AI for Cyber Security

Assignment – 4

Name: Harsh Pravin Gharlute
Email: harshpravin.gharlute2021@vitstudent.ac.in

What is a Burp Suite?

Burp Suite is a popular and powerful cybersecurity tool designed for web application security testing and vulnerability assessment. Developed by PortSwigger, it is widely used by security professionals, ethical hackers, and penetration testers to identify and mitigate security issues in web applications.

Burp Suite provides a comprehensive set of features and functionalities for assessing the security of web applications, including:

- **Proxy:** Burp Suite acts as a proxy server, allowing users to intercept and inspect the traffic between their web browser and a target web application. This feature is valuable for understanding how web applications work and for manually testing for vulnerabilities.
- **Scanner:** It includes an automated vulnerability scanner that can identify common security issues in web applications, such as SQL injection, cross-site scripting (XSS), and more. The scanner helps in quickly identifying potential vulnerabilities.
- **Spider:** Burp's web crawler can be used to map the structure of a web application by following links and discovering hidden or unlinked pages. This is essential for understanding the scope of a web application during testing.
- **Intruder:** The Intruder tool is used for automated attacks, such as brute force attacks, fuzzing, and payload manipulation, to find vulnerabilities in input fields and parameters.
- **Repeater:** This tool allows testers to manually modify and resend HTTP requests to the web application, making it easier to understand how different inputs affect the application's behavior.
- **Sequencer:** It analyzes the quality of randomness in tokens or session identifiers used

by the application, helping to identify potential security weaknesses.

- **Decoder:** Burp Suite can decode various data formats, such as URL encoding or base64 encoding, making it easier to analyze and manipulate data during testing.
- **Comparer:** This tool helps identify differences between two pieces of data, which can be useful for detecting changes in responses to input.
- **Extensions:** Burp Suite supports extensions and plugins that allow users to customize and extend its functionality to meet specific testing requirements.

Overall, Burp Suite is a versatile and comprehensive tool that aids security professionals in finding and addressing vulnerabilities in web applications. It is an essential tool in the toolkit of ethical hackers and security testers, helping organizations protect their web applications from potential threats.

Why Burp Suite?

Certainly, here are several reasons why Burp Suite is a popular choice for web application security testing, broken down into paragraph-sized points:

- **Comprehensive Toolset:** Burp Suite offers a wide range of tools and features that cater to various aspects of web application security testing. Its all-in-one platform includes functionalities for intercepting traffic, scanning for vulnerabilities, crawling websites, and more, making it a one-stop solution for security professionals.
- **User-Friendly Interface:** Burp Suite's user interface is intuitive and user-friendly, making it accessible to both novice and experienced testers. This ease of use is essential for efficiently conducting security assessments without a steep learning curve.
- **Active Development:** PortSwigger, the company behind Burp Suite, continuously updates and enhances the tool. This ensures that it remains effective in identifying emerging vulnerabilities and security challenges, keeping security professionals ahead of the curve.
- **Large User Community:** Burp Suite has a substantial and active user community. This means there is a wealth of online documentation, tutorials, forums, and

community support available, making it easier for users to find solutions to their queries and share knowledge.

- **Customization:** One of Burp Suite's strengths is its extensibility. It supports a wide range of extensions and plugins, allowing users to customize and extend its functionality according to their specific testing needs. This flexibility is invaluable when dealing with unique or specialized web applications.

In summary, Burp Suite stands out as a versatile, user-friendly, and continually evolving toolset for web application security testing. Its comprehensive features, combined with an active user community and extensibility, make it a preferred choice for security professionals seeking to assess and enhance the security of web applications.

What are the features of Burp Suite?

Burp Suite is a comprehensive web application security testing tool that offers a wide range of features and functionalities to help security professionals assess and improve the security of web applications. Here are some of its key features:

- **Proxy:** Burp Suite acts as an intercepting proxy server, allowing you to capture, inspect, and manipulate HTTP requests and responses between your web browser and the target web application. This is essential for understanding how the application works and for manual testing.
- **Scanner:** The automated vulnerability scanner in Burp Suite can identify common web application vulnerabilities, such as SQL injection, cross-site scripting (XSS), CSRF, and more. It helps in quickly identifying potential security issues.
- **Spider:** Burp's web crawler can be used to map the structure of a web application by following links and discovering hidden or unlinked pages. This is crucial for comprehensively testing the application and understanding its scope.
- **Intruder:** The Intruder tool is used for automated attacks, such as brute force attacks, fuzzing, and payload manipulation, to find vulnerabilities in input fields and parameters.

- **Repeater:** This tool allows testers to manually modify and replay HTTP requests to the web application, making it easier to understand how different inputs affect the application's behavior and for fine-tuning tests.
- **Sequencer:** Burp Suite's Sequencer analyzes the quality of randomness in tokens or session identifiers used by the application. This helps identify potential security weaknesses related to randomness and session management.
- **Decoder:** Burp can decode various data formats, such as URL encoding, base64 encoding, and more. This is useful for analyzing and manipulating data during testing.
- **Comparer:** The Comparer tool helps identify differences between two pieces of data, which can be useful for detecting changes in responses to input.
- **Extensions:** Burp Suite supports extensions and plugins, which allow users to customize and extend its functionality. This extensibility is essential for adapting the tool to specific testing requirements.
- **Collaborator:** Burp Collaborator helps identify interactions made by the target application with external entities. This is particularly useful for detecting blind vulnerabilities where the application does not directly reveal the result of an attack.
- **Session Handling:** Burp Suite offers session management features, enabling testers to maintain and manipulate user sessions during testing, which is important for testing authenticated areas of an application.
- **Reporting:** It provides robust reporting capabilities to document and communicate identified vulnerabilities and testing results effectively.

These features, combined with a user-friendly interface and extensive documentation, make Burp Suite a powerful and widely-used tool for web application security testing and vulnerability assessment. It's an essential tool for security professionals looking to identify and remediate security issues in web applications.

Test the vulnerabilities of http://testfire.net:

Introduction:

This report outlines the discovery and responsible disclosure of a SQL injection vulnerability identified on testfire.net using a burp suite.

Background:

Testfire.net is a simulated web application created by a cybersecurity company to provide a safe environment for users to practice and learn about ethical hacking and security testing. It is not a real website but rather a controlled platform designed for educational and training purposes in the field of cybersecurity.

Vulnerability Description:

The SQL injection vulnerability allows an attacker to execute arbitrary SQL queries through the search functionality.

This vulnerability affects the website's database, potentially compromising user data and system integrity

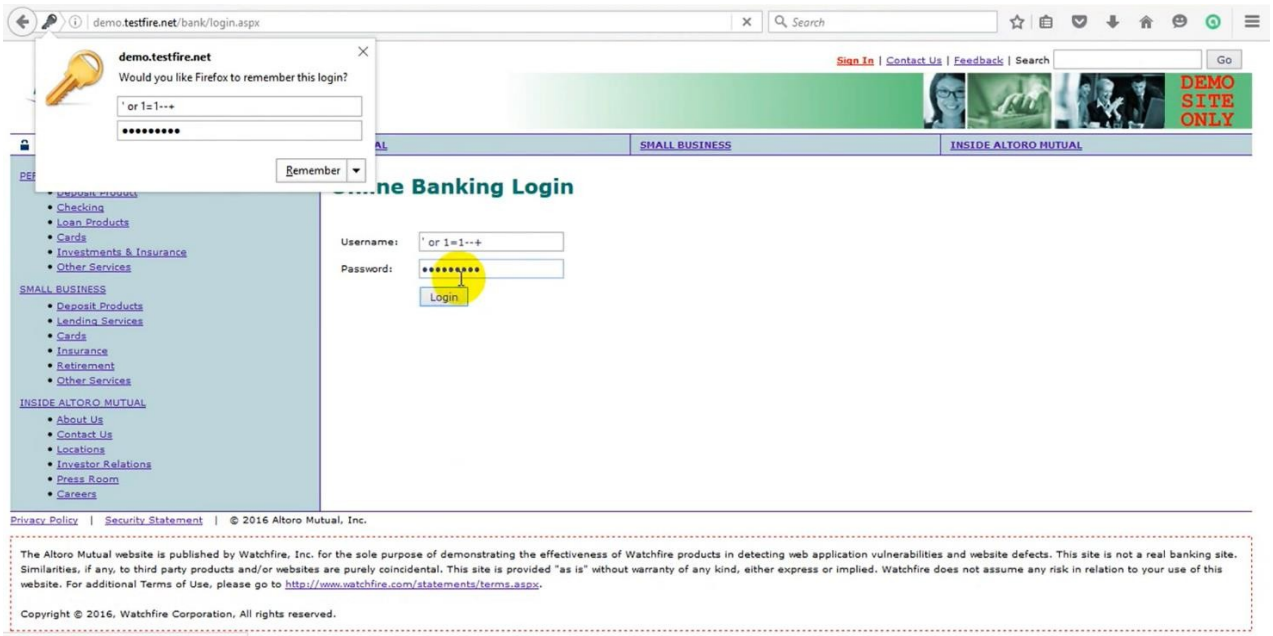
Discovery and steps:

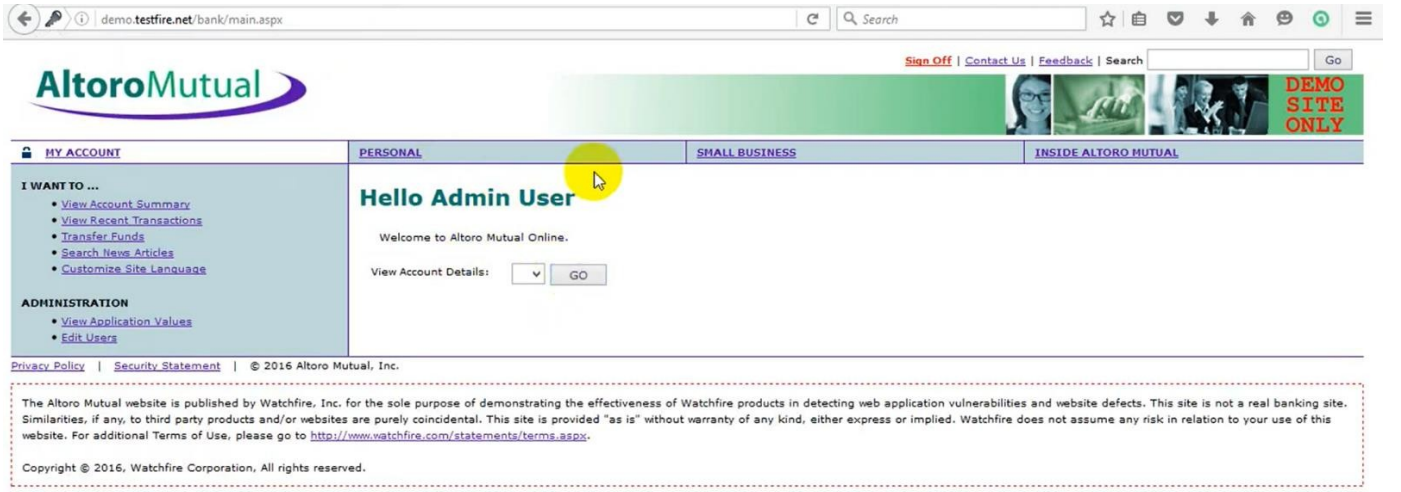
Access the TestWebsite.com search bar.

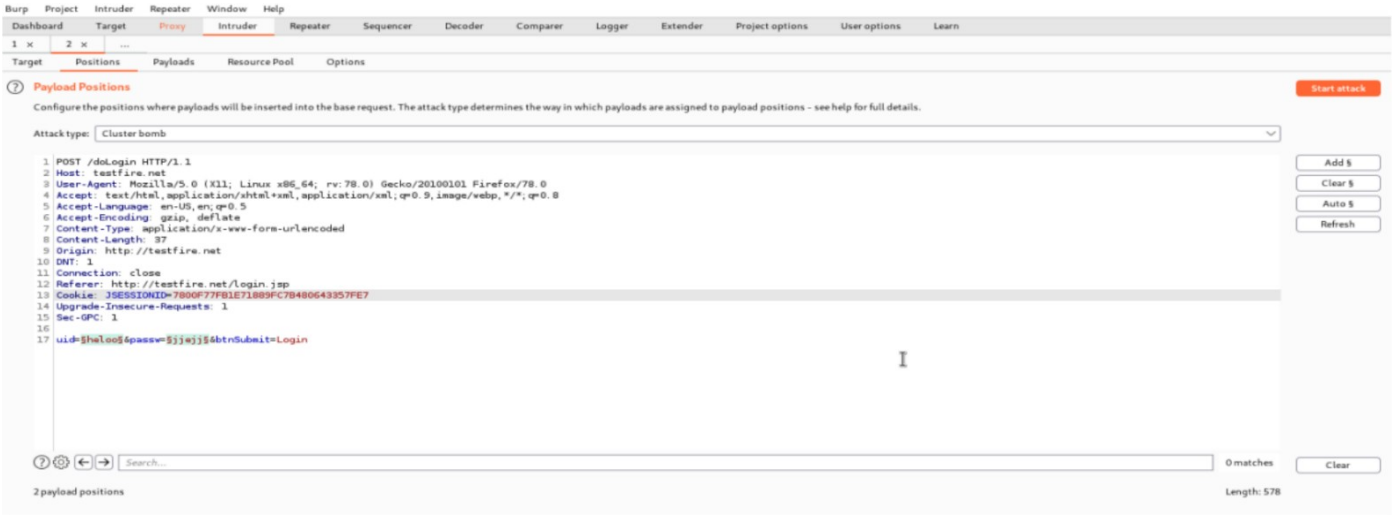
Input the following payload: ' OR '1'='1.

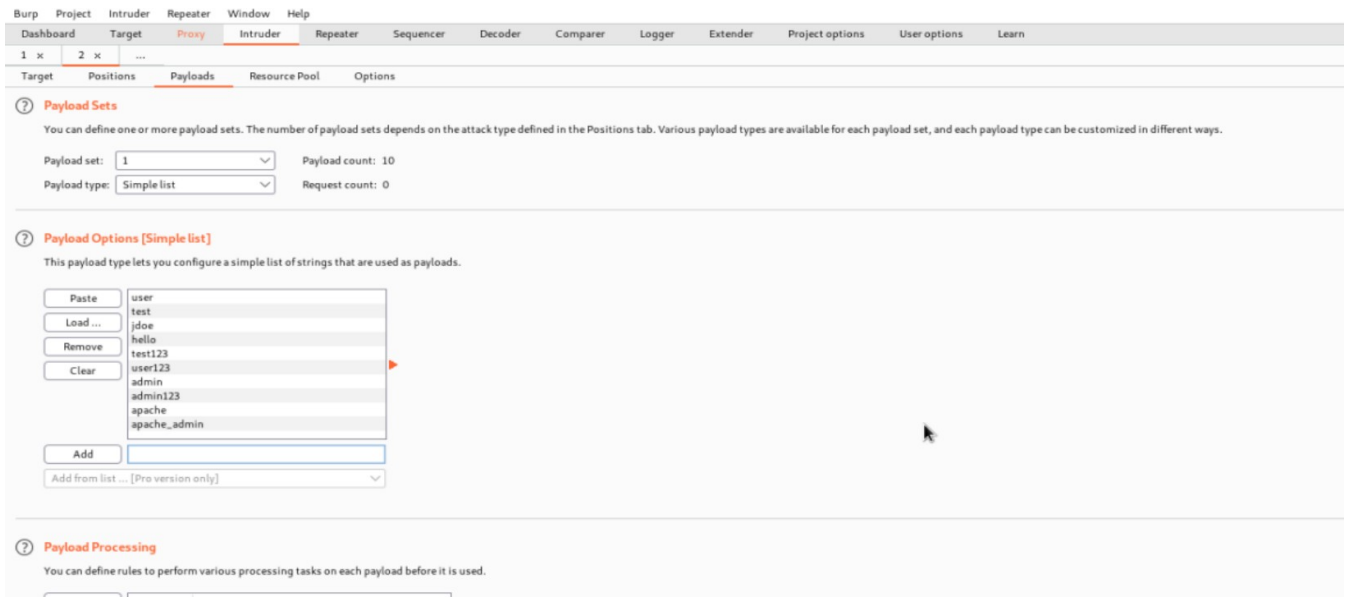
Observe that the search results do not change, indicating a potential SQL injection vulnerability.

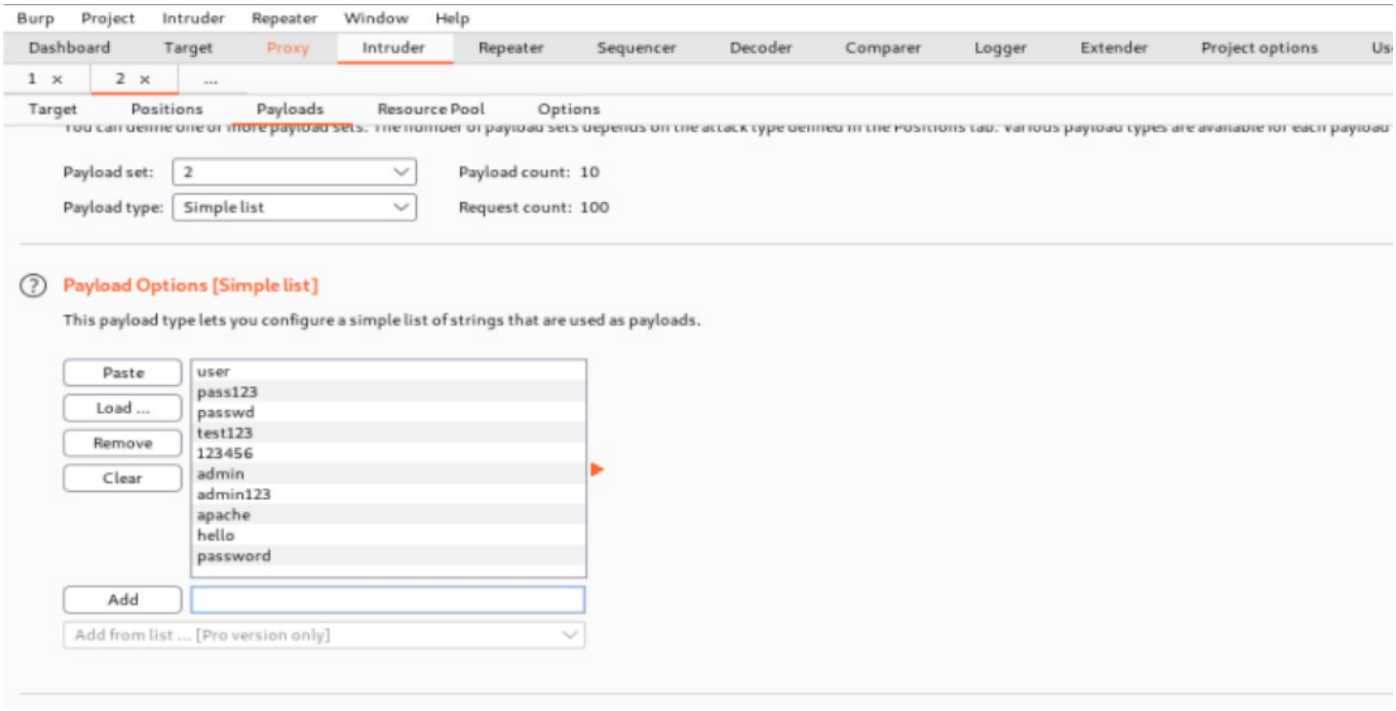
Evidence:

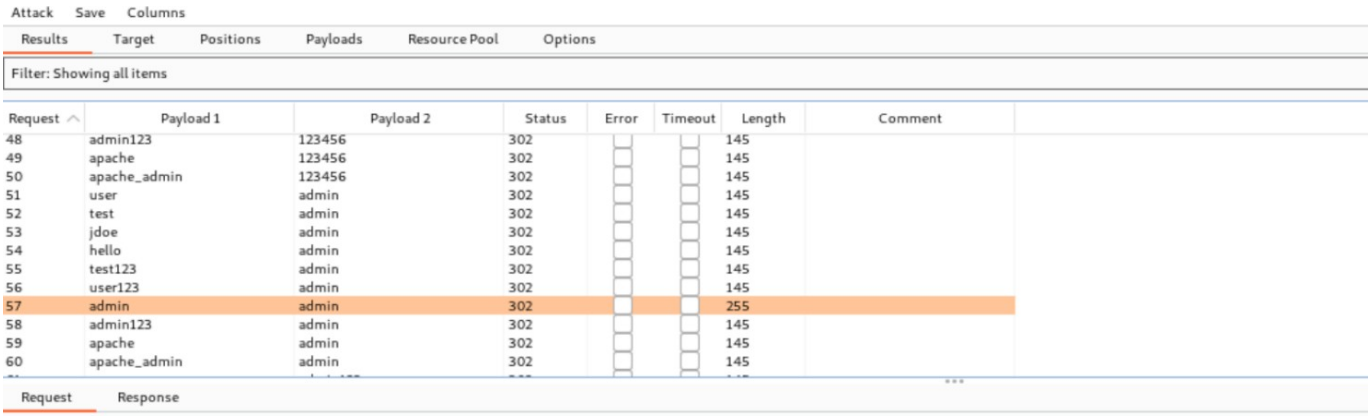



demo.testfire.net/bank/main.aspx
Search
Sign Off | Contact Us | Feedback | Search
Go
AltoroMutual
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
ADMINISTRATION
View Application Values
Edit Users
Hello Admin User
Welcome to Altoro Mutual Online.
View Account Details:
GO
Privacy Policy | Security Statement | © 2016 Altoro Mutual, Inc.
The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to http://www.watchfire.com/statements/terms.aspx.
Copyright © 2016, Watchfire Corporation, All rights reserved.


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Target Positions Payloads Resource Pool Options
Payload Positions
Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.
Attack type: Cluster bomb
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 37
Origin: http://testfire.net
DNT: 1
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=7800F77FB1E71809FC78480643357FE7
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
uid=$heloo$&passw=$jjejj$&btnSubmit=Login
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear
2 payload positions
Length: 578


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Target Positions Payloads Resource Pool Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 10
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
user
test
jdoe
hello
test123
user123
admin
admin123
apache
apache_admin
Add
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.





Potential Mitigations

To mitigate this vulnerability, input validation and sanitization should be implemented in the search functionality.

Prepared statements or parameterized queries should be used to prevent SQL injection attacks

Impact and Risks

If left unaddressed, this vulnerability could allow attackers to access, modify, or delete sensitive data from the database.

It poses a significant risk to user privacy and data integrity