Name : SAIRAM B
Reg no: 21BLC1468

ASSIGNMENT - 4

Burp Suite :-

A popular web vulnerability scanner and security testing tool used by cybersecurity professionals and ethical hackers to assess the security of web applications. It's developed by PortSwigger and provides a wide range of features for web application security testing, assessment, and penetration testing.

Why Burp Suite:-

- Burp Suite is widely used in the field of web application security because of its robust set of features and userfriendly interface.
- It allows security professionals to identify, analyze, and exploit security vulnerabilities in web applications, helping organizations improve their security posture.
- Burp Suite is highly customizable and extensible, making it suitable for various types of web application testing scenarios.
- It provides detailed reports and logs that help security teams understand and address vulnerabilities effectively.

Key Features of Burp Suite:-

Proxy: Burp Suite acts as an intercepting proxy, allowing you to inspect and modify HTTP requests and responses between your browser and the web application. This is useful for understanding how the application behaves and identifying potential vulnerabilities.

Scanner: Burp Scanner is an automated vulnerability scanner that identifies common security issues, such as SQL injection, cross-site scripting (XSS), and more. It helps in identifying vulnerabilities quickly.

Spider: The Spider tool crawls through a web application to map out its structure and discover hidden or unlinked pages, potentially uncovering additional attack surfaces.

Repeater: Repeater allows you to repeat and modify specific requests to the web application, making it useful for testing and exploiting vulnerabilities.

Intruder: The Intruder tool is used for performing automated attacks on web applications. It can help with tasks like password guessing, parameter fuzzing, and more.

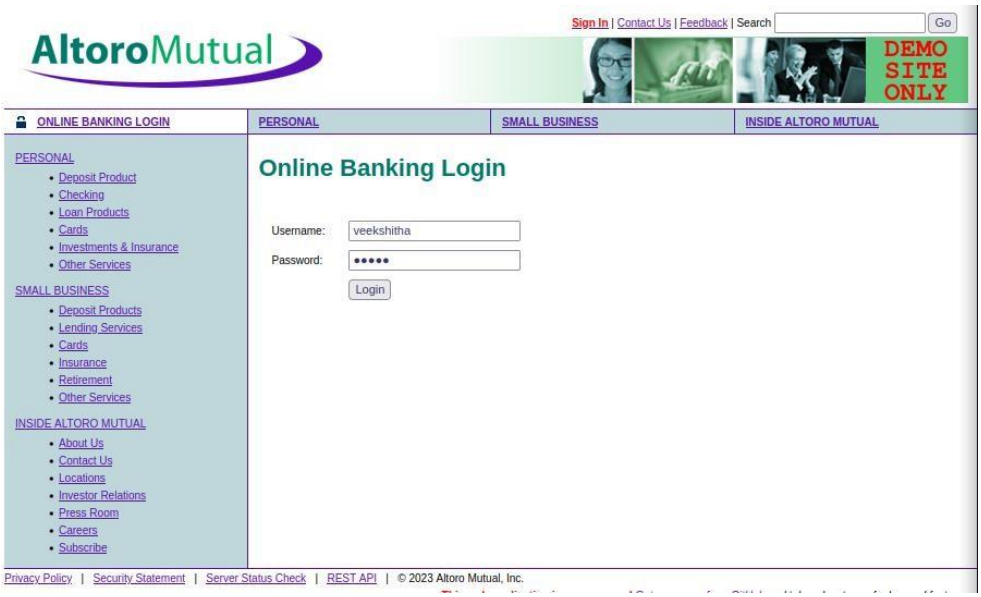
Decoder: Decoder assists in decoding and encoding data using various encoding schemes, which is valuable for understanding how input data is processed by the application.

Comparer: This tool helps you compare two requests or responses, making it easier to spot differences and potential vulnerabilities.

Extensions: Burp Suite supports extensions and has an active community that develops add-ons to enhance its functionality. You can create custom extensions to tailor the tool to your specific needs.

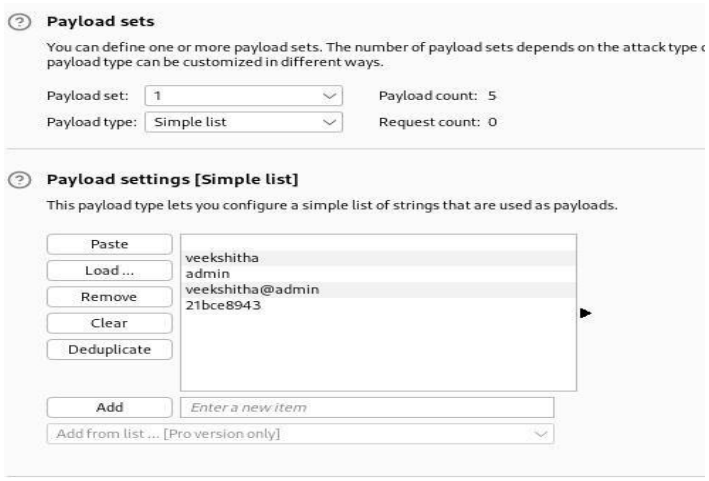
Session Management: Burp Suite includes tools for managing user sessions, cookies, and authentication mechanisms, making it easier to test authenticated areas of a web application.

Testing on testfire.net :



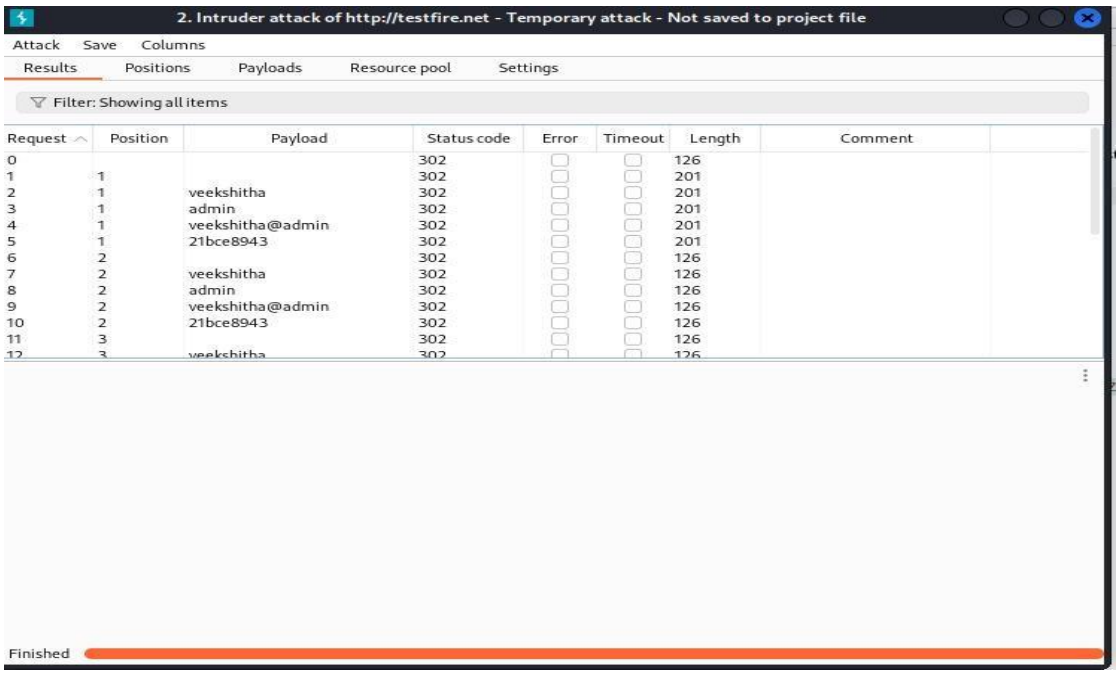
When we login in our website, burp suite has captured the login details ,it has also captured cookie id, j session id,
By poisoning them we can perform session hijacking attack as well as man in the middle attack.

Adding payloads :

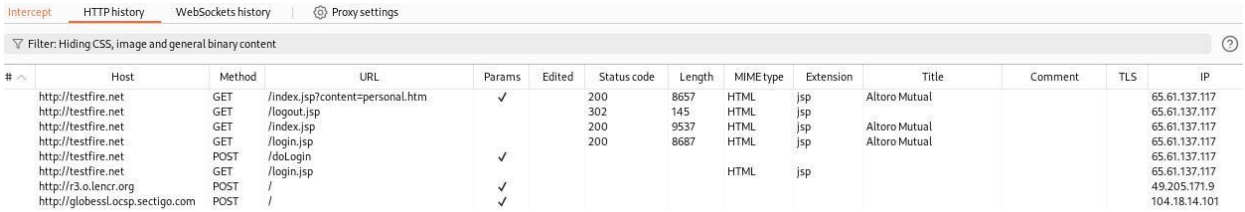


Payload positions :

Attack :



HTTPS History :



Intercept | HTTP history | WebSockets history | Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP
	http://testfire.net	GET	/index.jsp?content=personal.htm	✓		200	8657	HTML	jsp	Altoro Mutual			65.61.137.117
	http://testfire.net	GET	/logout.jsp			302	145	HTML	jsp				65.61.137.117
	http://testfire.net	GET	/index.jsp			200	9537	HTML	jsp	Altoro Mutual			65.61.137.117
	http://testfire.net	GET	/login.jsp			200	8687	HTML	jsp	Altoro Mutual			65.61.137.117
	http://testfire.net	POST	/doLogin	✓									65.61.137.117
	http://testfire.net	GET	/login.jsp					HTML	jsp				65.61.137.117
	http://r3.o.lencr.org	POST	/	✓									49.205.171.9
	http://globessl.ocsp.sectigo.com	POST	/	✓									104.18.14.101