Burp Suite

Burp Suite Documentation

CSE-406 Project

Submitted by:
Udayon Paul Dhrubo(1805109)
Anika Monir(1805110)

November 11, 2023

Table of Contents

Introduction

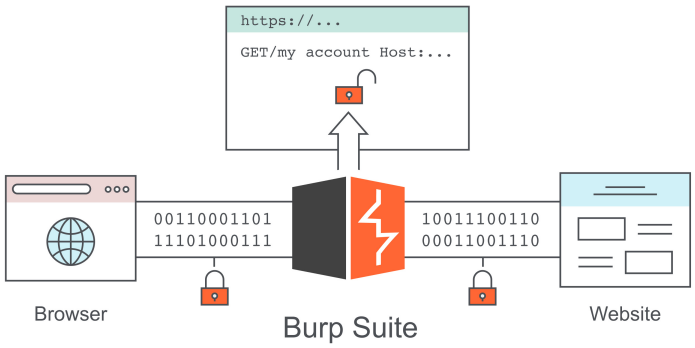
Burp Suite is a powerful and widely used cybersecurity tool designed for web application security testing and penetration testing. It is primarily used by security professionals, penetration testers, and developers to identify and address vulnerabilities in web applications, assess their security posture, and ensure compliance with security standards.Burp Suite contains a wealth of features and capabilities to support manual and automated security testing.

Key Features

Burp Suite offers a wide range of features and functionalities, including:

- **Proxy**

  Intercept and modify web traffic between your browser and the target application to analyze and manipulate requests and responses.



- **Scanner**

  Automatically scan web applications for common security vulnerabilities such as SQL injection, cross-site scripting (XSS), and more. It can also crawl a website to discover and map its structure and content

- **Intruder**

  Burp Intruder is a tool for automating customized attacks against web applications. It en-

  ables you to configure attacks that send the same HTTP request over and over again, in-

  serting different payloads into predefined positions each time.

  7 of 16

- **Repeater**

  It is used to manually manipulate and re-send requests to test how the application responds to different inputs. Burp Repeater used to send a request of interest over and over again. This let us to study the target website's response to different input without having to intercept the request each time.

Getting Started

Let's look at Burp Suite installation and usage before diving deeply into how to test a website. We will cover the following subjects in this section:

1. Downloading and installing Burp Suite.
2. Intercepting HTTP traffic with Burp Proxy.
3. Modifying requests in Burp Proxy.
4. Manually reissuing requests with Burp Repeater.
5. Automatically test on payloads with Burp Intruder.
6. Running your first scan.

Download and install

Step 1: Download

Use the links below to download the latest version of Burp Suite **Professional** or **Community** Edition.

Professional Edition Community Edition

Though Professional version is paid, you can apply for free trial —Anika fill these —.

Step 1: Install

Just run the **installer** downloaded.

Intercepting HTTP traffic with Burp Proxy.

to use proxy, open burp suite. Go to proxy tab. Make sure that intercept is turned off and go to http history and study the incoming and outgoing data traffic.

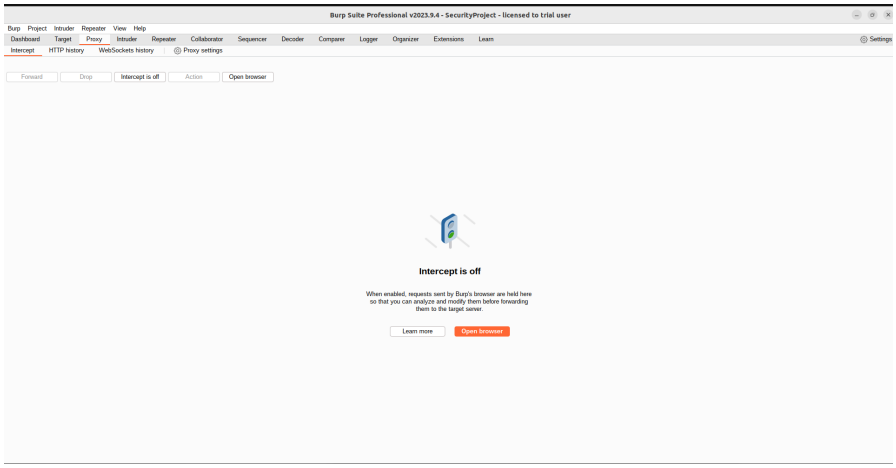


Figure 1: go to proxy tab

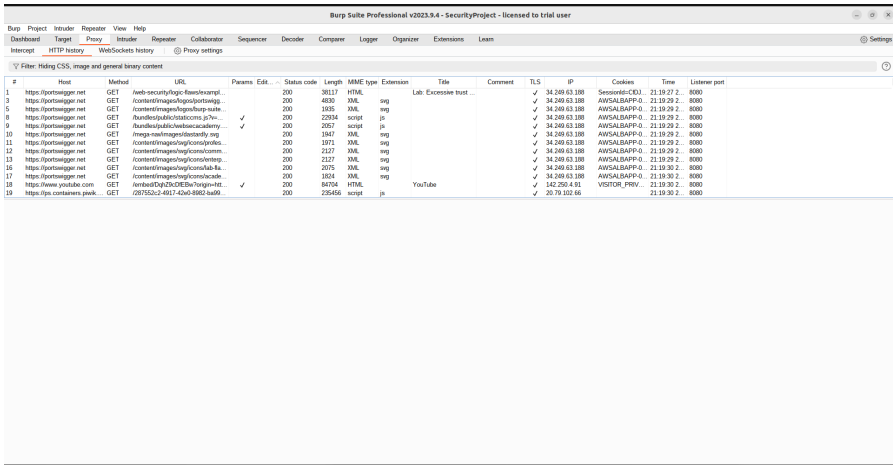


Figure 2: examine http history

examine each request in details by by clicking on a request

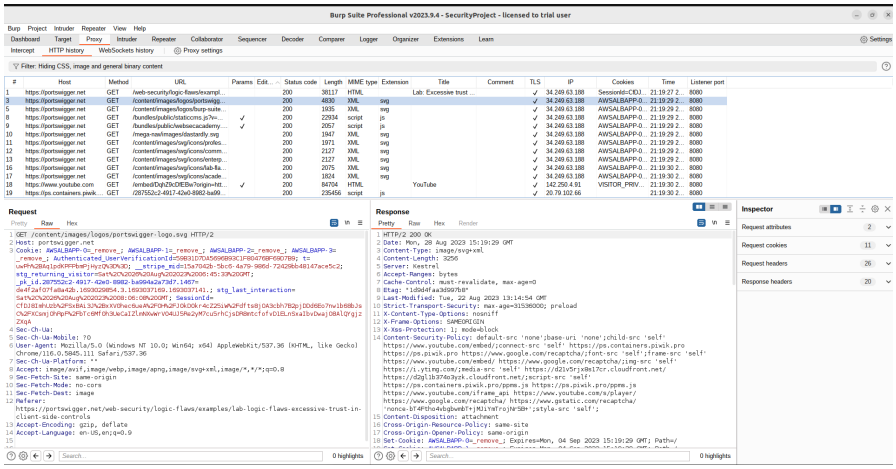


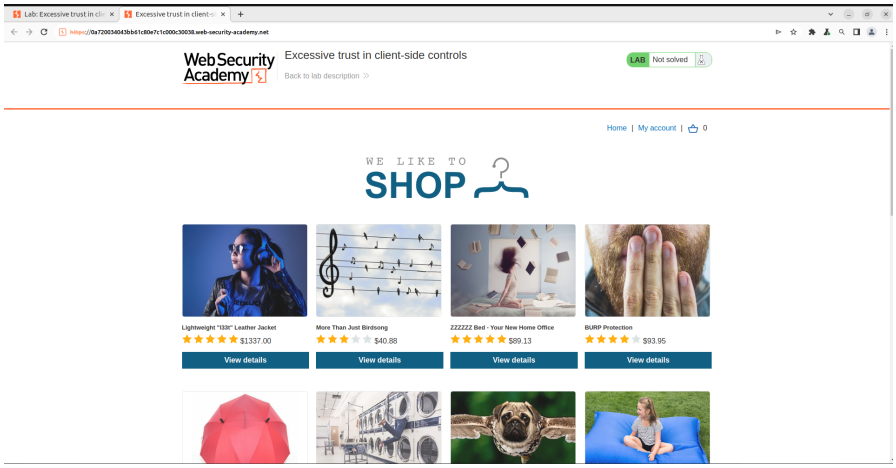
Figure 3: examine request

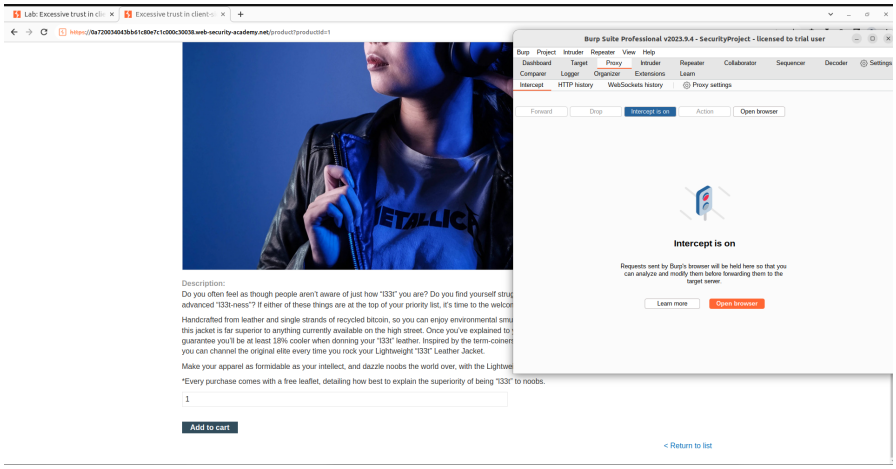
Modifying Request in Burp Proxy.

Burp Proxy lets you intercept HTTP requests and responses sent between Burp's browser and the target server. This enables you to study how the website behaves when you perform different actions. Then we can intercept that request and modify it any way we went

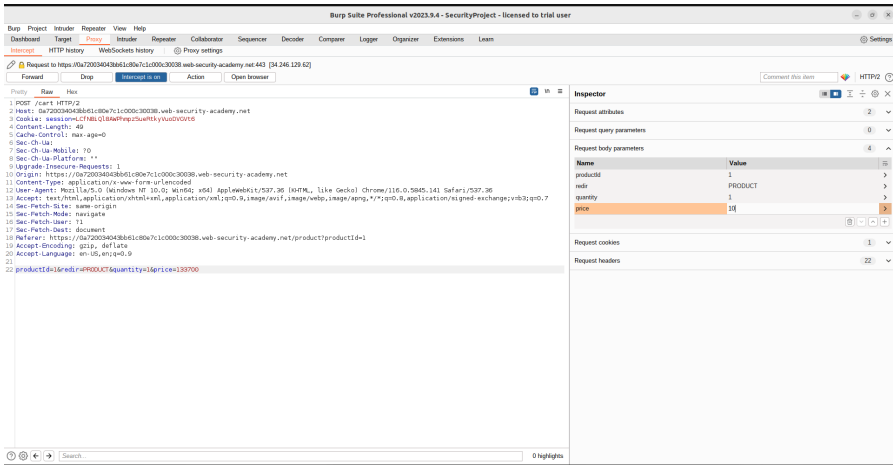
Steps

We will use an website that's vulnerable. First we will go the website, add the item we want to buy on cart

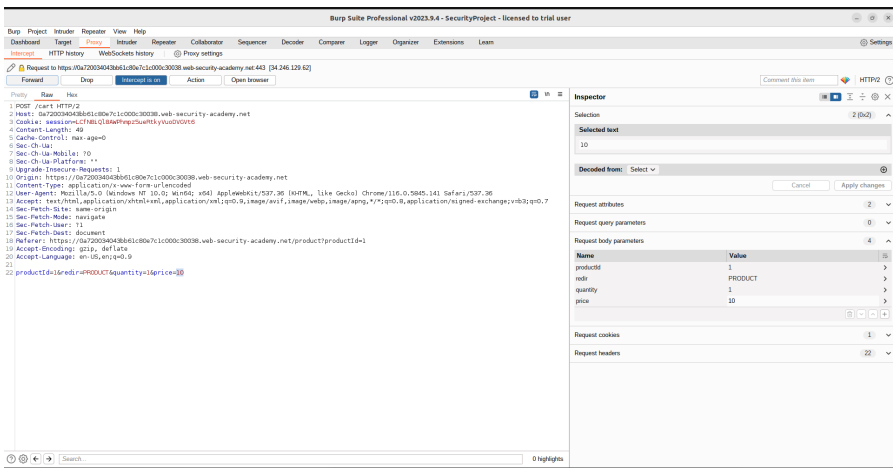




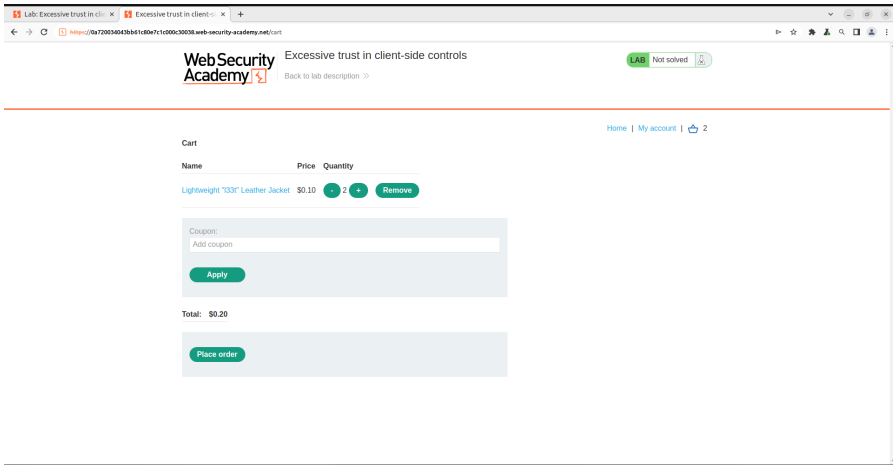
we will turn intercept on before clicking on adding to cart and then examine the intercepted request in burp suite.



We can see that the price and quantity are right there in the http request and we can modify it to change the price value from high to very very low. And then we will forward that request



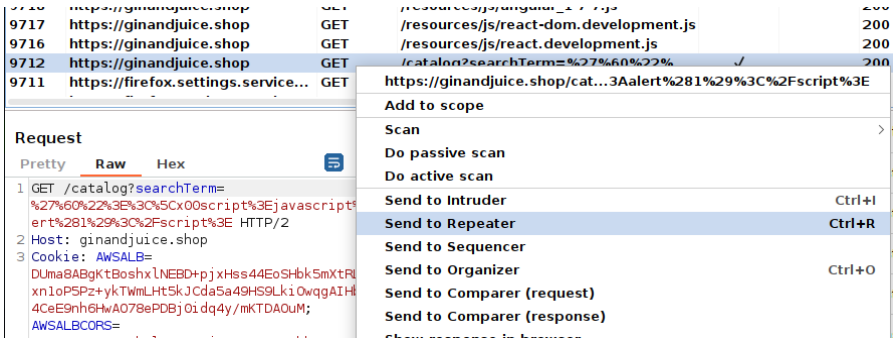
we see that in the cart two items have been added to cart significantly below their actual price.



Reissuing requests with Burp Repeater

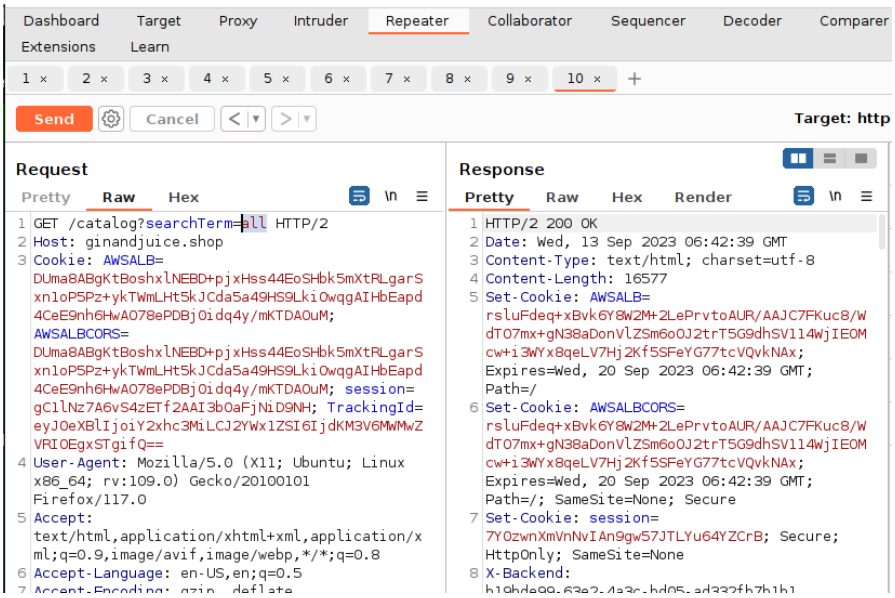
Step 1: Identify an interesting request

Go to **Proxy** > **HTTP history**. Choose a request of interest from the list. And select **Send to Repeater**



Step 2: Explore the request

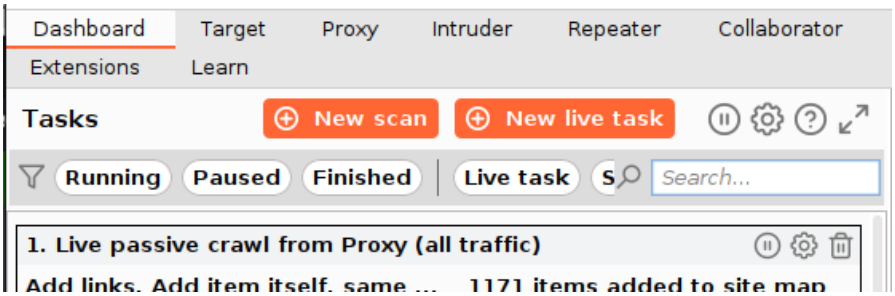
Change in any place of interest and click **Send**. Observe the request for any change you made.



Running your first scan.

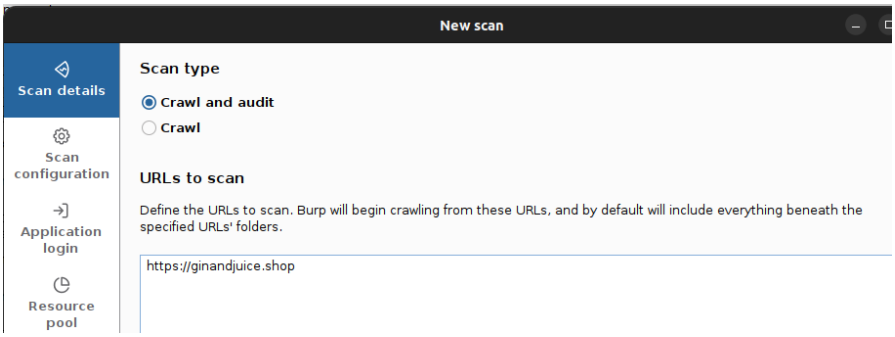
Step 1: Open the Scan Launcher

Go to the **Dashboard** tab and select **New Scan**.



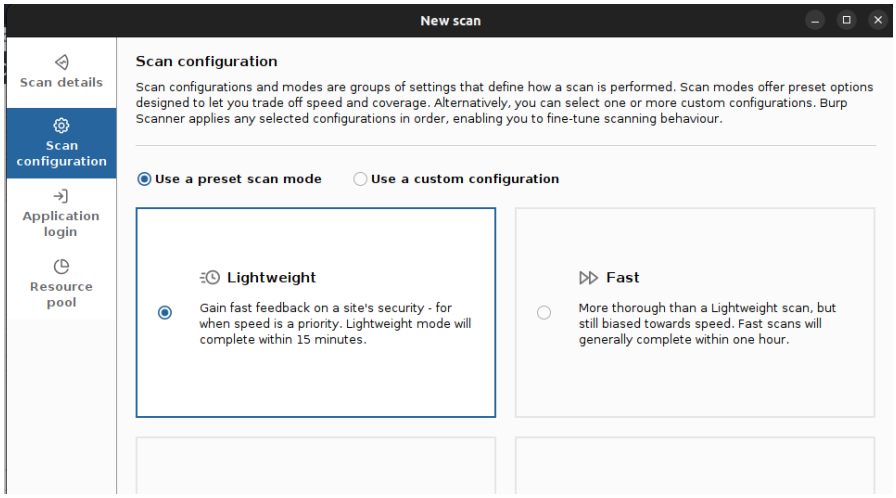
Step 2: Enter the URL of the target site

Let's say, we want to scan the site gin&juice.shop



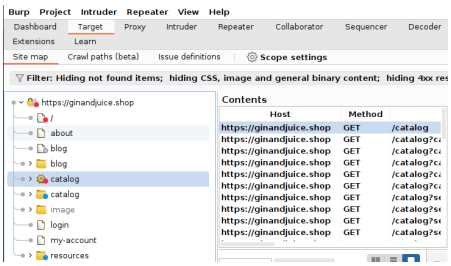
Step 3: Configure the scan

In the **Scan Configuration** make sure that **Use a preset scan mode** and select any scan mode of your choice.



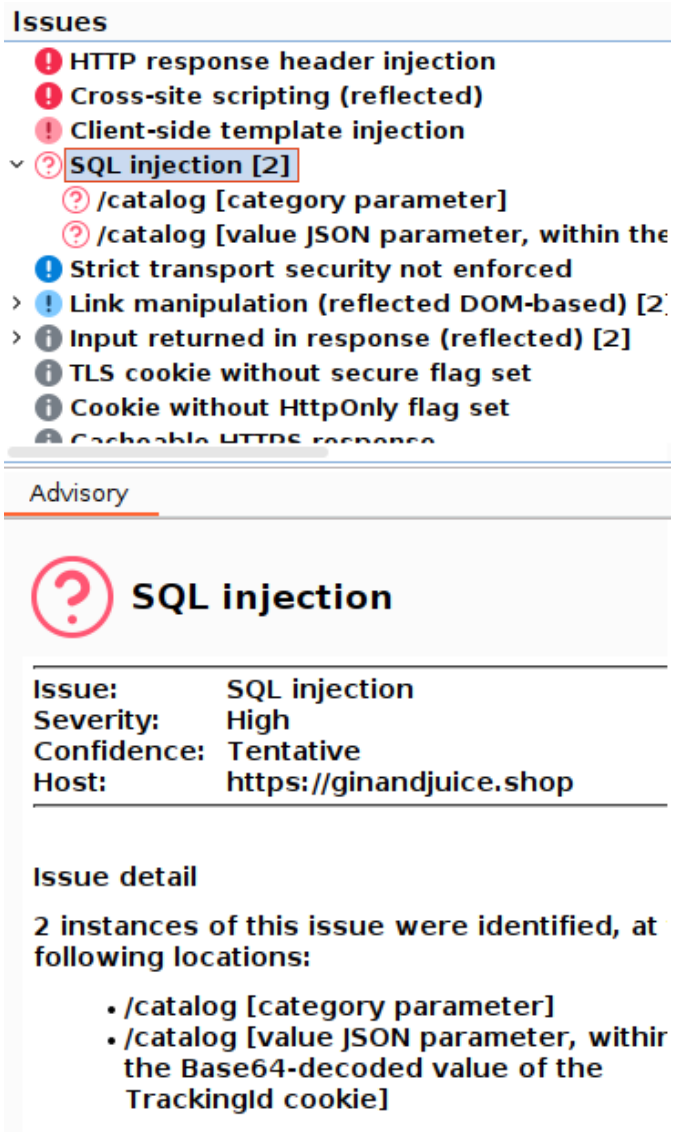
Step 4: See the mapping of the site

Go to **Target** > **Site map**. You'll see there is a new entry for **ginandjuice.shop**. Expand this node to see all of the content that the crawler has managed to discover so far.



Step 5: View the identified issues

In the **Target** > **Site map** > **Issues**, you'll see the issue found while scanning the site. If you select an issue it'll indicate where the issue were found and also gives details of that issue below.



Penetration testing workflow

Penetration testing with Burp Suite involves a structured workflow to identify and exploit vulnerabilities in web applications. You can use Burp's automated and manual tools to obtain detailed information about your target applications. Below is a step-by-step guide to the typical penetration testing process using Burp Suite:

1. Setting Test Scope
2. Map the target application
3. Analyzing the attack surface
4. Testing authentication mechanisms
5. Testing session management mechanisms

Note :
There are many other ways to test an website. But here we cover only these stages. To explore more, you can visit :
Testing-Workflow

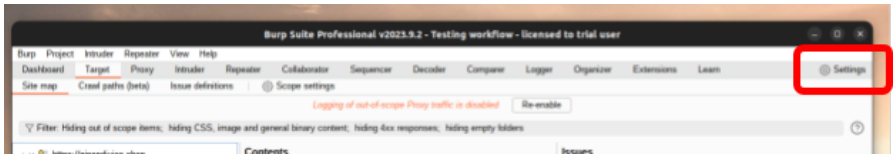
6. Testing input validation

Stage-1 : Setting Test Scope

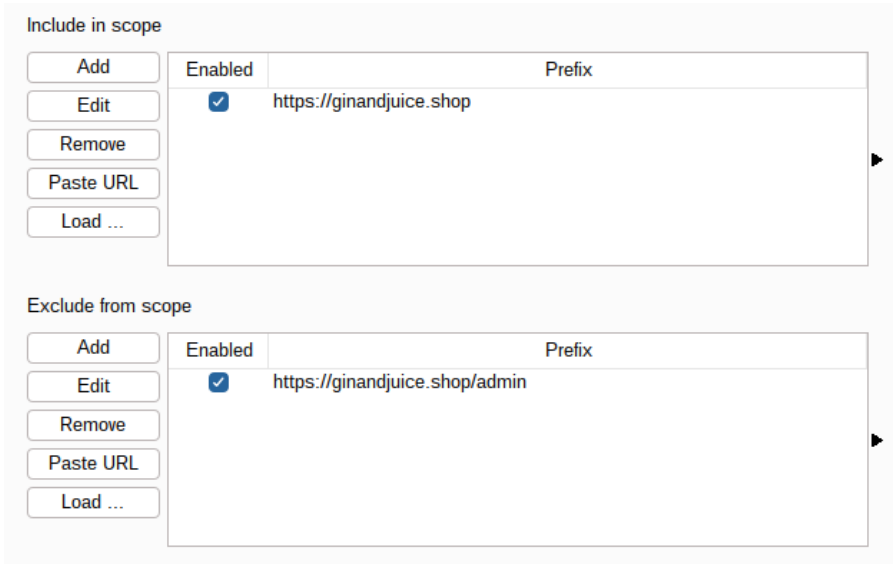
As Burp Suite capture your browsing, so there will be many unnecessary things as we browse. But we only want to focus on our target site. For this we have to Configure Project Scope of Burp Suite.
For example, let's use gin&juice.shop as our test scope. Now we have to configure Burp Suite's project scope settings.

Step-1 : Change in Project Scope

- Go to project **settings**

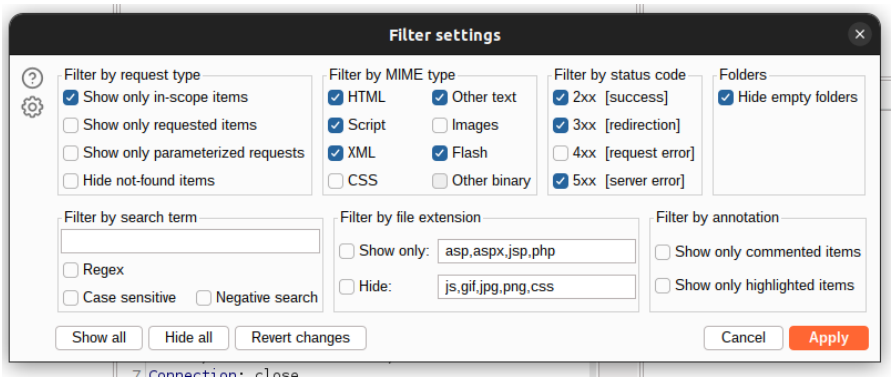


- Go to **Project** > **Scope**
  - Here, 2 options will show - **Include in scope** and **Exclude in scope.** For our case we did



Step-2 : Filter out Out-of-Scope capturing

- Then close the Settings tab. And go to the **Target** tab.
- There may be other http requests included in that window. You can filter out the un-wanted request by

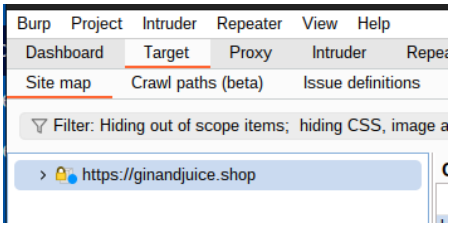


Stage-2 : Mapping the web application

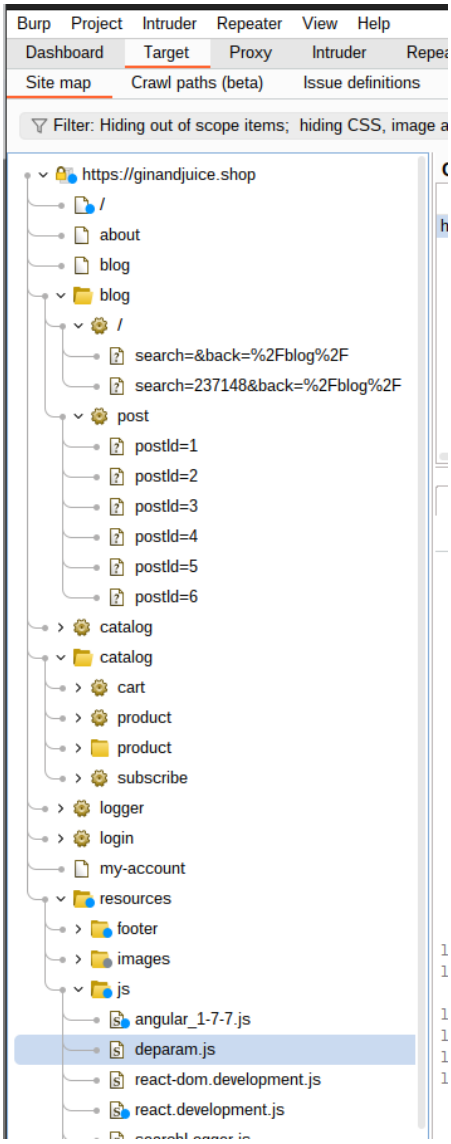
The best way to start testing an application is to map its contents. This enables you to understand what the application does and how it behaves. You can then identify interesting areas that you want to probe for vulnerabilities.

Step-1 : Begin Scan

- If you have done the previous stage, then go to **Target** > **Site Map**. You'll notice that automatically there is a node created to represent the target domain.



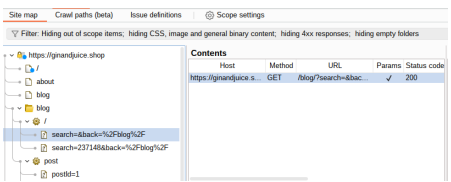
- Right-click the root node for the domain, then select Scan. The New scan dialog opens:
  - If you have any application login credentials, select Application login and enter the credentials. (In our case we don't do this)
  - Under **Scan type**, select **Crawl** or **Crawl and Audit**.
  - Click OK to start the scan. Burp Scanner crawls the application. Notice that the site map automatically populates as Burp Scanner discovers content



Stage-3 : Analyzing the attack surface

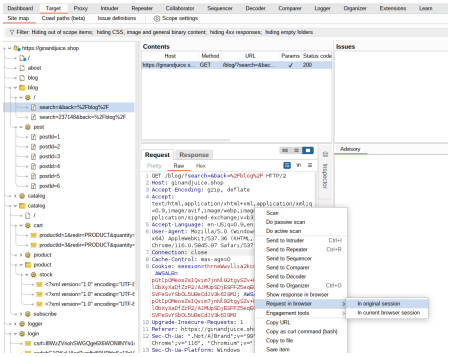
While you map the application, you should analyze your findings to identify key attack surfaces. You can use this information to plan your approach for auditing the application. Use Target > Site Map to analyze the information that Burp captures about the application.

- Suppose, select any request from the nodes.



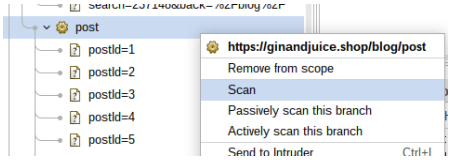
- You can send HTTP messages that you want to investigate further.

- Either by directly sending the request in the browser.



- Or you can just send the request to the **Repeater**.

- You can also use other Burp tools to help you analyze the attack surface and decide where to focus your attention:
  - Use Burp Scanner to scan a specific interesting request. Burp Scanner audits only this request. This can flag issues quickly.



Stage-4 : Testing for vulnerabilities

Testing authentication mechanism

Testing authentication mechanisms using Bu rp Intruder is a crucial step in assessing the security of a tion. Authentication is a critical component that safeguards user accounts and sensitive data. Burp In security testers to perform various types of attacks to identify vulnerabilities in the authentication pro

Enumerating usernames

Using burp intruder, we can enumerate a registration or login form. First we will try to login using a ra and password. Then we will examine the request and send it to burp intruder. Burp intruder will keep quest with possible different usernames and passwords. We will check the responses to find out any one of the inputs in the hope that it might gain us some information

Steps

To test authentication mechanism we will try to login in to a vulnerable website.

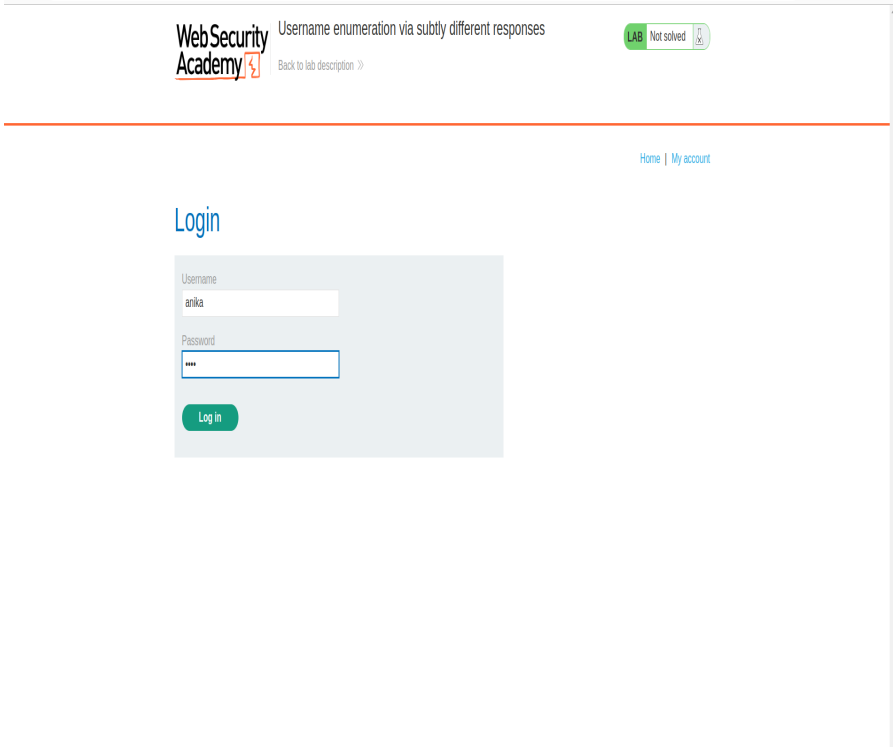


Figure 4: trying to login with incorrect usernames and passwords

the we will open burp suite and send the request to intruder.

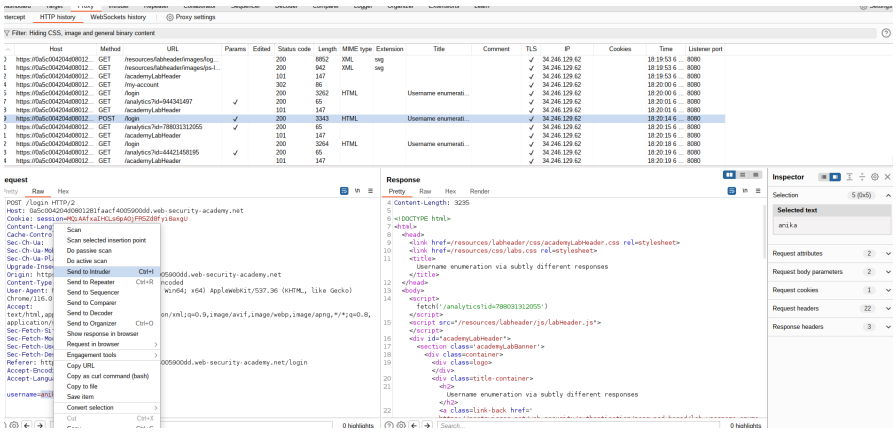


Figure 5: send the request to intruder

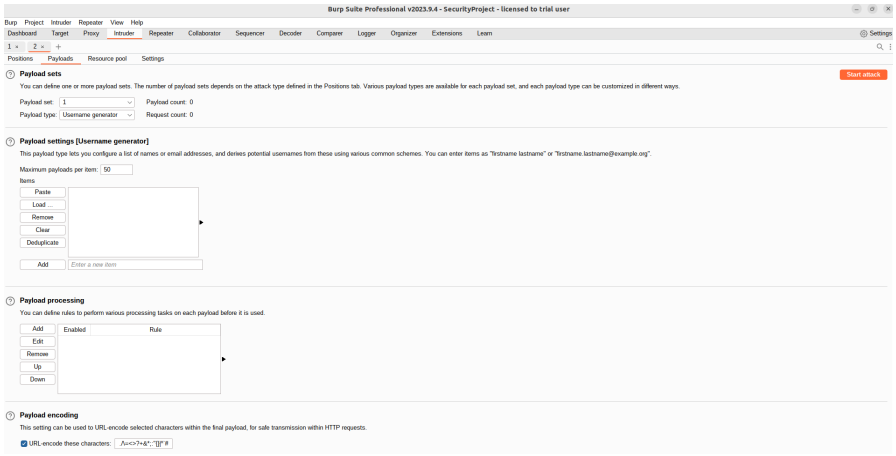


Figure 6: setting the payload

and click on start attack.

Guessing usernames

If we know an user, we can use that name to generate user names based on that knowledge. From th
we will use username generator – we can enter the number of usernames we] want Burp to generate
mum payloads per item. For exam, if we know that the name of the attacker is anika monir- burp can
anikamonir, anika_monir and so on.

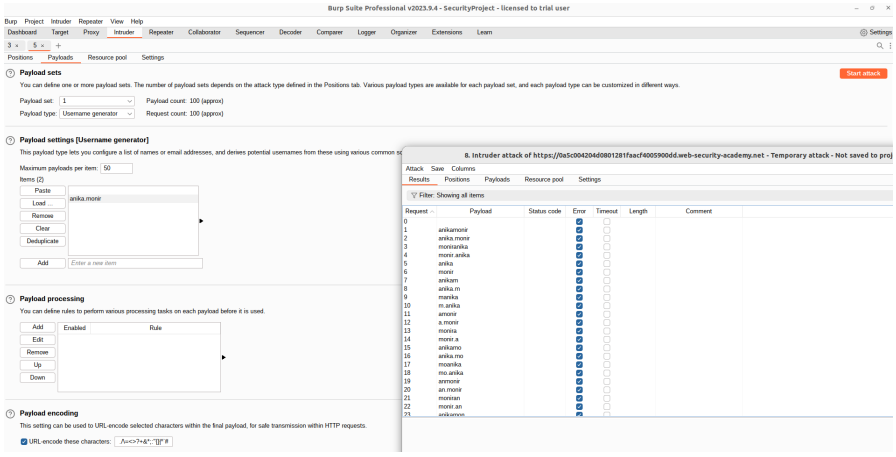


Figure 7: implementing the username generator

Brute Forcing Password

Dictionary Attack

For dictionary attack- We need to make sure that we know at least one valid username. Then we will u
list of passwords that we may have gained from previous breach attacks.For example, let's say we kn
name is weiner. Now we will possible passwords from burp suite known password list

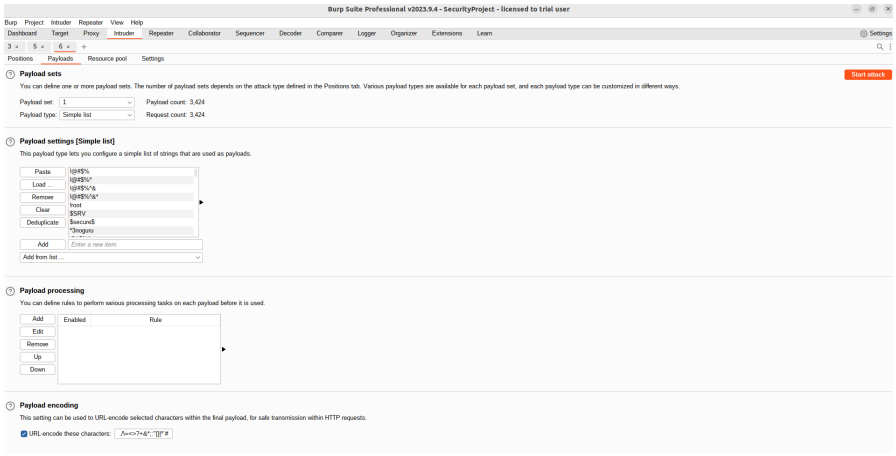


Figure 8: setting the payload a list of known passwords

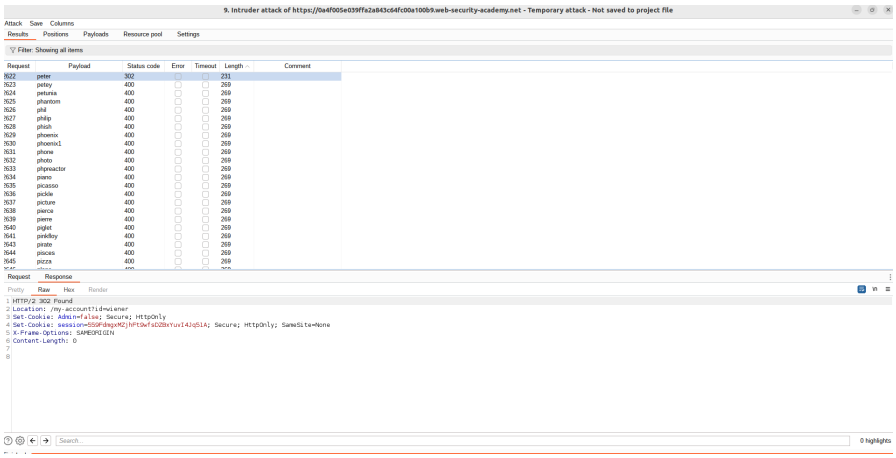


Figure 9: checking the status for different request

Exhaustive Brute Force Attack

Here we will try every possible combination of character set. This way we will even be able to check f
that is uncommon. But we still still need a username that's valid. Here we can enter the full character
minimum and maximum password length that we want to test for.

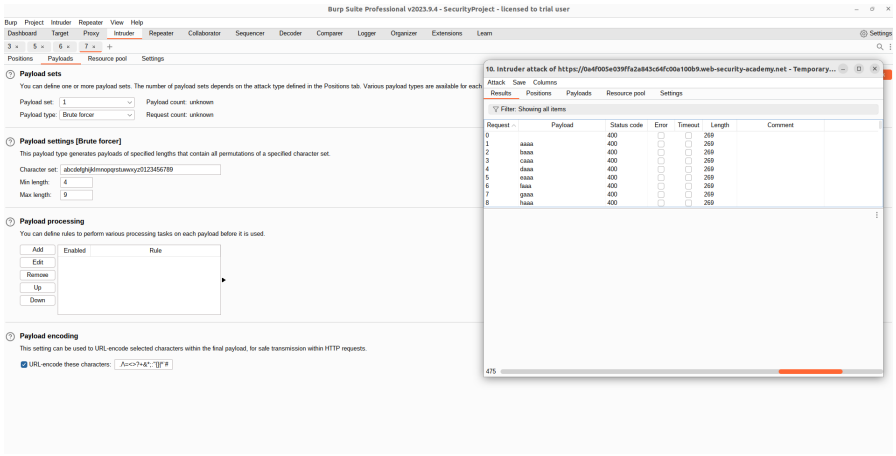


Figure 10

Credential Stuffing

Here we use known possible usernames and passwords from websites. This knowledge is usually bui
from previous breaches. For this we will use the intruder tool and the pitchfork attack type.

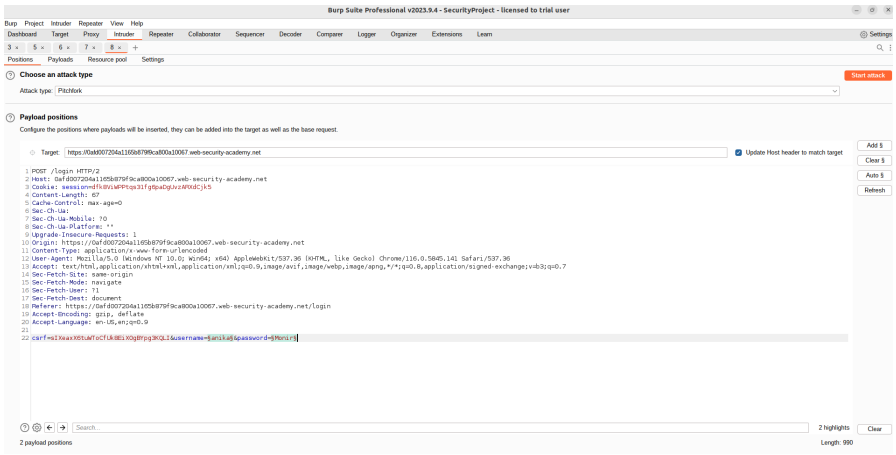


Figure 11: setting the attack type as pitch fork

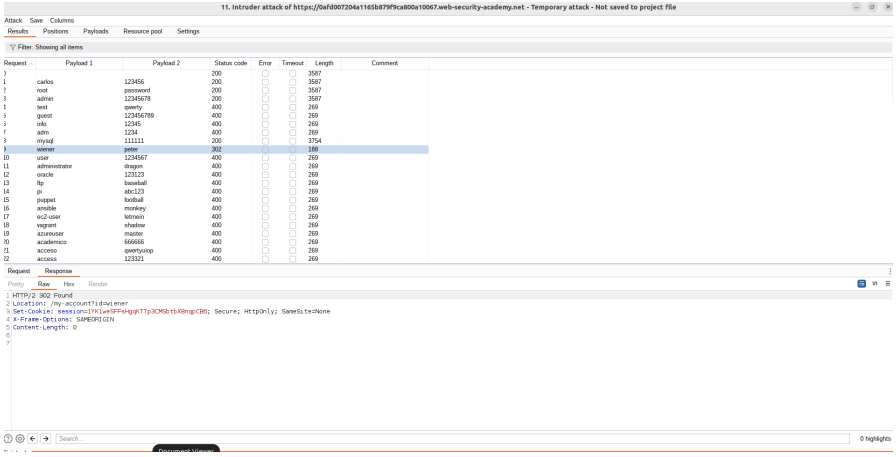


Figure 12: setting the payload as known password list from previous breaches

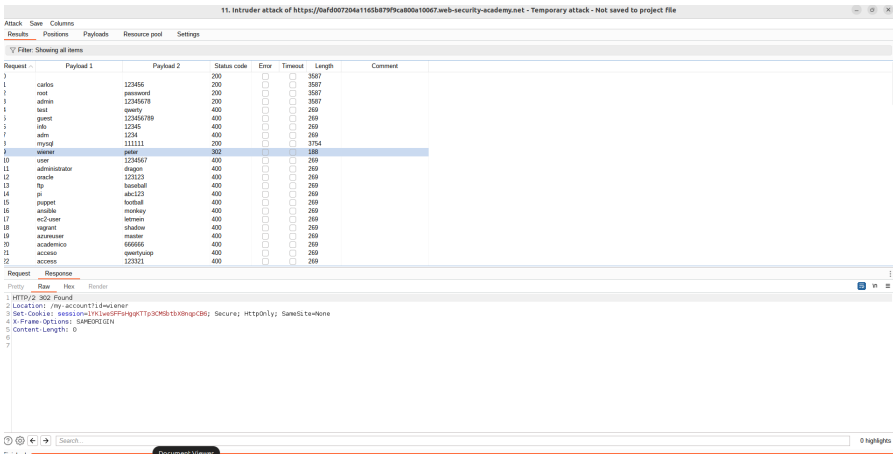


Figure 13: checking the response for each request and check for anomalies to gain knowledge

Brute force login

Since we may not always have any information on usernames and passwords- we can also brute force the cluster bomb attack type of intruder tool.

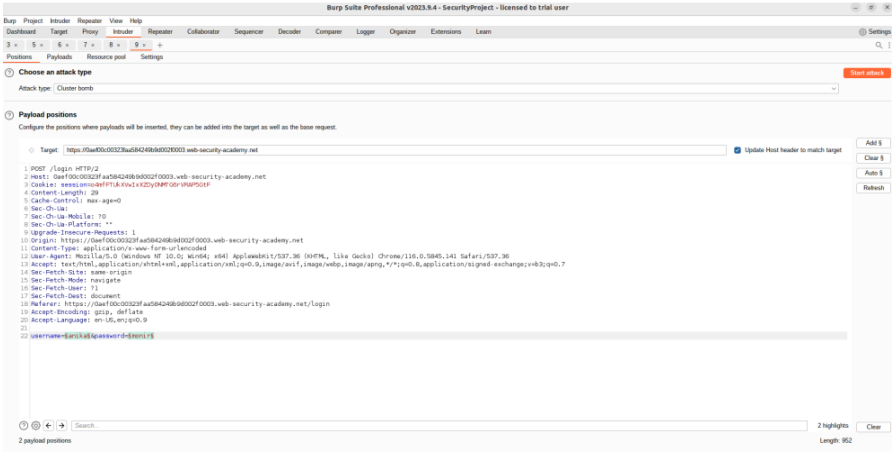


Figure 14: setting the attack type as pitch fork

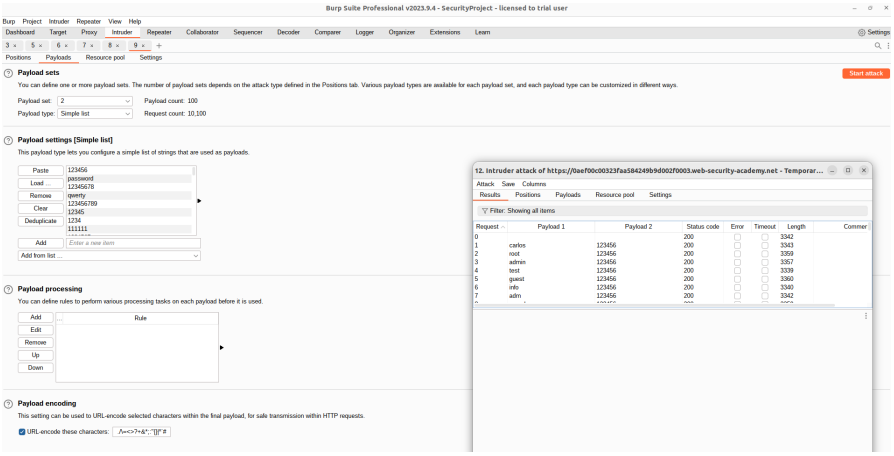


Figure 15: setting the payload as known password list from previous breaches

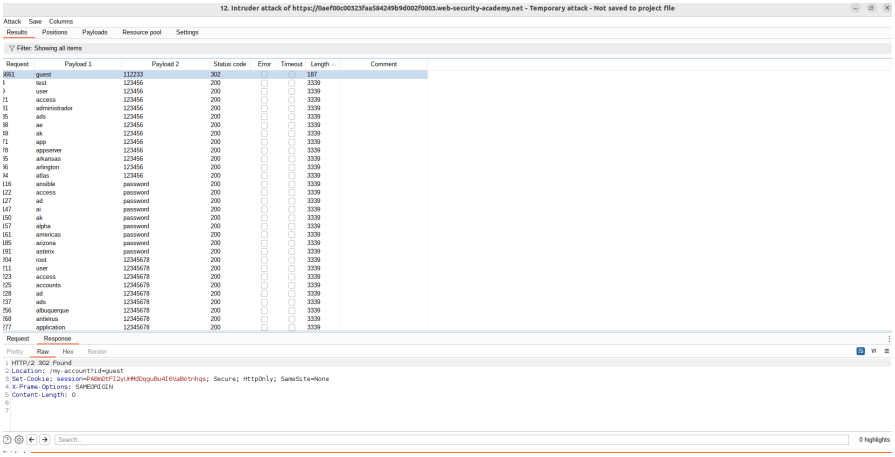


Figure 16: checking the response for each request and check for anomalies to gain knowledge

Privilege escalation

When a user logs in to an application, they usually only have access to the parts of the application tha
perform their specific tasks. If access controls are incorrectly set, a user can gain access to functiona
only be available to higher-privileged users.

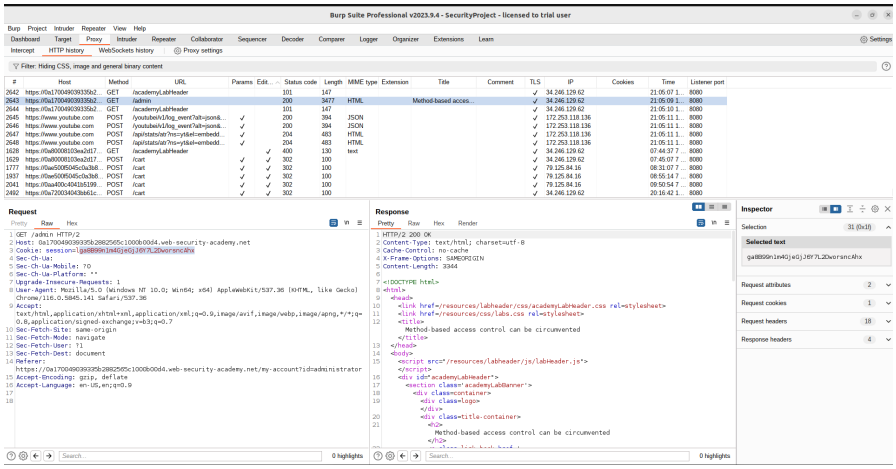


Figure 17: log in as an administrator and access the admin panel

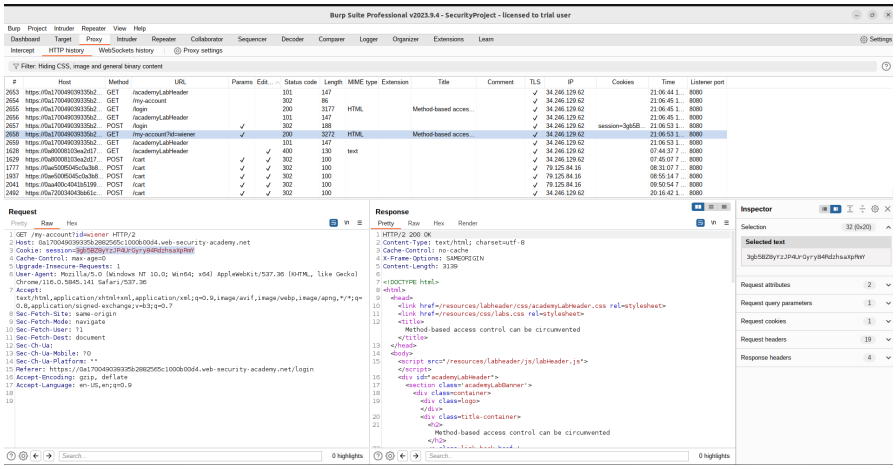


Figure 18: login as a normal user

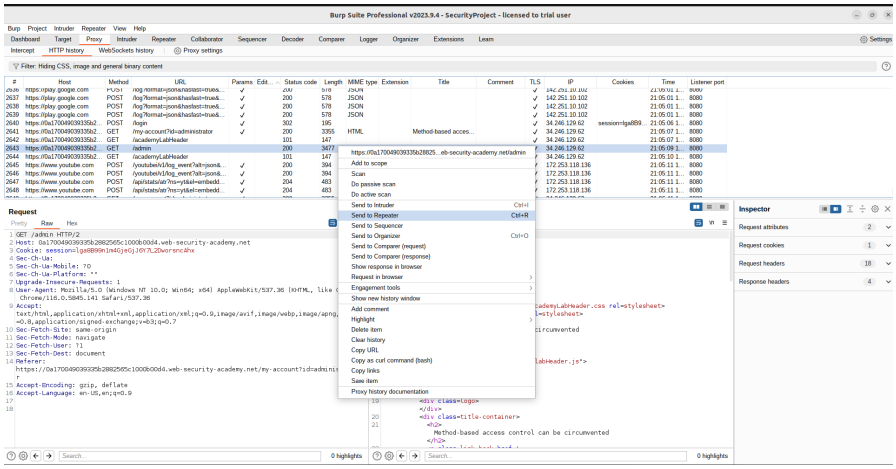


Figure 19: send the recent request of normal user to repeater

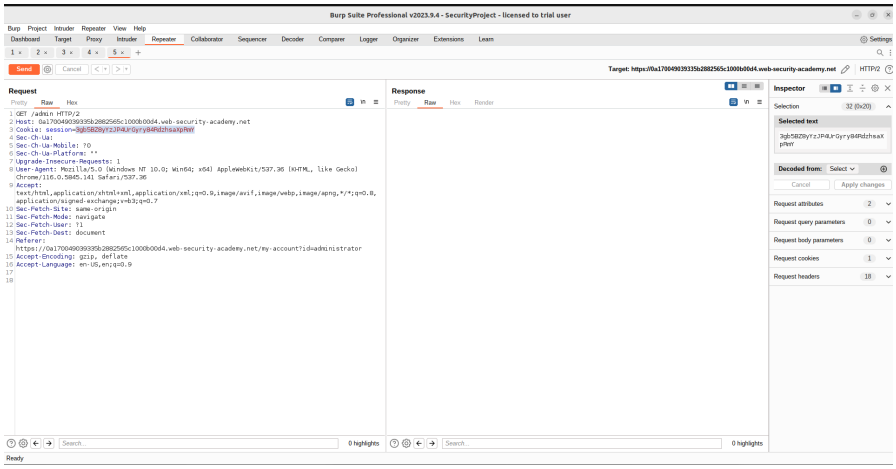


Figure 20: copy the session cookie of normal user to the administrative user

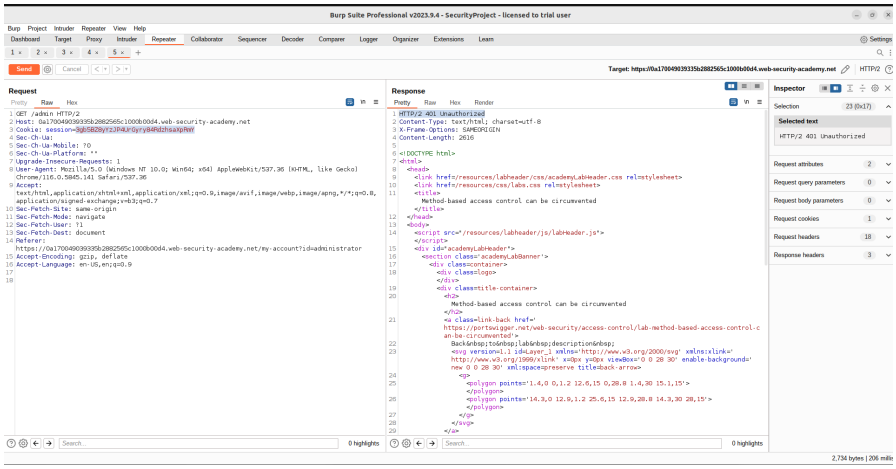
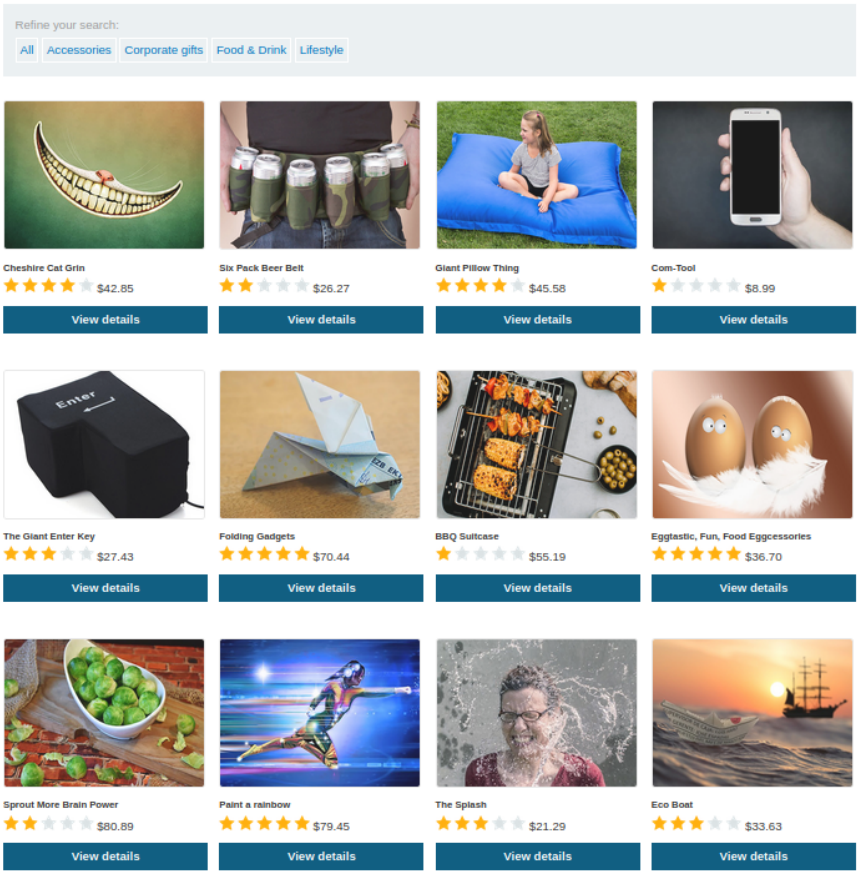


Figure 21: send the request and check if the security breach works.Here we got a 401 confirming that the endpoint is not vulnerable

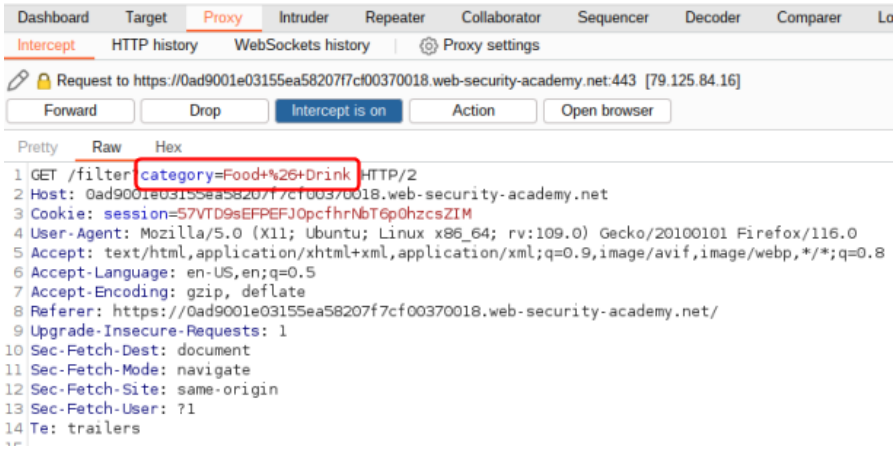
Testing SQL Injection vulnerabilities

SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally enables an attacker to view data that they are not normally able to retrieve. An attacker may then be able to modify or delete this data.
For this, let test for this educational lab : sql_injection_lab

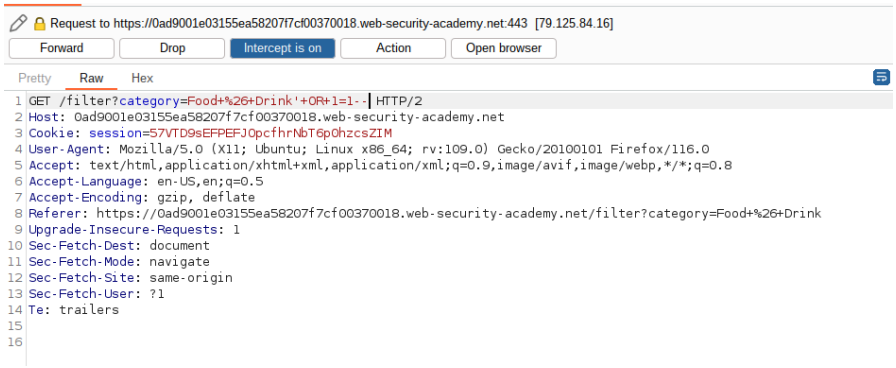
- select category All
- Then go to the browser and select any category.

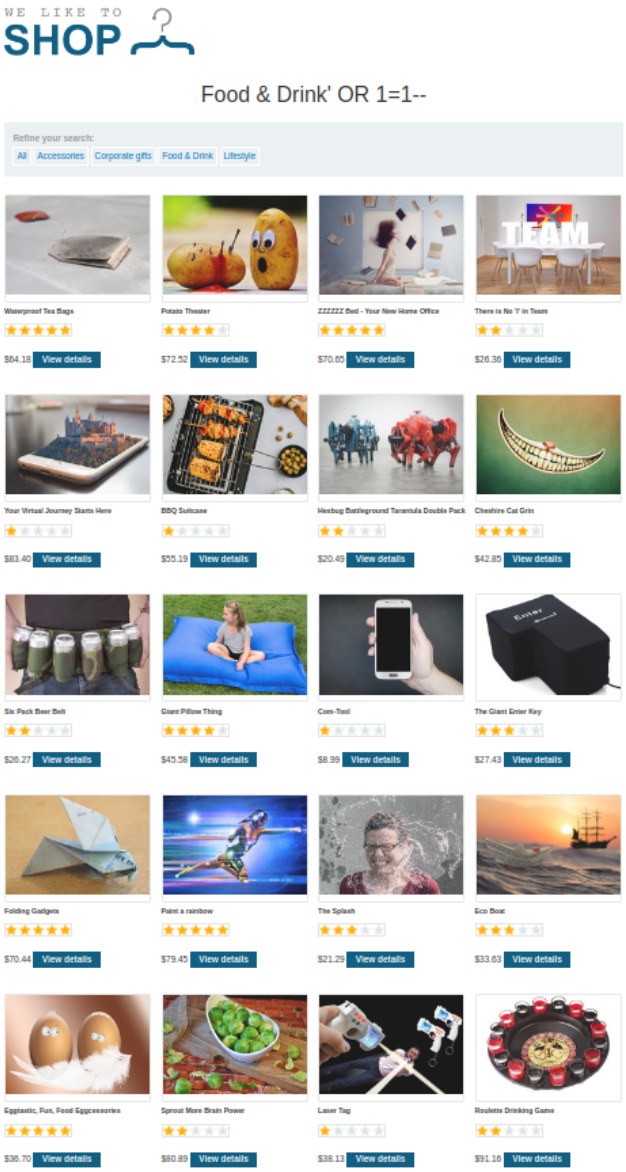


- So, this is all the website shows us.
- now turn on the intercept in proxy
- select any category. and go to **Proxy** > **Intercept**



- let append **'+OR+1=1–** to the request like below





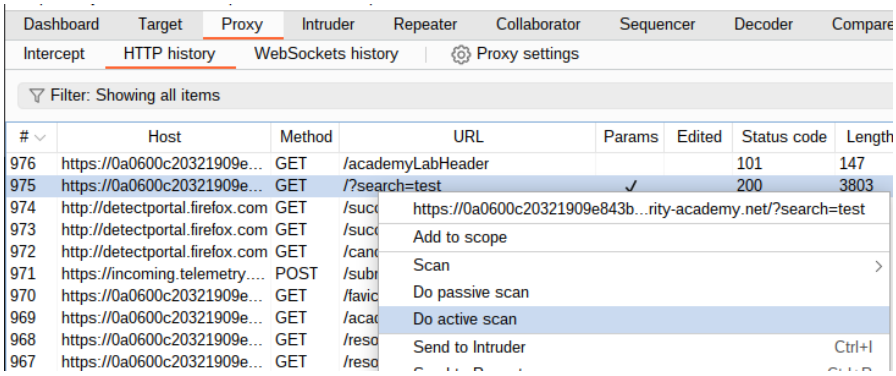
- Now we can see that, there are now even many hidden contents, which the site didn't show us in first place.

Testing XSS(Cross Site Scripting) Vulnerabilities

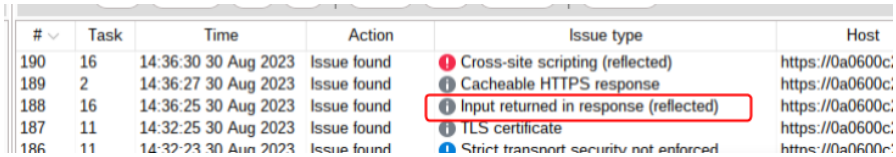
Stage-1: Identifying reflected input

Reflected input is when data is copied from a request and echoed into the application's immediate response.
Let's test this lab : reflected _input _lab

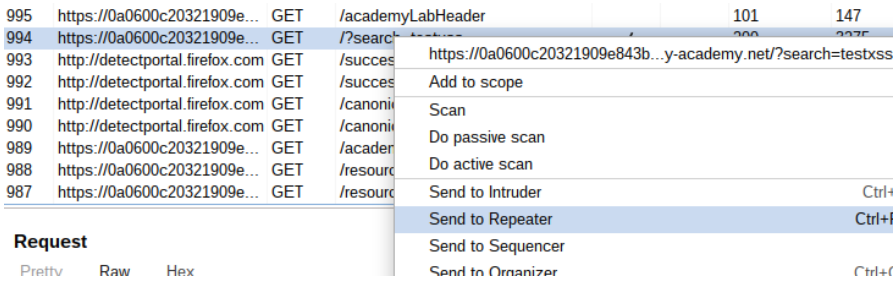
- Input anything. And go to **proxy** > **http history**. And send that request to active scan.



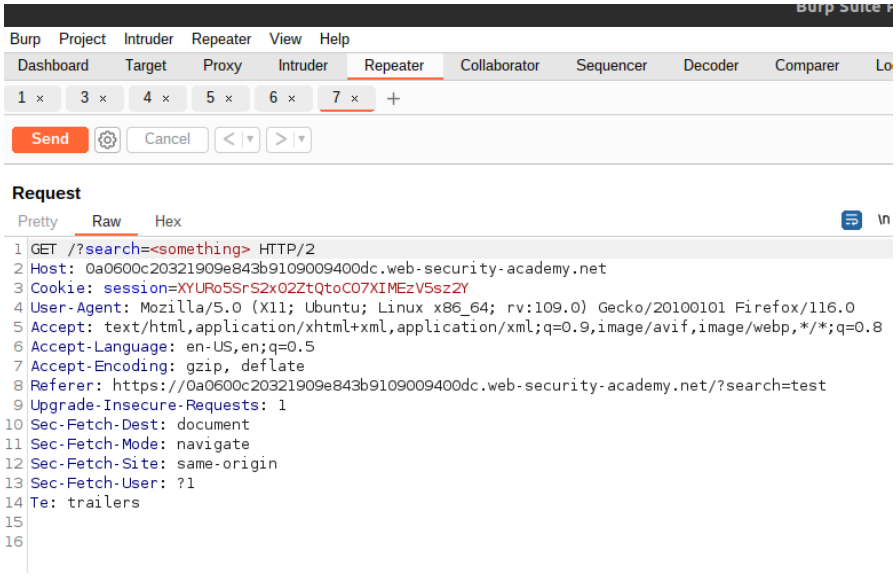
- Look any issue arises related XSS

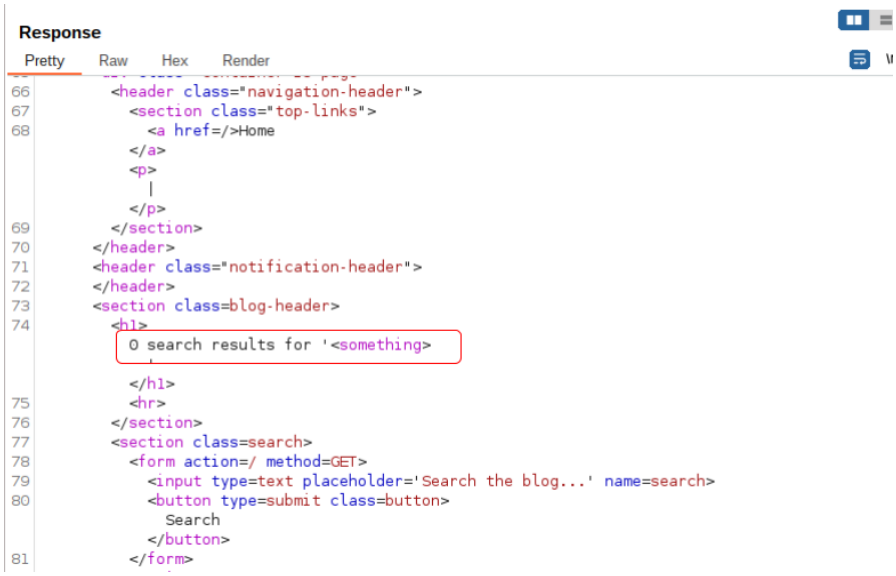


- Let's investigate the request. Send the request to the repeater.

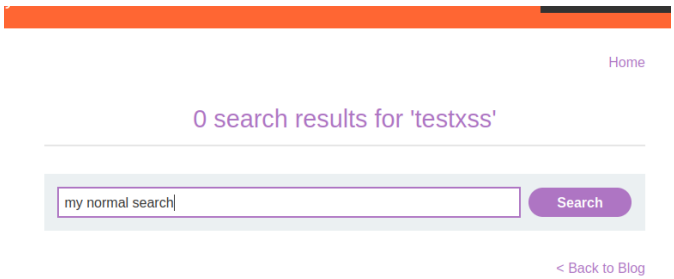


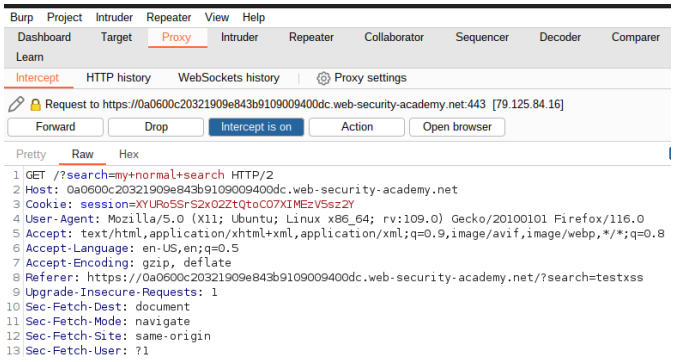
- Change the input field to anything.



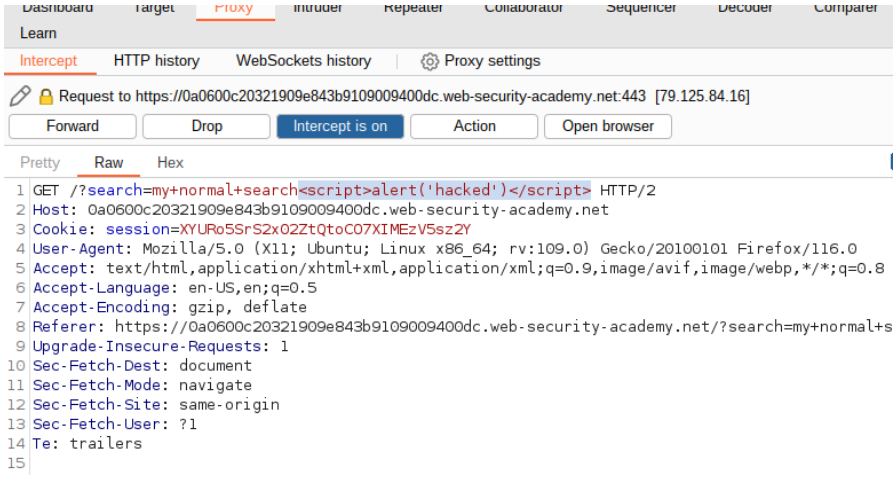


- So, we now know how our input is reflected. Let's start attacking.
- For this, we have to turn on the intercept. And make request from browser.





- append **<script>alert('hacked')</script>**



- check the response now.