|  |  |
| --- | --- |
|  | final logo jawi UTeM-01 |

Fakulti Teknologi Maklumat dan Komunikasi

Universiti Teknikal Malaysia Melaka

**Analyze Security Tools**

Security Tools:

Burp Suite, Hping

# Demonstration Video:

<https://youtu.be/au6R5tQV_aY>

**GROUP 7**

1. Muhammad Izham Bin Norhamadi (B032020039)
2. Ahmad Sha Herizam Bin Tahir (B032020009)
3. Affendy Elyas bin Azhari Sharidan (B032020024)
4. Nor Adzeezul Asrie Bin Norafandi (B031910012)
5. Muhammad Farhan Bin Mohamad Tahir (B031910105)

Table of Contents

|  |  |  |
| --- | --- | --- |
| 1. | Brief Introduction of Selected Security Tools | 1 |
| 2. | Overview of Burp Suite | 1 |
| 3. | Burp Suite Instruction Demo | 2 |
| 4. | Advantages of Burp Suite | 9 |
| 5. | Overview of Hping | 10 |
| 6. | Hping Instruction Demo | 10 |
| 7. | Advantages of Hping | 12 |
| 8. | Conclusion | 13 |

1. Brief Introduction of Selected Security Tools

In this millennium era, security is becoming a hot topic to be discussed in everyday life whether in a business environment or even in daily conversation as a security measure becomes the core of protection of any kinds of information or confidential assets. One of the security measures that needs to be paid attention to is the security tools itself since the tools will help users to implement security into their respective machines.

Now, security tools come in several types and features with specific purpose on their own to complete specific security tasks. These security tools come for a variety of purposes such as web-based application security evaluation and TCP/IP packet analyzer. Examples of security tools which are popular nowadays include Burp Suite and Hping. Both tools are handy in terms of providing such a good security environment. Burp Suite is a tool for analyzing and testing web applications and on the other hand Hping is a TCP/IP packet analyzer which specifically for network auditing and firewall testing.

2. Overview of Burp Suite

Logo

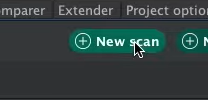
Description automatically generated

Burp Suite is a Java application for testing and analyzing web application security. It is a widely used tool to evaluate the security of web-based applications and hands-on testing. It has a robust and modular framework and packed with optional extensions that can increase web application testing efficiency. It has a user-friendly UI making it accessible for learning the basics of web security testing. Burp Suite features includes a proxy server, spider bot, automate requests and much more penetration testing tools.

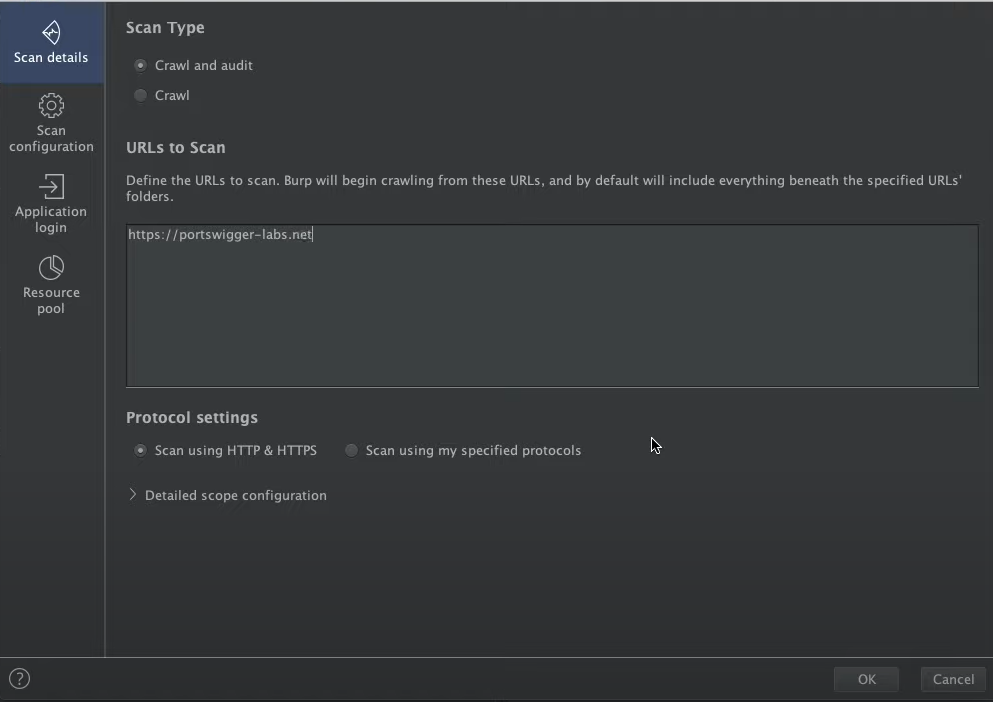
3. Burp Suite Instruction Demo

Scanning a website for vulnerabilities

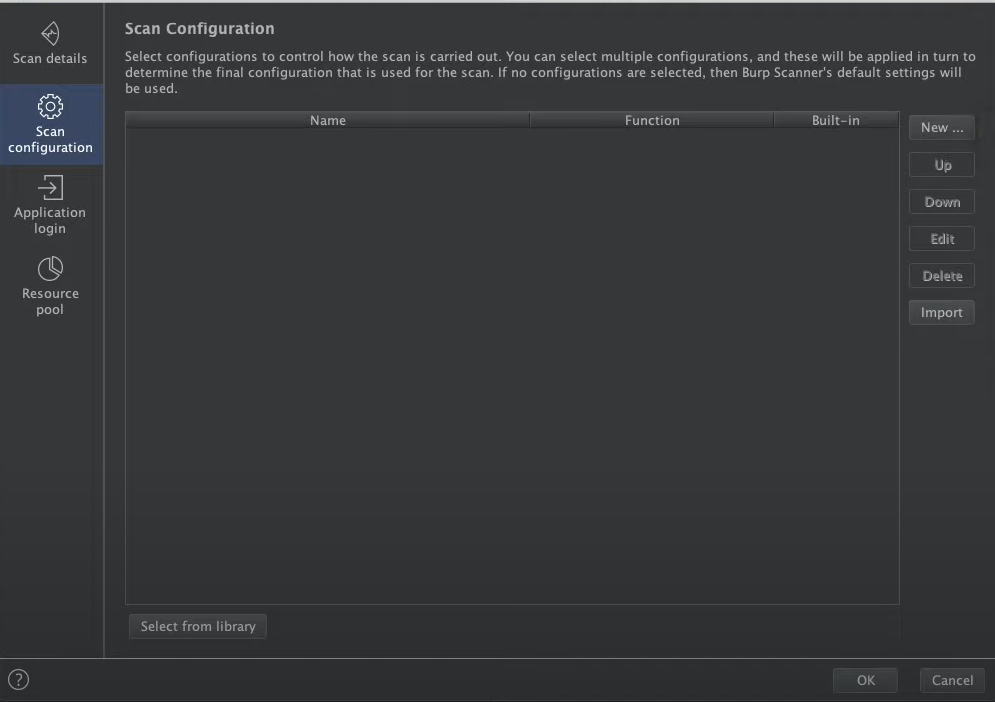
1. Click on burp dashboard and click scan

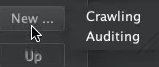


1. New scan launcher open up and then click crawler and audit, if crawler only, it will just discover the contents. Place URL that needs to scan in the text box. In protocol setting, it is recommended to stay default that is scan using HTTPS and HTTPS.



1. Next go to scan configuration, and click new and choose whether crawling or audit.

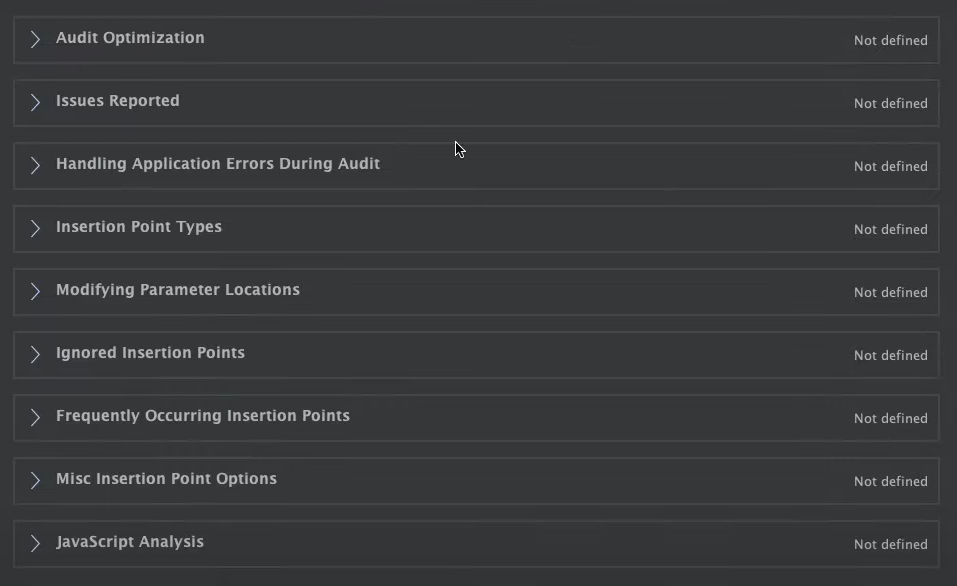




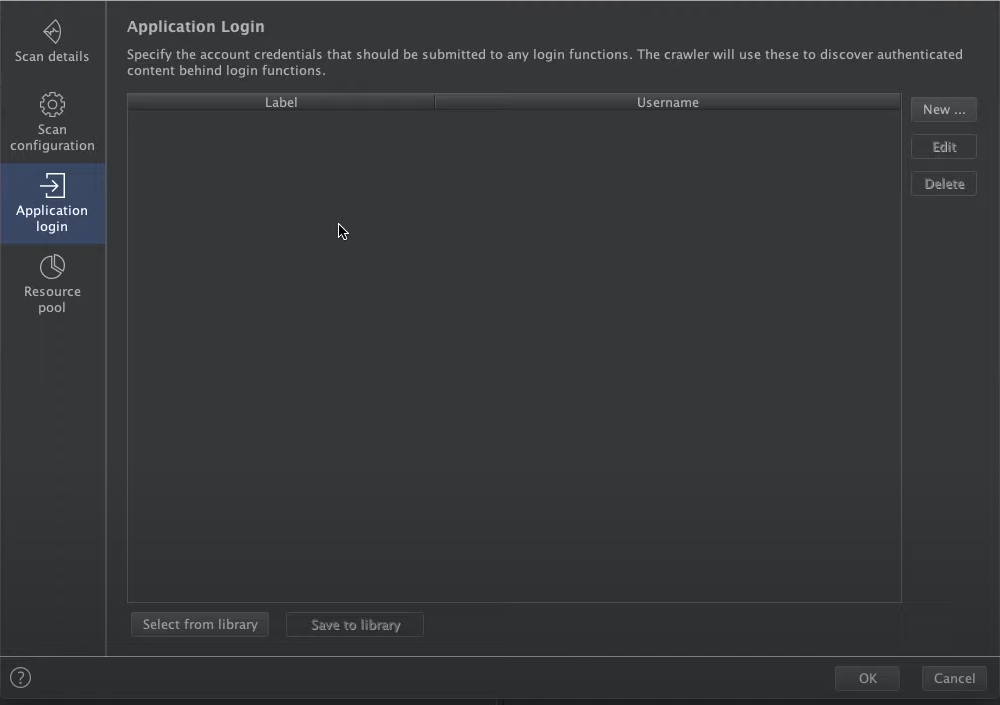
1. In crawl option there are configuration can be use such as crawl optimization, crawl limits, login functions and handling application errors during crawl.



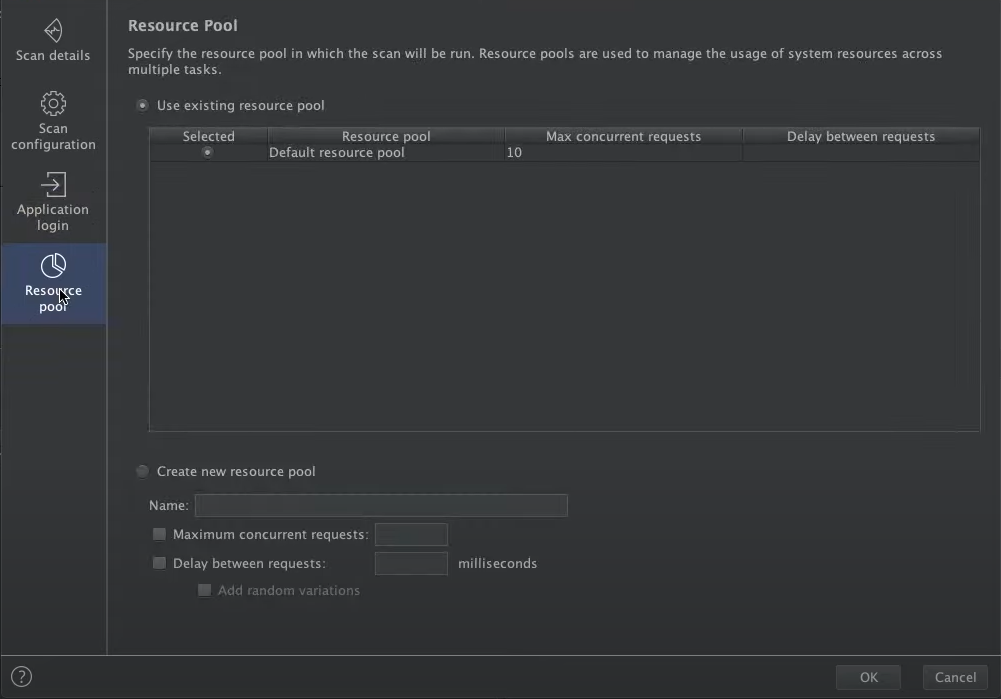
1. In crawl option there are configuration can be used such as audit optimization, issues reported, handling applications errors during audit, etc.



1. Next, in application login setting that can be used to specify the account credentials that should be submitted to any login functions. The crawler will use these to discover authenticated content behind login functions.



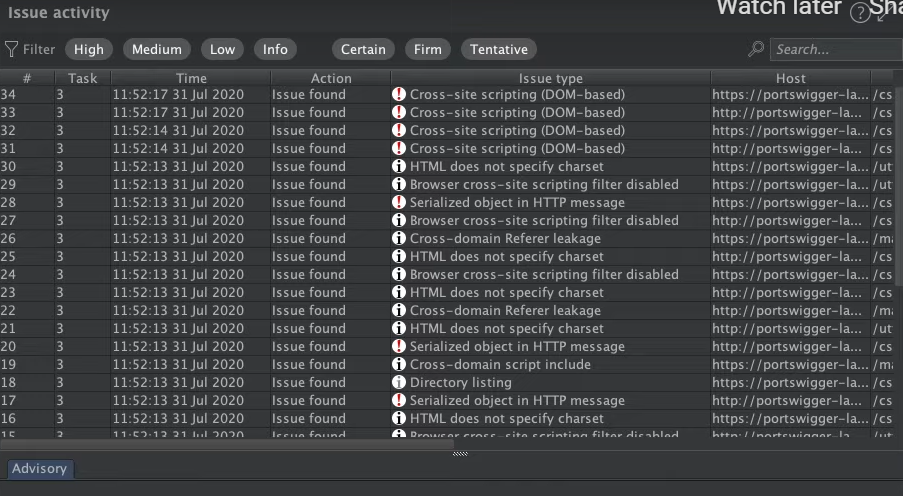
1. Next, in a resource pool setting that can be used to specify the resource pool in which the scan will be run. Resource pools are used to manage the usage of system resources across multiple task.

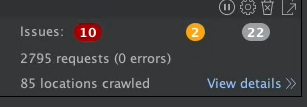


1. After finished setting the scanner, click ok and the scan will start

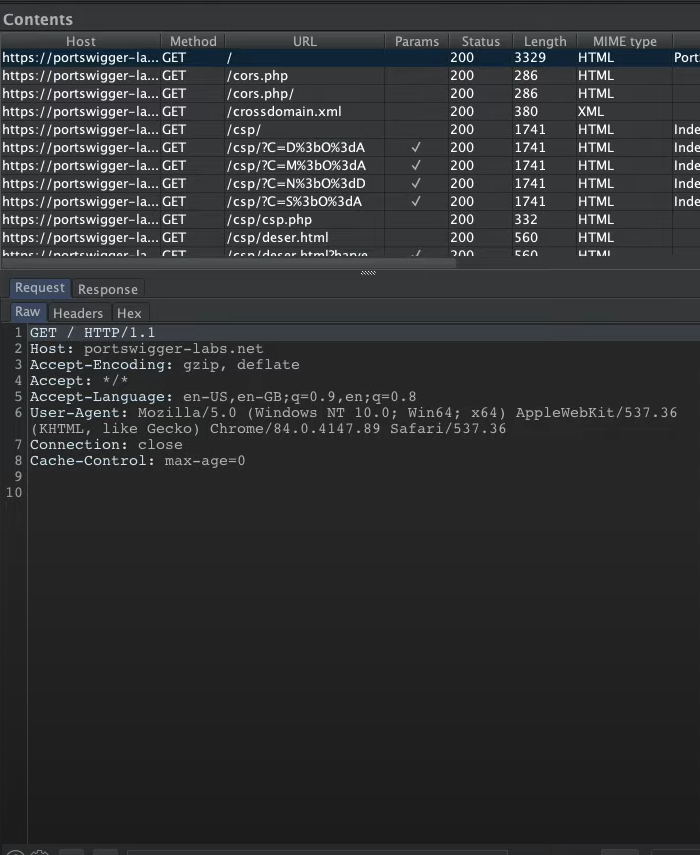


1. After scan finished, a list of issue activity show up.





1. In the content, we can see the response of the website if click any of it



**4. Advantage of Burp Suite**

* **Have variety of features**

Burp Suite provides various kinds of features or sub-tools that can be used for a specific purpose such as manual penetration testing and configuration, automated bulk scanning as well as report generation.

* **Use local proxy**

Allow users to intercept application’s traffic to discover vulnerabilities. From this interception, users can manipulate the attribute fields to find more vulnerabilities inside the application

* **Spidering Features**

The spidering is to follow all the links on a web page to discover both dynamic and static web resource of the web application. This can be done in manual or automated process and will give a flow chart representation of the workflow which can easily acquire with a click only.

* **Testing can be done manually or automatically**

Usually automated and manual tools are only available in several types of tools. However, Burp Suite is one of the tools that provide utility to perform both tasks in a single tool.

* **Have a powerful extension ready to be used**

Burp Suite has an application store called BApp Store which users can install ready-to-use extension, manage the extension, and configure the option of the extension. Users also can create their own extension and can submit to BApp Store after getting approval.

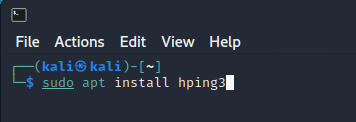
5. Overview of Hping



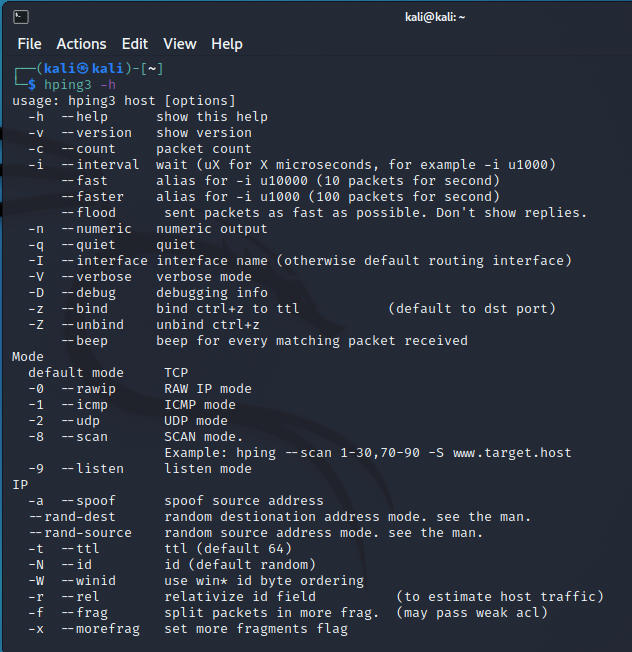
hping is a command-line oriented TCP/IP packet assembler/analyzer. The interface is inspired by the ping (8) UNIX command, but hping is not only able to send ICMP echo requests. It supports TCP (Transmission Control Protocol), UDP, ICMP and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features. It is one of the common tools used for security auditing and testing of firewalls and networks and was used to exploit the idle scan scanning technique.

6. Hping Instruction Demo

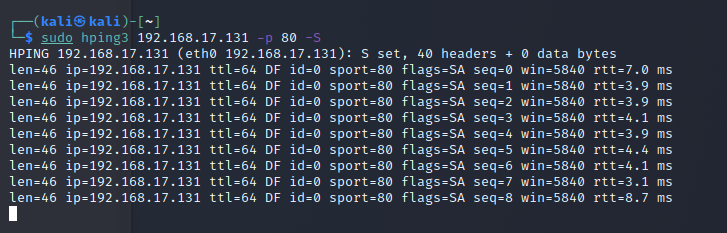
1. Kali Linux comes pre-installed with hping tool, but if it isn’t simply using the apt package command



2. hping3 has several parameters to operate the software, you can view the list with the -help command



3. To start using the tool, provide the target destination IP, its port, and the desired parameter options



7. Advantage of Hping

* Useful for Firewall penetration testing.

This tool can penetrate Firewall by using command available in hping to deploy such as DoS attack to see the performance of the server.

* Can be used to check if the port is opened or filtered.

We can analyze our port whether the host network is opened or filtered. For example, by using the command that are available in hping, if it finds a live host and an open port, it returns an RST response.

8. Conclusion

In conclusion, in this modern era of globalization, security tools have been popular in this digital world of security system. ‘Prevention is better than cure.’ This proverb really describes how security tools are all about. As modern people, evolution of security tools needs to be paid attention so that any kinds of threats that would lead to the harm of a system can be mitigated by simply having a right tool to counter specific threats.

Day by day, vulnerability and threats keep expanding and can be more harmful and harder to detect by recent security tools and software. That is why this type of tool needs to be updated regularly so that it can detect either advanced threats or new undiscovered type of vulnerabilities. Plus, we need to always keep up to date with the latest trends of threats to make sure our security tools and software are always prepared for any new type of threats.

Everyone, either a person in corporate business or even a student who studies in security field, needs to learn, and have a better understanding of the importance of security tools. Especially someone who works in web-based industries, using Burp Suite is a high recommendation since this software is extremely reliable and helpful in making sure that any web we develop or take care of always in secure conditions from any kinds of threats either physically or digitally meanwhile Hping can be handy towards individual in charge of network security auditing and firewall testing.