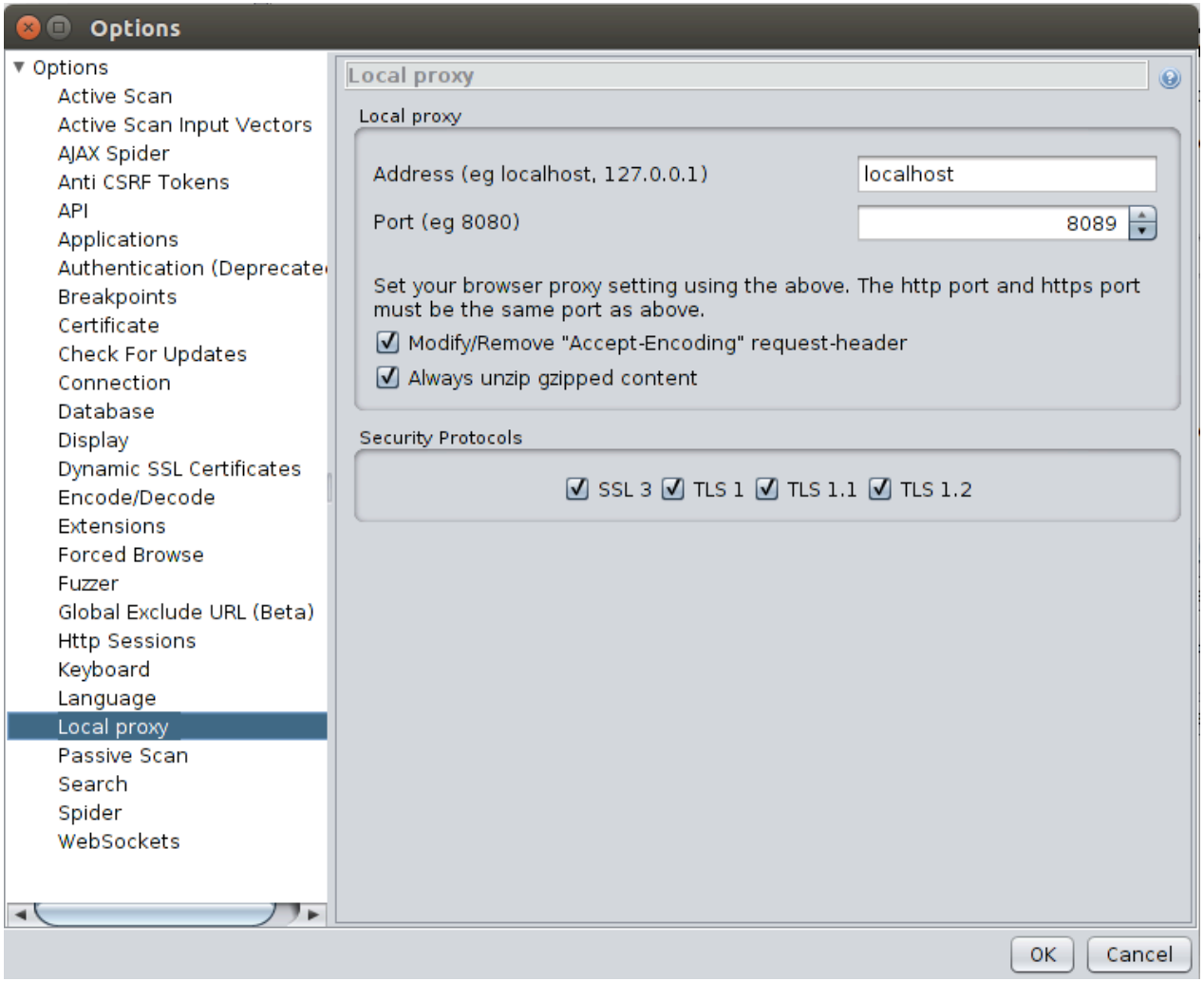
UNIVERSITY OF TRENTO



Configure ZAP

UNIVERSITY OF TRENTO

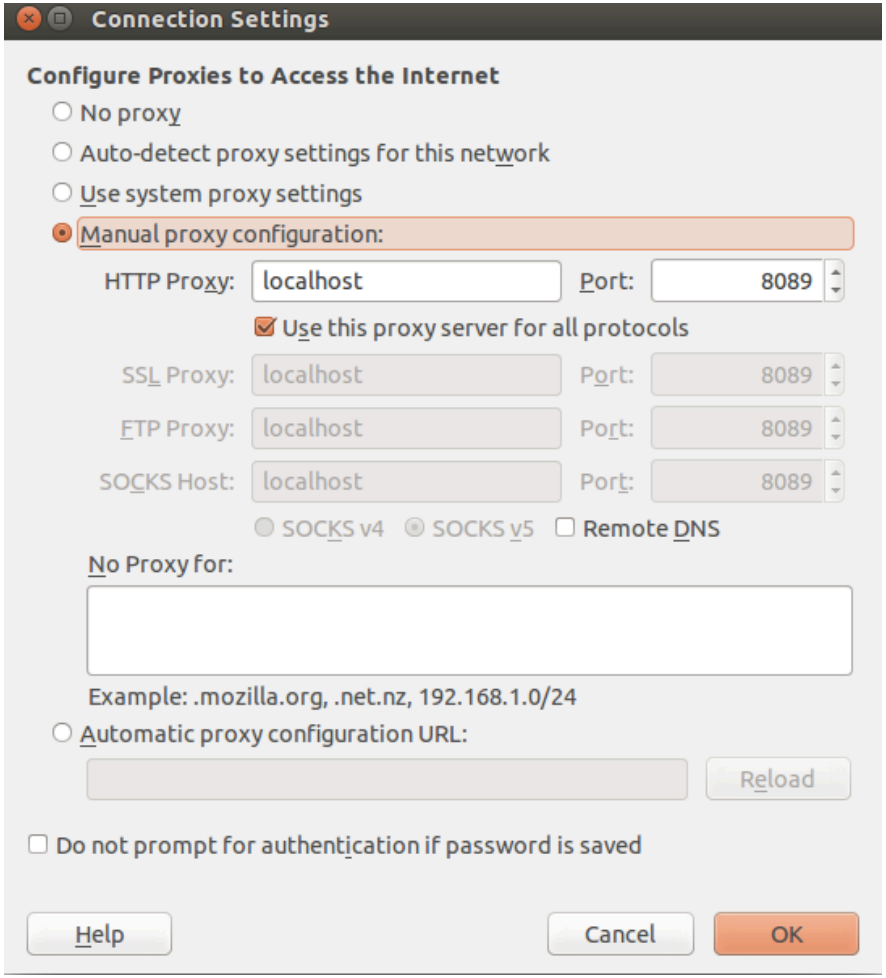
- **Go to Tools→Option→ Local Proxy**



Configure ZAP as a Proxy

UNIVERSITY OF TRENTO

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



Run WebGoat

UNIVERSITY OF TRENTO

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

Run WebGoat

UNIVERSITY OF TRENTO