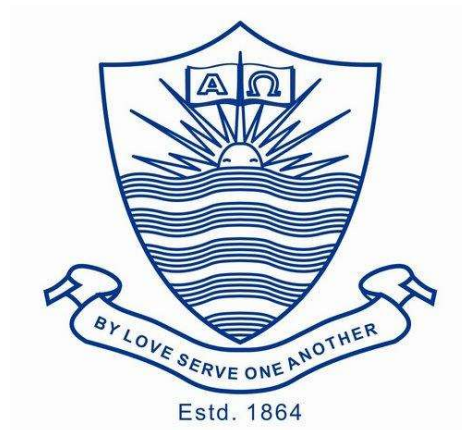


FORMAN CHRISTIAN COLLEGE (A CHARTERED UNIVERSITY)



COMP 421 (Information Security)

SECTION - B

2023 FALL

QUIZ # 4

BURP SUITE: THE BASICS

Gulraiz Noor Bari (231-525536)

TryHackMe

Dashboard

Learn

Compete


Other

Access Machines

Go Premium

1

699





Burp Suite: The Basics

An introduction to using Burp Suite for web application pentesting.

Help

100%

Task 1  Introduction



Welcome to Burp Suite Basics!

This particular room aims to understand the basics of the Burp Suite web application security testing framework. Our focus will revolve around the following key aspects:

1. A thorough introduction to Burp Suite.
2. A comprehensive overview of the various tools available within the framework.
3. Detailed guidance on the process of installing Burp Suite on your system.
4. Navigating and configuring Burp Suite.

We will also introduce the core of the Burp Suite framework, which is the Burp Proxy. It is important to note that this room primarily serves as a foundational resource for acquiring knowledge about Burp Suite. Subsequent rooms in the Burp module will adopt a more practical approach. Thus, this room will contain a greater emphasis on theoretical content. If you have not yet utilised Burp Suite, it is recommended to carefully read the provided information and actively engage with the tool. Experimentation is essential for grasping the fundamentals of this framework. Combining the information presented here with hands-on exploration will establish a strong foundation for utilising the framework. This will significantly assist you in future rooms.

Answer the questions below

Let us start!

No answer needed

Question Done

TASK # 2 – WHAT IS BURP SUITE

Answer the questions below

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

Burp Suite Enterprise Correct Answer

Burp Suite is frequently used when attacking web applications and _____ applications.

Mobile Correct Answer Hint

TASK # 3 – FEATURES OF BURP COMMUNITY

Answer the questions below

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

Proxy Correct Answer

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

Intruder Correct Answer

TASK # 4 – INSTALLATION

Try Hack Me

Dashboard

Learn

Compete

Other

Access Machines

Go Premium

1

699

Burp Suite: The Basics
An introduction to using Burp Suite for web application pentesting.

Help

100%

Task 1 Introduction

Task 2 What is Burp Suite

Task 3 Features of Burp Community

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

To download the latest version of Burp Suite for other systems, you may click this [button](#) to go to their download page.

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

ALL EDITIONS

PROFESSIONAL

COMMUNITY

ENTERPRISE

CI/CD DRIVER

DASTARDLY

Professional / Community 2023.7

Released Thursday 6 July 2023

Burp Suite Professional

Windows (64 bit)

DOWNLOAD

view checksums

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](#).

read more

No answer needed

Question Done

TASK # 5 – THE DASHBOARD

By exploring the different tabs and functionalities of Burp Suite, you will gradually become familiar with its capabilities.

Answer the questions below

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

Correct Answer

TASK # 6 – NAVIGATION

Ctrl + Shift + R

Repeater tab

Answer the questions below

Which tab **Ctrl + Shift + P** will switch us to?

Correct Answer

TASK # 7 – OPTIONS

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

Take some time to familiarise yourself with the range of configurable options in Burp Suite. Once you are comfortable, you can proceed with the exercises related to configuring Burp Suite settings.

Answer the questions below

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

Correct Answer

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

Correct Answer

Hint

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

Correct Answer

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

Correct Answer

Hint

Task 8 Introduction to the Burp Proxy

TASK # 8 – INTRODUCTION TO BURP PROXY

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, 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.



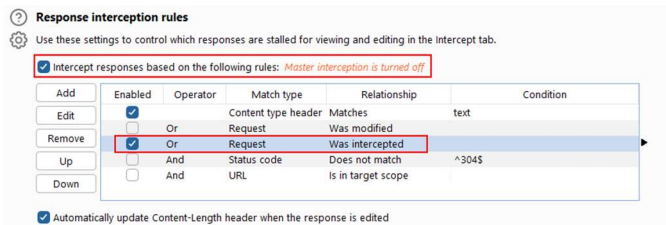
- Taking Control:** The ability to intercept requests empowers testers to gain complete control over web traffic, making it invaluable for testing web applications.
- Capture and Logging:** Burp Suite captures and logs requests made through the proxy by default, even when the interception is turned off. 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 analysing 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.

#	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://ken Wheeler.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/path.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 behaviour and functionality. Familiarise 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.



- 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.

Take the time to explore and experiment with the Proxy options, as this will enhance your understanding and proficiency with the tool.

Answer the questions below

Click me to proceed to the next task.

No answer needed

Question Done

TASK # 9 – CONNECTING THROUGH THE PROXY (FOXYPROXY)

Task 9 Connecting through the Proxy (FoxyProxy)



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

Start Machine

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.

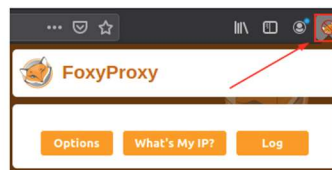
Please note that the instructions provided are specific to Firefox. If you are using a different browser, you may need to find alternative methods or use the TryHackMe AttackBox.

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.

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://MACHINE_IP/`. 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.

Answer the questions below

Click me to proceed to the next task.

No answer needed

Question Done

TASK # 10 – SITE MAP AND ISSUE DEFINITIONS

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://MACHINE_IP/` — 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)

Answer the questions below

What is the flag you receive after visiting the unusual endpoint?

THM{NmNIZTiNGE1MWU1ZTQzMgzNmFINWVk}

Correct Answer

Hint

TASK # 11 – THE BURP SUITE BROWSER

Task 11 The Burp Suite Browser

If the previous tasks seemed overly complex, rest assured, this topic will be a lot simpler.

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.

Answer the questions below

Click me to proceed to the next task.

No answer needed

Question Done

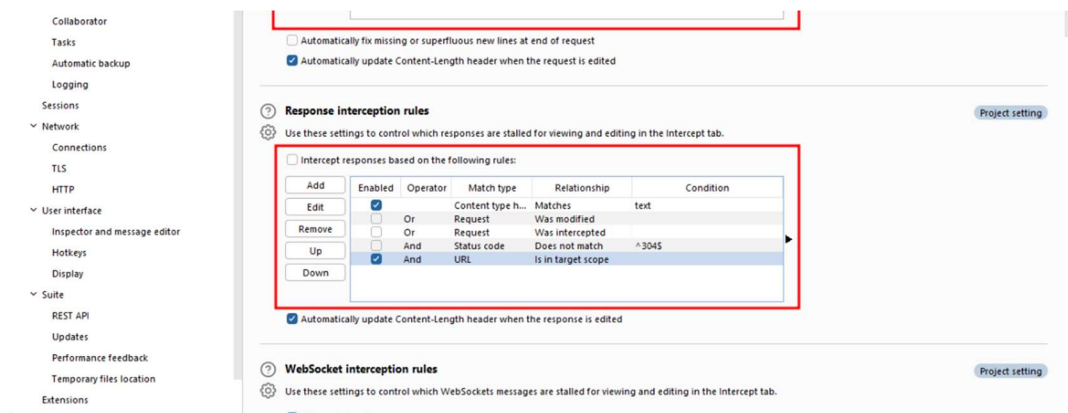
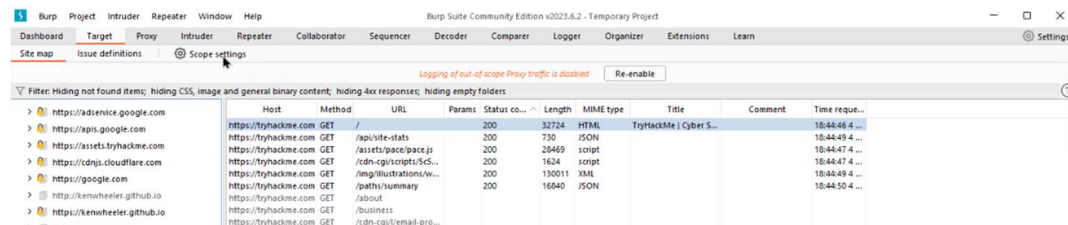
TASK # 12 – SCOPING AND TARGETING

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**.



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.

Answer the questions below

Add `http://MACHINE_IP/` to your scope and change the proxy settings to only intercept traffic to in-scope targets.

See the difference between the amount of traffic getting caught by the proxy before and after limiting the scope.

No answer needed

Question Done

TASK # 13 – PROXYING HTTPS

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

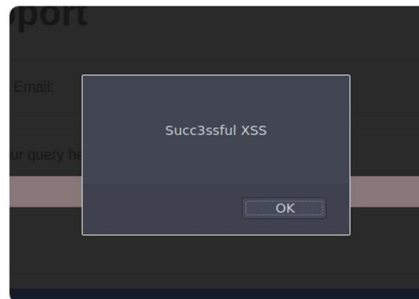
www.google.com is most likely a safe site, but a secure connection could not be established. This issue is caused by **PortSwigger CA**, which is either software on your computer or your network.

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.

[Learn more...](#)



Answer the questions below

Click me to proceed to the next task.

No answer needed

Question Done

Task 15 ✓ Conclusion

Created by [tryhackme](#) and [MuirlandOracle](#) and [l000g1c](#)

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 33426 users are in here and this room is 96 days old.



TASK # 14 – EXAMPLE ATTACK

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/`:

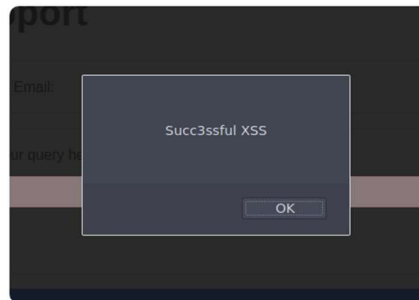
Support

Contact Email:

Type your query here:

Submit Query!

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.



Answer the questions below

Click me to proceed to the next task.

No answer needed

Question Done

Task 15 ✓ Conclusion

Created by tryhackme and MuirlandOracle and l000g1c

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 33426 users are in here and this room is 96 days old.



TASK # 15 – CONCLUSION

Task 15 Conclusion

Congratulations on completing the Burp Basics room! You now have a solid understanding of the Burp Suite interface, configuration options, and the Burp Proxy. These skills will be essential as you continue your journey in web and mobile application penetration testing.

To further enhance your skills, I encourage you to practice and experiment with Burp Suite. Explore its features, try different configurations, and familiarise yourself with its various tools. The more you use Burp Suite, the more proficient you will become in identifying and exploiting vulnerabilities in web applications.

In the next room of the module, we will dive deeper into [Burp Suite Repeater](#), another powerful tool for manual testing and manipulation of web application requests. Stay curious and keep learning!

Stay curious and keep learning!

Answer the questions below

I understand the fundamentals of using Burp Suite!

Question Done

Created by tryhackme and MuirlandOracle and l000g1c

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 33426 users are in here and this room is 96 days old.

ACCOUNT PROOF

TryHackMe Dashboard Learn Compete Other

Go Premium 1

469234
Rank

5
Rooms Complete

3
Level

1
Badges

gulraizzz.exe [0x3]

Get Profile Badge ID Share Room Badges

Rooms Complete Badges Created Rooms Yearly Activity Tickets

Burp Suite: The...
An introduction to using Burp Suite for web...

Red Team...
Learn the steps and procedures of a red team...

Metasploit...
An introduction to the main components of the...

Pentesting...
Learn the important ethics and methodologies behind...

Principles of...
Learn the principles of information security that...



My Rooms

All the rooms that you have joined and saved.

6

Rooms Joined

Find posts by a keyword...

☐ Hide Completed rooms

[Joined rooms](#)

[Saved](#)



Pentesting Fundamentals

Learn the important ethics and methodologies behind every pentest.

[cybersecurity](#) [framework](#) [penetration testing](#) [ethics](#)

[Info](#)



Metasploit: Introduction

An introduction to the main components of the Metasploit Framework.

[security](#) [metasploit](#) [msfconsole](#)

Easy



Burp Suite: The Basics

An introduction to using Burp Suite for web application pentesting.

[burp suite](#) [webapp](#) [tutorial](#) [toolkit](#)

[Info](#)



Principles of Security

Learn the principles of information security that secures data and protects systems from abuse

[cia triad](#) [information security](#) [incidence response](#) [threat model](#)

[Info](#)



Red Team Engagements

Learn the steps and procedures of a red team engagement, including planning, frameworks, and documentation.

[Red Team](#) [Engagements](#) [Planning](#) [Documentation](#)

Easy



Advent of Cyber 2023

Get started with Cyber Security in 24 Days - Learn the basics by doing a new, beginner friendly security challenge every day leading up to Christmas.

[security](#)

Easy



[Dashboard](#)[Learn](#)[Compete](#)[Other](#)[Access Machines](#)[Go Premium](#)

1



700



Burp Suite: The Basics

An introduction to using Burp Suite for web application pentesting.

[Start AttackBox](#)[Help](#)

100%

Task 1 Introduction



Task 2 What is Burp Suite



Task 3 Features of Burp Community



Task 4 Installation



Task 5 The Dashboard



Task 6 Navigation



Task 7 Options



Task 8 Introduction to the Burp Proxy



Task 9 Connecting through the Proxy (FoxyProxy)



Task 10 Site Map and Issue Definitions



Task 11 The Burp Suite Browser



Task 12 Scoping and Targeting



Task 13 Proxying HTTPS



Task 14 Example Attack



Task 15 Conclusion



Created by tryhackme and MuirlandOracle and l000g1c

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 33436 users are in here and this room is 96 days old.

