Name: Shivani Narayan L

Regno: 21BLC1119

Week 4 Burp Suite

Burp Suite is a popular cybersecurity tool developed by PortSwigger. It's used by cybersecurity professionals and ethical hackers to test the security of web applications. The tool helps identify and exploit security vulnerabilities, making web applications more secure. Its features include intercepting and modifying HTTP requests, automated vulnerability scanning, web crawling, and session management. The user-friendly interface and powerful capabilities make it a go-to tool for web application security testing.

Burp Suite is favored for its robust features, user-friendly interface, efficient vulnerability detection, customization options, powerful proxy capabilities, active community support, effective exploitation abilities, and comprehensive reporting, making it a top choice for web application security testing.

It provides a wide range of features to help identify, analyze, and mitigate security vulnerabilities in web applications. Here's a detailed overview of its key features:

1. **Proxy:** The Proxy feature acts as an intercepting proxy between your browser and the target web application. It allows you to intercept, view, and modify HTTP/S requests and responses. This interception capability is crucial for understanding application behavior, identifying potential security vulnerabilities, and making necessary modifications for testing purposes. Essentially, it serves as a bridge, giving you control over the communication between your browser and the web application, enabling a deeper understanding and analysis of the traffic.

2. **Scanner:** The Scanner is an automated tool that tests web applications for vulnerabilities. It sends various requests and payloads to the application, analyzing responses to identify security flaws like SQL injection or cross-site scripting. It's a time-saving way to detect vulnerabilities, providing detailed reports for efficient analysis and remediation.

3. **Spider:** The Spider is a web application crawler that automatically navigates through the target application, exploring its structure and endpoints. It follows links and maps out the application's pages and content, helping testers identify the application's attack surface. This tool is essential for comprehending the layout of the application, which is vital for effective security testing and vulnerability analysis.

4. **Repeater:** Repeater is a tool that allows security professionals to manually send and modify HTTP requests to a web application. It's like a "request playground" where you can tweak and replay requests, observe responses, and analyze how the application behaves. Repeater is invaluable for fine-tuning payloads, testing different scenarios, and deeply understanding how the application handles various inputs, aiding in vulnerability testing and exploitation.

5. **Intruder:** Intruder is a robust automated testing tool in web application security. It allows users to systematically test web applications by automating the process of injecting and testing various payloads into specific positions within the HTTP requests. Payloads, which can range from simple lists to complex custom sets of data, are inserted into defined payload positions like headers, URLs,

or request bodies. Intruder offers different attack types, such as Sniper, Battering Ram, Pitchfork, and Cluster Bomb, each tailored for specific testing scenarios. Users can define payload processing rules to modify payloads before sending and handle responses effectively. The tool provides comprehensive results, including HTTP response codes, response lengths, and identified matches, aiding in vulnerability analysis. Intruder's automation enhances efficiency and accuracy, making it an essential component for security professionals conducting thorough web application assessments.

6. **Decoder:** The Decoder is a tool that helps analyze and modify data by encoding or decoding it using various encoding schemes. It's invaluable for understanding how the application processes input. You can input data and choose encoding or decoding schemes like base64, URL encoding, HTML entities, etc. Decoder assists in transforming the data, allowing testers to manipulate and observe how the application handles different encoded or decoded inputs. Essentially, it's a tool to unveil the hidden aspects of how the application deals with various types of data, aiding in vulnerability identification and understanding the application's behavior.

7. **Comparer:** The Comparer tool allows users to compare two requests or responses quickly. It helps in identifying differences between them, aiding in pinpointing potential vulnerabilities or discrepancies. Comparer is invaluable when assessing the impact of specific changes or modifications made during testing. It highlights variations in content, headers, or other crucial elements, making it easier to detect anomalies. Essentially, Comparer is a tool for side-by-side comparison, streamlining the process of identifying divergences in requests or responses and assisting in pinpointing critical areas for further investigation or validation.

8. **Extension:** Extensions are additional components that enhance the tool's functionality. They are custom-built or third-party modules that extend the capabilities of Burp Suite beyond its default features. These extensions can add new tools, modify existing functionalities, integrate with external systems, or automate specific tasks. Extensions allow users to tailor Burp Suite to their specific needs, making it a versatile and adaptable tool for web application security testing and analysis. Essentially, extensions empower users to customize and extend Burp Suite based on their requirements, enhancing its effectiveness and efficiency in identifying vulnerabilities and securing web applications.

9. **Collaborator Client:** the Collaborator Client is a tool that helps testers identify potential out-of-band vulnerabilities. It interacts with Burp Collaborator, a server provided by PortSwigger. The Collaborator Client assists in generating and managing interactions with this server during security testing. It allows testers to observe and analyze the interactions between the target application and the Collaborator server, aiding in the detection of vulnerabilities like blind SSRF (Server-Side Request Forgery) or blind XXE (XML External Entity). Essentially, the Collaborator Client is a vital component for detecting vulnerabilities that might not directly return responses but can be inferred through specific interactions with an external server.

10. **Target Analyzer:** Target Analyzer is a tool that automatically analyzes the scope and structure of the target web application. It helps security professionals identify potential points of interest, such as URLs, parameters, and directories, within the application. The tool gathers information about the application's layout, aiding in efficient testing and vulnerability assessment. Target Analyzer is especially useful for comprehending the application's attack surface and focusing testing efforts

effectively. Essentially, it automates the initial analysis of the target application, providing valuable insights that assist in planning and conducting comprehensive security testing.

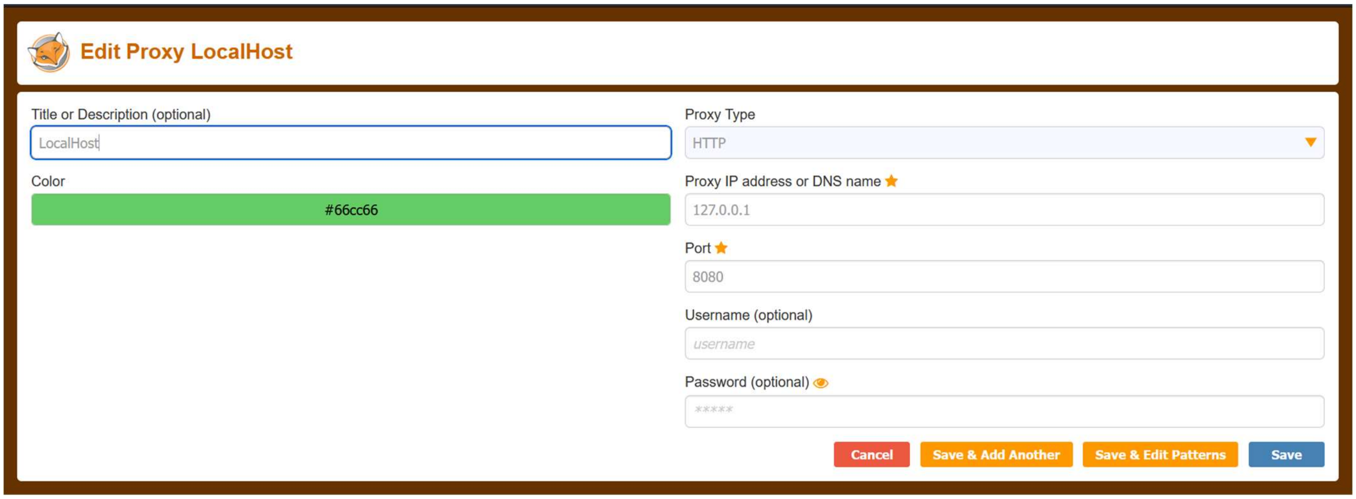
11. **Content Discovery:** Content Discovery is a feature that helps identify hidden or lesser-known parts of a web application. It systematically crawls through the application, mapping out its structure and uncovering endpoints or directories that may not be directly linked from the main pages. This tool is valuable for security professionals to discover potentially overlooked areas of the application, which could pose security risks. Essentially, Content Discovery provides a way to thoroughly explore the application, aiding in identifying security weaknesses that might otherwise remain unnoticed.

12. **Content Sniffer:** Content Sniffer is a tool that allows users to analyse and identify various file types based on their content. It helps in recognizing potential security risks within files by examining their content. Content Sniffer is valuable for security professionals to quickly ascertain the nature of files encountered during web application testing. In essence, it aids in categorizing and understanding the content of files, providing insights into potential security threats that may be present in the application.

13. **Session Management:** Session Management involves tools and features that assist in managing user sessions, cookies, and authentication mechanisms during web application testing. It allows security professionals to manipulate and analyze these aspects effectively. This is crucial for testing authenticated areas of a web application, understanding how session-related information is handled, and identifying potential vulnerabilities related to session handling. Session Management tools in Burp Suite provide functionalities to view, modify, and analyze session tokens and cookies, facilitating a comprehensive examination of the application's authentication and session handling mechanisms. In summary, it's a set of tools and capabilities that aid in testing and analyzing user sessions within a web application.

SQL injection using Burp Suite:

1. Configuring the browser to use Burp Suite as a proxy using FoxyProxy extension:



Edit Proxy LocalHost

Title or Description (optional): LocalHost

Color: #66cc66

Proxy Type: HTTP

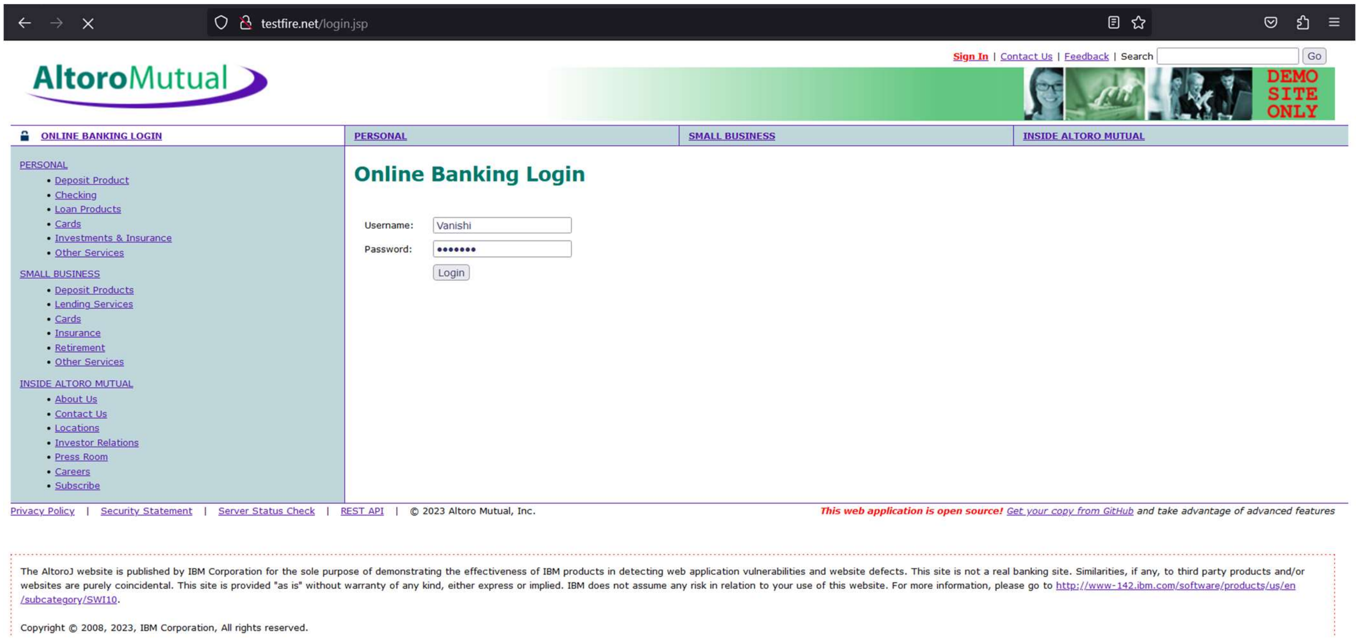
Proxy IP address or DNS name: 127.0.0.1

Port: 8080

Username (optional): username

Password (optional): *****

2. Open the target website (testfire.net signup page) in the browser.



Online Banking Login

Username: Vanishi

Password: •••••••

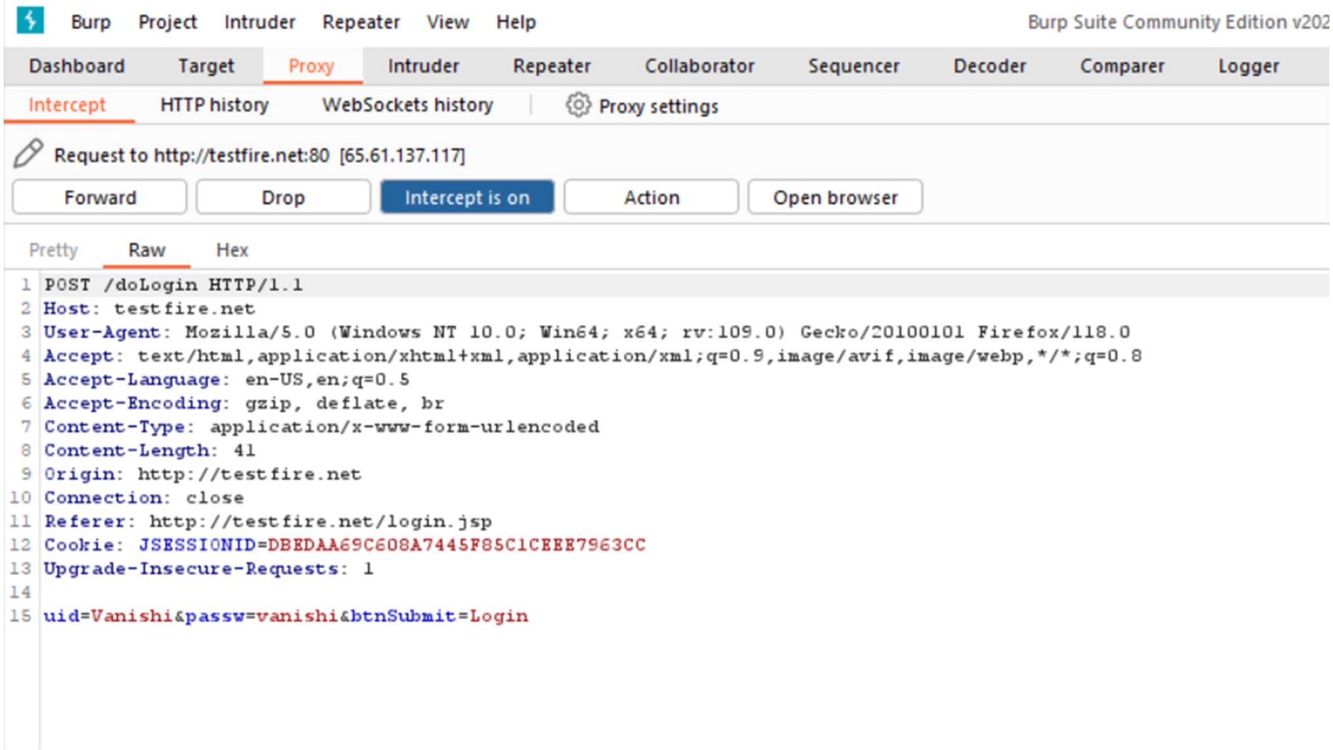
© 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM 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. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

3. Intercept the request using Burp Suite's Proxy.

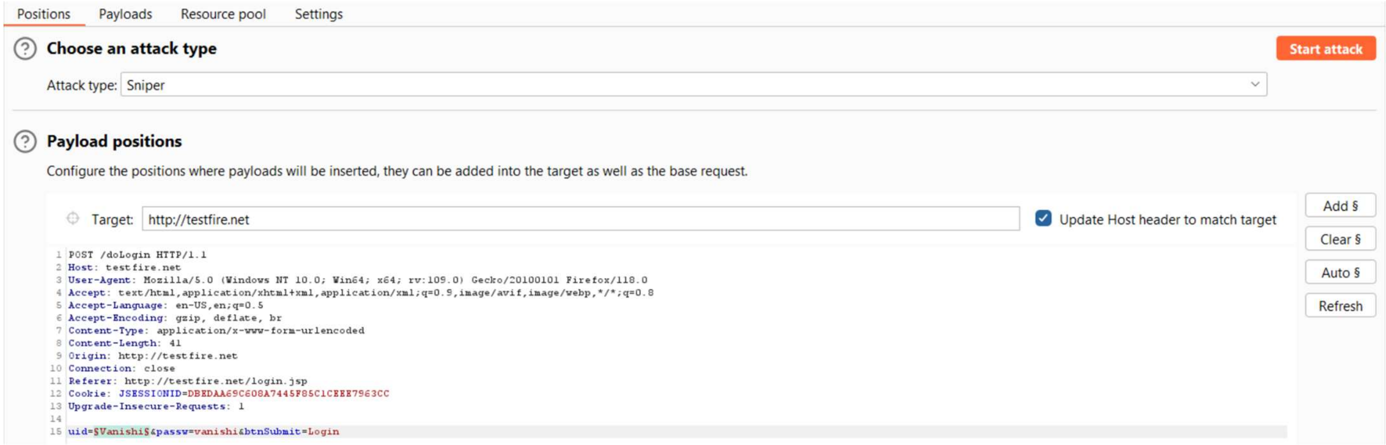


Request to http://testfire.net:80 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=DBEDAA69C608A7445F85C1CEEE7963CC
Upgrade-Insecure-Requests: 1

uid=Vanishi&passw=vanishi&btnSubmit=Login
```

4. Send the intercepted request to the Intruder
5. In the Intruder tab, in the Positions tab and Add § to the uid



Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

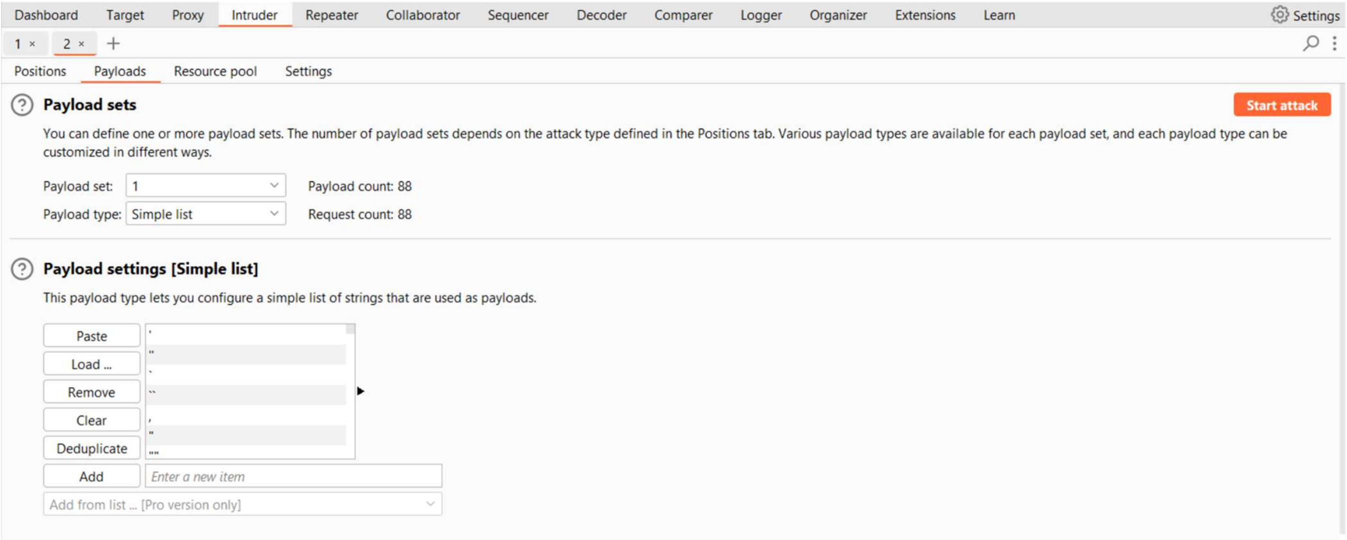
Target: http://testfire.net

☑ Update Host header to match target

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=DBEDAA69C608A7445F85C1CEEE7963CC
Upgrade-Insecure-Requests: 1

uid=§Vanishi§&passw=vanishi&btnSubmit=Login
```

6. Go to the Payloads tab and select the Sniper attack type and paste the generic SQL injection Payloads from GitHub and paste in Payload Settings



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: 88

Payload type: Simple list

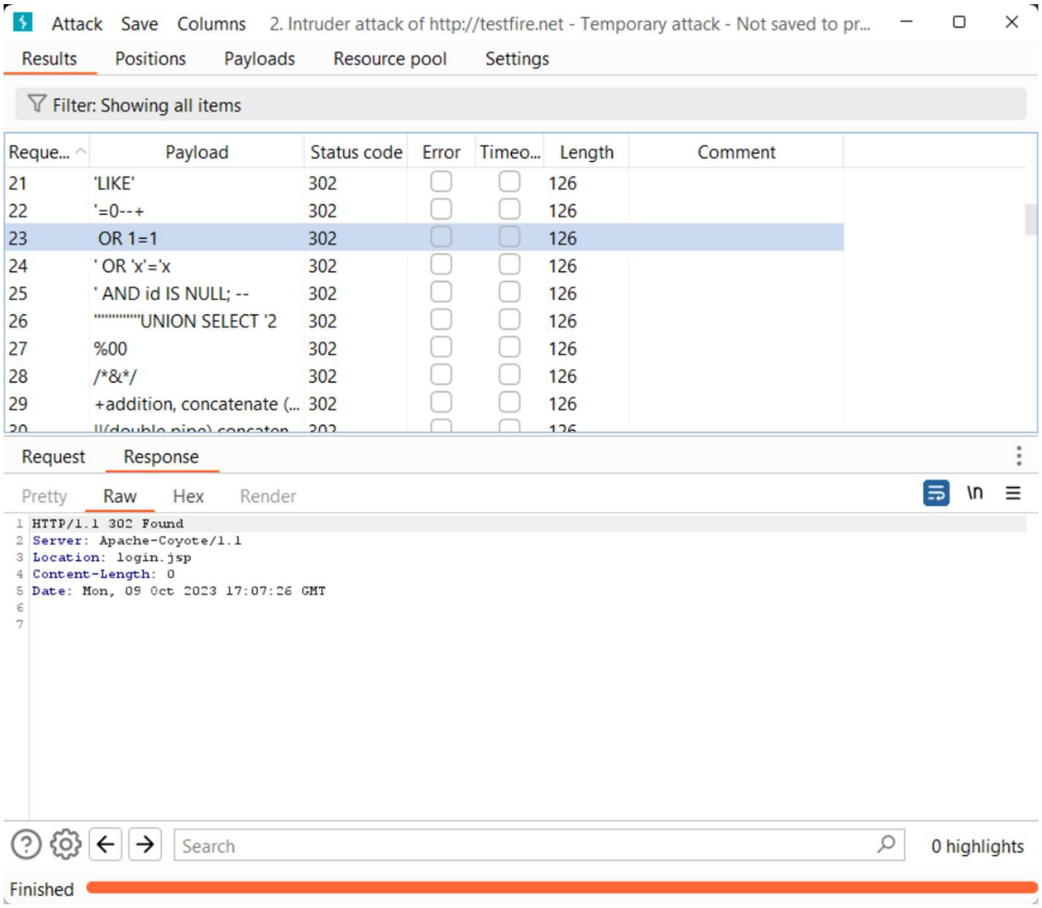
Request count: 88

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
'
"
`
``
,
"
""
```

7. Click on start Attack:

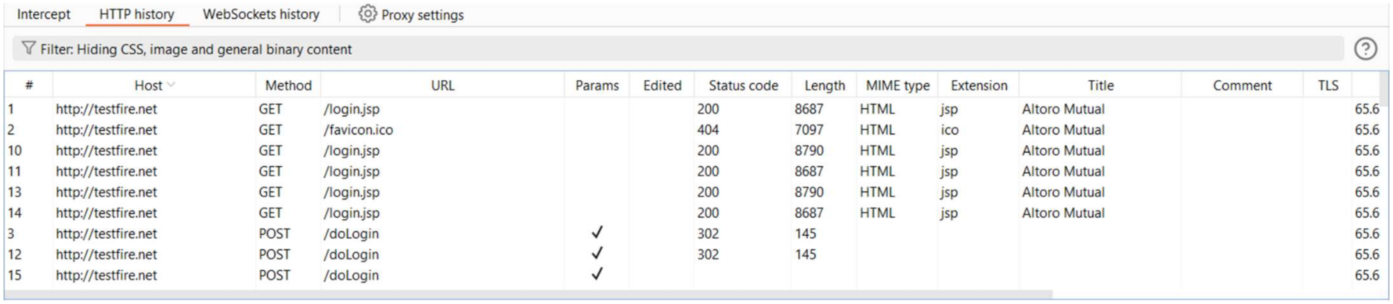

Attack
Save
Columns
2. Intruder attack of http://testfire.net - Temporary attack - Not saved to pr...
Results
Positions
Payloads
Resource pool
Settings
Filter: Showing all items

Reque...	Payload	Status code	Error	Timeo...	Length	Comment
21	'LIKE'	302	□	□	126	
22	'=0--+	302	□	□	126	
23	OR 1=1	302	□	□	126	
24	' OR 'x'='x	302	□	□	126	
25	' AND id IS NULL; --	302	□	□	126	
26	'''''''''''''''UNION SELECT '2	302	□	□	126	
27	%00	302	□	□	126	
28	/*&*/	302	□	□	126	
29	+addition, concatenate (...	302	□	□	126	
30	||(double pipe) concaten...	302	□	□	126	

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Mon, 09 Oct 2023 17:07:26 GMT


```

8. To view the HTTP requests sent and their corresponding response check the HTTP history



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	
1	http://testfire.net	GET	/login.jsp			200	8687	HTML	jsp	Altoro Mutual			65.6
2	http://testfire.net	GET	/favicon.ico			404	7097	HTML	ico	Altoro Mutual			65.6
10	http://testfire.net	GET	/login.jsp			200	8790	HTML	jsp	Altoro Mutual			65.6
11	http://testfire.net	GET	/login.jsp			200	8687	HTML	jsp	Altoro Mutual			65.6
13	http://testfire.net	GET	/login.jsp			200	8790	HTML	jsp	Altoro Mutual			65.6
14	http://testfire.net	GET	/login.jsp			200	8687	HTML	jsp	Altoro Mutual			65.6
3	http://testfire.net	POST	/doLogin	✓		302	145						65.6
12	http://testfire.net	POST	/doLogin	✓		302	145						65.6
15	http://testfire.net	POST	/doLogin	✓									65.6

Instead of using the Sniper Attack, Battering Ram Attack, Pitchfork Attack or Cluster Bomb Attack could be used for obtaining more comprehensive results.