AI FOR CYBER SECURITY WITH IBM QRADAR
ASSIGNMENT-4

Name:Vishnubhatla V
L Sruta Keerthi

BURPSUITE

What is Burp Suite?

Burp Suite is a comprehensive set of cybersecurity tools designed for web application security testing and vulnerability assessment. It is developed by PortSwigger, a UK-based software company. Burp Suite is widely used by security professionals, penetration testers, and ethical hackers to identify and mitigate security vulnerabilities in web applications.

Why is Burp Suite used?

Burp Suite is used for several important purposes in the field of cybersecurity:

1. Web Application Security Testing: Burp Suite helps security professionals assess the security of web applications by identifying vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and more.
2. Vulnerability Assessment: It scans web applications to detect potential security weaknesses, misconfigurations, and other issues that could be exploited by attackers.
3. Penetration Testing: Ethical hackers and penetration testers use Burp Suite to simulate attacks on web applications, uncover vulnerabilities, and provide recommendations for remediation.
4. Security Research: Researchers use Burp Suite to analyse and study web application security, helping to improve the overall security of web applications.
5. Web Application Development: Developers can use Burp Suite to test their own applications during development to catch and fix security issues before they reach production.

Features of Burp Suite:

Burp Suite offers a wide range of features to support web application security testing:

1. Proxy: Allows intercepting and modifying HTTP/S requests and responses between the client and server, making it possible to analyse and manipulate web traffic.
2. Scanner: Automatically scans web applications for common vulnerabilities, such as SQL injection, XSS, and more, providing detailed reports.
3. Intruder: Facilitates automated and customizable attacks on web applications to discover vulnerabilities and weak points.
4. Repeater: Allows manual modification and resending of individual HTTP/S requests to observe how the application responds, aiding in vulnerability discovery and testing.
5. Sequencer: Analyses the randomness of tokens and session identifiers to assess the strength of session management and authentication mechanisms.
6. Spider: Crawls and maps the structure of a web application, helping testers understand its functionality and potential attack surfaces.
7. Decoder: Provides tools to decode and encode data in various formats, such as Base64 and URL encoding.

8. Collaborator: Assists in detecting out-of-band vulnerabilities by creating unique payloads that trigger external interactions and reporting the results.

9. Extensibility: Burp Suite supports the development of custom extensions and plugins, allowing users to add additional functionality.

10. Reporting: Generates detailed reports with vulnerability findings and recommendations for remediation.

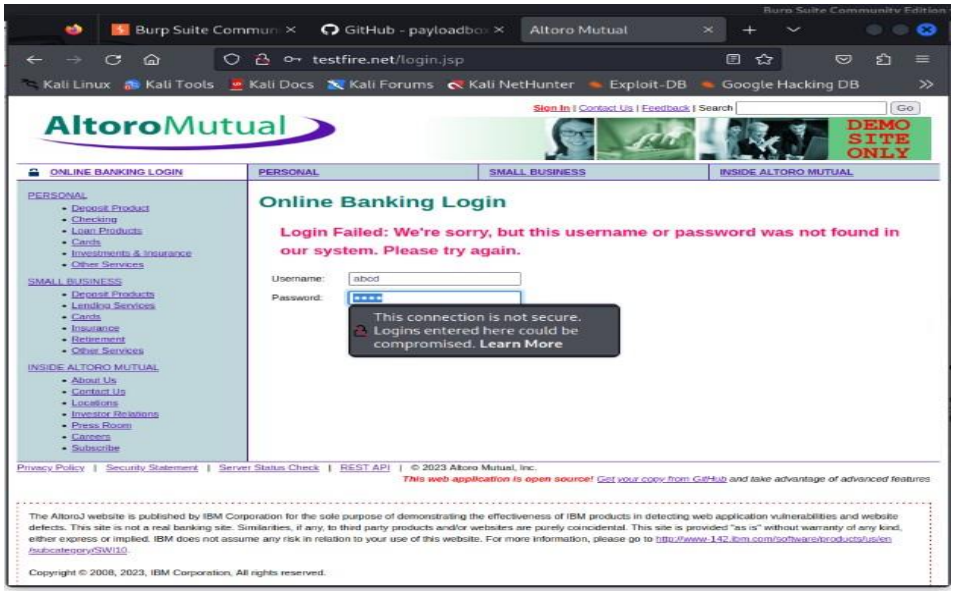
11. Target Scope Control: Allows users to define the scope of testing by specifying which parts of a web application should be included or excluded.

12. Session Handling: Manages and maintains user sessions to test authentication and authorization mechanisms thoroughly.

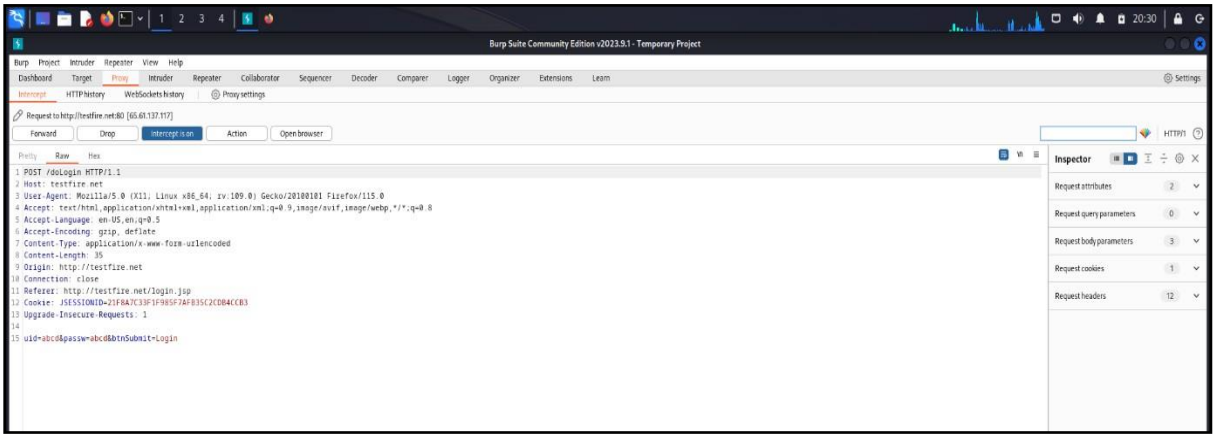
These features collectively make Burp Suite a powerful tool for identifying and mitigating web application security vulnerabilities.

Testing the vulnerabilities of testfire.net website

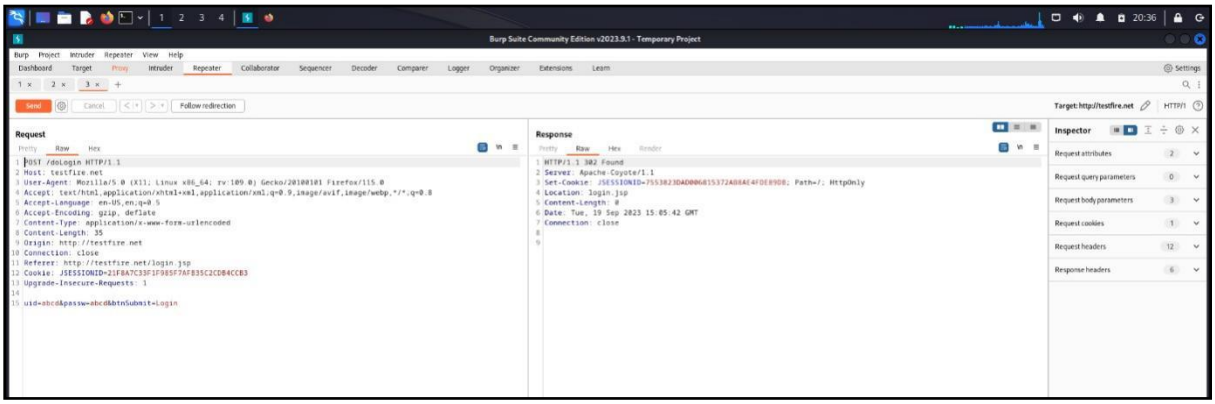
First, the website is opened and credentials are entered.



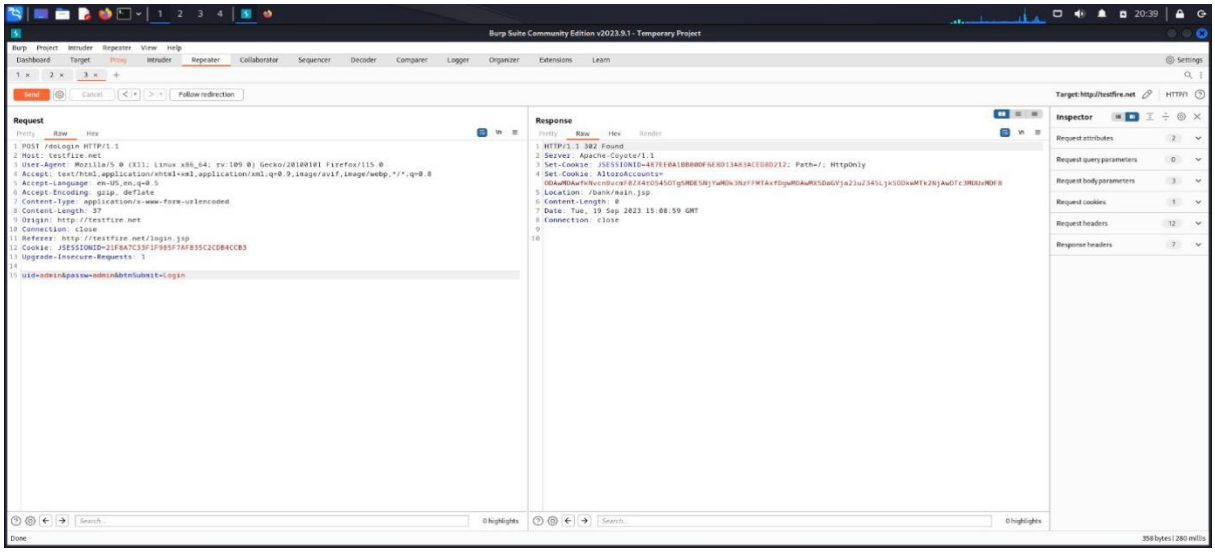
Next, the intercept in the proxy section of Burpsuite is turned on. After that, login button is clicked. After this, the below details are sent to repeater.



Here, as wrong credentials were entered, error is found.

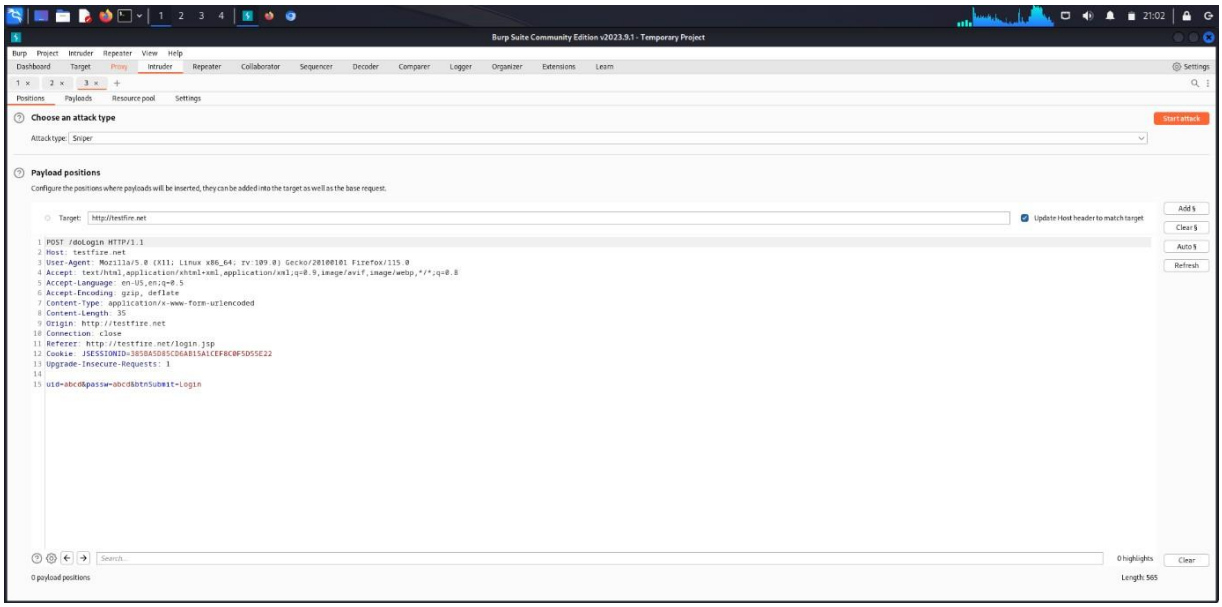


After entering the correct details, we got the source of the information below.

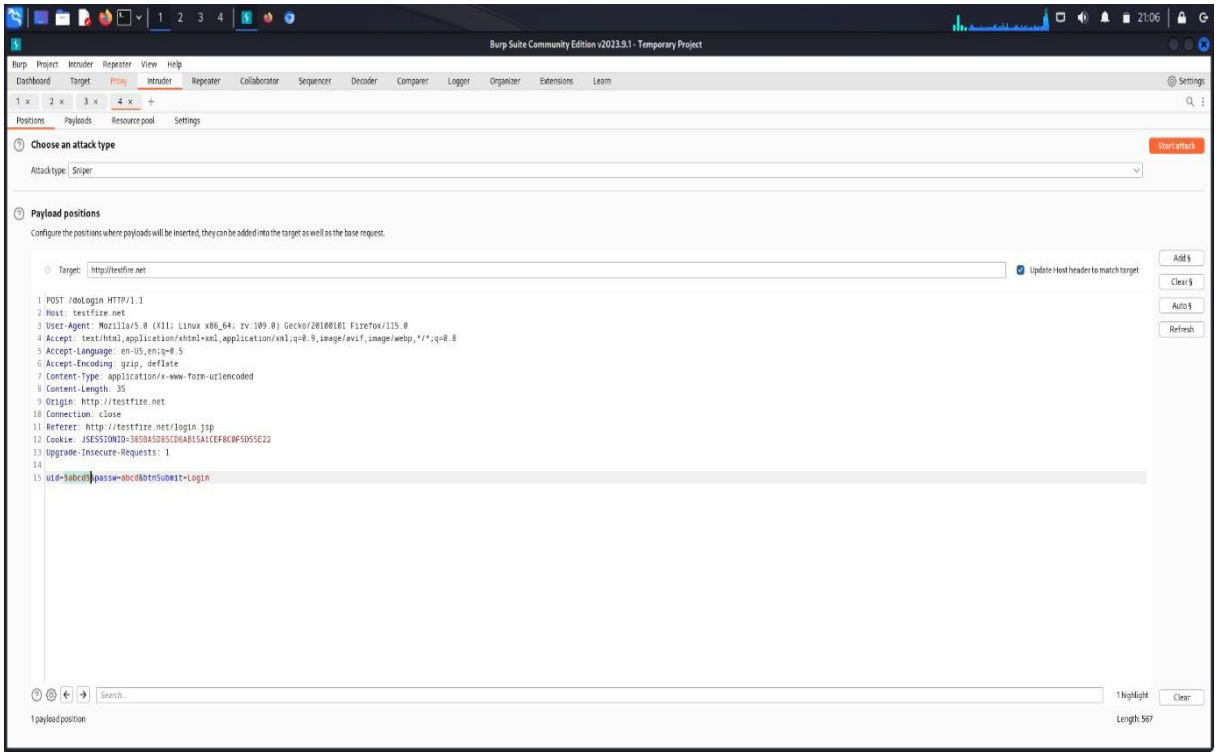


SQL INJECTION

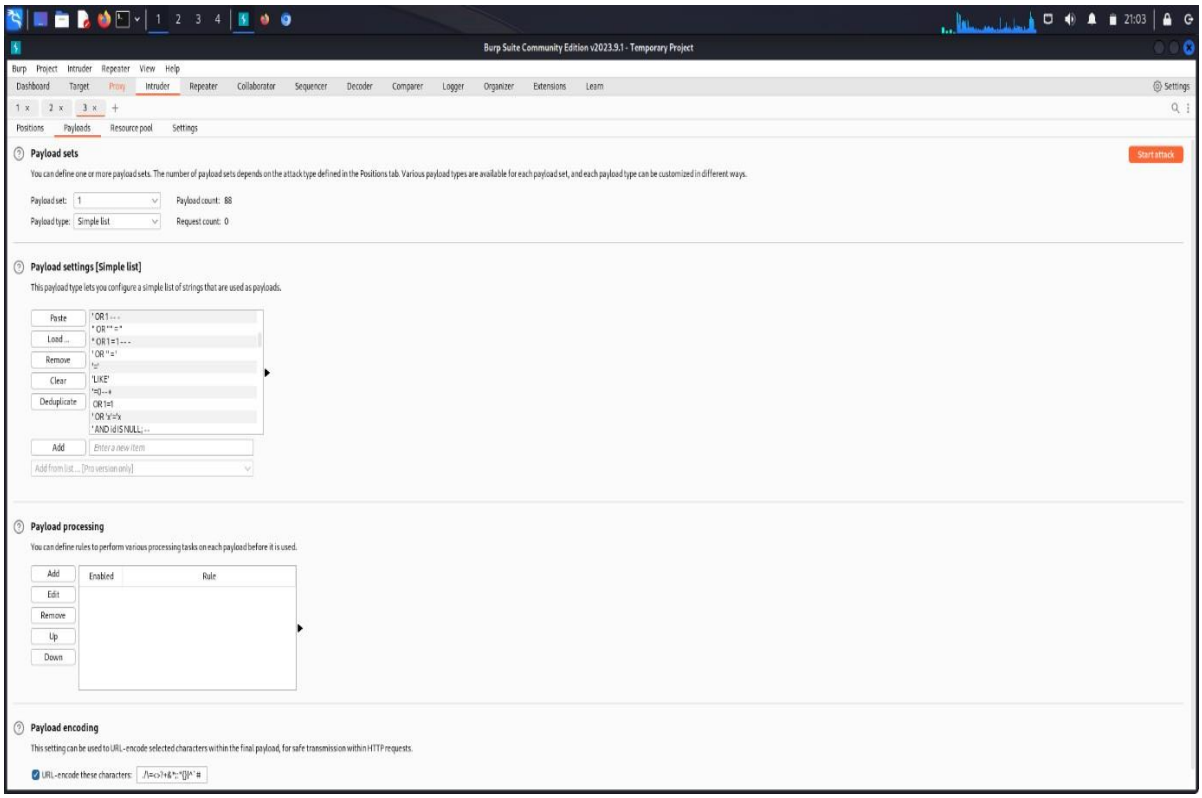
SQL injection is a technique where a malicious code is injected in a website which leads to hacking of a web page and destroying of database of the website.



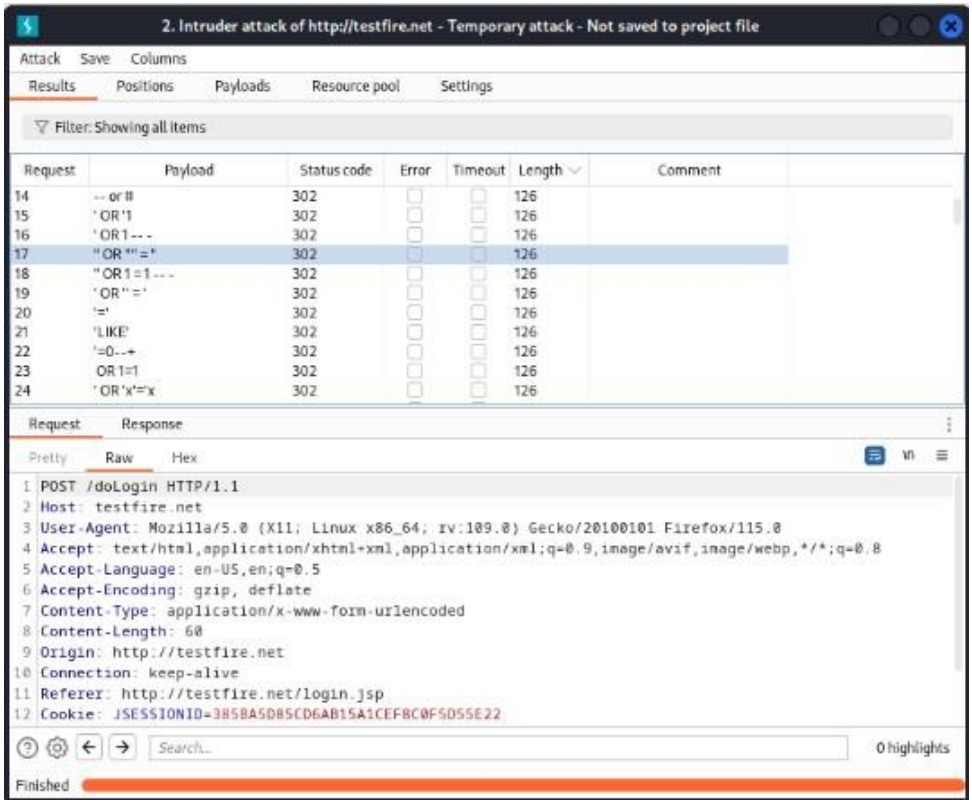
SQL injection attack is performed in the intruder tab. For this, the above code was used. The username is added as an element.



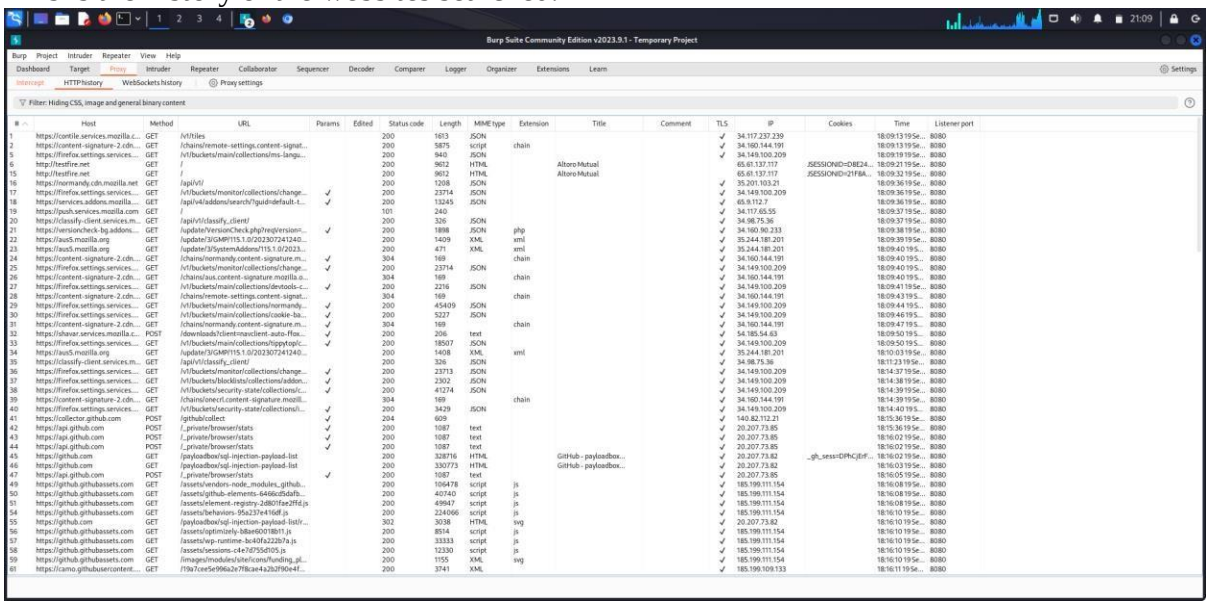
In the payloads section, paste the payload code which was copied from github. After this, click on start attack button.



We can see that the attack has been started.



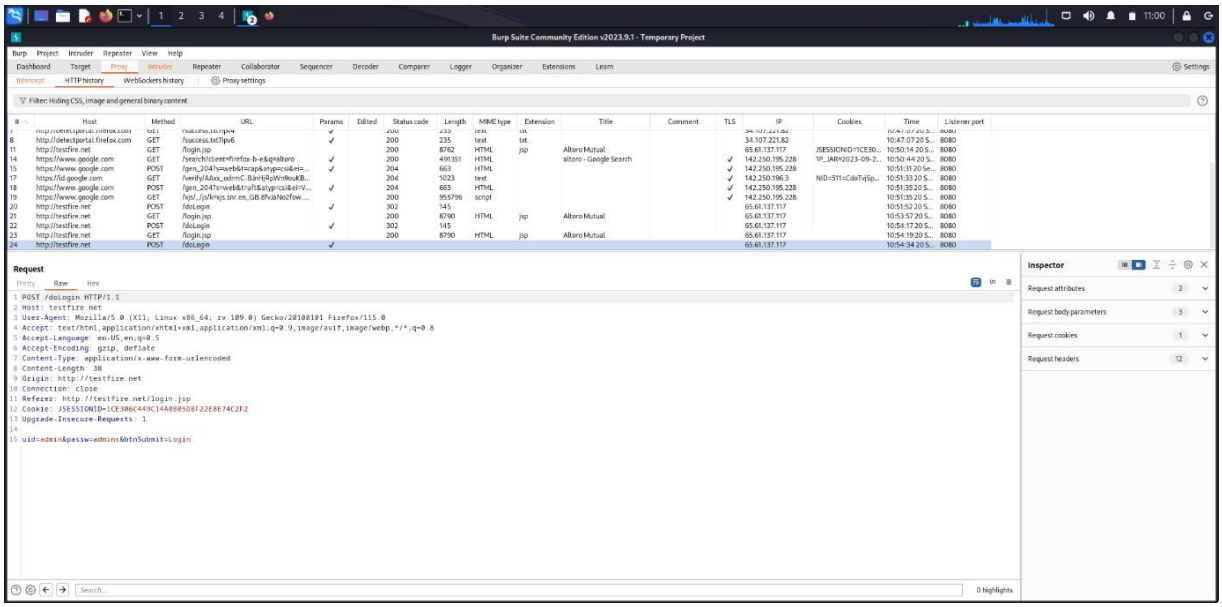
This is the history of the websites searched.



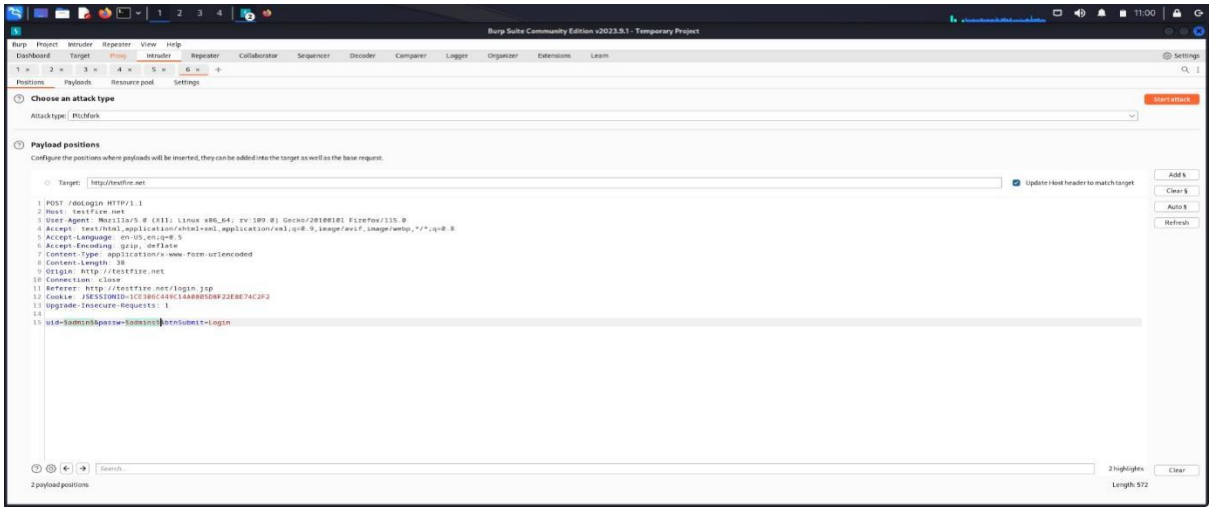
CREDENTIAL BYPASSING

Credential bypassing is an attack where the attacker does not have the credentials but enters the website by cracking the credentials.

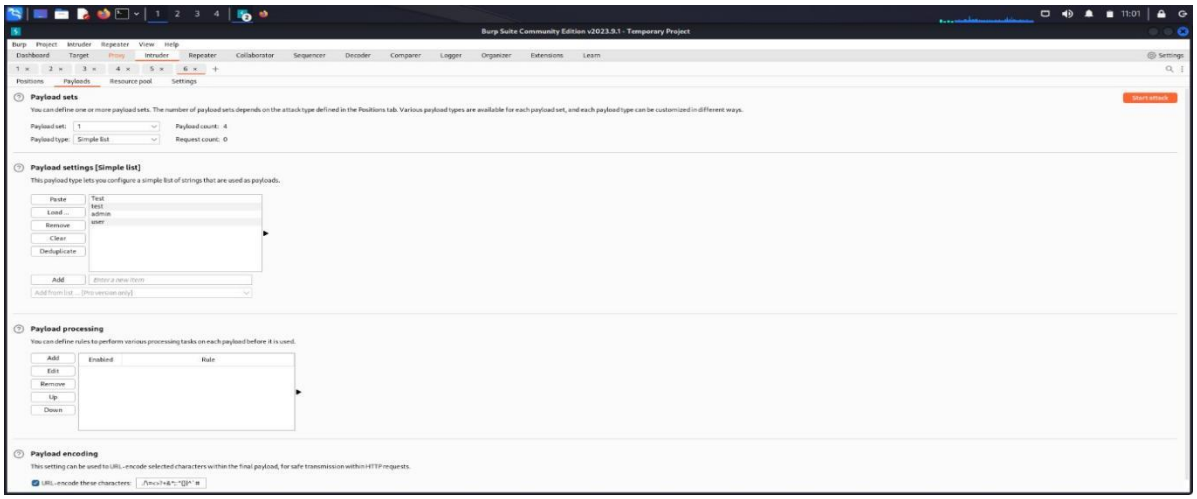
First of all, go to the desired website and turn on the intercept in burpsuite under proxy tab. Under HTTP history, we can see what all websites we have searched for. Right click on the code and send it to the intruder.



Under intruder tab, select the attack type as pitchfork. Then add the username and password as elements.



Insert the list of usernames and passwords and start the attack.



Among the 4 credentials entered, only one credential has the length of 264 which means it is the correct one.