UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

Universiti Teknikal Malaysia Melaka

LAB 6: Vulnerability Assessment

Assessment Tool:

Burp Suite

GROUP 5

1. Muhammad Izham Bin Norhamadi (B032020039)
2. Ahmad Sha Herizam Bin Tahir (B032020009)
3. Affendy Elyas bin Azhari Sharidan (B032020024)

Table of Contents

1. Introduction of Vulnerability Assessment

Vulnerability Assessment is process of analysis the weaknesses or exposure of an assets from a specific information system. It determines whether the system is vulnerable to any known and malicious vulnerabilities. These vulnerabilities will be assigned the severity levels to make sure that every vulnerability can be determined their impacts toward the system. This is to make sure we ready to face off any cyberattacks of virus attacks. This evaluation can offer us the perfect and suitable recommendations of mitigation and remediation for the vulnerabilities so that system can safely remove these dangerous attacks without triggering any other unwanted consequences.

Having this vulnerable assessment can prevents a lot of threats from harming our machines. These threats can be classified as any injection attacks such as SQL injection, privileges problems due to faulty authentication mechanism and insecure defaults. Because of that, every information system either for business or personal use, it should have at least one vulnerable assessment software that can take care of any vulnerability that could lead towards the harm for the system. One of the best examples of software that can used to analyze it is Burp Suite. This piece of software is reliable for testing and analyzing web application security.

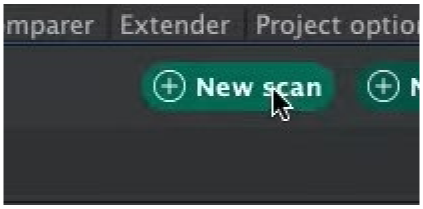
2. Overview of Burp Suite

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.

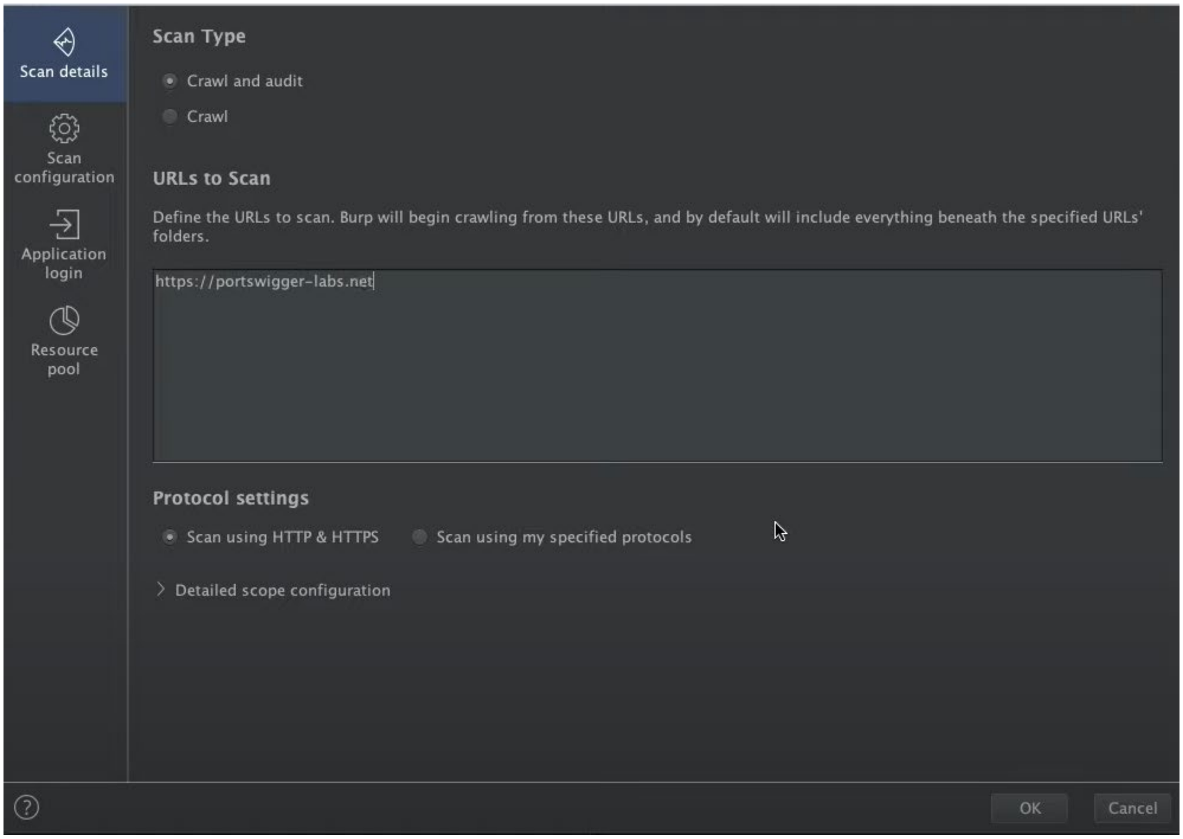
3. User’s Instruction

Scanning a website for vulnerabilities

1. Click on burp dashboard and click scan



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



Scan Type

● Crawl and audit
○ Crawl

URLs to Scan

Define the URLs to scan. Burp will begin crawling from these URLs, and by default will include everything beneath the specified URLs' folders.

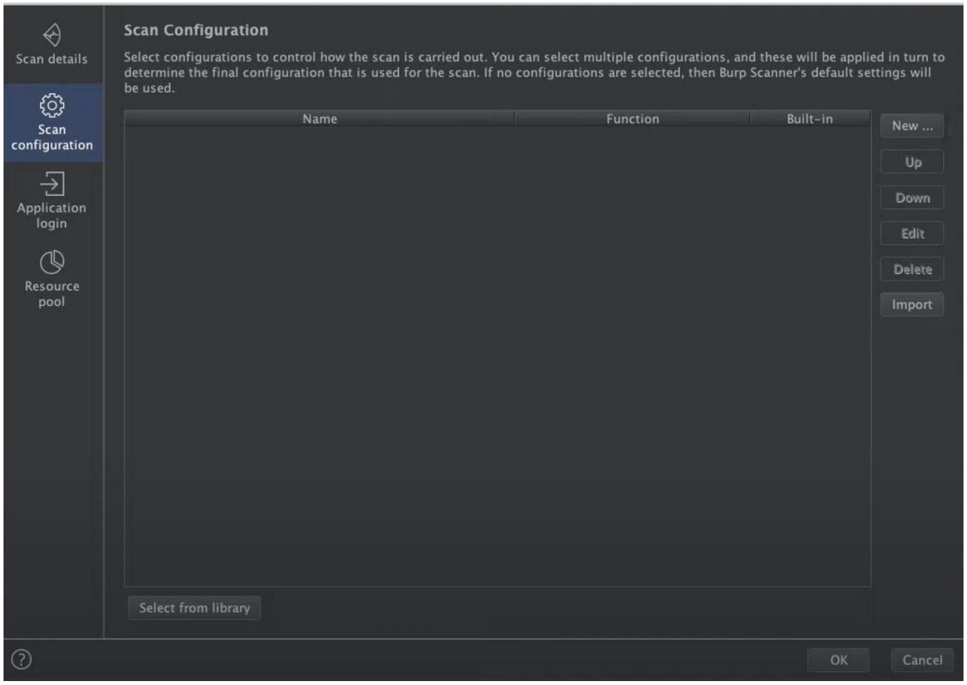
https://portswigger-labs.net

Protocol settings

● Scan using HTTP & HTTPS ○ Scan using my specified protocols

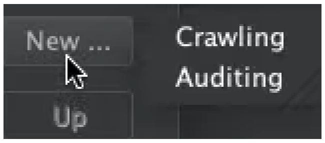
> Detailed scope configuration

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

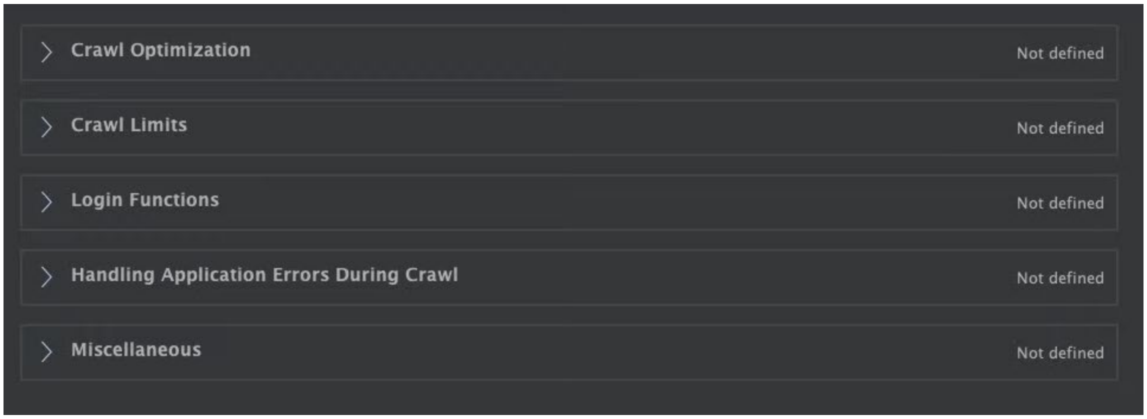


Scan Configuration

Select configurations to control how the scan is carried out. You can select multiple configurations, and these will be applied in turn to determine the final configuration that is used for the scan. If no configurations are selected, then Burp Scanner's default settings will be used.



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



Crawl Optimization — Not defined

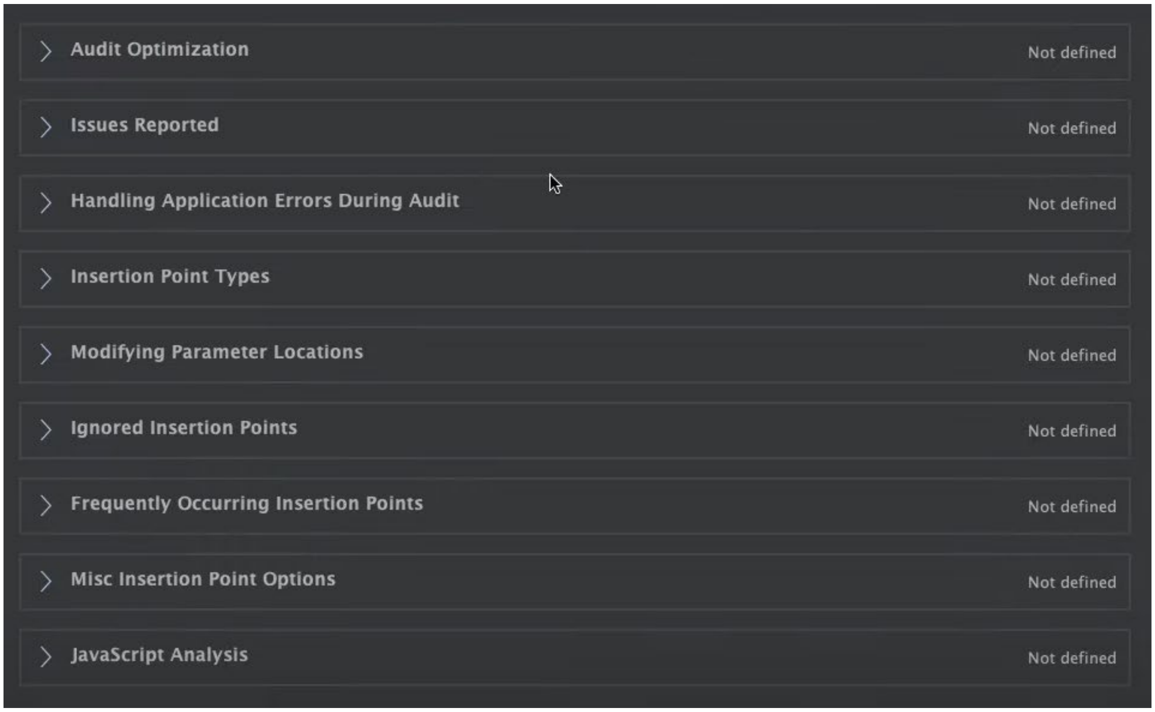
Crawl Limits — Not defined

Login Functions — Not defined

Handling Application Errors During Crawl — Not defined

Miscellaneous — Not defined

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



Audit Optimization Not defined

Issues Reported Not defined

Handling Application Errors During Audit Not defined

Insertion Point Types Not defined

Modifying Parameter Locations Not defined

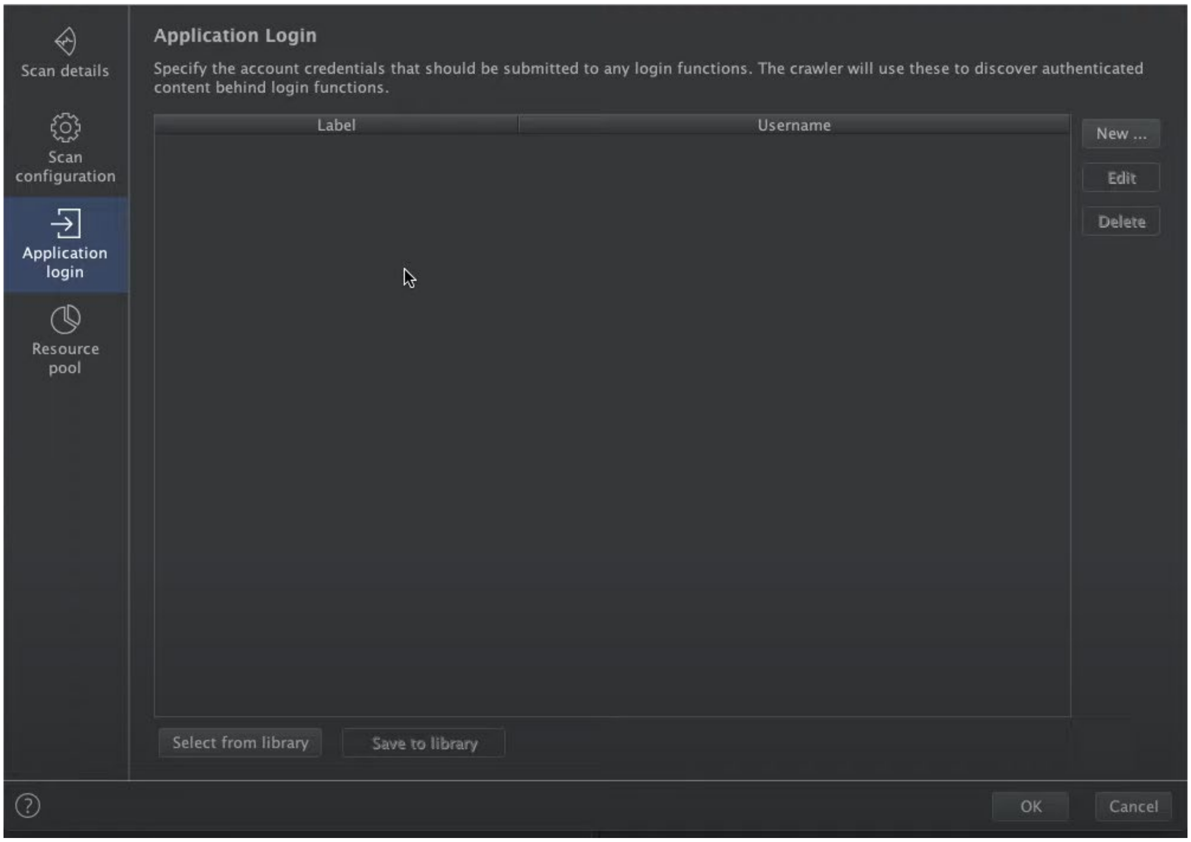
Ignored Insertion Points Not defined

Frequently Occurring Insertion Points Not defined

Misc Insertion Point Options Not defined

JavaScript Analysis Not defined

6. Next is in application login setting that can be use 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.

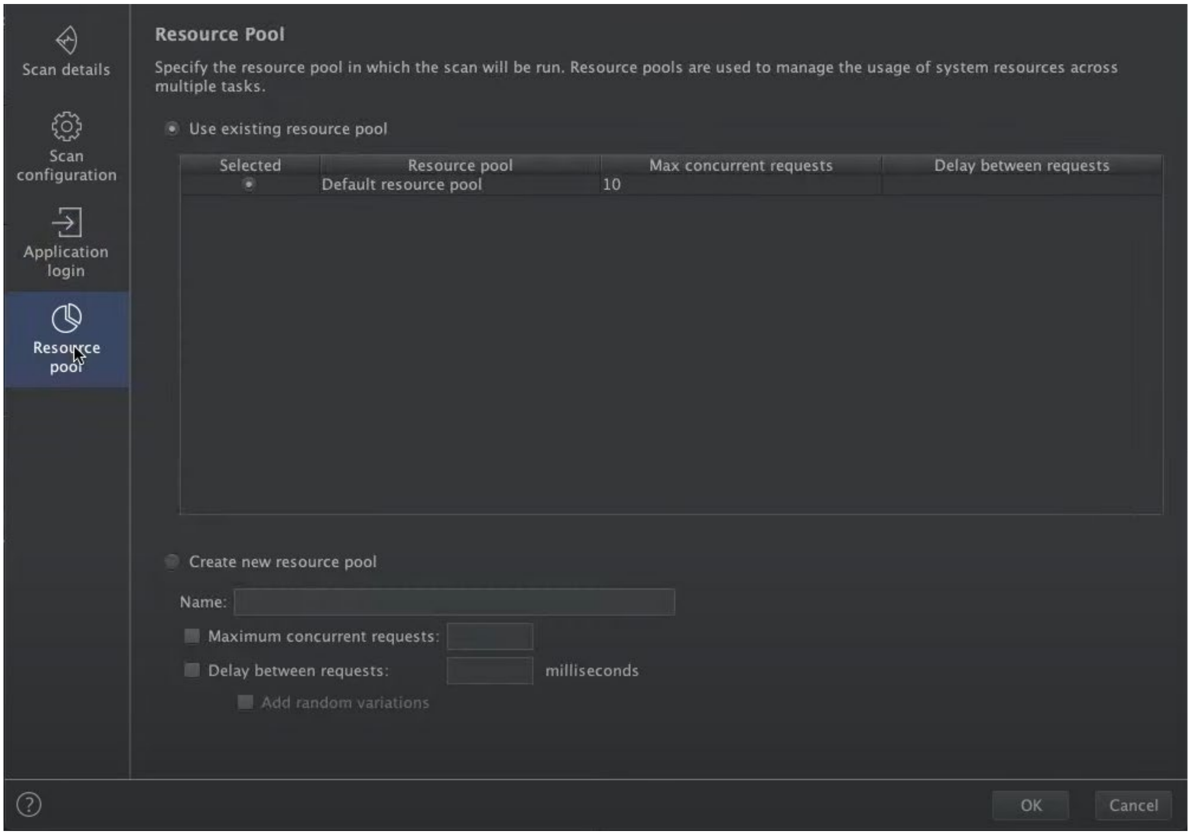


Application Login

Specify the account credentials that should be submitted to any login functions. The crawler will use these to discover authenticated content behind login functions.

Label	Username

7. Next is in resource pool setting that can be use 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.



Resource Pool

Specify the resource pool in which the scan will be run. Resource pools are used to manage the usage of system resources across multiple tasks.

● Use existing resource pool

Selected	Resource pool	Max concurrent requests	Delay between requests
●	Default resource pool	10	

○ Create new resource pool

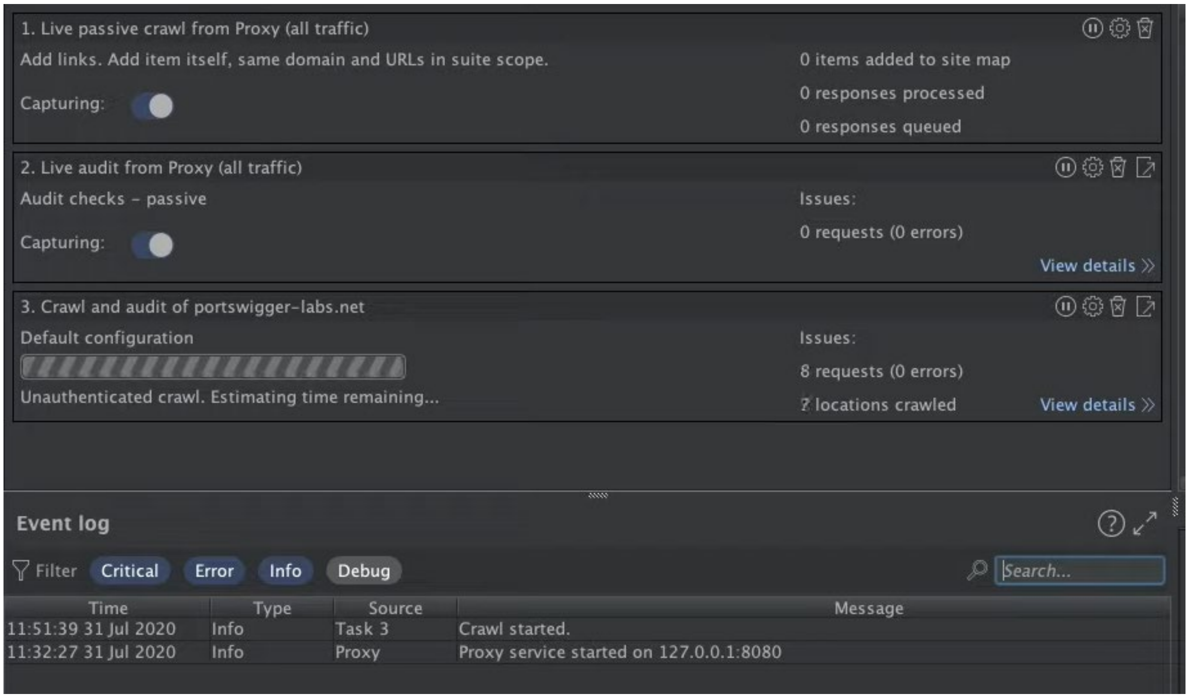
Name:

☐ Maximum concurrent requests:

☐ Delay between requests: milliseconds

☐ Add random variations

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



1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain and URLs in suite scope.
Capturing:
0 items added to site map
0 responses processed
0 responses queued

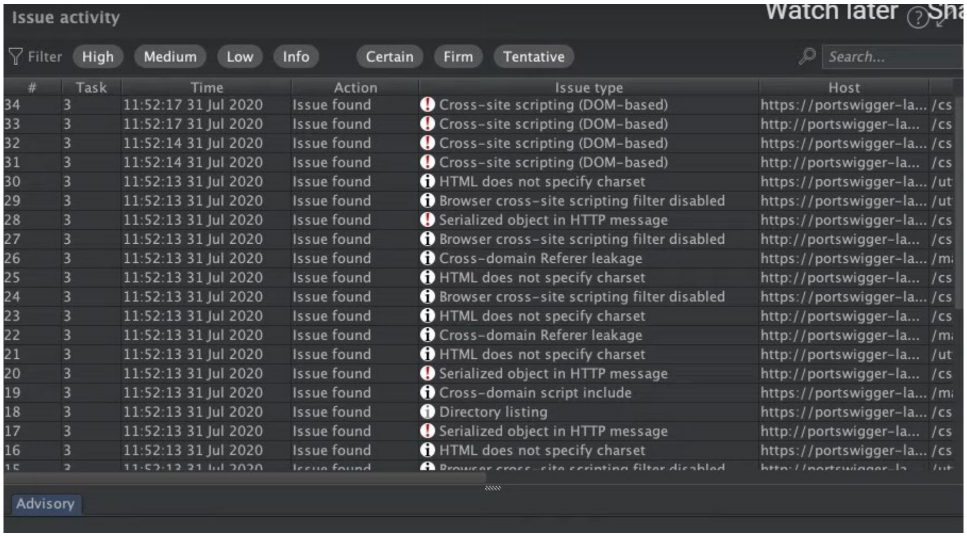
2. Live audit from Proxy (all traffic)
Audit checks - passive
Capturing:
Issues:
0 requests (0 errors)
View details »

3. Crawl and audit of portswigger-labs.net
Default configuration
Unauthenticated crawl. Estimating time remaining...
Issues:
8 requests (0 errors)
7 locations crawled
View details »

Event log

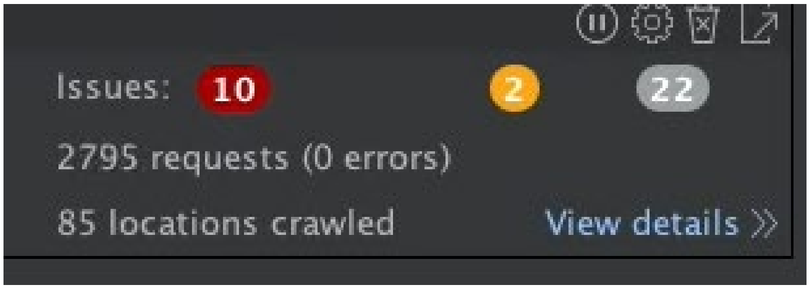
Time	Type	Source	Message
11:51:39 31 Jul 2020	Info	Task 3	Crawl started.
11:32:27 31 Jul 2020	Info	Proxy	Proxy service started on 127.0.0.1:8080

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



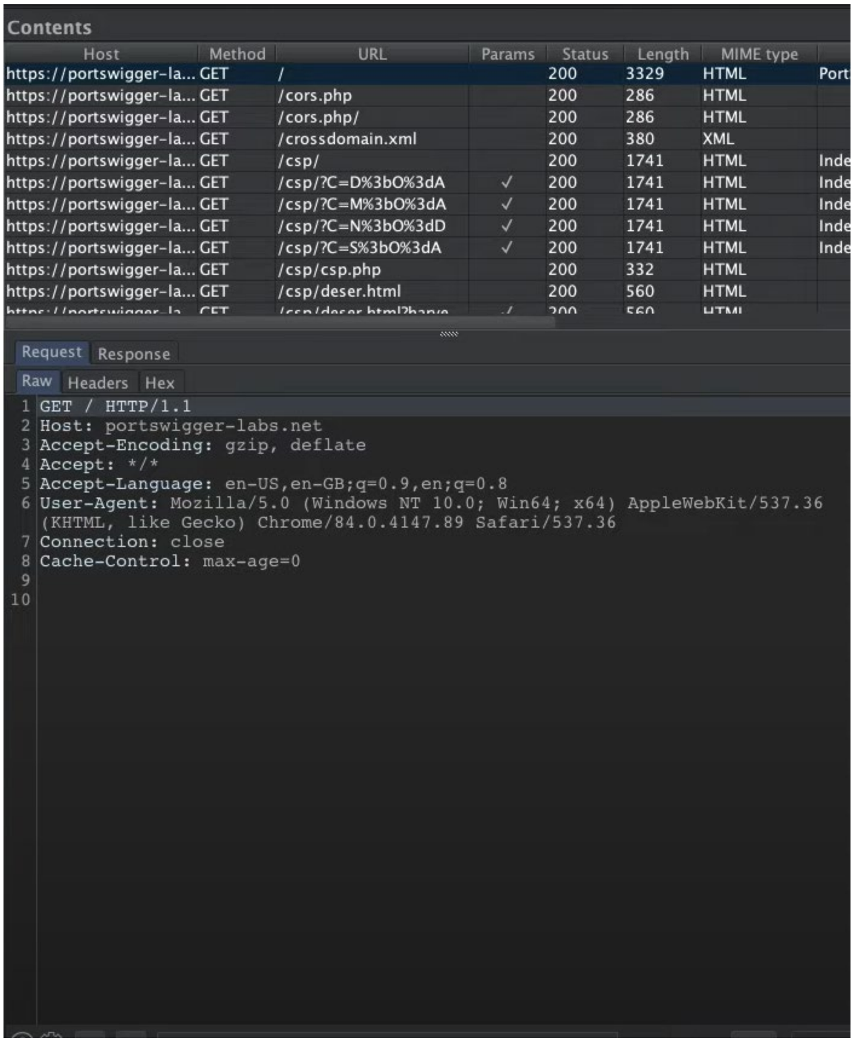
Issue activity

#	Task	Time	Action	Issue type	Host	
34	3	11:52:17 31 Jul 2020	Issue found	❗ Cross-site scripting (DOM-based)	https://portswigger-la...	/cs
33	3	11:52:17 31 Jul 2020	Issue found	❗ Cross-site scripting (DOM-based)	http://portswigger-la...	/cs
32	3	11:52:14 31 Jul 2020	Issue found	❗ Cross-site scripting (DOM-based)	https://portswigger-la...	/cs
31	3	11:52:14 31 Jul 2020	Issue found	❗ Cross-site scripting (DOM-based)	http://portswigger-la...	/cs
30	3	11:52:13 31 Jul 2020	Issue found	ℹ HTML does not specify charset	https://portswigger-la...	/ut
29	3	11:52:13 31 Jul 2020	Issue found	ℹ Browser cross-site scripting filter disabled	https://portswigger-la...	/ut
28	3	11:52:13 31 Jul 2020	Issue found	❗ Serialized object in HTTP message	https://portswigger-la...	/cs
27	3	11:52:13 31 Jul 2020	Issue found	ℹ Browser cross-site scripting filter disabled	http://portswigger-la...	/cs
26	3	11:52:13 31 Jul 2020	Issue found	ℹ Cross-domain Referer leakage	https://portswigger-la...	/m
25	3	11:52:13 31 Jul 2020	Issue found	ℹ HTML does not specify charset	http://portswigger-la...	/cs
24	3	11:52:13 31 Jul 2020	Issue found	ℹ Browser cross-site scripting filter disabled	https://portswigger-la...	/cs
23	3	11:52:13 31 Jul 2020	Issue found	ℹ HTML does not specify charset	http://portswigger-la...	/cs
22	3	11:52:13 31 Jul 2020	Issue found	ℹ Cross-domain Referer leakage	http://portswigger-la...	/m
21	3	11:52:13 31 Jul 2020	Issue found	ℹ HTML does not specify charset	http://portswigger-la...	/ut
20	3	11:52:13 31 Jul 2020	Issue found	❗ Serialized object in HTTP message	http://portswigger-la...	/cs
19	3	11:52:13 31 Jul 2020	Issue found	ℹ Cross-domain script include	https://portswigger-la...	/m
18	3	11:52:13 31 Jul 2020	Issue found	ℹ Directory listing	https://portswigger-la...	/cs
17	3	11:52:13 31 Jul 2020	Issue found	❗ Serialized object in HTTP message	http://portswigger-la...	/cs
16	3	11:52:13 31 Jul 2020	Issue found	ℹ HTML does not specify charset	https://portswigger-la...	/cs
15	3	11:52:13 31 Jul 2020	Issue found	ℹ Browser cross-site scripting filter disabled	http://portswigger-la...	/ut



Issues: 10 2 22
2795 requests (0 errors)
85 locations crawled
View details »

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



Host	Method	URL	Params	Status	Length	MIME type	
https://portswigger-la...	GET	/		200	3329	HTML	Port
https://portswigger-la...	GET	/cors.php		200	286	HTML	
https://portswigger-la...	GET	/cors.php/		200	286	HTML	
https://portswigger-la...	GET	/crossdomain.xml		200	380	XML	
https://portswigger-la...	GET	/csp/		200	1741	HTML	Inde
https://portswigger-la...	GET	/csp/?C=D%3bO%3dA	✓	200	1741	HTML	Inde
https://portswigger-la...	GET	/csp/?C=M%3bO%3dA	✓	200	1741	HTML	Inde
https://portswigger-la...	GET	/csp/?C=N%3bO%3dD	✓	200	1741	HTML	Inde
https://portswigger-la...	GET	/csp/?C=S%3bO%3dA	✓	200	1741	HTML	Inde
https://portswigger-la...	GET	/csp/csp.php		200	332	HTML	
https://portswigger-la...	GET	/csp/deser.html		200	560	HTML	
https://portswigger-la...	GET	/csp/deser.html?hanve	✓	200	560	HTML	

```
GET / HTTP/1.1
Host: portswigger-labs.net
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/84.0.4147.89 Safari/537.36
Connection: close
Cache-Control: max-age=0


```

4. Features in Vulnerability Assessment

I. **Intercept everything your browser sees**
   - A powerful proxy/history lets you modify all HTTP(S) communications passing through your browser.

II. **Manage recon data**
   - All target data is aggregated and stored in a target site map - with filtering and annotation functions.

III. **Expose hidden attack surface**
   - Find hidden target functionality with an advanced automatic discovery function for "invisible" content.

IV. **Test for clickjacking attacks**
   - Generate and confirm clickjacking attacks for potentially vulnerable web pages, with specialist tooling.

V. **Work with WebSockets**
   - WebSockets messages get their own specific history - allowing you to view and modify them.

VI. **Break HTTPS effectively**
   - Proxy even secure HTTPS traffic. Installing your unique CA certificate removes associated browser security warnings.

VII. **Manually test for out-of-band vulnerabilities**
   - Make use of a dedicated client to incorporate Burp Suite's out-of-band (OAST) capabilities during manual testing.

VIII. **Speed up granular workflows**
   - Modify and reissue individual HTTP and WebSocket messages, and analyze the response - within a single window.

IX. **Quickly assess your target**

- Determine the size of your target application. Auto-enumeration of static and dynamic URLs, and URL parameters.

X. **Assess token strength**

- Easily test the quality of randomness in data items intended to be unpredictable (e.g. tokens).

5. Significance of Conducting Vulnerability Assessment

A vulnerability assessment informs organizations on the weaknesses present in their environment and provides direction on how to reduce the risk those weaknesses cause. It also helps to reduce the chances of an attacker able to breach the organization’s IT systems while yielding a better understanding of assets, their vulnerabilities, and the overall risk to an organization.

For organizations seeking to reduce their security risk, a vulnerability assessment is a good place to start. It provides a thorough, inclusive assessment of hardware and software assets, identifying vulnerabilities and providing an intuitive risk score. A regular assessment program assists organizations with managing their risk in the face of an ever-evolving threat environment, identifying and scoring vulnerabilities so that attackers do not catch organizations unprepared. Some of the primary benefits of vulnerability assessment are:

- Identify known security exposures before an attacker finds them
- Define the level of risk that exists in a network
- Establish business risk/benefit curve
- Optimize security investments and reduces security risks by apply remediation tools that patches vulnerability

6. Conclusion

In conclusion, in this modern era of globalization, vulnerability threat has been popular in this digital world of security system. ‘Prevention is better than cure’. This proverb is really describing how vulnerability assessment is all about. As a modern people, this process of vulnerability assessment needs to be pay attention so that any kinds of threats that would lead to the harm of a system can be mitigate by simply having a deep analysis of a certain threat.

Day by day, vulnerability and threats keep expanding and can be more harmful and harder to detect by recent vulnerable assessment software. That’s why this type of software 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 to new trends of thread to make sure our vulnerabilities assessment software is always prepared for any new type of threats.

Everyone either a person in corporate business or even a student who study in security field need to learn and have a better understanding of vulnerabilities assessment. 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.