Rohit Patiballa
21BCI0278

ASSIGNMENT - 4

What is burp suite?

Burp Suite is a web application security testing tool that can be used to find and exploit security holes in web applications. It is a comprehensive set of tools that can be used to perform security testing of all web applications, from initial mapping and analysis to vulnerability discovery and exploitation.

Why burp suite?

- Comprehensiveness: Burp Suite provides a comprehensive set of tools for all aspects of WAST, including manual testing, automated scanning, and intrusion detection. This makes it a one-stop shop for security professionals looking to test the security of their web applications.
- Flexibility: Burp Suite is a very flexible tool that can be used to test a wide variety of web applications, regardless of the technology stack being used. It also supports a wide range of customization options, allowing users to tailor it to their specific needs.
- Ease of use: Burp Suite is relatively easy to use, even for beginners. It has a user-friendly interface and provides extensive documentation and tutorials.
- Community support: Burp Suite has a large and active community of users who are always willing to help each other out. This makes it a great resource for learning about the tool and getting help with specific problems.

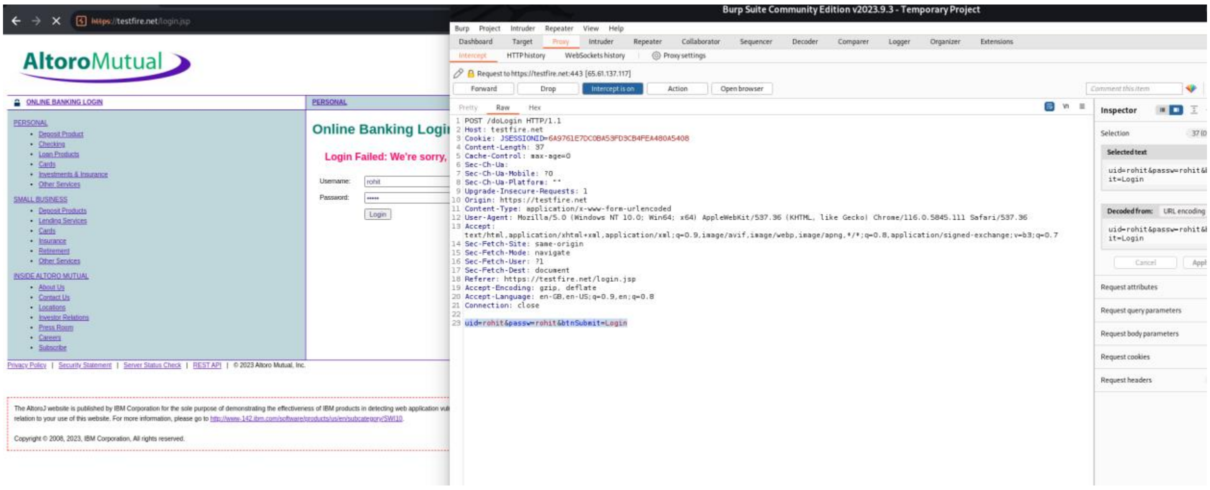
What are the features of burp suite?

- Capture intermediary: You can inspect, modify, and intercept HTTP traffic between your browser and the intended web application using the interception proxy. This can be utilized to physically test for weaknesses, or to mechanize tests utilizing other Burp Suite instruments.
- Scanner: The scanner is a strong computerized weakness scanner that can check web applications for a large number of weaknesses. The scanner can be utilized to check individual pages or whole sites, and meeting your particular needs can be tweaked.
- Intruder: The gatecrasher instrument can be utilized to robotize assaults against web applications. This can be utilized to test for weaknesses, for example, savage power assaults and SQL infusion.
- Repeater: The repeater instrument can be utilized to rehash HTTP demands. This can be utilized to test the way of behaving of a web application under various circumstances, or to take advantage of weaknesses.
- Sequencer: The sequence of HTTP requests required to carry out a particular action on a web application can be analyzed using the sequencer tool. This can be utilized to recognize weaknesses, for example, cross-site prearranging and shaky direct item references.
- Decoder: Data can be encoded and decoded in a variety of formats with the decoder tool. This can be valuable for testing for weaknesses, for example, SQL infusion and cross-site prearranging.
- BApp add-ons: Burp Suite upholds custom augmentations, known as BApps. Adding new scanning features or integrating with other security tools are two examples of how BApps can be used to enhance Burp Suite's capabilities.

Rohit Patiballa
21BCI0278

Test the vulnerabilities of testfire.net

http://testfire.net


https://testfire.net/login.jsp
AltoroMutual
ONLINE BANKING LOGIN
PERSONAL
Deposit Product
Checking
Loan Products
Cards
Investments & Insurance
Other Services
SMALL BUSINESS
Deposit Products
Lending Services
Cards
Insurance
Retirement
Other Services
INSIDE ALTORO MUTUAL
About Us
Contact Us
Locations
Investor Relations
Press Room
Careers
Subscribe
Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.
Burp Suite Community Edition v2023.9.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
Intercept HTTP history WebSockets history Proxy settings
Forward
Drop
Intercept is on
Action
Open browser
Pretty Raw Hex
Inspector

Online Banking Login

Login Failed: We're sorry,

Username: rohit
Password: •••••
Login

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vul relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

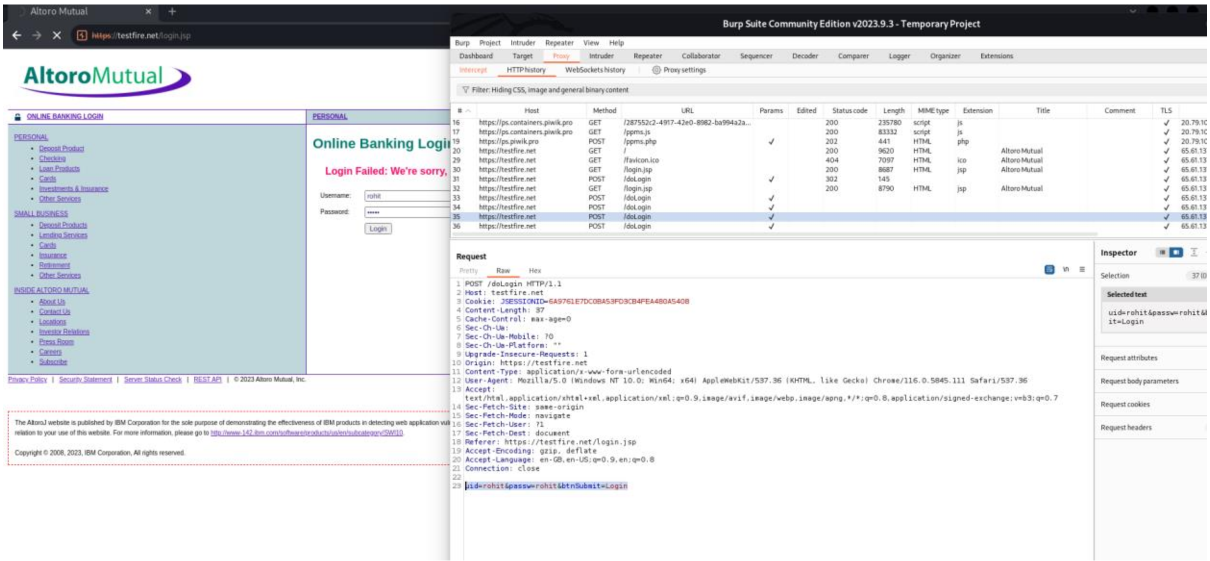
Copyright © 2008, 2023, IBM Corporation, All rights reserved.

Request to https://testfire.net:443 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: testfire.net
Cookie: JSESSIONID=6A9761E7DC0BA53FD3CB4FEA480A5408
Content-Length: 37
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
Origin: https://testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

uid=rohit&passw=rohit&btnSubmit=Login
```

Selection 37
Selected text
uid=rohit&passw=rohit&btnSubmit=Login
Decoded from: URL encoding
uid=rohit&passw=rohit&btnSubmit=Login


Altoro Mutual
https://testfire.net/login.jsp
AltoroMutual
Burp Suite Community Edition v2023.9.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
Intercept HTTP history WebSockets history Proxy settings
Request
Pretty Raw Hex
Inspector

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	
16	https://ps.containers.piwik.pro	GET	/287552c2-4917-42e0-8982-ba994a2a...			200	235780	script	js			✓	20.79.1C
17	https://ps.containers.piwik.pro	GET	/ppms.js			200	83332	script	js			✓	20.79.1C
19	https://ps.piwik.pro	POST	/ppms.php	✓		202	441	HTML	php			✓	20.79.1C
20	https://testfire.net	GET	/			200	9620	HTML		Altoro Mutual		✓	65.61.13
29	https://testfire.net	GET	/favicon.ico			404	7097	HTML	ico	Altoro Mutual		✓	65.61.13
30	https://testfire.net	GET	/login.jsp			200	8687	HTML	jsp	Altoro Mutual		✓	65.61.13
31	https://testfire.net	POST	/doLogin	✓		302	145					✓	65.61.13
32	https://testfire.net	GET	/login.jsp			200	8790	HTML	jsp	Altoro Mutual		✓	65.61.13
33	https://testfire.net	POST	/doLogin	✓								✓	65.61.13
34	https://testfire.net	POST	/doLogin	✓								✓	65.61.13
35	https://testfire.net	POST	/doLogin	✓								✓	65.61.13
36	https://testfire.net	POST	/doLogin	✓								✓	65.61.13

```
POST /doLogin HTTP/1.1
Host: testfire.net
Cookie: JSESSIONID=6A9761E7DC0BA53FD3CB4FEA480A5408
Content-Length: 37
Cache-Control: max-age=0
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
Origin: https://testfire.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://testfire.net/login.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Connection: close

uid=rohit&passw=rohit&btnSubmit=Login
```

The given website is vulnerable for it’s http protocol as passwords can be extracted via burpsuite.