

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



TryHackMe: Burp Suite: Intruder



Ayan Mukherjee · [Follow](#)

8 min read · Nov 6, 2023



Listen



Share

... More

Intruder is an important part of Burp Suite. But in general, except just to do a simple recursive requests, Intruder can be made much refined to perform more complex tasks. The room link is <https://tryhackme.com/room/burpsuiteintruder>

INTRODUCTION

Burp Suite's Intruder module is a powerful tool that allows for automated and customisable attacks. It provides the ability to modify specific parts of a request and perform repetitive tests with variations of input data. Intruder is particularly useful for tasks like fuzzing and brute-forcing, where different values need to be tested against a target.

No Answer required for this section

WHAT IS INTRUDER

Intruder is Burp Suite's built-in fuzzing tool that allows for automated request modification and repetitive testing with variations in input values. By using a captured request (often from the Proxy module), Intruder can send multiple requests with slightly altered values based on user-defined configurations. It serves various purposes, such as brute-forcing login forms by substituting username and password fields with values from a wordlist or performing fuzzing attacks using wordlists to test subdirectories, endpoints, or virtual hosts. Intruder's functionality is comparable to command-line tools like **Wfuzz** or **ffuf**.

However, it's important to note that while Intruder can be used with Burp Community Edition, it is rate-limited, significantly reducing its speed compared to Burp Professional. This limitation often leads security practitioners to rely on other tools for fuzzing and brute-forcing. Nonetheless, Intruder remains a valuable tool and is worth learning how to use it effectively.

There are 4 major tabs in Intruder namely : Positions, Payloads, Resource Pool, Settings. We will learn Positions and Payload in details in below sections.

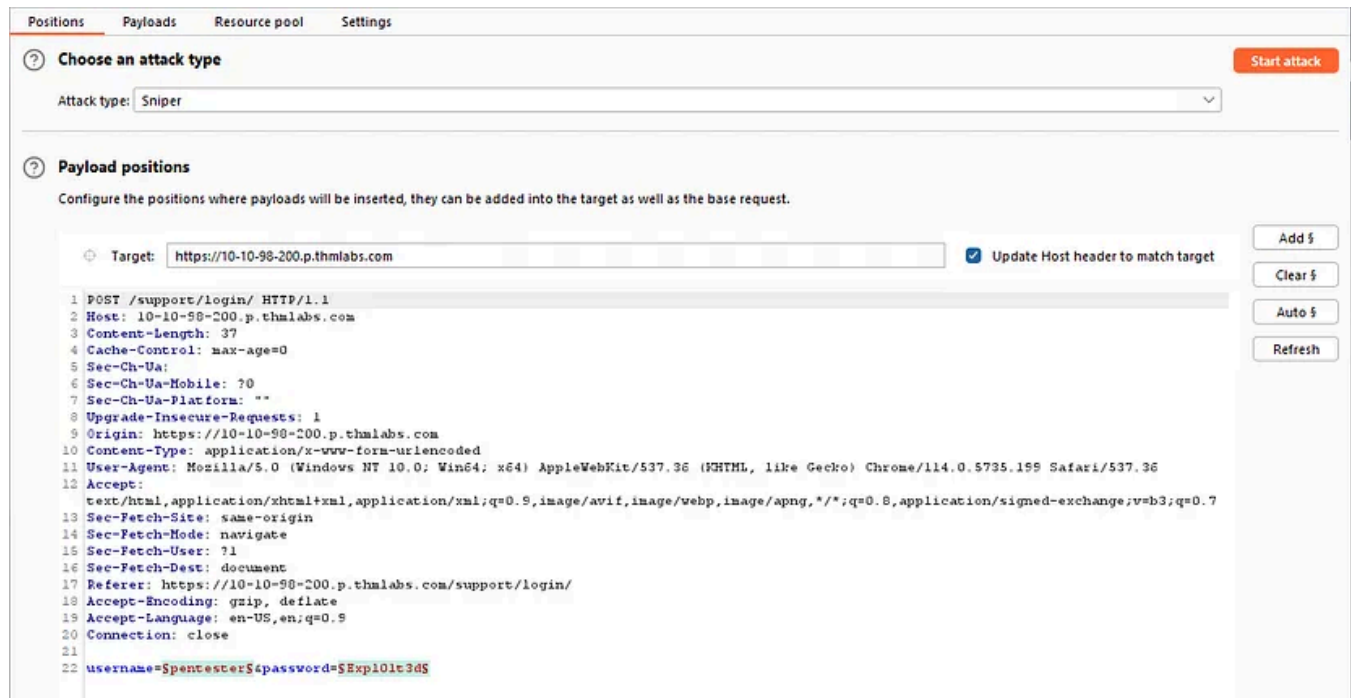
In which Intruder tab can we define the "Attack type" for our planned attack?

Positions

Correct Answer

POSITIONS

This tab allows us to select an attack type (which we will cover in a future task) and configure where we want to insert our payloads in the request template. When using Burp Suite Intruder to perform an attack, the first step is to examine the positions within the request where we want to insert our payloads. These positions inform Intruder about the locations where our payloads will be introduced



On the right-hand side of the interface, we find the following buttons: Add \$, Clear \$, and Auto \$:

- The Add \$ button allows us to define new positions manually by highlighting them within the request editor and then clicking the button.

- The `Clear $` button removes all defined positions, providing a blank canvas where we can define our own positions.
- The `Auto $` button automatically attempts to identify the most likely positions based on the request. This feature is helpful if we previously cleared the default positions and want them back.

What symbol defines the start and the end of a payload position?

\$

Correct Answer

PAYLOADS

Here we can select values to insert into the positions defined in the **Positions** tab. We have various payload options, such as loading items from a wordlist. The way these payloads are inserted into the template depends on the attack type chosen in the **Positions** tab. The **Payloads** tab also enables us to modify Intruder's behavior regarding payloads, such as defining pre-processing rules for each payload (e.g., adding a prefix or suffix, performing match and replace, or skipping payloads based on a defined regex).

Payload Sets: This section allows us to choose the position for which we want to configure a payload set and select the type of payload we want to use.

Payload settings: This section provides options specific to the selected payload type for the current payload set.

Payload Processing: In this section, we can define rules to be applied to each payload in the set before it is sent to the target.

Payload Encoding: The section allows us to customize the encoding options for our payloads.

Which **Payload processing** rule could we use to add characters at the end of each payload in the set?

Add suffix

Correct Answer

SNIPER

The **Sniper** attack type is the default and most commonly used attack type in Burp Suite Intruder. It is particularly effective for single-position attacks, such as password brute-force or fuzzing for API endpoints. In a Sniper attack, we provide a

set of payloads, which can be a wordlist or a range of numbers, and Intruder inserts each payload into each defined position in the request. The total number of requests made by Intruder Sniper can be calculated as $\text{requests} = \text{numberOfWords} * \text{numberOfPositions}$.

The Sniper attack type is beneficial when we want to perform tests with single-position attacks, utilizing different payloads for each position. It allows for precise testing and analysis of different payload variations.

If you were using Sniper to fuzz three parameters in a request with a wordlist containing 100 words, how many requests would Burp Suite need to send to complete the attack?

Correct Answer

How many sets of payloads will Sniper accept for conducting an attack?

Correct Answer

BATTERING RAM

The **Battering ram** attack type in Burp Suite Intruder differs from Sniper in that it places the same payload in every position simultaneously, rather than substituting each payload into each position in turn. In a Battering Ram attack, the same payload is thrown at every defined position simultaneously, providing a brute-force-like approach to testing.

The Battering Ram attack type is useful when we want to test the same payload against multiple positions at once without the need for sequential substitution.

As a hypothetical question: You need to perform a Battering ram Intruder attack on the example request above.

If you have a wordlist with two words in it (`admin` and `Guest`) and the positions in the request template look like this:

```
username=$pentester&password=$Exploited$
```

What would the body parameters of the *first* request that Burp Suite sends be?

Correct Answer

Hint

Open in app ↗

Medium



Search



positions simultaneously, Pitchfork utilises one payload set per position (up to a maximum of 20) and iterates through them all simultaneously. Pitchfork takes the first item from each list and substitutes them into the request, one per position. It then repeats this process for the next request by taking the second item from each list and substituting it into the template. Intruder continues this iteration until one

or all of the lists run out of items. It's important to note that Intruder stops testing as soon as one of the lists is complete. Therefore, in Pitchfork attacks, it is ideal for the payload sets to have the same length. If the lengths of the payload sets differ, Intruder will only make requests until the shorter list is exhausted, and the remaining items in the longer list will not be tested.

The Pitchfork attack type is especially useful when conducting credential-stuffing attacks or when multiple positions require separate payload sets. It allows for simultaneous testing of multiple positions with different payloads.

What is the maximum number of payload sets we can load into Intruder in Pitchfork mode?

Correct Answer

CLUSTER BOMB

The **Cluster bomb** attack type in Burp Suite Intruder allows us to choose multiple payload sets, one per position (up to a maximum of 20). Unlike Pitchfork, where all payload sets are tested simultaneously, Cluster bomb iterates through each payload set individually, ensuring that every possible combination of payloads is tested.

the Cluster bomb attack type iterates through every combination of the provided payload sets. It tests every possibility by substituting each value from each payload set into the corresponding position in the request.

Cluster bomb attacks can generate a significant amount of traffic as it tests every combination. The number of requests made by a Cluster bomb attack can be calculated by multiplying the number of lines in each payload set together. It's important to be cautious when using this attack type, especially when dealing with large payload sets. Additionally, when using Burp Community and its Intruder rate-limiting, the execution of a Cluster bomb attack with a moderately sized payload set can take a significantly longer time.

The Cluster bomb attack type is particularly useful for credential brute-forcing scenarios where the mapping between usernames and passwords is unknown.

We have three payload sets. The first set contains 100 lines, the second contains 2 lines, and the third contains 30 lines.

How many requests will Intruder make using these payload sets in a Cluster bomb attack?

Correct Answer

Hint

INTRODUCTION TO ATTACK TYPES

Just as a brief summary.

1. **Sniper:** The Sniper attack type is the default and most commonly used option. It cycles through the payloads, inserting one payload at a time into each position defined in the request. Sniper attacks iterate through all the payloads in a linear fashion, allowing for precise and focused testing.
2. **Battering ram:** The Battering ram attack type differs from Sniper in that it sends all payloads simultaneously, each payload inserted into its respective position. This attack type is useful when testing for race conditions or when payloads need to be sent concurrently.
3. **Pitchfork:** The Pitchfork attack type enables the simultaneous testing of multiple positions with different payloads. It allows the tester to define multiple payload sets, each associated with a specific position in the request. Pitchfork attacks are effective when there are distinct parameters that need separate testing.
4. **Cluster bomb:** The Cluster bomb attack type combines the Sniper and Pitchfork approaches. It performs a Sniper-like attack on each position but simultaneously tests all payloads from each set. This attack type is useful when multiple positions have different payloads, and we want to test them all together.

What attack type cycles through the payloads inserting one payload at a time into each position defined in the request?

Sniper

Correct Answer

PRACTICAL EXAMPLE

This example shows how to perform basics Intruder Tasks. It helps to learn in a step by step method, how to load worklist for various position. Its highly recommended to do a Hand-on practice on all the rest of the practical examples.

What username and password combination indicates a successful login attempt? The answer format is "username:password".

m.rivera:letmein1

Correct Answer

PRACTICAL CHALLENGE

It tells about what kind of vulnerabilities which can happen vulnerabilities which can happen when you open support tickets like IDOR.

Which attack type is best suited for this task?

Sniper

Correct Answer

Hint

Configure an appropriate position and payload (the tickets are stored at values between 1 and 100), then start the attack.

You should find that at least five tickets will be returned with a status code 200, indicating that they exist.

No answer needed

Question Done

Hint

Either using the **Response** tab in the **Attack Results** window or by looking at each successful (i.e. 200 code) request manually in your browser, find the ticket that contains the flag.

What is the flag?

THM{MTMxNTg5NTUzMWM0OWRIYzUzMDVjMzJl}

Correct Answer

EXTRA MILE CHALLENGE

This Task helps the user to learn how to configure Macro for a Burp Suite Intruder. This is a helpful functionality when considering ever changing Cookies and Tokens in the requests.

ITS HIGHLY RECOMMENDED TO GO THROUGH THE SECTION AND PRACTICE THE CHALLENGE. THE ANSWER PASTED HERE IS JUST TO HELP IN CASE NOTHING WORKS OUT.

What username and password combination indicates a successful login attempt? The answer format is "username:password".

o.bennet:bella1

Correct Answer

Tryhackme Walkthrough

Tryhackme Writeup

Tryhackme

Burpsuite

Burpsuite Extension



Follow

Written by Ayan Mukherjee

12 Followers · 1 Following

Responses (1)



What are your thoughts?

Respond



Samar

2 months ago



What attack type cycles through the payloads inserting one payload at a time into each position defined in the request?

> Sniper



Reply

More from Ayan Mukherjee

reference to a "Cookie jar"?

Correct Answer

find the "Updates" sub-category, which controls the Burp Suite update behaviour?

Correct Answer

category which allows you to change the keybindings for shortcuts in Burp Suite?

Correct Answer

TLS certificates, can we override these on a per-project basis (yea/nay)?

Correct Answer



Ayan Mukherjee

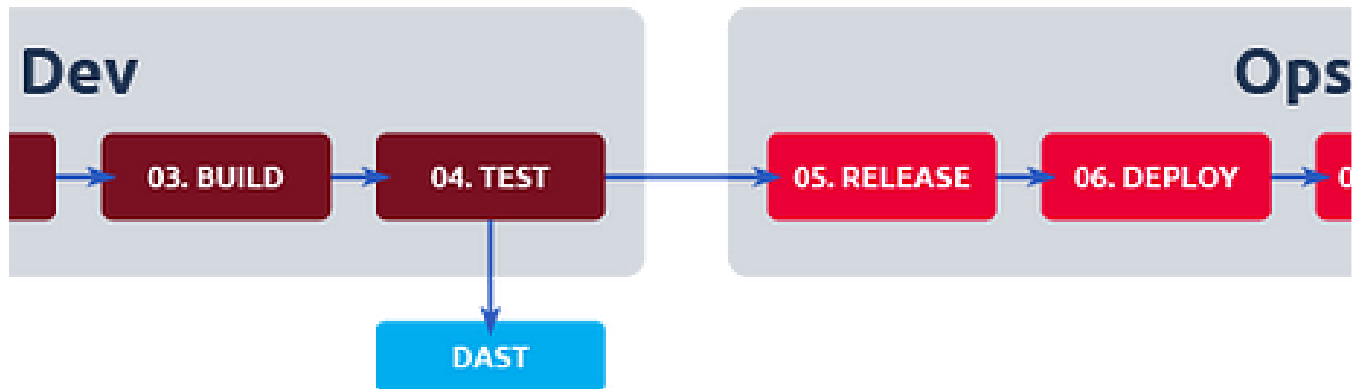
TryHackMe: Burp Suite The Basic

This particular room in TryHackme (<https://tryhackme.com/room/burpsuitebasics>) aims to understand the basics of the Burp Suite web...

Oct 30, 2023 🖱 63



Secure Software Development Life Cycle (SSDI)



 Ayan Mukherjee

DAST in TryHackMe

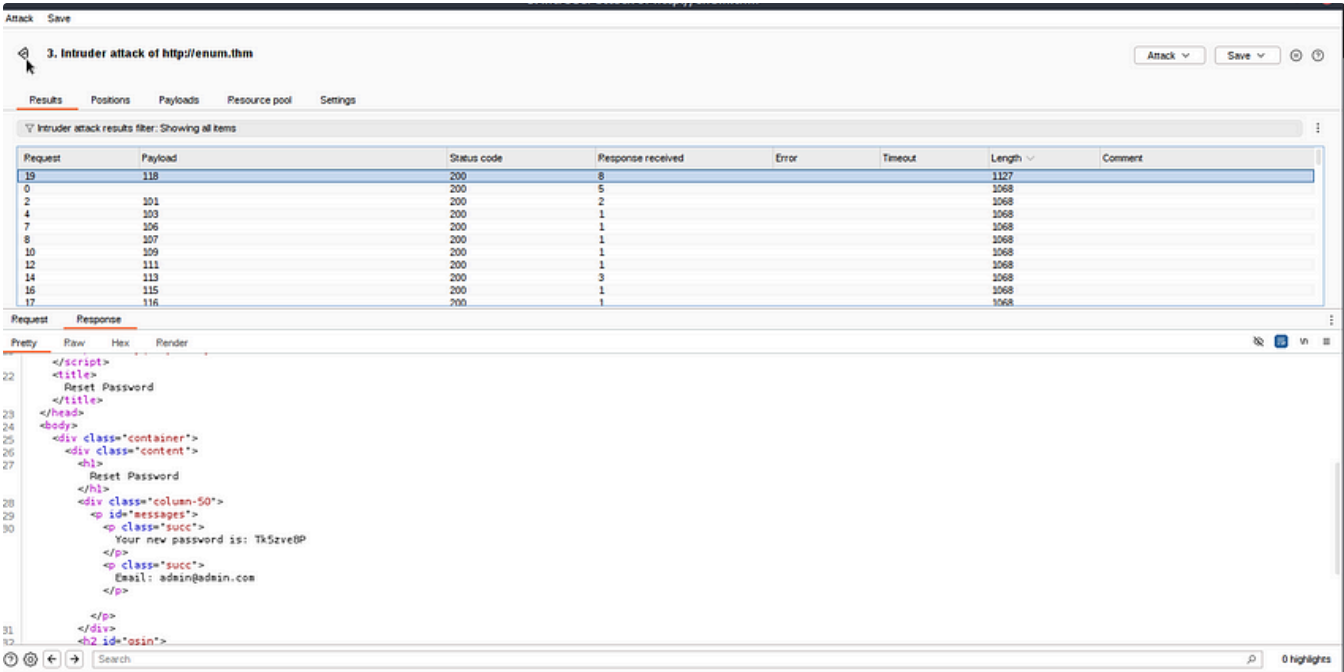
This is a writeup for the room DAST on Tryhackme


May 14, 2023 🖱 3



See all from Ayan Mukherjee

Recommended from Medium

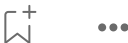


 embosssdotar

TryHackMe—Enumeration & Brute Force—Writeup

Key points: Enumeration | Brute Force | Exploring Authentication Mechanisms | Common Places to Enumerate | Verbose Errors | Password Reset...

🌟 Jul 31, 2024 🙌 26



 IritT

Burp Suite: Intruder—TryHackMe Walkthrough

Learn how to use Intruder to automate requests in Burp Suite.

Sep 18, 2024

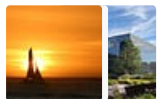


Lists



Staff picks

793 stories · 1546 saves



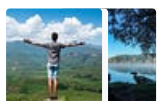
Stories to Help You Level-Up at Work

19 stories · 908 saves



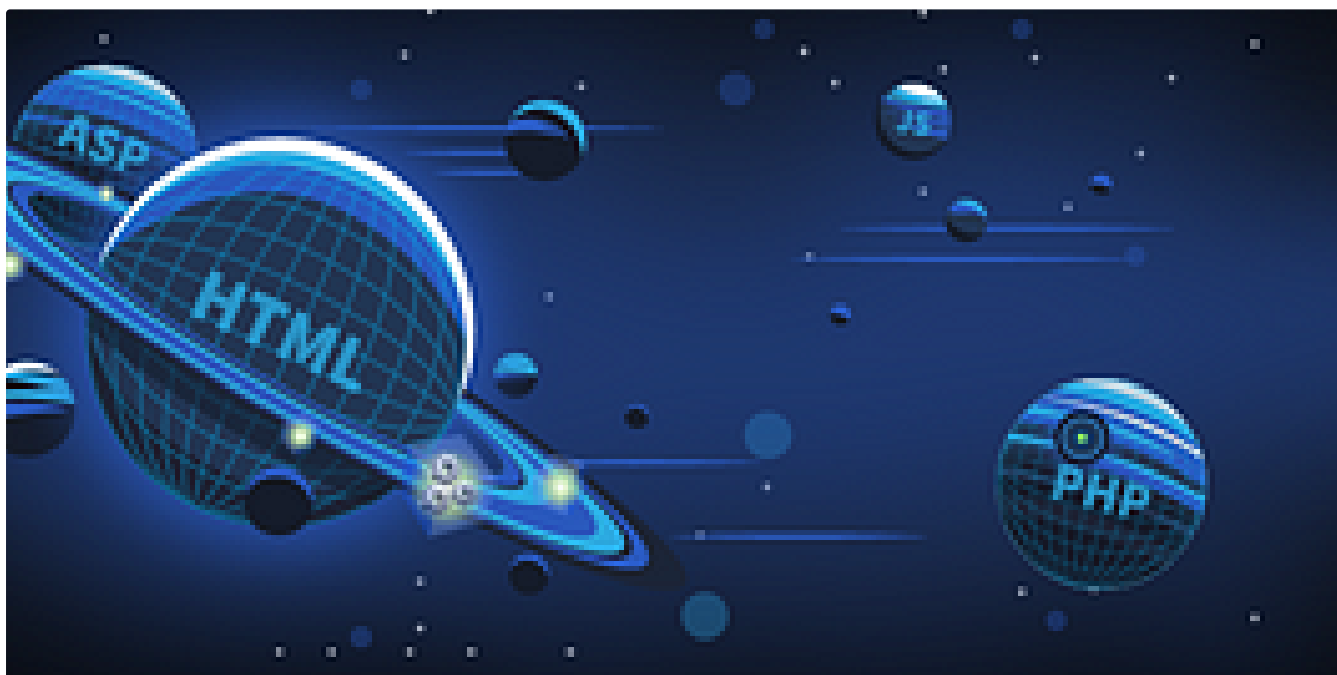
Self-Improvement 101

20 stories · 3182 saves



Productivity 101

20 stories · 2696 saves



In T3CH by Axoloth

TryHackMe | Web Application Basics | WriteUp

Learn the basics of web applications: HTTP, URLs, request methods, response codes, and headers



Oct 26, 2024



56





In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations



Nov 5, 2024



60



Repeater room!

...ed capabilities of the Burp Suite framework by focusing on the Burp Suite Repeater module. Building on the [Burp Basics room](#), we will delve into the powerful features of the Repeater tool. You will learn how to use the various options and functionalities available in this exceptional module. Throughout the room, we will ensure a deep understanding of the concepts discussed.

After completing the Burp Basics room, we recommend doing so before proceeding. The Burp Basics room will enhance your learning experience.

Get started by pressing the green **Start Machine** button. Also, start the AttackBox by pressing the blue **Start Machine**. Then, start Burp and follow along with the next tasks.

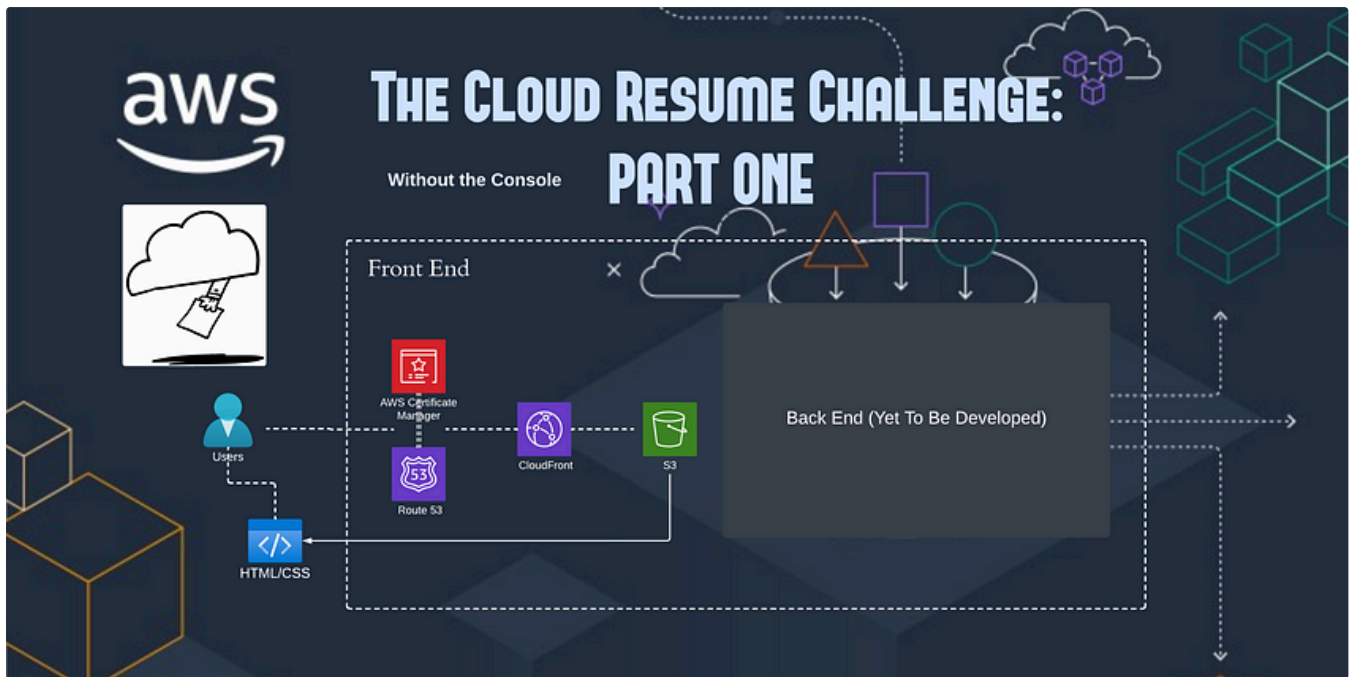


Daniel Schwarzentraub

Tryhackme Free Walk-through Room: Burp Suite: Repeater (Updated room)

Tryhackme Free Walk-through Room: Burp Suite: Repeater (Updated room)

Aug 27, 2024



Gabriel Binion

The Cloud Resume Challenge (AWS): Part One

Hello everyone, this is part one of my documentation of 'The Cloud Resume Challenge' my first cloud project where I showcase my knowledge...

Nov 18, 2024

[See more recommendations](#)