TryHackMe – Burp Suite: The Basics

An introduction to using Burp Suite for web application pentesting.

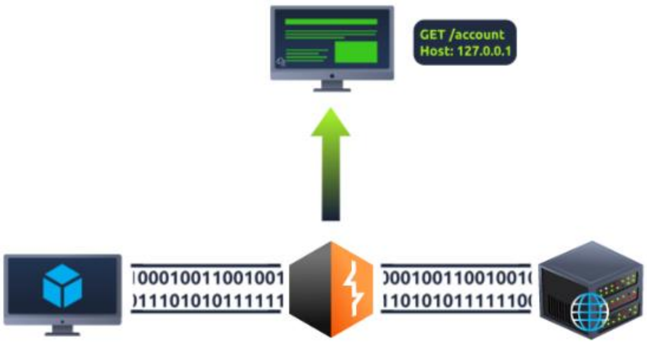
Task 1: Introduction

Burp Suite is an integrated platform for performing security testing of web applications. It includes various tools for scanning, fuzzing, intercepting, and analyzing web traffic. It is used by security professionals worldwide to find and exploit vulnerabilities in web applications.

Task 2: What is Burp Suite?

In essence, Burp Suite is a Java-based framework designed to serve as a comprehensive solution for conducting web application penetration testing. It has become the industry standard tool for hands-on security assessments of web and mobile applications, including those that rely on **a**pplication **p**rogramming **i**nterface**s** (APIs).

Simply put, Burp Suite captures and enables manipulation of all the HTTP/HTTPS traffic between a browser and a web server. By intercepting requests, users have the flexibility to route them to various components within the Burp Suite framework. The ability to intercept, view, and modify web requests before they reach the target server or even manipulate responses before, they are received by our browser makes Burp Suite an invaluable tool for manual web application testing.

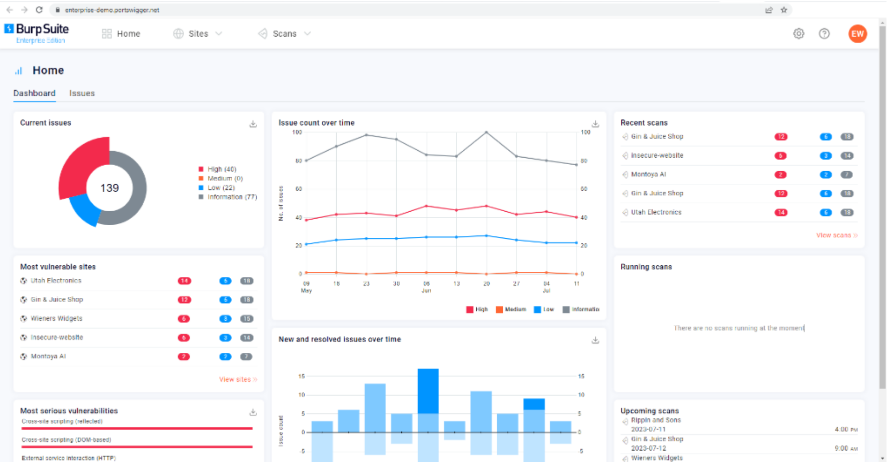


Burp Suite is available in different editions. For our purposes, we will focus on the **Burp Suite Community Edition**, which is freely accessible for non-commercial use within legal boundaries. However, it's worth noting that Burp Suite also offers Professional and Enterprise editions, which come with advanced features and require licensing:

1. **Burp Suite Professional** is an unrestricted version of Burp Suite Community. It comes with features such as:
    - An automated vulnerability scanner.
    - A fuzzer/brute-forcer that isn't rate limited.
    - Saving projects for future use and report generation.
    - A built-in API to allow integration with other tools.
    - Unrestricted access to add new extensions for greater functionality.
    - Access to the Burp Suite Collaborator (effectively providing a unique request catcher self-hosted or running on a Portswigger-owned server).

    In short, Burp Suite Professional is a highly potent tool, making it a preferred choice for professionals in the field.

2. **Burp Suite Enterprise**, in contrast to the community and professional editions, is primarily utilized for continuous scanning. It features an automated scanner that periodically scans web applications for vulnerabilities, similar to how tools like Nessus perform automated infrastructure scanning. Unlike the other editions, which allow manual attacks from a local machine, Burp Suite Enterprise resides on a server and constantly scans the target web applications for potential vulnerabilities.



Most vulnerable sites			
Utah Electronics	14	6	18
Gin & Juice Shop	12	6	18
Wieners Widgets	6	3	15
Insecure-website	6	3	14
Montoya AI	2	2	7

Recent scans			
Gin & Juice Shop	12	6	18
insecure-website	6	3	14
Montoya AI	2	2	7
Gin & Juice Shop	12	6	18
Utah Electronics	14	6	18

There are no scans running at the moment

Most serious vulnerabilities
Cross-site scripting (reflected)
Cross-site scripting (DOM-based)
External service interaction (HTTP)

Upcoming scans
Rippin and Sons 2023-07-11 4:00 PM
Gin & Juice Shop 2023-07-12 9:00 AM
Wieners Widgets

Due to requiring a license for the Professional and Enterprise editions, we will focus on the core feature set provided by the Burp Suite Community Edition.

Note: The provided demonstrations utilize Burp Suite for Windows. However, the functionality remains consistent with the version installed on the AttackBox from THM.

Question 1: Which edition of Burp Suite runs on a server and provides constant scanning for target web apps?

Answer: ***Burp Suite Enterprise***

Question 2: Burp Suite is frequently used when attacking web applications and _______ applications.

Answer: ***mobile***

Task 3: Features of Burp Community

Although Burp Suite Community offers a more limited feature set compared to the Professional edition, it still provides an impressive array of tools that are highly valuable for web application testing. Let's explore some of the key features:

- **Proxy**: The Burp Proxy is the most renowned aspect of Burp Suite. It enables interception and modification of requests and responses while interacting with web applications.
- **Repeater**: Another well-known feature. Repeater allows for capturing, modifying, and resending the same request multiple times. This functionality is particularly useful when crafting payloads through trial and error (e.g., in SQLi - Structured Query Language Injection) or testing the functionality of an endpoint for vulnerabilities.
- **Intruder**: Despite rate limitations in Burp Suite Community, Intruder allows for spraying endpoints with requests. It is commonly utilized for brute-force attacks or fuzzing endpoints.
- **Decoder**: Decoder offers a valuable service for data transformation. It can decode captured information or encode payloads before sending them to the target. While alternative services exist for this purpose, leveraging Decoder within Burp Suite can be highly efficient.
- **Comparer**: As the name suggests, Comparer enables the comparison of two pieces of data at either the word or byte level. While not exclusive to Burp Suite, the ability to send potentially large data segments directly to a comparison tool with a single keyboard shortcut significantly accelerates the process.
- **Sequencer**: Sequencer is typically employed when assessing the randomness of tokens, such as session cookie values or other supposedly randomly generated data. If the algorithm used for generating these values lacks secure randomness, it can expose avenues for devastating attacks.

Question 3: Which Burp Suite feature allows us to intercept requests between ourselves and the target?

Answer: *Proxy*

Question 4: Which Burp tool would we use to brute-force a login form?

Answer: *Intruder*

Task 4: Installation

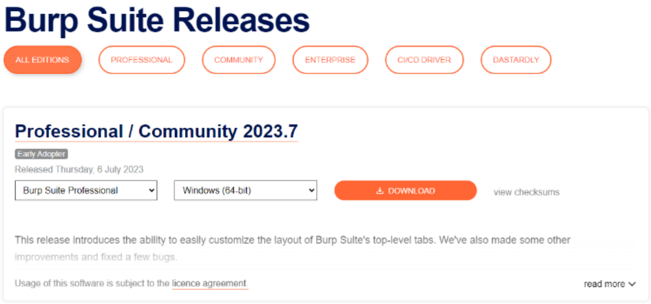
Burp Suite is one of those tools that is very useful to have around, whether for web or mobile application assessments, pentesting, bug bounty hunting, or even debugging features in web app development. Here's a guide on installing Burp Suite on different platforms:

Note: If you use the AttackBox, Burp Suite is already installed, so you can skip this step.

Downloads

Kali Linux: Burp Suite comes pre-installed with Kali Linux. In case it is missing on your Kali installation, you can easily install it from the Kali apt repositories.

Linux, macOS, and Windows: For other operating systems, PortSwigger provides dedicated installers for Burp Suite Community and Burp Suite Professional on the Burp Suite downloads page. Choose your operating system from the dropdown menu and select **Burp Suite Community Edition**. Then, click the **Download** button to initiate the download.



Burp Suite Releases

Professional / Community 2023.7

Early Adopter

Released Thursday, 6 July 2023

Burp Suite Professional | Windows (64-bit)

This release introduces the ability to easily customize the layout of Burp Suite's top-level tabs. We've also made some other improvements and fixed a few bugs.

Usage of this software is subject to the licence agreement.

Installation

Install Burp Suite using the appropriate method for your operating system. On Windows, run the executable file, while on Linux, execute the script from the terminal (with or without sudo). If you choose not to use **sudo** during installation on Linux, Burp Suite will be installed in your home directory at **~/BurpSuiteCommunity/BurpSuiteCommunity** and will not be added to your **PATH**.

The installation wizard provides clear instructions, and it is generally safe to accept the default settings. However, it is always recommended to review the installer carefully.

With Burp Suite successfully installed, you can now launch the application. In the next task, we will explore the initial setup and configuration.

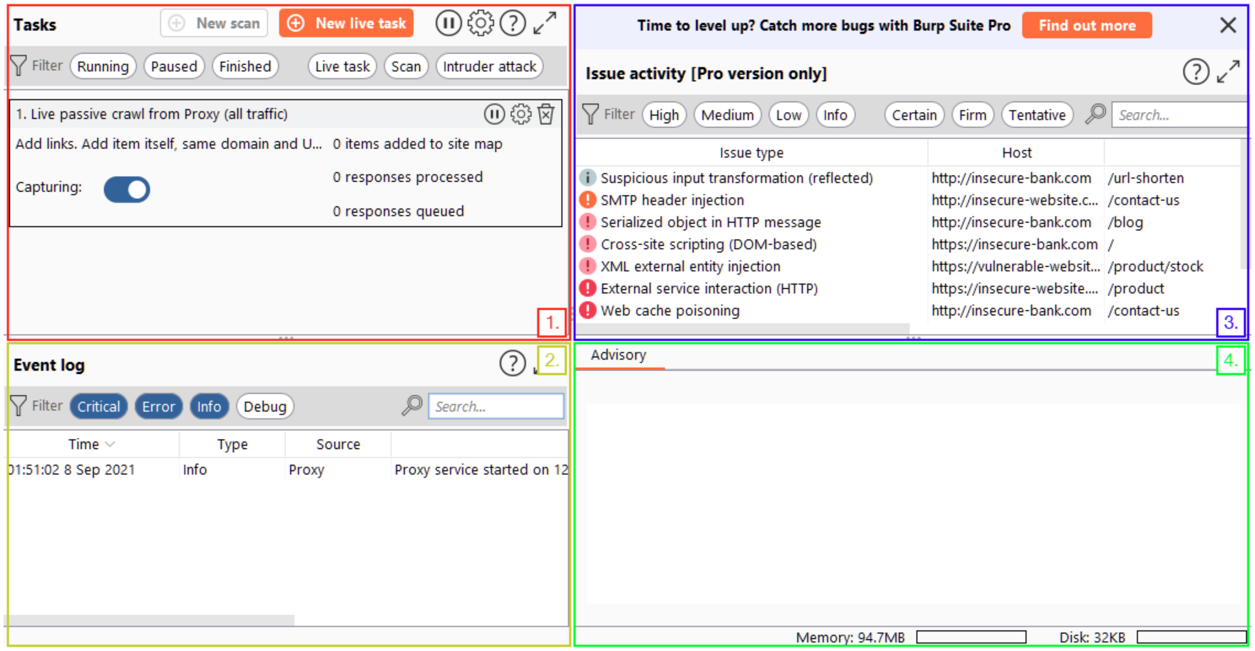
Task 5: The Dashboard

You may use the pre-installed Burp Suite Community Edition in THM AttackBox. To launch the AttackBox, click the **Start AttackBox** button at the top of the page.

Once you launch Burp Suite and accept the terms and conditions, you will be prompted to select a project type. In Burp Suite Community, the options are limited, and you can simply click **Next** to proceed.

The next window allows you to choose the configuration for Burp Suite. It is generally recommended to keep the default settings, which are suitable for most situations. Click **Start Burp** to open the main Burp Suite interface.

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

1. **Tasks**: The Tasks menu allows you to define background tasks that Burp Suite will perform while you use the application. In Burp Suite Community, the default "Live Passive Crawl" task, which automatically logs the pages visited, is sufficient for our purposes in this module. Burp Suite Professional offers additional features like on-demand scans.
2. **Event log**: The Event log provides information about the actions performed by Burp Suite, such as starting the proxy, as well as details about connections made through Burp.
3. **Issue Activity**: This section is specific to Burp Suite Professional. It displays the vulnerabilities identified by the automated scanner, ranked by severity and filterable based on the certainty of the vulnerability.
4. **Advisory**: The Advisory section provides more detailed information about the identified vulnerabilities, including references and suggested remediations. This information can be exported into a report. In Burp Suite Community, this section may not show any vulnerabilities.

Question 5: What menu provides information about the actions performed by Burp Suite, such as starting the proxy, and details about connections made through Burp?

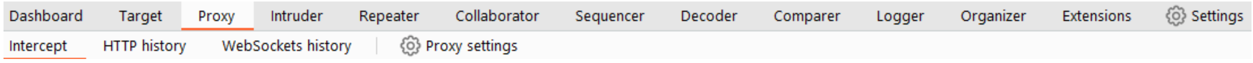
Answer: *Event log*

Task 6: Navigation

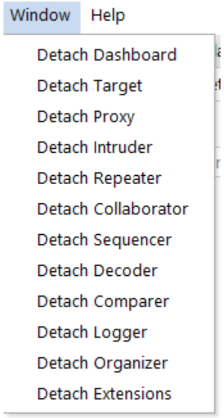
In Burp Suite, the default navigation is primarily done through the top menu bars, which allow you to switch between modules and access various sub-tabs within each module. The sub-tabs appear in a second menu bar directly below the main menu bar.

Here's how the navigation works:

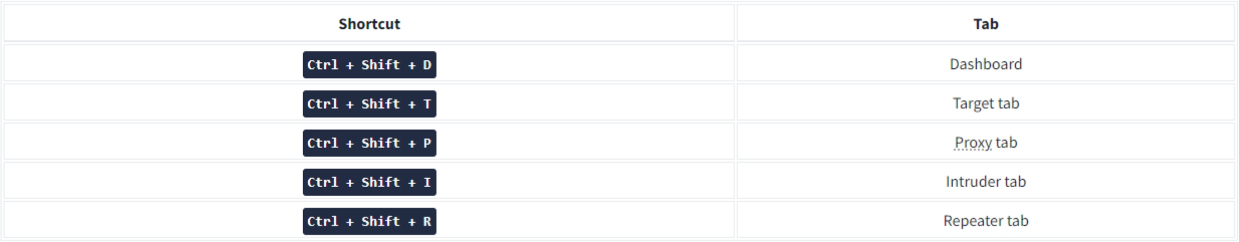
1. **Module Selection**: The top row of the menu bar displays the available modules in Burp Suite. You can click on each module to switch between them. For example, the Burp Proxy module is selected in the image below.



2. **Sub-Tabs**: If a selected module has multiple sub-tabs, they can be accessed through the second menu bar that appears directly below the main menu bar. These sub-tabs often contain module-specific settings and options. For example, in the image above, the Proxy Intercept sub-tab is selected within the Burp Proxy module.
3. **Detaching Tabs**: If you prefer to view multiple tabs separately, you can detach them into separate windows. To do this, go to the **Window** option in the application menu above the **Module Selection** bar. From there, choose the "Detach" option, and the selected tab will open in a separate window. The detached tabs can be reattached using the same method.



Burp Suite also provides keyboard shortcuts for quick navigation to key tabs. By default, the following shortcuts are available:



Shortcut	Tab
`Ctrl + Shift + D`	Dashboard
`Ctrl + Shift + T`	Target tab
`Ctrl + Shift + P`	Proxy tab
`Ctrl + Shift + I`	Intruder tab
`Ctrl + Shift + R`	Repeater tab

Question 6: Which tab Ctrl + Shift + P will switch us to?

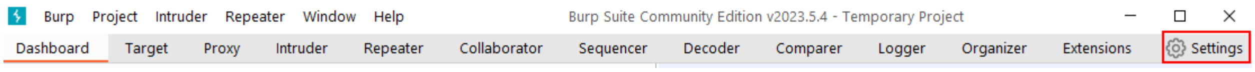
Answer: *Proxy tab*

Task 7: Options

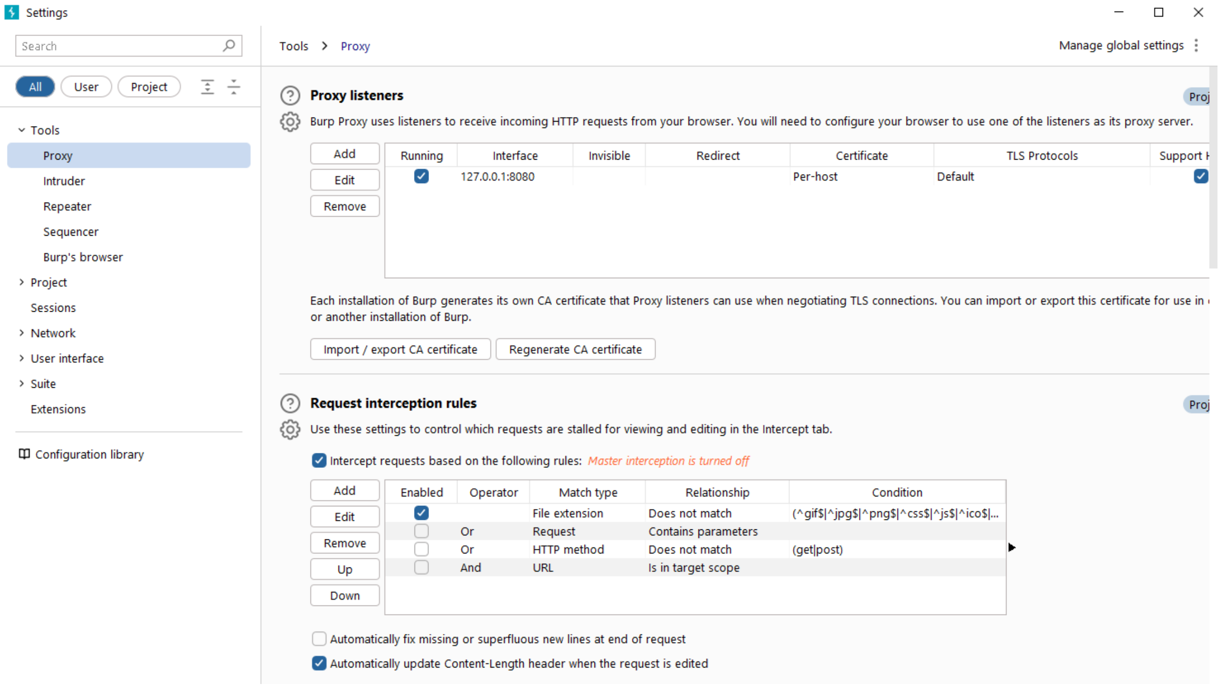
Before diving into the Burp Proxy, let's explore the available options for configuring Burp Suite. There are two types of settings: Global settings (also known as User settings) and Project settings.

- **Global Settings**: These settings affect the entire Burp Suite installation and are applied every time you start the application. They provide a baseline configuration for your Burp Suite environment.
- **Project Settings**: These settings are specific to the current project and apply only during the session. However, please note that Burp Suite Community Edition does not support saving projects, so any project-specific options will be lost when you close Burp.

  To access the settings, click on the **Settings** button in the top navigation bar. This will open a separate settings window.



Below is the image showing the separate settings window.



Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols	Support H
☑	127.0.0.1:8080			Per-host	Default	☑

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in
or another installation of Burp.

Request interception rules

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

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

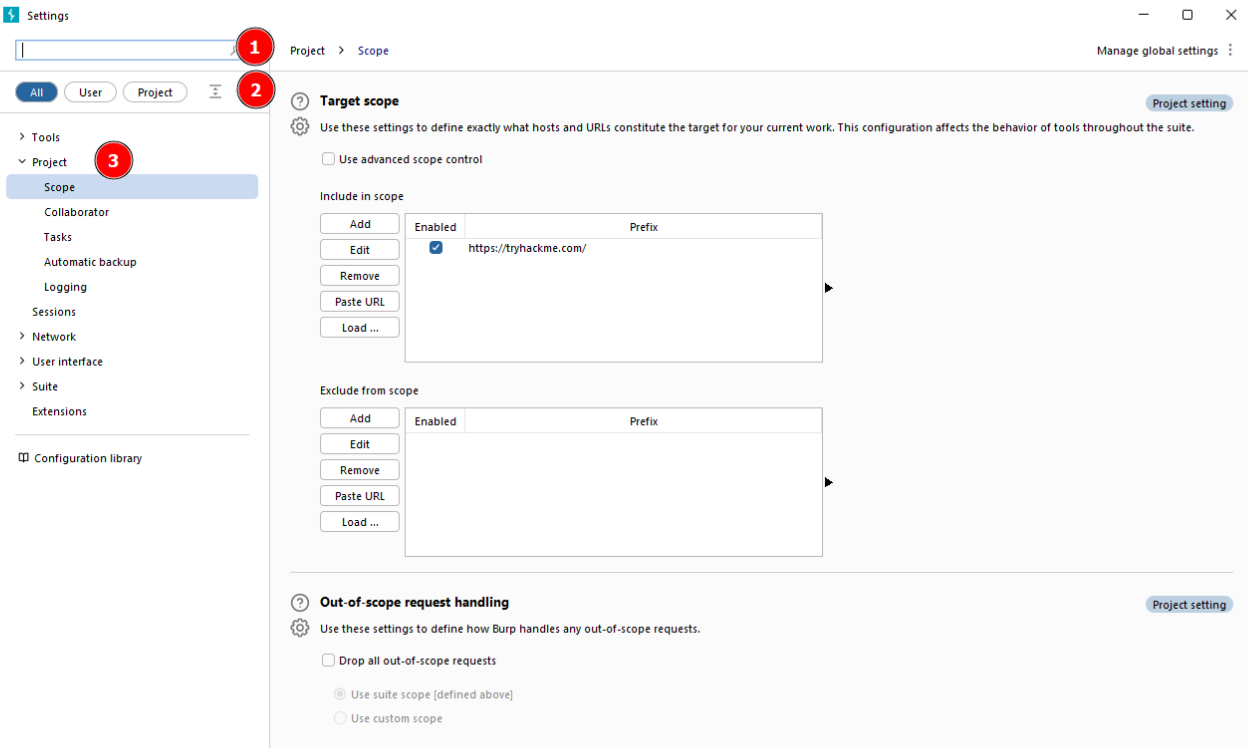
Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$\|^ico$|...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
□	And	URL	Is in target scope	

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

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

In the Settings window, you will find a menu on the left-hand side. This menu allows you to switch between different types of settings, including:

1. **Search**: Enables searching for specific settings using keywords.
2. **Type filter**: Filters the settings for **User** and **Project** options.
   - **User settings**: Shows settings that affect the entire Burp Suite installation.
   - **Project settings**: Displays settings specific to the current project.
3. **Categories**: Allows selecting settings by category.



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

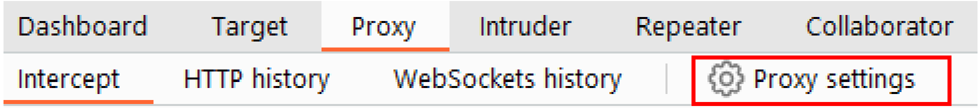
Use these settings to define how Burp handles any out-of-scope requests.

☐ Drop all out-of-scope requests

● Use suite scope [defined above]

○ Use custom scope

It's worth noting that many tools within Burp Suite provide shortcuts to specific categories of settings. For example, the **Proxy** module includes a **Proxy settings** button that opens the settings window directly to the relevant proxy section.



The search feature on the settings page is a valuable addition, allowing you to quickly search for settings using keywords.

Question 7: In which category can you find a reference to a "Cookie jar"?

Answer: *sessions*

Question 8: In which base category can you find the "Updates" sub-category, which controls the Burp Suite update behaviour?

Answer: *suite*

Question 9: What is the name of the sub-category which allows you to change the keybindings for shortcuts in Burp Suite?

Answer: *Hotkeys*

Question 10: If we have uploaded Client-Side TLS certificates, can we override these on a per-project basis (yea/nay)?

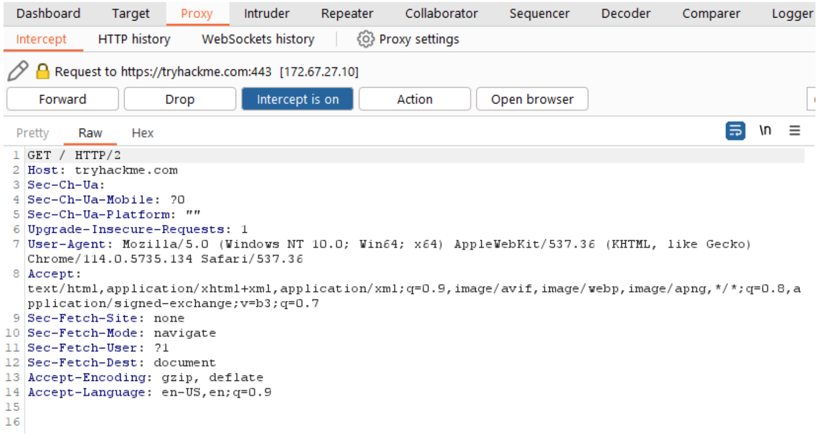
Answer: *yea*

Task 8: Introduction to the Burp Proxy

The Burp Proxy is a fundamental and crucial tool within Burp Suite. It enables the capture of requests and responses between the user and the target web server. This intercepted traffic can be manipulated, sent to other tools for further processing, or explicitly allowed to continue to its destination.

Key Points to Understand About the Burp **Proxy**

- **Intercepting Requests:** When requests are made through the Burp Proxy, they are intercepted and held back from reaching the target server. The requests appear in the Proxy tab, allowing for further actions such as forwarding, dropping, editing, or sending them to other Burp modules. To disable the intercept and allow requests to pass through the proxy without interruption, click the **Intercept is on** button.

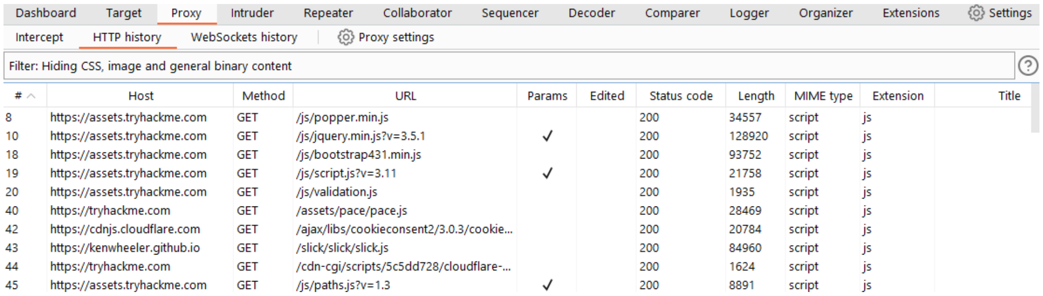


Request to https://tryhackme.com:443 [172.67.27.10]

```
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:** The ability to intercept requests empowers testers to gain complete control over web traffic, making it invaluable for testing web applications.
- **Capture and Logging:** Burp Suite captures and logs requests made through the proxy by default, even when the interception is turned off. This logging functionality can be helpful for later analysis and review of prior requests.
- **WebSocket Support:** Burp Suite also captures and logs WebSocket communication, providing additional assistance when analyzing web applications.
- **Logs and History:** The captured requests can be viewed in the **HTTP history** and **WebSockets history** sub-tabs, allowing for retrospective analysis and sending the requests to other Burp modules as needed.



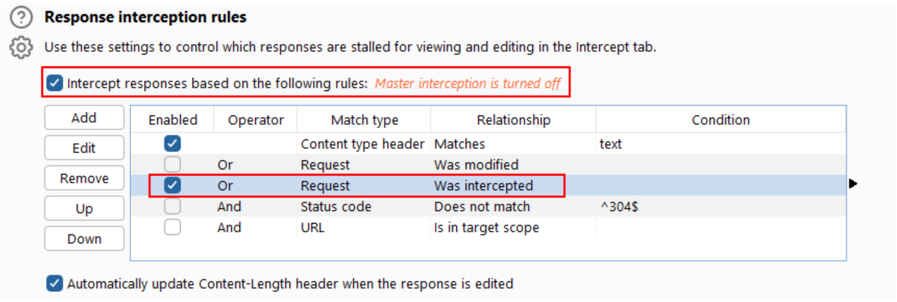
Filter: Hiding CSS, image and general binary content

#	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 options can be accessed by clicking the **Proxy settings** button. These options provide extensive control over the Proxy's behavior and functionality. Familiarize yourself with these options to optimize your Burp Proxy usage.

Some Notable Features in the **Proxy** Settings

- **Response Interception:** By default, the proxy does not intercept server responses unless explicitly requested on a per-request basis. The "Intercept responses based on the following rules" checkbox, along with the defined rules, allows for a more flexible response interception.



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" section in the **Proxy settings** enables the use of regular expressions (regex) to modify incoming and outgoing requests. This feature allows for dynamic changes, such as modifying the user agent or manipulating cookies.

Task 9: Connecting through the Proxy (FoxyProxy)

Start the machine by clicking the **Start Machine** button at the upper right corner of this task in THM.

To use the Burp Suite Proxy, we need to configure our local web browser to redirect traffic through Burp Suite. In this task, we will focus on configuring the proxy using the FoxyProxy extension in Firefox.

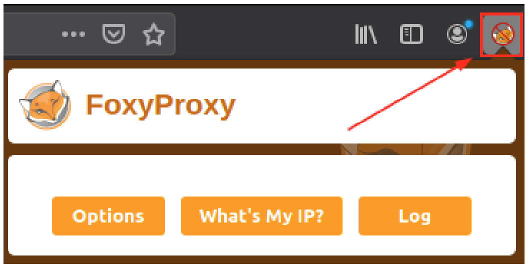
Please note that the instructions provided are specific to Firefox. If you are using a different browser, you may need to find alternative methods or use the TryHackMe AttackBox.

Here are the steps to configure the Burp Suite Proxy with FoxyProxy:

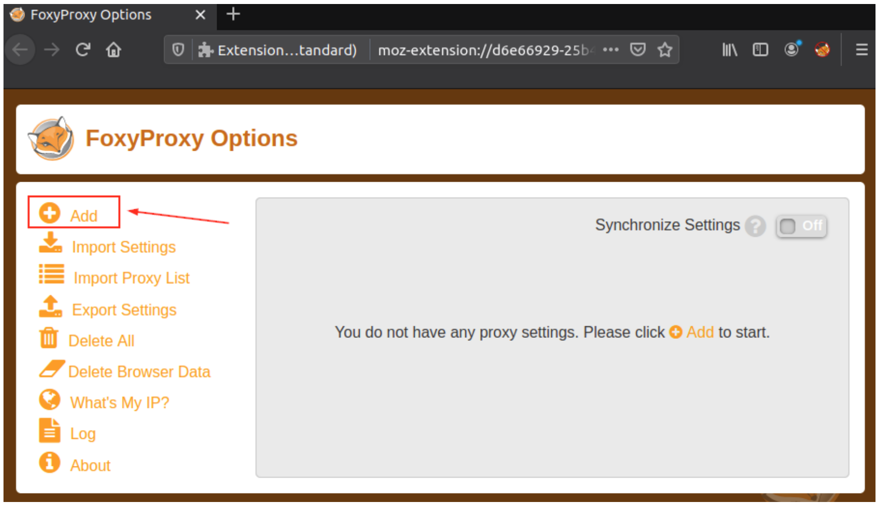
1. **Install FoxyProxy:** Download and install the FoxyProxy Basic extension.

   Note: FoxyProxy is already installed on the AttackBox.

2. **Access FoxyProxy Options:** Once installed, a button will appear at the top right of the Firefox browser. Click on the FoxyProxy button to access the FoxyProxy options pop-up.

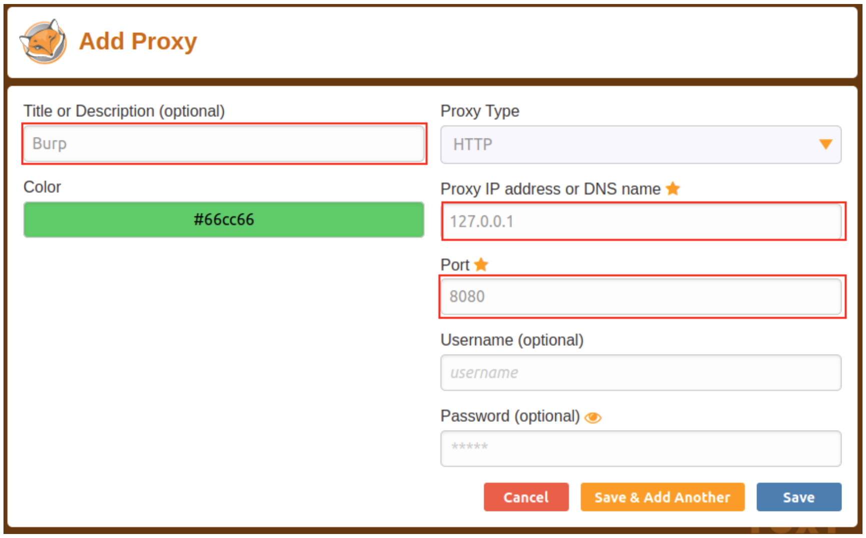


3. **Create Burp Proxy Configuration:** In the FoxyProxy options pop-up, click the **Options** button. This will open a new browser tab with the FoxyProxy configurations. Click the **Add** button to create a new proxy configuration.



You do not have any proxy settings. Please click Add to start.

4. **Add Proxy Details:** On the "Add Proxy" page, fill in the following values:
   - Title: Burp (or any preferred name)
   - Proxy IP: 127.0.0.1
   - Port: 8080



Add Proxy

Title or Description (optional): Burp

Color: #66cc66

Proxy Type: HTTP

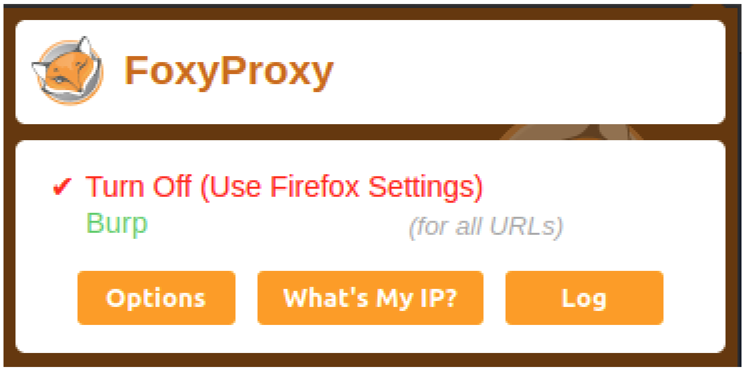
Proxy IP address or DNS name: 127.0.0.1

Port: 8080

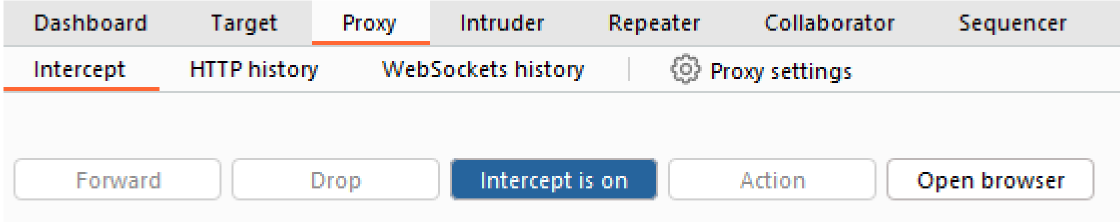
Username (optional): username

Password (optional): *****

5. **Save Configuration:** Click **Save** to save the Burp Proxy configuration.
6. **Activate Proxy Configuration:** Click on the FoxyProxy icon at the top-right of the Firefox browser and select the Burp configuration. This will redirect your browser traffic through 127.0.0.1:8080. Note that Burp Suite must be running for your browser to make requests when this configuration is activated.



7. **Enable Proxy Intercept in Burp Suite:** Switch to Burp Suite and ensure that Intercept is turned on in the **Proxy** tab.



8. **Test the Proxy:** Open Firefox and try accessing a website, such as the homepage for http://10.10.13.4/. Your browser will hang, and the proxy will populate with the HTTP request. Congratulations, you have successfully intercepted your first request!

Remember the following:

- When the proxy configuration is active, and the intercept is switched on in Burp Suite, your browser will hang whenever you make a request.
- Be cautious not to leave the intercept switched on unintentionally, as it can prevent your browser from making any requests.
- Right-clicking on a request in Burp Suite allows you to perform various actions, such as forwarding, dropping, sending to other tools, or selecting options from the right-click menu.

Take note of these details as you begin using the Burp Suite Proxy.

Note: Consider closing the other tabs in the AttackBox browser before enabling interception, as you will receive some WebSocket requests instead of request from the target VM.

Task 10: Site Map and Issue Definitions

The **Target** tab in Burp Suite provides more than just control over the scope of our testing. It consists of three sub-tabs:

1. **Site map**: This sub-tab allows us to map out the web applications we are targeting in a tree structure. Every page that we visit while the proxy is active will be displayed on the site map. This feature enables us to automatically generate a site map by simply browsing the web application. In Burp Suite Professional, we can also use the site map to perform automated crawling of the target, exploring links between pages and mapping out as much of the site as possible. Even with Burp Suite Community, we can still utilize the site map to accumulate data during our initial enumeration steps. It is particularly useful for mapping out APIs, as any API endpoints accessed by the web application will be captured in the site map.
2. **Issue definitions**: Although Burp Community does not include the full vulnerability scanning functionality available in Burp Suite Professional, we still have access to a list of all the vulnerabilities that the scanner looks for. The **Issue definitions** section provides an extensive list of web vulnerabilities, complete with descriptions and references. This resource can be valuable for referencing vulnerabilities in reports or assisting in describing a particular vulnerability that may have been identified during manual testing.
3. **Scope settings**: This setting allows us to control the target scope in Burp Suite. It enables us to include or exclude specific domains/IPs to define the scope of our testing. By managing the scope, we can focus on the web applications we are specifically targeting and avoid capturing unnecessary traffic.

Overall, the **Target** tab offers features beyond scoping, allowing us to map out web applications, fine-tune our target scope, and access a comprehensive list of web vulnerabilities for reference purposes.

Challenge

Take a look around the site on **http://10.10.13.4/** — we will be using this a lot throughout the module. Visit every other page that is linked on the homepage, then check your sitemap — one endpoint should stand out as being very unusual!

Visit this in your browser (or use the "Response" section of the site map entry for that endpoint).

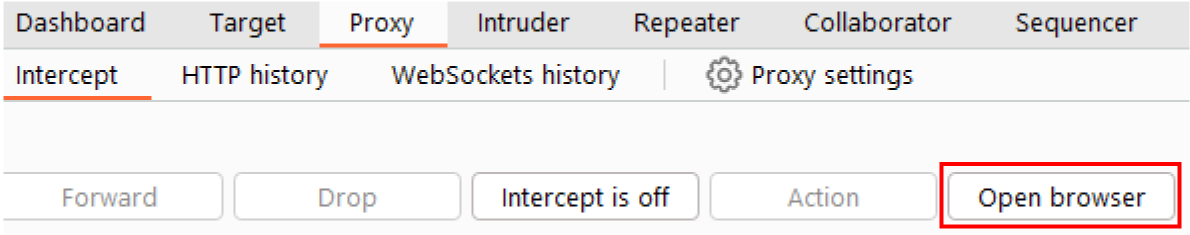
Question 11: What is the flag you receive after visiting the unusual endpoint?

Answer: ***THM{NmNlZTliNGE1MWU1ZTQzMzgzNmFiNWVk}***

Task 11: The Burp Suite Browser

In addition to modifying our regular web browser to work with the proxy, Burp Suite also includes a built-in Chromium browser that is pre-configured to use the proxy without any of the modifications we just had to do.

To start the Burp Browser, click the **Open Browser** button in the proxy tab. A Chromium window will pop up, and any requests made in this browser will go through the proxy.



Note: There are many settings related to the Burp Browser in the project options and user options settings. Make sure to explore and customise them as needed.

However, if you are running Burp Suite on Linux as the root user (as is the case with the AttackBox), you may encounter an error preventing the Burp Browser from starting due to the inability to create a sandbox environment.

There are two simple solutions to this:

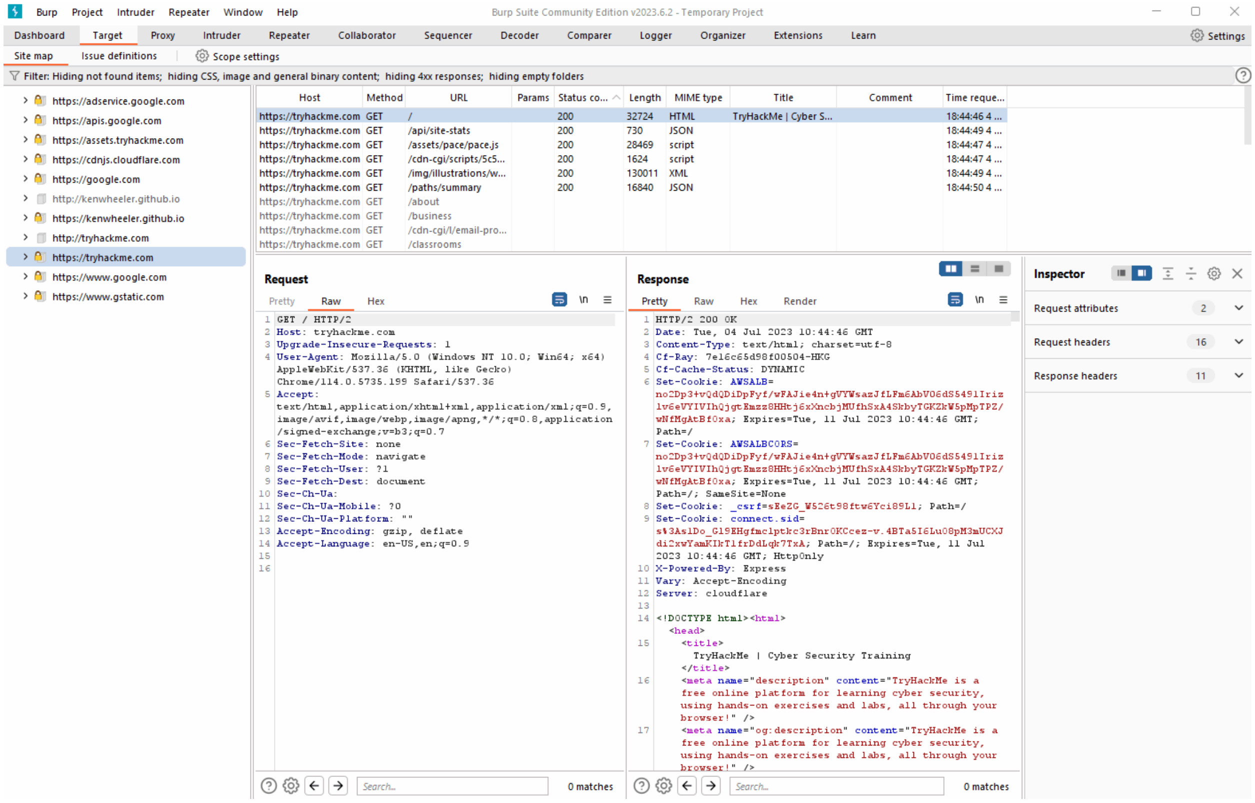
1. **Smart option:** Create a new user and run Burp Suite under a low-privilege account to allow the Burp Browser to run without issues.
2. **Easy option:** Go to **Settings -> Tools -> Burp's browser** and check the **Allow Burp's browser to run without a sandbox** option. Enabling this option will allow the browser to start without a sandbox. However, please be aware that this option is disabled by default for security reasons. If you choose to enable it, exercise caution, as compromising the browser could grant an attacker access to your entire machine. In the training environment of the AttackBox, this is unlikely to be a significant issue, but use it responsibly.

Task 12: Scoping and Targeting

Finally, we come to one of the most important aspects of using the Burp Proxy: **Scoping**.

Capturing and logging all of the traffic can quickly become overwhelming and inconvenient, especially when we only want to focus on specific web applications. This is where scoping comes in.

By setting a scope for the project, we can define what gets proxied and logged in Burp Suite. We can restrict Burp Suite to target only the specific web application(s) we want to test. The easiest way to do this is by switching to the **Target** tab, right-clicking on our target from the list on the left, and selecting **Add To Scope**. Burp will then prompt us to choose whether we want to stop logging anything that is not in scope, and in most cases, we want to select **yes**.



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status co...	Length	MIME type	Title	Comment	Time reque...
https://tryhackme.com	GET	/		200	32724	HTML	TryHackMe | Cyber S...		18:44:46 4 ...
https://tryhackme.com	GET	/api/site-stats		200	730	JSON			18:44:49 4 ...
https://tryhackme.com	GET	/assets/pace/pace.js		200	28469	script			18:44:47 4 ...
https://tryhackme.com	GET	/cdn-cgi/scripts/5c5...		200	1624	script			18:44:47 4 ...
https://tryhackme.com	GET	/img/illustrations/w...		200	130011	XML			18:44:49 4 ...
https://tryhackme.com	GET	/paths/summary		200	16840	JSON			18:44:50 4 ...
https://tryhackme.com	GET	/about							
https://tryhackme.com	GET	/business							
https://tryhackme.com	GET	/cdn-cgi/l/email-pro...							
https://tryhackme.com	GET	/classrooms							

```
GET / HTTP/2
Host: tryhackme.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/114.0.5735.199 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,
image/avif,image/webp,image/apng,*/*;q=0.8,application
/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


```

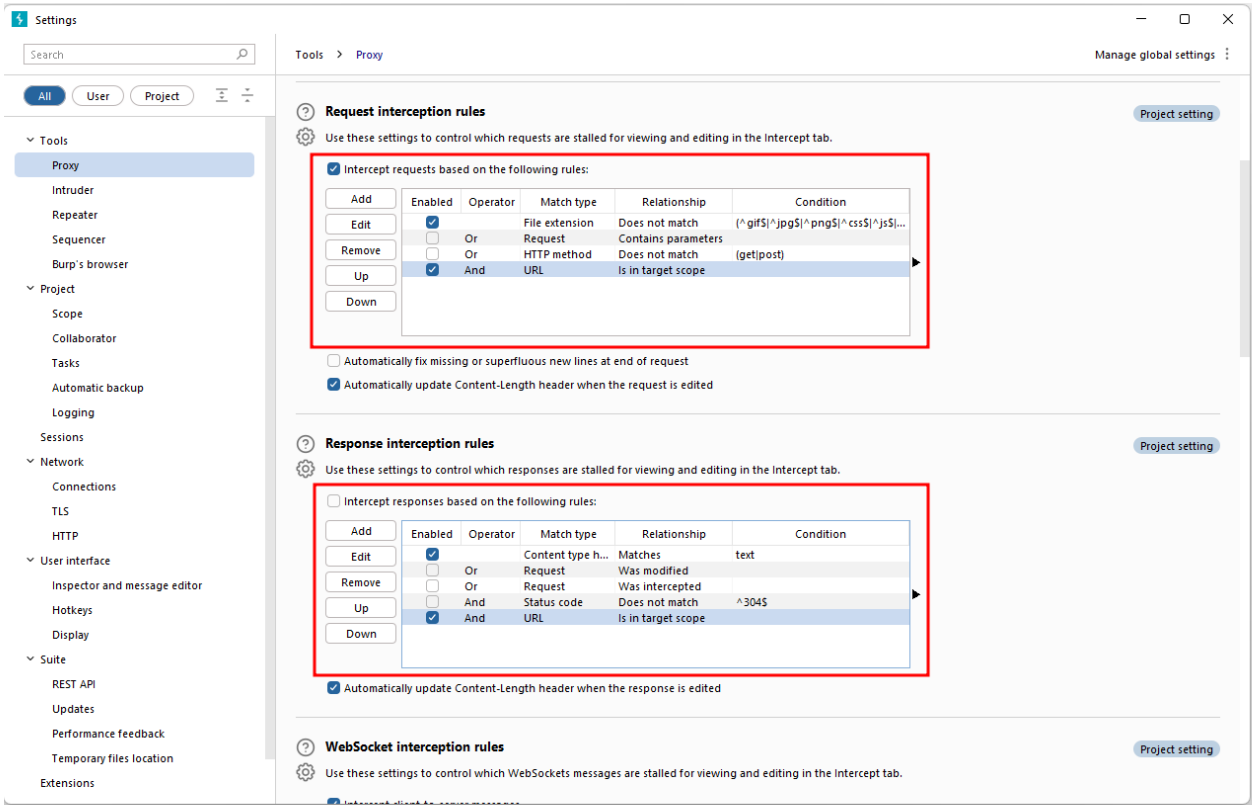
```
HTTP/2 200 OK
Date: Tue, 04 Jul 2023 10:44:46 GMT
Content-Type: text/html; charset=utf-8
Cf-Ray: 7e16c65d98f00504-HKG
Cf-Cache-Status: DYNAMIC
Set-Cookie: AWSALB=
no2Dp3+vQdQDiDpFyf/wFAJie4n+gVYWsazJfLFm6AbV06dS5491Iriz
lv6eVYIVIhQjgtEmzz8HHtj6xXncbjMUfhSxA4SkbyTGKZkW5pMpTPZ/
wNfMgAtBf0xa; Expires=Tue, 11 Jul 2023 10:44:46 GMT;
Path=/
Set-Cookie: AWSALBCORS=
no2Dp3+vQdQDiDpFyf/wFAJie4n+gVYWsazJfLFm6AbV06dS5491Iriz
lv6eVYIVIhQjgtEmzz8HHtj6xXncbjMUfhSxA4SkbyTGKZkW5pMpTPZ/
wNfMgAtBf0xa; Expires=Tue, 11 Jul 2023 10:44:46 GMT;
Path=/; SameSite=None
Set-Cookie: _csrf=sEeZG_W526t98ftw6Yci89L1; Path=/
Set-Cookie: connect.sid=
s%3As1Do_Gl9EHgfmclptkc3rBnr0KCcez-v.4BTa5I6Lu08pM3mUCXJ
di2xwYamKIkTlfrDdLqk7TxA; Path=/; Expires=Tue, 11 Jul
2023 10:44:46 GMT; HttpOnly
X-Powered-By: Express
Vary: Accept-Encoding
Server: cloudflare

<!DOCTYPE html><html>
  <head>
    <title>
      TryHackMe | Cyber Security Training
    </title>
    <meta name="description" content="TryHackMe is a
    free online platform for learning cyber security,
    using hands-on exercises and labs, all through your
    browser!" />
    <meta name="og:description" content="TryHackMe is a
    free online platform for learning cyber security,
    using hands-on exercises and labs, all through your
    browser!" />
```

To check our scope, we can switch to the **Scope settings** sub-tab within the **Target** tab.

The Scope settings window allows us to control our target scope by including or excluding domains/IPs. This section is powerful and worth spending time getting familiar with.

However, even if we disabled logging for out-of-scope traffic, the proxy will still intercept everything. To prevent this, we need to go to the **Proxy settings** sub-tab and select **And URL Is in target scope** from the "Intercept Client Requests" section.



Request interception rules

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	

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

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

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:

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	

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

WebSocket interception rules

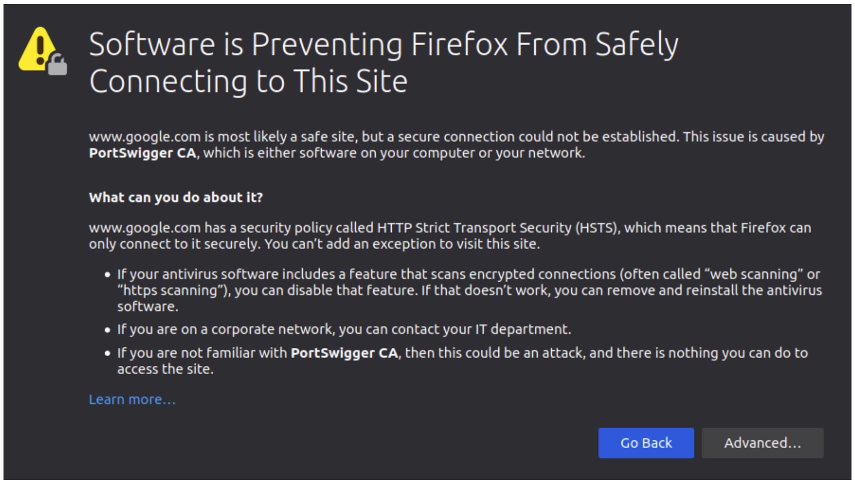
Use these settings to control which WebSockets messages are stalled for viewing and editing in the Intercept tab.

Enabling this option ensures that the proxy completely ignores any traffic that is not within the defined scope, resulting in a cleaner traffic view in Burp Suite.

Task 13: Proxying HTTPS

Note: The AttackBox is already configured to solve the problem posed in this task. If you use the AttackBox and don't wish to read through the information here, you can skip to the next task.

When intercepting HTTP traffic, we may encounter an issue when navigating to sites with TLS enabled. For example, when accessing a site like **https://google.com/**, we may receive an error indicating that the PortSwigger Certificate Authority (CA) is not authorised to secure the connection. This happens because the browser does not trust the certificate presented by Burp Suite.



Software is Preventing Firefox From Safely Connecting to This Site

www.google.com is most likely a safe site, but a secure connection could not be established. This issue is caused by **PortSwigger CA**, which is either software on your computer or your network.

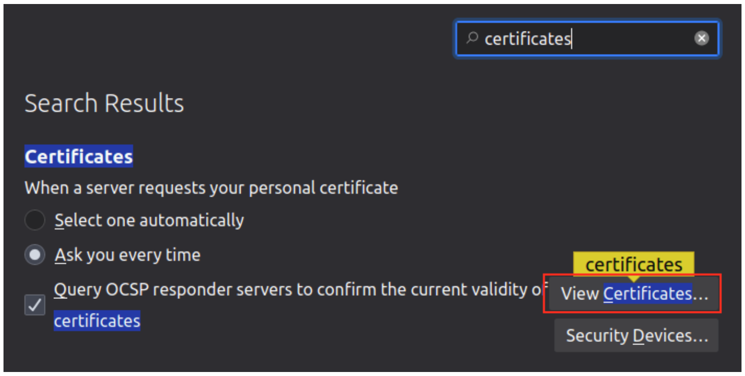
What can you do about it?

www.google.com has a security policy called HTTP Strict Transport Security (HSTS), which means that Firefox can only connect to it securely. You can't add an exception to visit this site.

- If your antivirus software includes a feature that scans encrypted connections (often called "web scanning" or "https scanning"), you can disable that feature. If that doesn't work, you can remove and reinstall the antivirus software.
- If you are on a corporate network, you can contact your IT department.
- If you are not familiar with **PortSwigger CA**, then this could be an attack, and there is nothing you can do to access the site.

To overcome this issue, we can manually add the PortSwigger CA certificate to our browser's list of trusted certificate authorities. Here's how to do it:

1. **Download the CA Certificate:** With the Burp Proxy activated, navigate to http://burp/cert. This will download a file called **cacert.der**. Save this file somewhere on your machine.
2. **Access Firefox Certificate Settings:** Type **about:preferences** into your Firefox URL bar and press **Enter**. This will take you to the Firefox settings page. Search the page for "certificates" and click on the **View Certificates** button.



certificates

Search Results

Certificates

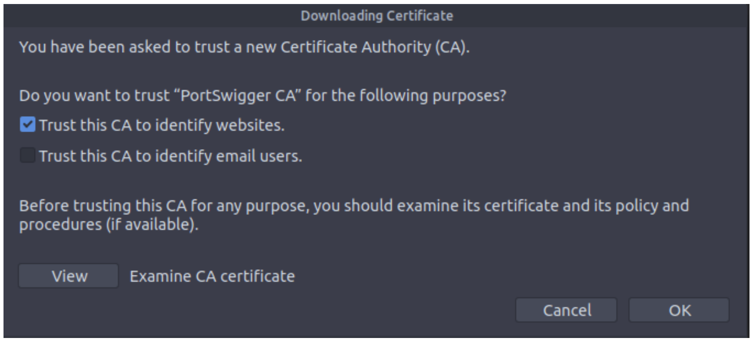
When a server requests your personal certificate

○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

3. **Import the CA Certificate:** In the Certificate Manager window, click on the **Import** button. Select the **cacert.der** file that you downloaded in the previous step.
4. **Set Trust for the CA Certificate:** In the subsequent window that appears, check the box that says: "Trust this CA to identify websites" and click OK.



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust “PortSwigger CA” for the following purposes?

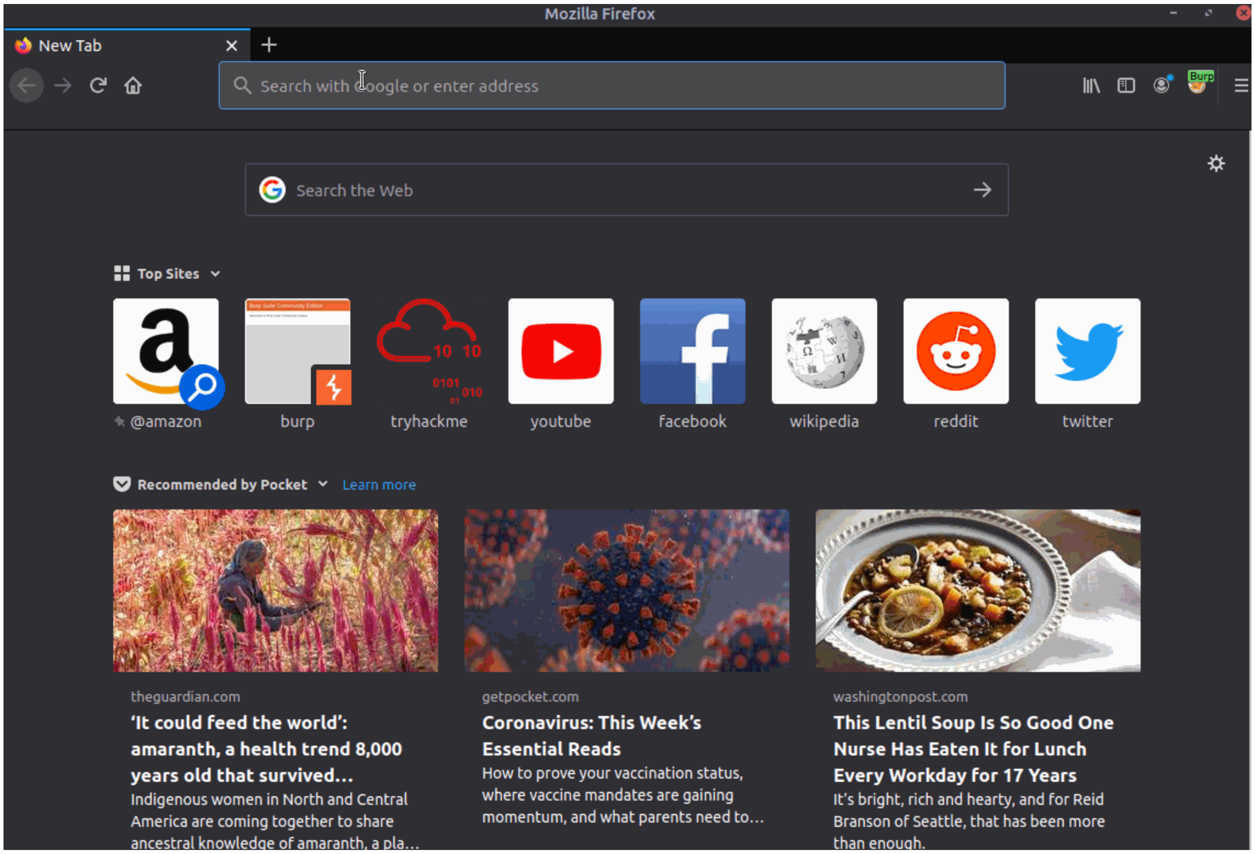
☑ Trust this CA to identify websites.

☐ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

By completing these steps, we have added the PortSwigger CA certificate to our list of trusted certificate authorities. Now, we should be able to visit any TLS-enabled site without encountering the certificate error.

You can watch the following video for a visual demonstration of the full certificate import process:



‘It could feed the world’: amaranth, a health trend 8,000 years old that survived…
Indigenous women in North and Central America are coming together to share ancestral knowledge of amaranth, a pla…

Coronavirus: This Week’s Essential Reads
How to prove your vaccination status, where vaccine mandates are gaining momentum, and what parents need to…

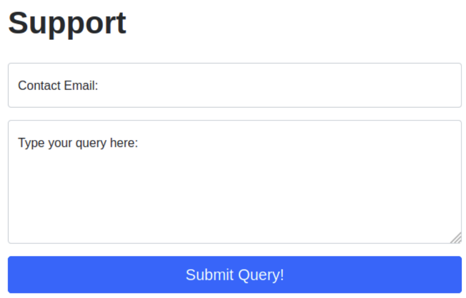
This Lentil Soup Is So Good One Nurse Has Eaten It for Lunch Every Workday for 17 Years
It’s bright, rich and hearty, and for Reid Branson of Seattle, that has been more than enough.

By following these instructions, you can ensure that your browser trusts the PortSwigger CA certificate and securely communicates with TLS-enabled websites through the Burp Suite Proxy.

Task 14: Example Attack

Having looked at how to set up and configure our proxy, let's go through a simplified real-world example.

We will start by taking a look at the support form at **http://MACHINE_IP/ticket/**:



Support

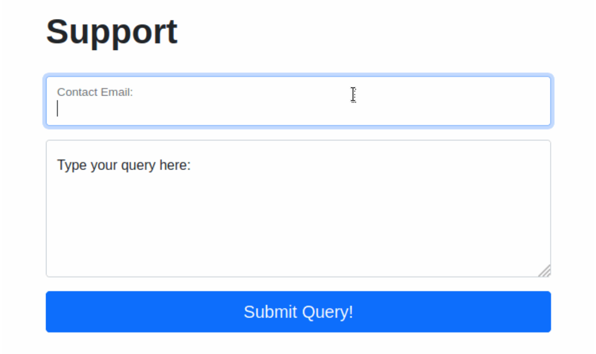
Contact Email:

Type your query here:

In a real-world web app pentest, we would test this for a variety of things, one of which would be Cross-Site Scripting (or XSS). If you have not yet encountered XSS, it can be thought of as injecting a client-side script (usually in Javascript) into a webpage in such a way that it executes. There are various kinds of XSS – the type that we are using here is referred to as "Reflected" XSS, as it only affects the person making the web request.

Walkthrough

Try typing: **<script>alert("Succ3ssful XSS")</script>**, into the "Contact Email" field. You should find that there is a client-side filter in place which prevents you from adding any special characters that aren't allowed in email addresses:



Support

Contact Email:

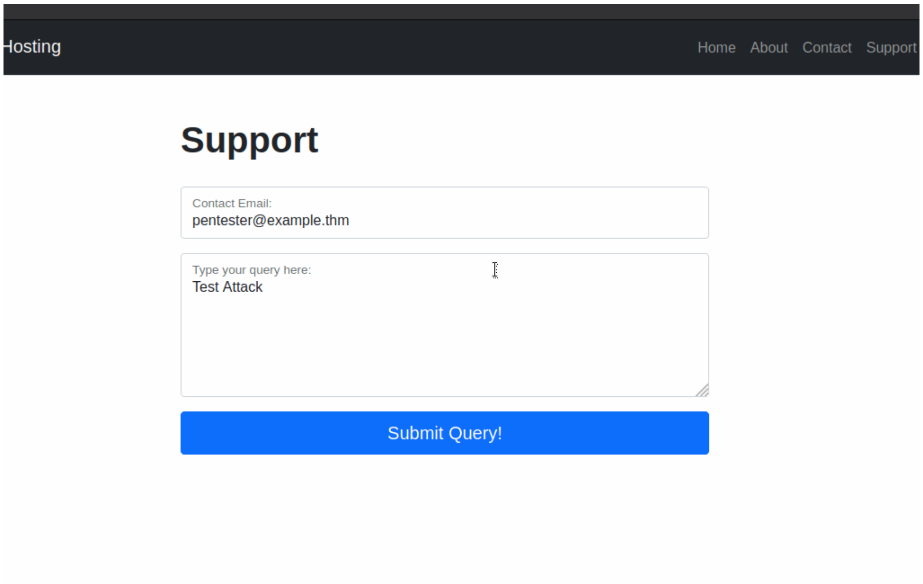
Type your query here:

Fortunately for us, client-side filters are absurdly easy to bypass. There are a variety of ways we could disable the script or just prevent it from loading in the first place. Let's focus on simply bypassing the filter for now. First, make sure that your Burp Proxy is active, and that intercept is on.

Now, enter some legitimate data into the support form. For example: "pentester@example.thm" as an email address, and "Test Attack" as a query.

Submit the form — the request should be intercepted by the proxy.

With the request captured in the proxy, we can now change the email field to be our very simple payload from above: `<script>alert("Succ3ssful XSS")</script>`. After pasting in the payload, we need to select it, then URL encode it with the `Ctrl + U` shortcut to make it safe to send. This process is shown in the GIF below:



Support

Contact Email:
pentester@example.thm

Type your query here:
Test Attack

Finally, press the "Forward" button to send the request.

You should find an alert box from the site indicating a successful XSS attack!

Happy Hacking! 😸

> *Thanks and Regards,*
>
> *ShadowGirl* 🦹‍♀️😉