Introduction to Burp Suite

Khoi Nguyen Pham
Swinburne University of Technology
School of Science, Computing and Engineering Technologies
Hawthorn, Victoria 3122, Australia
Email: nguyenpham1441887@gmail.com

I. Introduction

The goal of this project is to deepen my understanding of the Burp Suite, a critical tool in the field of cybersecurity and penetration testing. By documenting my learnings from TryHackMe's "Burp Suite: The Basics" room, I aim to reinforce the concepts and techniques explored.

II. Burp Suite

A. What is Burp Suite?

Burp Suite is a Java-based platform designed to be a comprehensive solution for web application penetration testing. It is widely regarded as the industry standard for manual security assessments of web and mobile applications, including those relying on APIs (Application Programming Interfaces).

Essentially, Burp Suite works by intercepting and enabling the manipulation of HTTP/HTTPS traffic between a web browser and a web server. This interception capability is at the core of Burp Suite's functionality. It allows users to examine, modify, and route requests to different components of the Burp Suite framework. By modifying requests before they reach the server or altering responses before they return to the browser, Burp Suite becomes a powerful tool for manual web application testing.

B. Burp Suite Editions

Burp Suite is available in three main editions:

1) **Community Edition**: A free version suitable for non-commercial use, providing basic features for manual testing.
2) **Professional Edition**: An advanced, unrestricted version of the Community Edition that offers additional features for professionals:
   - An automated vulnerability scanner.
   - An unrestricted fuzzer/brute-forcer.
   - The ability to save projects for future use and generate reports.
   - A built-in API for integrating with other tools.
   - Support for adding new extensions to enhance functionality.
   - Access to the Burp Suite Collaborator, a tool for capturing external service interactions (self-hosted or hosted by PortSwigger).
3) **Enterprise Edition**: A server-based version focused on continuous scanning of web applications for vulnerabilities. This edition features an automated scanner for scheduled scans, making it comparable to infrastructure scanning tools like Nessus. Unlike the other editions, it emphasizes automation rather than manual testing.

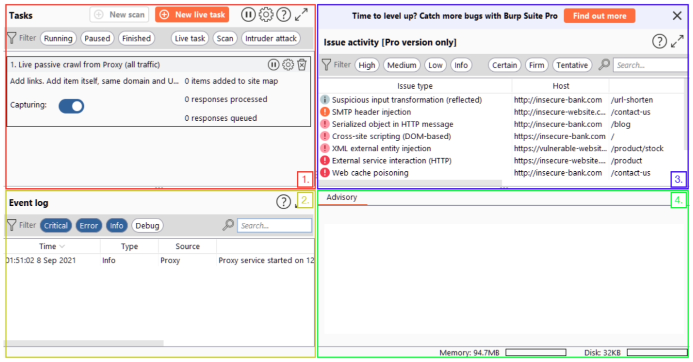
C. Key Features of Burp Suite Community Edition

Although the Community Edition of Burp Suite has a more limited feature set compared to the Professional Edition, it still offers a powerful range of tools for web application penetration testing. Below are its key features:

- **Proxy:** Burp Proxy is the most prominent tool in Burp Suite. It enables users to intercept and modify HTTP/HTTPS requests and responses when interacting with web applications.
- **Repeater:** This feature allows users to capture a request, modify it, and resend it multiple times. It is particularly useful for iterative testing, such as crafting payloads for SQL Injection (SQLi) or testing endpoint vulnerabilities.
- **Intruder:** Despite rate limitations in the Community Edition, Intruder enables sending numerous requests to endpoints, often used for brute-force attacks or fuzzing endpoints for vulnerabilities.
- **Decoder:** This tool supports encoding and decoding of data. It is useful for transforming captured information or preparing payloads within Burp Suite, streamlining the process.
- **Comparer:** Allows for comparison of two data sets at the byte or word level. The ability to send data directly from Burp Suite to this tool simplifies and accelerates the comparison process.
- **Sequencer:** Used to assess the randomness of tokens, such as session cookies or other supposedly random values. If randomness is insufficient, it could lead to significant security risks.

D. The Dashboard

The Burp Dashboard is divided into four quadrants, as labelled in counter-clockwise order starting from the top left:



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

Issue type	Host	
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten
SMTP header injection	http://insecure-website.c...	/contact-us
Serialized object in HTTP message	http://insecure-bank.com	/blog
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-websit...	/product/stock
External service interaction (HTTP)	https://insecure-website....	/product
Web cache poisoning	http://insecure-bank.com	/contact-us

Time	Type	Source	
01:51:02 8 Sep 2021	Info	Proxy	Proxy service started on 12

Fig. 1. The Dashboard

1) **Tasks:** The Tasks menu enables you to define background tasks for Burp Suite to perform while using the application. In Burp Suite Community, the default *Live Passive Crawl* task, which logs visited pages, is sufficient for this module. Burp Suite Professional provides additional tasks, such as on-demand scans.
2) **Event Log:** The Event Log records actions taken by Burp Suite, such as starting the proxy, along with details of the connections made through Burp Suite.
3) **Issue Activity:** Available in Burp Suite Professional, this section displays vulnerabilities identified by the automated scanner, ranked by severity and filterable based on certainty.
4) **Advisory:** The Advisory section offers detailed information on identified vulnerabilities, including references and suggested remediations. This can be exported into a report. In Burp Suite Community, this section may not display any vulnerabilities.

E. Navigating Burp Suite

Burp Suite's interface uses a straightforward navigation system primarily managed through its menu bars, making it easy to switch between modules and access sub-tabs.

- **Module Selection:** The top menu bar displays the available modules in Burp Suite. Clicking on a module switches to its interface. For example, selecting the *Burp Proxy* module will open its specific functionalities.
- **Sub-Tabs:** Modules with additional settings or options have sub-tabs located in a secondary menu bar below the main menu bar. For instance, within the *Burp Proxy* module, you can select the *Intercept* sub-tab.
- **Detaching Tabs:** Tabs can be detached into separate windows for multitasking. Navigate to the *Window* menu above the Module Selection bar, select the *Detach* option to open the tab in a new window, and reattach tabs using the same steps.
- **Keyboard Shortcuts:** Burp Suite offers keyboard shortcuts for quick navigation:
  - `Ctrl + Shift + D`: Dashboard
  - `Ctrl + Shift + T`: Target tab
  - `Ctrl + Shift + P`: Proxy tab
  - `Ctrl + Shift + I`: Intruder tab
  - `Ctrl + Shift + R`: Repeater tab

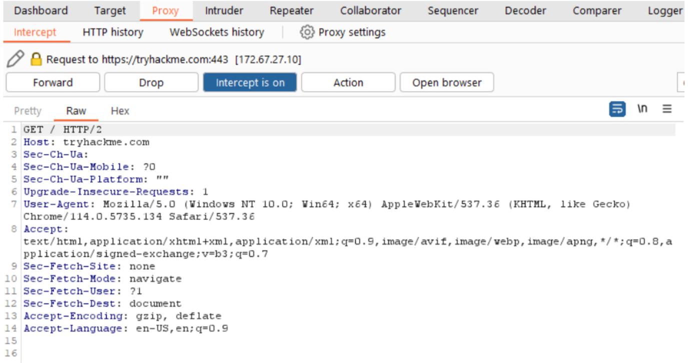
III. Burp Proxy

A. What is Burp Proxy?

The Burp Proxy is an essential tool within Burp Suite, allowing for the interception of requests and responses between the user and the target web server. This captured traffic can be modified, forwarded to other tools for additional analysis, or permitted to reach its intended destination.

Key Points to Understand About the Burp Proxy:

- **Intercepting Requests**: Requests passing through the Burp Proxy are intercepted and held back from reaching the target server. These requests appear in the Proxy tab, where actions such as forwarding, dropping, editing, or routing them to other Burp modules can be performed. To stop interception and allow requests to pass through, simply click the ”Intercept is on” button to disable it.

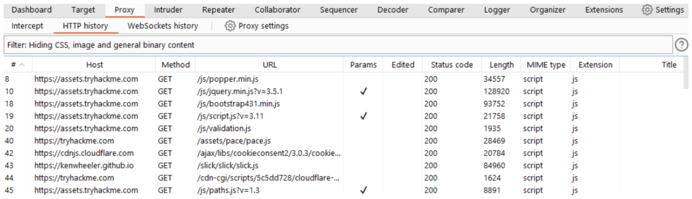


Request to https://tryhackme.com:443 [172.67.27.10]

```
GET / HTTP/2
Host: tryhackme.com
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.5735.134 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


```

- **Taking Control**: Intercepting requests allows testers to fully control web traffic, which is invaluable for web application testing.
- **Capture and Logging**: By default, Burp Suite captures and logs all requests made through the proxy, even if interception is disabled. This logged data can be useful for later analysis and review of past requests.
- **WebSocket Support**: Burp Suite also captures and logs WebSocket traffic, providing additional insights when analyzing web applications.
- **Logs and History**: Captured requests can be accessed through the HTTP history and WebSockets history sub-tabs, enabling retrospective analysis and the ability to forward them to other Burp modules as necessary.



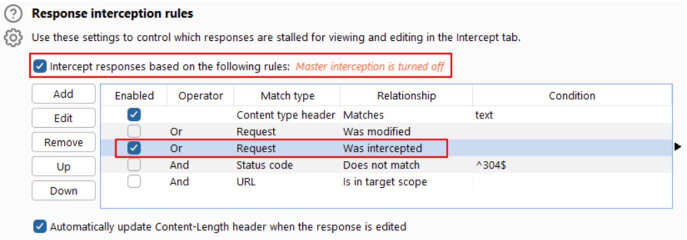
Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title
8	https://assets.tryhackme.com	GET	/js/popper.min.js			200	34557	script	js	
10	https://assets.tryhackme.com	GET	/js/jquery.min.js?v=3.5.1	✓		200	128920	script	js	
18	https://assets.tryhackme.com	GET	/js/bootstrap431.min.js			200	93752	script	js	
19	https://assets.tryhackme.com	GET	/js/script.js?v=3.11	✓		200	21758	script	js	
20	https://assets.tryhackme.com	GET	/js/validation.js			200	1935	script	js	
40	https://tryhackme.com	GET	/assets/pace/pace.js			200	28469	script	js	
42	https://cdnjs.cloudflare.com	GET	/ajax/libs/cookieconsent2/3.0.3/cookie...			200	20784	script	js	
43	https://kenwheeler.github.io	GET	/slick/slick/slick.js			200	84960	script	js	
44	https://tryhackme.com	GET	/cdn-cgi/scripts/5c5dd728/cloudflare-...			200	1624	script	js	
45	https://assets.tryhackme.com	GET	/js/paths.js?v=1.3	✓		200	8891	script	js	

- Proxy-specific settings are available by clicking the Proxy settings button, allowing extensive control over its functionality. It's recommended to familiarize yourself with these options to maximize the utility of Burp Proxy.

Some Notable Features in the Proxy Settings

- **Response Interception**: By default, the proxy does not intercept server responses unless explicitly configured. The option ”Intercept responses based on the following rules” allows for more flexible response interception through defined rules.


Response interception rules

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

☑ Intercept responses based on the following rules: *Master interception is turned off*

Enabled	Operator	Match type	Relationship	Condition
☑		Content type header	Matches	text
□	Or	Request	Was modified	
☑	Or	Request	Was intercepted	
□	And	Status code	Does not match	^304$
□	And	URL	Is in target scope	

☑ Automatically update Content-Length header when the response is edited

- **Match and Replace**: The ”Match and Replace” feature in the Proxy settings enables the use of regular expressions (regex) to modify both incoming and outgoing requests. This functionality supports dynamic alterations, such as changing the user agent or adjusting cookies.

B. *Connecting through the Proxy (FoxyProxy)*

Follow these steps to configure the Burp Suite Proxy using the FoxyProxy extension:

1) **Install FoxyProxy**: Download and install the FoxyProxy Basic extension for your browser.
   - *Note*: FoxyProxy is pre-installed on the AttackBox.
2) **Access FoxyProxy Options**: After installation, a FoxyProxy icon will appear at the top-right corner of your Firefox browser. Click on this icon to open the FoxyProxy options pop-up.
3) **Create a Burp Proxy Configuration**: In the FoxyProxy options pop-up, click on the *Options* button. This will open a new browser tab with configuration settings. Click the *Add* button to create a new proxy configuration.

4) **Add Proxy Details**: On the *Add Proxy* page, provide the following values:
   - **Title**: Burp (or any other preferred name)
   - **Proxy IP**: `127.0.0.1`
   - **Port**: `8080`
5) **Save Configuration**: Click the *Save* button to finalize and store the Burp Proxy configuration.
6) **Activate the Proxy Configuration**: Click the FoxyProxy icon in Firefox and select the Burp configuration. This will route your browser's traffic through `127.0.0.1:8080`. Ensure Burp Suite is running to successfully redirect browser traffic through this configuration.
7) **Enable Proxy Interception in Burp Suite**: Open Burp Suite and verify that the *Intercept* option is enabled within the Proxy tab.
8) **Test the Proxy**: Open Firefox and navigate to a website (e.g., `http://10.10.169.244/`). If configured correctly, the browser will pause while Burp Suite captures the HTTP request. Congratulations! You have successfully intercepted your first request.

C. Site Map and Issue Definitions

The **Target** tab in Burp Suite offers features that go beyond scoping, comprising the following sub-tabs:

1) **Site Map**: Displays a tree structure of web applications targeted during testing. Any pages visited while the proxy is active are automatically added to the site map. This is particularly useful for mapping APIs, as API endpoints accessed by the application are captured here.
2) **Issue Definitions**: Lists all vulnerabilities that Burp Suite scans for, along with descriptions and references. While full scanning capabilities are unavailable in the Community Edition, this section serves as a valuable reference for reports and manual testing.
3) **Scope Settings**: Allows inclusion or exclusion of specific domains or IPs to define the testing scope. This helps testers focus on relevant web applications while avoiding unnecessary traffic.

The **Target** tab thus enables efficient mapping of web applications, fine-tuning of target scopes, and access to a comprehensive vulnerability reference.

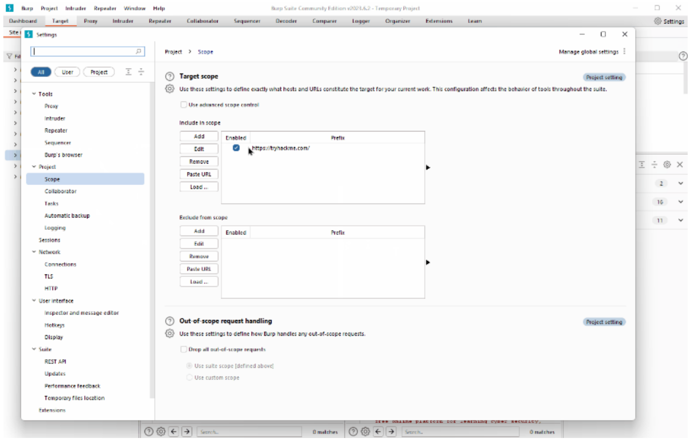
D. The Burp Suite Browser

Burp Suite comes with a built-in Chromium browser that is pre-configured to work seamlessly with the proxy, eliminating the need for manual setup. If running Burp Suite as the root user on Linux (e.g., on the AttackBox), the Burp Browser may fail to start due to sandboxing issues.

***Solution*:** Go to **Settings** → **Tools** → **Burp's browser** and enable the **Allow Burp's browser to run without a sandbox** option.

E. Scoping and Targeting

Scoping helps avoid overwhelming traffic by focusing Burp Suite on specific web applications. To set the scope, go to the **Target** tab, right-click on your target, and select *Add to Scope*. Burp will ask if you want to stop logging traffic outside the scope—select *Yes* to limit the focus to your target web application(s).



Target scope

Use these settings to define exactly what hosts and URLs constitute the target for your current work. This configuration affects the behavior of tools throughout the suite.

☐ Use advanced scope control

Include in scope

Enabled	Prefix
☑	https://tryhackme.com/

Exclude from scope

Enabled	Prefix

Out-of-scope request handling

Use these settings to define how Burp handles any out-of-scope requests.

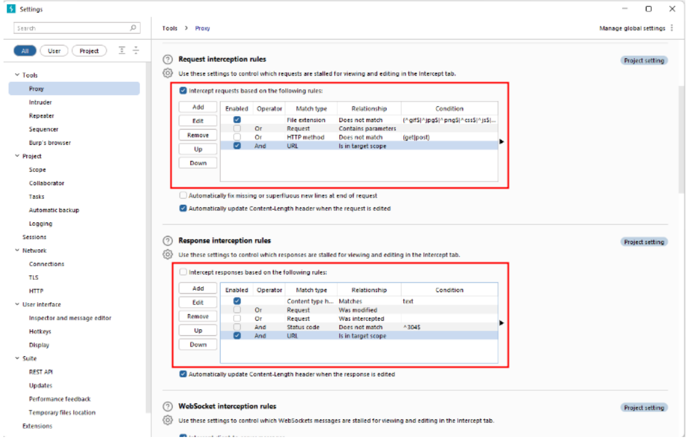
☐ Drop all out-of-scope requests

● Use suite scope [defined above]

○ Use custom scope

To verify the scope, navigate to the **Scope settings** sub-tab under the **Target** tab. This window lets us manage the target scope by including or excluding domains/IPs. It's a powerful tool worth exploring.

Even if out-of-scope traffic logging is disabled, the proxy still intercepts all traffic. To prevent this, go to the **Proxy settings** sub-tab and select *And URL is in target scope* under the *Intercept Client Requests* section.



Request interception rules Project setting

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$|...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
☑	And	URL	Is in target scope	

Add | Edit | Remove | Up | Down

□ Automatically fix missing or superfluous new lines at end of request

☑ Automatically update Content-Length header when the request is edited

Response interception rules Project setting

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

□ Intercept responses based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		Content type h...	Matches	text
□	Or	Request	Was modified	
□	Or	Request	Was intercepted	
□	And	Status code	Does not match	^304$
☑	And	URL	Is in target scope	

Add | Edit | Remove | Up | Down

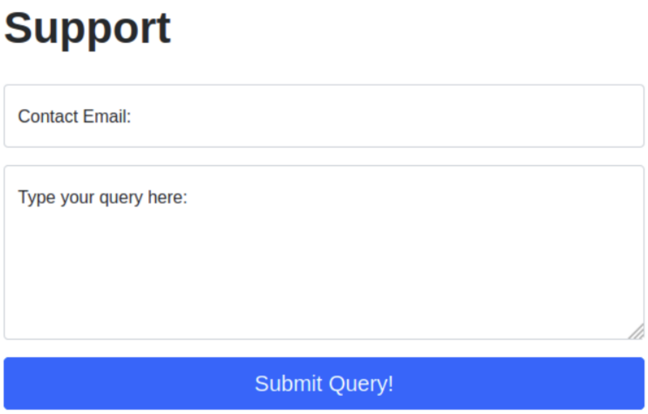
☑ Automatically update Content-Length header when the response is edited

WebSocket interception rules Project setting

Use these settings to control which WebSockets messages are stalled for viewing and editing in the Intercept tab.

F. *Example Attack*

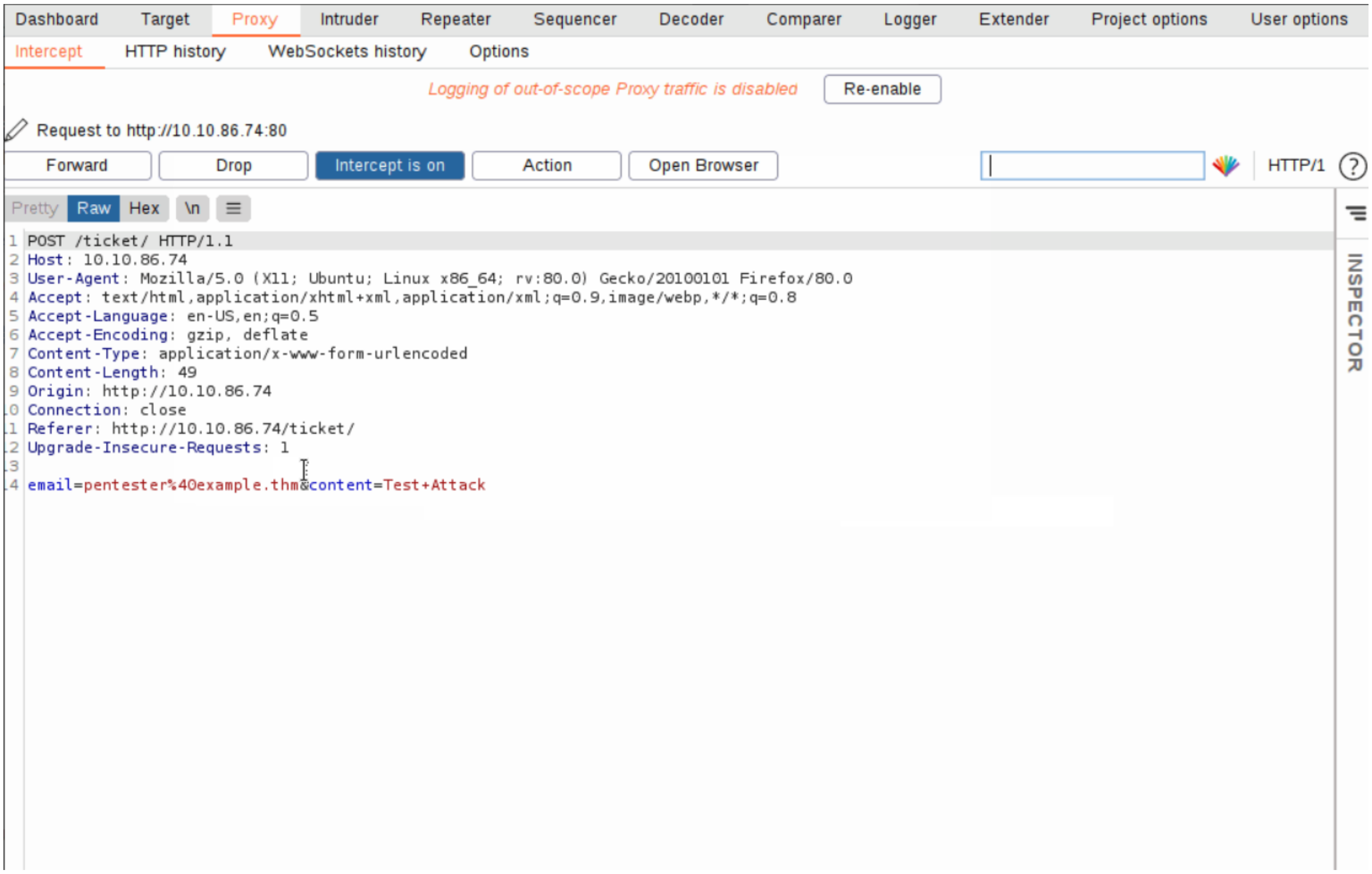
We will start by taking a look at the support form at `http://10.10.169.244/ticket/`:



Try typing: `<script>alert("Succ3ssful XSS")</script>` into the ”Contact Email” field. You should notice a client-side filter that prevents special characters not allowed in email addresses.

Fortunately, client-side filters are easy to bypass. Here’s how to do it:

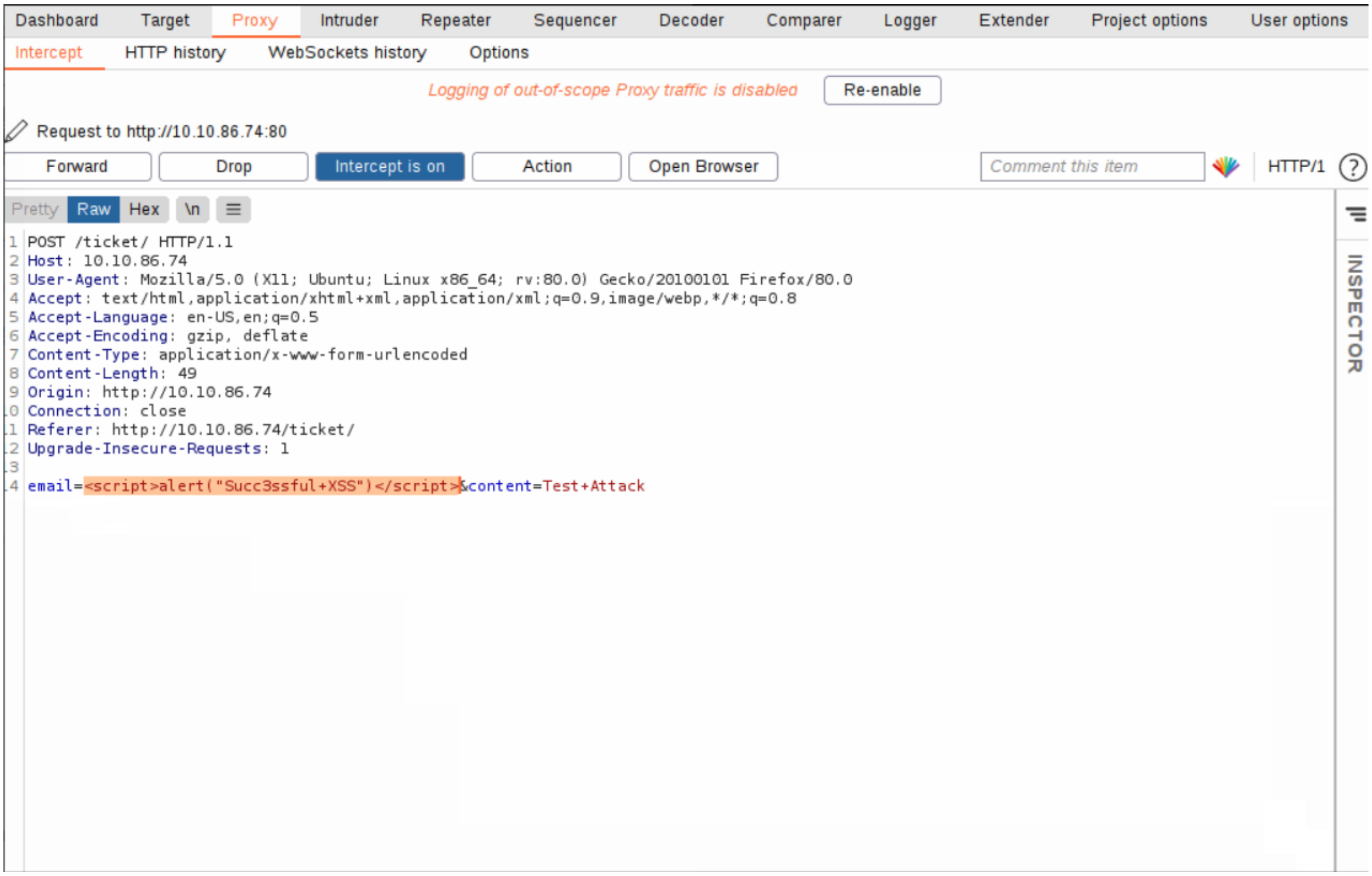
1) Ensure that Burp Proxy is active and intercepting requests.
2) Enter valid data into the support form, such as ”pentester@example.thm” for the email address and ”Test Attack” for the query.
3) Submit the form so the request will be intercepted by Burp Proxy.
4) In Burp, modify the email field to: `<script>alert("Succ3ssful XSS")</script>`.



```
POST /ticket/ HTTP/1.1
Host: 10.10.86.74
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://10.10.86.74
Connection: close
Referer: http://10.10.86.74/ticket/
Upgrade-Insecure-Requests: 1

email=pentester%40example.thm&content=Test+Attack
```

5) Select the payload, then URL encode it using the `Ctrl + U` shortcut.



Logging of out-of-scope Proxy traffic is disabled

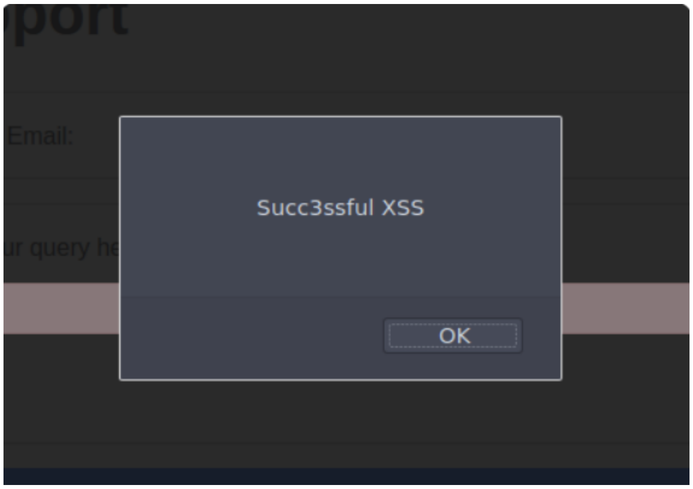
Request to http://10.10.86.74:80

```
POST /ticket/ HTTP/1.1
Host: 10.10.86.74
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 49
Origin: http://10.10.86.74
Connection: close
Referer: http://10.10.86.74/ticket/
Upgrade-Insecure-Requests: 1

email=<script>alert("Succ3ssful+XSS")</script>&content=Test+Attack
```

6) Press ”Forward” to send the modified request.

If successful, an alert box should appear from the site confirming the XSS attack.



Succ3ssful XSS

IV. Conclusion

In conclusion, Burp Suite has proven to be a valuable tool for security testing and vulnerability scanning. Its features, such as traffic interception and automated scans, make it essential for cybersecurity tasks. I look forward to expanding my knowledge of Burp Suite in the future and using its advanced capabilities for more complex security assessments.