IFS4103 Lab 2:
Setting up and Using Burp Proxy

Notes:

- The first step of using Burp Suite is to set up **Burp Proxy** as **a** ***web intercepting proxy*** on your web pen-testing host. With the proxy running, **web client requests** from your host's browser, and optionally **the server responses**, can be intercepted for inspection and possible manipulation.
- All proxied URLs recorded by Burp Proxy are available for subsequent **further processing** using Burp Suite's other components/modules, including for ***target scoping***, ***crawling*** (previously called ***spidering***), and ***auditing*** (previously called ***scanning***). You can also refer to Burp Suite's web penetration-testing **workflow diagram** shown in Figure 1.
- To practise using Burp Proxy in this lab and Burp's other components in the subsequent labs, you can set up a VM running **vulnerable web applications**.

Objectives:

For Lab 2, you will perform the following:

1. To set up **Burp Proxy** to work with **browsers**, including Burp Suite's **embedded/internal browser** and your **external browser**;
2. To use **Burp Proxy** for inspecting and modifying intercepted client requests, as well as to **configure its options** in intercepting client requests and server responses;
3. To inspect Burp Suite's **user interface** including for other Burp's modules;
4. To set up a VM running **vulnerable web applications**.

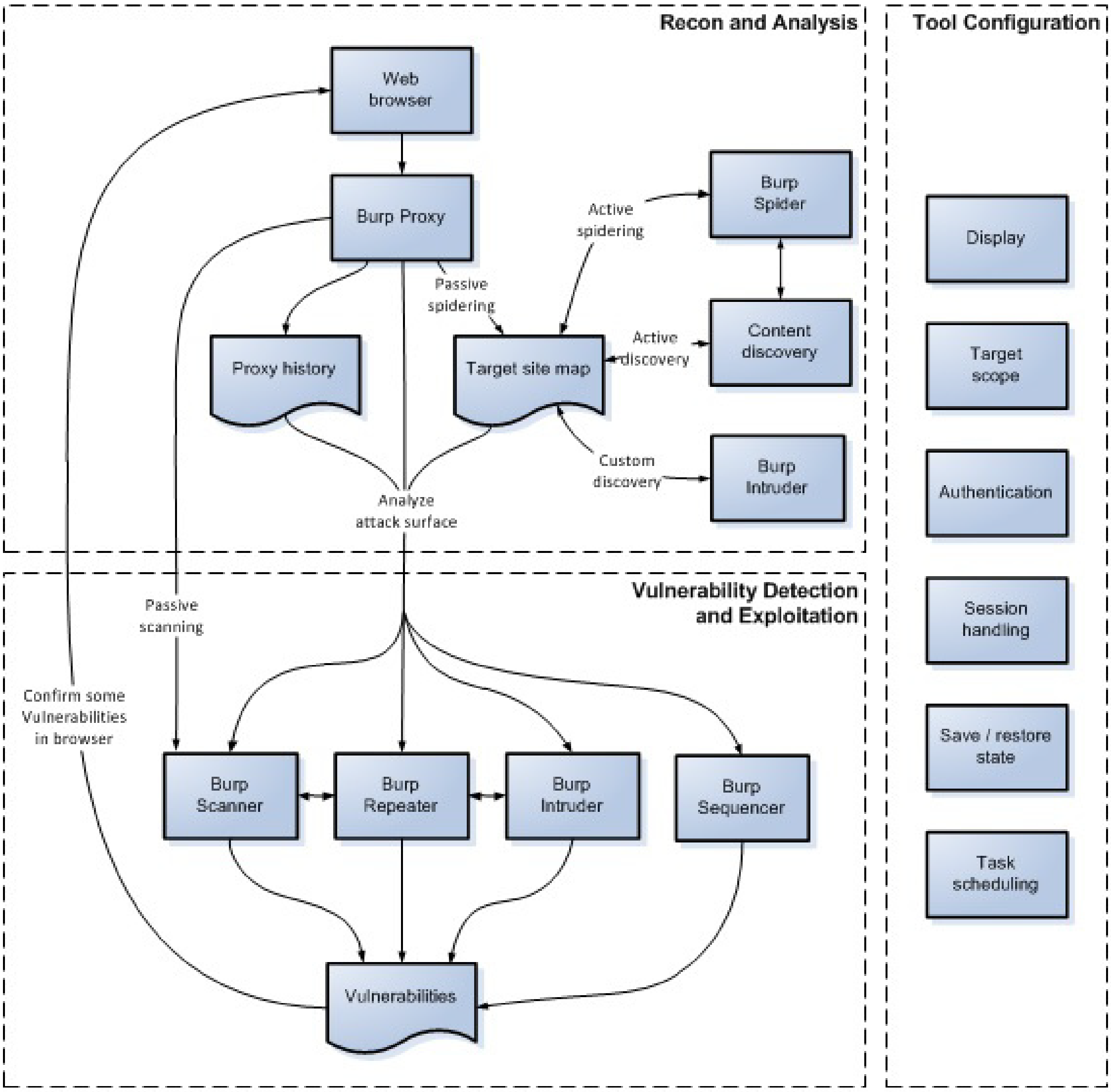


Figure 1. Burp Suite's web penetration testing workflow diagram

(Source: https://portswigger.net/burp/documentation/desktop/penetration-testing)

Task 1: Setting up Burp Proxy to Work with Browsers

The latest **Burp Suite 2** now has an ***embedded/internal*** **browser**. This simplifies the web proxy setting. You can simply use the embedded browser which has been **pre-configured** to be proxied by Burp Suite.

Alternatively, you can configure an **external browser** such as Firefox to work with Burp Suite. For Firefox's proxy set-up, you can follow the steps shown in the following videos:

- “**Getting started** with Burp”: https://www.hacker101.com/sessions/burp101.html: 2:06-5:00
- “**Configure Firefox** with Burp Suite”: https://www.youtube.com/watch?v=7ePmWhypzBI

Task 2: Using Burp Proxy & Configuring Its Options

Once Burp Suite functions as a web intercepting proxy, you can use its **Proxy module**. You can refer to the following videos from PortSwigger, which are viewable on YouTube, on how you can use Burp Proxy:

- “How to **intercept** HTTP requests and responses using Burp Suite”: https://www.youtube.com/watch?v=ouDe5sJ_uC8
- “How to use Burp Proxy **interception rules**”: https://www.youtube.com/watch?v=SaRJgLQ5fOM

From observing the two videos, you should be able to use and also configure Burp Proxy for inspecting your visited web sites.

Subsequently, do use Burp Proxy for **manipulating the header and/or body** of some of your HTTP requests. You can refer to the **steps** listed in this tutorial page: https://portswigger.net/burp/documentation/desktop/getting-started/modifying-http-requests.

Task 3: Inspecting Burp Suite’s User Interface

Before you can further utilize Burp Suite, you need to understand its **user interface**. To have an overview of Burp Suite’s **general interface** to its various modules/components, do view the following video:

“A guide to the **Burp Suite user interface**”: https://www.youtube.com/watch?v=nECt-0zW0O4&t=1s

Task 4: Setting Up Target Web Applications

Lastly, for your practice, you need to set up **buggy/vulnerable web applications** as your target applications, including:

- ***Damn Vulnerable Web App* (*DVWA*)**: https://github.com/digininja/DVWA;
- ***Mutillidae***: https://github.com/webpwnized/mutillidae.

One easy way of making these applications available is by setting up a VM running **OWASP Broken Web Applications (BWA)**: https://sourceforge.net/projects/owaspbwa/. You can download its cached OVA file from: https://drive.google.com/file/d/1Sfd2bvqGRsVXbonkQGHSebkbKKXaG3_-/view. Follow some **simple steps to import** the OVA appliance into your VirtualBox's VM as described in: https://www.alphr.com/ova-virtualbox/. To make the web application accessible from your host OS (as your ***attack host***), you can simply set the OWASP-BWA VM with the "*Host-only Networking*" **networking mode** in VirtualBox. This way, your host OS can access the target web applications, but the buggy web applications are *not* accessible from the Internet.[1]

After your target host is running, do inspect its IP address using `ifconfig`. On your attack host, use a browser to visit http://<*target-host-IP-address*>. At the OWASP BWA's landing page, you should see links to several vulnerable web applications, including DVWA and Mutillidae.

4.1. Configuring "Damn Vulnerable Web App" (DVWA)

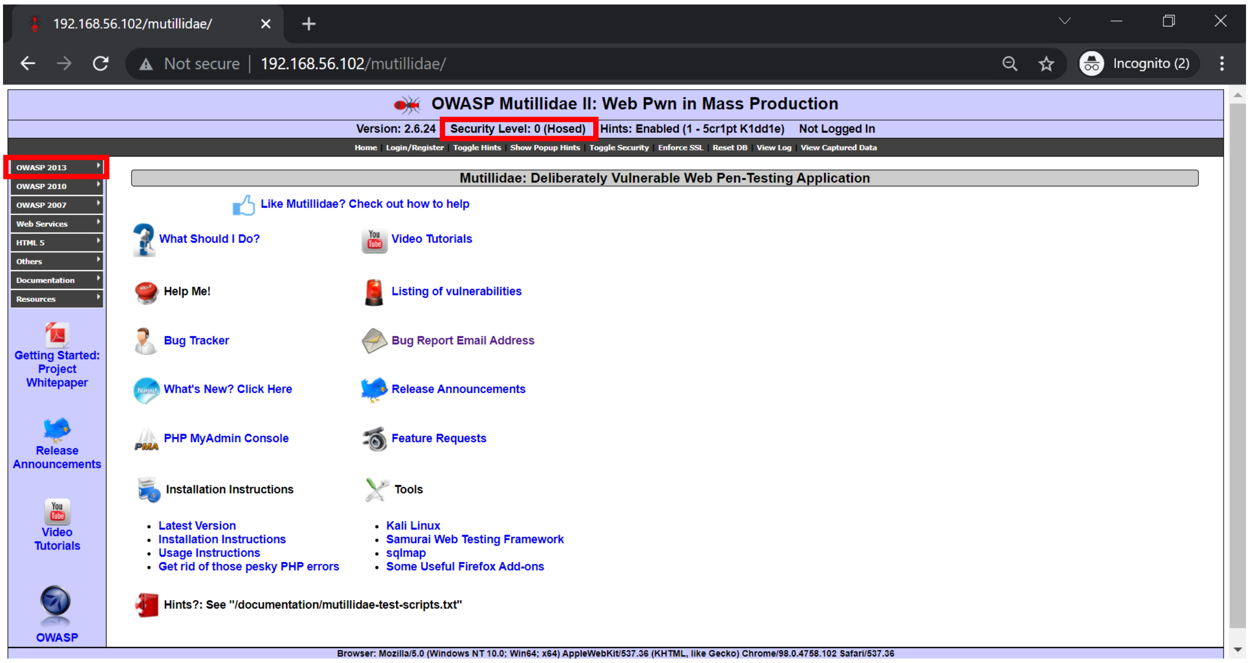
You can log into the PHP/MySQL-based DVWA using its **default credential**: `username`="`admin`" and `password`="`password`". To make it vulnerable, click on "DVWA Security" and set the "Script Security Level" to "**low**".

[1] If you alternatively run Burp Suite in a VM (as your attack VM), you can configure both your attack VM and OWASP-BWA VM with the "*Internal*" networking mode in VirtualBox.

4.2. Configuring Mutillidae

Mutillidae is a free, open-source, vulnerable web application, which also contains various **OWASP Top 10 vulnerabilities**. At the OWASP BWA's landing page, click on "OWASP Mutillidae II". You should see the landing page of OWASP Mutillidae II as shown in Figure 2 below. By default, the security level is set to **0 (hosed)**, i.e. completely vulnerable, as highlighted in Figure 2.

You can access Mutillidae's web pages related to vulnerabilities under **OWASP Top 10 2013** by clicking on the "OWASP 2013" menu item on the left-hand side of the application window as shown in Figure 2 below.



OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Mutillidae: Deliberately Vulnerable Web Pen-Testing Application

Hints?: See "/documentation/mutillidae-test-scripts.txt"

Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36

192.168.56.102/mutillidae/
Not secure | 192.168.56.102/mutillidae/
Incognito (2)
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
Release Announcements
Video Tutorials
OWASP
Like Mutillidae? Check out how to help
What Should I Do?
Video Tutorials
Help Me!
Listing of vulnerabilities
Bug Tracker
Bug Report Email Address
What's New? Click Here
Release Announcements
PHP MyAdmin Console
Feature Requests
Installation Instructions
Tools
Latest Version
Installation Instructions
Usage Instructions
Get rid of those pesky PHP errors
Kali Linux
Samurai Web Testing Framework
sqlmap
Some Useful Firefox Add-ons

Figure 2. The landing page of the OWASP Mutillidae II web application