SUBMITTED BY: Avvari Pratheek

REGISTRATION NO: 21BCE7819

E-mail: pratheek.21bce7819@vitapstudent.ac.in

WHAT IS BURP SUITE

Burp Suite is a popular cybersecurity tool used for web application security testing and penetration testing. It is developed by PortSwigger, a company specializing in web security tools. Burp Suite is widely used by security professionals, ethical hackers, and developers to identify vulnerabilities in web applications and to assess their security posture.

Key features of Burp Suite include:

1. Web Application Scanning: Burp Suite can automatically scan web applications for common security vulnerabilities such as cross-site scripting (XSS), SQL injection, CSRF (Cross-Site Request Forgery), and more. It helps security professionals identify and prioritize potential threats.

2. Proxy Server: Burp Suite acts as a proxy server, allowing users to intercept and inspect HTTP and HTTPS traffic between a web browser and the web server. This is useful for analyzing and manipulating requests and responses for security testing purposes.

3. Spidering and Crawling: Burp Suite can crawl and index a website's content to map its structure and identify potential entry points for testing. This helps testers understand the application's attack surface.

4. Intruder: This feature enables automated fuzzing and brute-force attacks on web applications to discover vulnerabilities or weak points in input fields and parameters.

5. Repeater: The Repeater tool allows testers to send modified requests to a web server and observe the responses, making it easier to test for vulnerabilities and verify findings.

6. Sequencer: Burp Suite's Sequencer tool analyzes the randomness of session tokens and other data to assess the quality of randomness and potential predictability.

7. Collaborator: Burp Collaborator is a feature for identifying out-of-band vulnerabilities, such as server-side request forgery (SSRF) and blind SQL injection.

8. Reporting: It provides customizable reports summarizing the findings and vulnerabilities discovered during a security assessment, making it easier to communicate issues to development teams or stakeholders.

Burp Suite is available in both free and paid versions. The free version, known as Burp Suite Community Edition, provides many of the essential features but with limitations. The paid version, Burp Suite Professional, offers advanced features and additional capabilities for security professionals and organizations that require comprehensive web application security testing.

It's important to note that Burp Suite should only be used for ethical and legal security testing, such as penetration testing with proper authorization, to assess the security of web applications. Unauthorized or malicious use of such tools is illegal and unethical.

WHY BURP SUITE

Burp Suite is a popular choice for web application security testing and penetration testing for several reasons:

1. Versatility: Burp Suite is a comprehensive tool that covers a wide range of security testing needs for web applications. It includes features for web crawling, scanning, intercepting and modifying requests, and more. This versatility makes it a valuable tool for both manual and automated testing.

2. User-Friendly Interface: Burp Suite provides a user-friendly and intuitive interface that makes it accessible to both novice and experienced security professionals. Its GUI (Graphical User Interface) simplifies the process of configuring and conducting security tests.

3. Active Development: Burp Suite is actively maintained and updated by PortSwigger, the company behind it. This means that it stays up-to-date with the latest web technologies and security threats. New features and bug fixes are regularly released to keep the tool relevant and effective.

4. Large User Community: Burp Suite has a large and active user community. This means that there is a wealth of knowledge, tutorials, and resources available online. Users can seek help from the community and share their experiences, which can be extremely valuable when working with the tool.

5. Extensibility: Burp Suite can be extended with custom plugins and scripts. This extensibility allows security professionals to tailor the tool to their specific testing needs, making it highly adaptable for various scenarios.

6. Regular Updates: Security vulnerabilities and threats are constantly evolving. Burp Suite's developers regularly update the tool to address new vulnerabilities and challenges, ensuring that it remains a reliable choice for web application security testing.

7. Reporting Capabilities: Burp Suite offers robust reporting capabilities, allowing security professionals to generate detailed reports summarizing vulnerabilities discovered during testing. These reports are essential for communication with development teams and stakeholders.

8. Comprehensive Testing: Burp Suite covers a wide range of security testing types, including automated scanning for common vulnerabilities and manual testing through tools like the Repeater and Intruder. This comprehensive approach helps testers identify and address various security issues.

9. Integration with Other Tools: Burp Suite can be integrated with other security tools and platforms, enhancing its effectiveness in a broader security testing ecosystem.

10. Professional Edition: While there is a free Community Edition of Burp Suite, the paid Burp Suite Professional edition offers additional features, such as advanced scanning capabilities, target management, and collaboration tools. This makes it suitable for professional security assessments and larger-scale security testing efforts.

Ultimately, the choice of Burp Suite for web application security testing depends on the specific needs of the security professional or organization. It is a versatile and well-regarded tool in the field of cybersecurity, and its popularity is a testament to its effectiveness in identifying and mitigating web application vulnerabilities.

WHAT ARE THE FEATURES OF BURP SUITE

Burp Suite is a powerful web application security testing tool that offers a wide range of features to assist security professionals, ethical hackers, and developers in identifying and mitigating vulnerabilities in web applications. Here are some of the key features of Burp Suite:
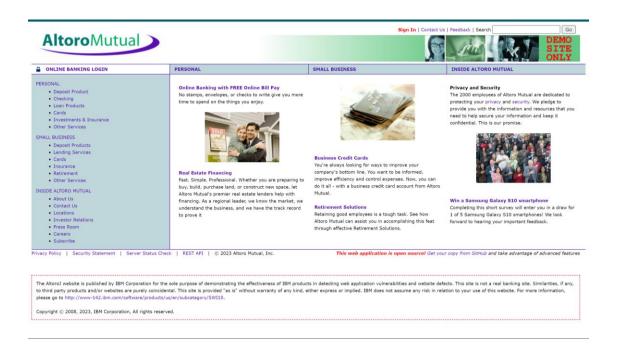
1. Proxy: Burp Suite acts as a proxy server, allowing you to intercept and modify HTTP/HTTPS requests and responses between your web browser and the target web application. This is useful for analyzing and manipulating traffic during testing.

2. Spider and Scanner: Burp Spider can crawl web applications to map their structure and discover new content, while Burp Scanner performs automated vulnerability scanning to identify common security issues like XSS, SQL injection, and more.

3. Intruder: This tool is used for automated testing of input fields and parameters. It can perform fuzzing attacks, brute-force attacks, and various payload-based tests to discover vulnerabilities in application inputs.

4. Repeater: The Repeater tool allows you to manually manipulate and send individual requests to the target application. It's useful for testing specific inputs and analyzing responses in detail.

5. Sequencer: Sequencer analyzes the randomness and quality of tokens, session identifiers, and other data generated by the application. It helps in identifying vulnerabilities related to predictable or weak randomness.

6. Decoder: Decoder can be used to decode and encode data in various formats (e.g., URL encoding, Base64) to understand how data is processed and transmitted by the application.

7. Comparer: This tool compares two HTTP requests or responses to identify differences, which can be useful for identifying subtle security issues.

8. Extensibility: Burp Suite can be extended with custom-written plugins and scripts, allowing users to add functionality or automate specific tasks to suit their testing needs.

9. Collaborator: Burp Collaborator helps in identifying out-of-band vulnerabilities by generating unique DNS and HTTP requests that can be monitored for interactions with the target application.

10. Target Scope: You can define the scope of your testing by specifying which parts of a web application are within scope and which are not. This helps focus testing efforts on specific areas.

11. Reporting: Burp Suite provides customizable reporting features, allowing you to generate detailed reports summarizing the vulnerabilities and findings discovered during the assessment.

12. Session Handling: It can manage and manipulate user sessions, including the ability to capture and restore sessions for testing purposes.

13. Authentication Testing: Burp Suite supports various authentication mechanisms, making it suitable for testing applications with login systems.

14. Integration: It can be integrated with other tools and platforms, making it a valuable part of a broader security testing ecosystem.

15. HTTP Message Editor: Burp Suite includes a powerful HTTP message editor for crafting custom requests and responses.

16. WebSocket Support: The tool provides WebSocket support for testing applications that use this communication protocol.

Please note that these features may vary between the free Community Edition and the paid Professional Edition of Burp Suite, with the Professional Edition typically offering more advanced capabilities and support. The choice of features and edition depends on your specific testing requirements and budget.
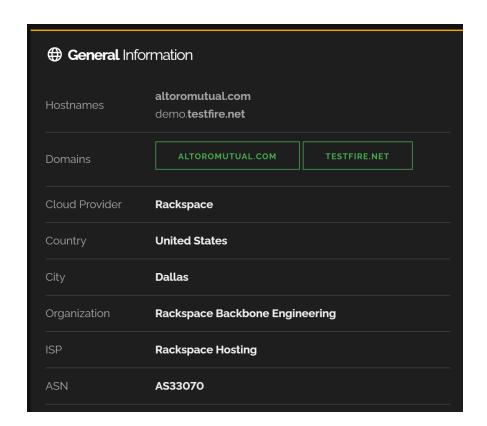
Vulnerability Test on testfire.net

IP ADDRESS of testfire.net

A records

IPv4 address	Revalidate in
> ⬛ 65.61.137.117	24h

🌐 **General** Information

Hostnames	**altoromutual.com** **demo.testfire.net**
Domains	ALTOROMUTUAL.COM TESTFIRE.NET
Cloud Provider	**Rackspace**
Country	**United States**
City	**Dallas**
Organization	**Rackspace Backbone Engineering**
ISP	**Rackspace Hosting**
ASN	**AS33070**

🖧 Open **Ports**

80	443	8080

Vulnerability	⊞	Severity ▼	QoD	Host IP	Name	Location	Created
Report outdated / end-of-life Scan Engine / Environment (local)	⚓	10.0 (High)	97 %	65.61.137.117	altoromutual.com	general/tcp	Sun, Oct 1, 2023 2:52 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	⊘	4.8 (Medium)	80 %	65.61.137.117	demo.testfire.net	8080/tcp	Sun, Oct 1, 2023 3:19 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	⊘	4.8 (Medium)	80 %	65.61.137.117	altoromutual.com	80/tcp	Sun, Oct 1, 2023 3:19 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	⊘	4.8 (Medium)	80 %	65.61.137.117	demo.testfire.net	80/tcp	Sun, Oct 1, 2023 3:19 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	⊘	4.8 (Medium)	80 %	65.61.137.117	altoromutual.com	8080/tcp	Sun, Oct 1, 2023 3:19 PM UTC
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	⇆	4.3 (Medium)	98 %	65.61.137.117	altoromutual.com	443/tcp	Sun, Oct 1, 2023 3:01 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	⊘	4.0 (Medium)	80 %	65.61.137.117	altoromutual.com	443/tcp	Sun, Oct 1, 2023 3:01 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	⊘	4.0 (Medium)	80 %	65.61.137.117	demo.testfire.net	443/tcp	Sun, Oct 1, 2023 3:01 PM UTC
TCP timestamps	⇆	2.6 (Low)	80 %	65.61.137.117	altoromutual.com	general/tcp	Sun, Oct 1, 2023 2:52 PM UTC

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity) ◁◁ 1 - 9 of 9 ▷▷|

◁◁ 1 - 1 of 1 ▷▷|

CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	1	1	4.3 (Medium)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity) ◁◁ 1 - 1 of 1 ▷▷|