

# ASSIGNMENT-4

## BURP SUITE

Burp Suite is a proxy tool that enables us to monitor, check, and modify requests performed by our browsers prior to transmission to a remote server. Burp Suite is a prominent web application security solution. It enables manual vulnerability testing, intercepts HTTP communications, and modifies the body and header of messages. BurpSuite is designed to be an all-in-one toolkit, and BApps are add-ons that may be installed to expand its functionality. It is the most widely used tool among experts in online app security and bug bounty hunters. It is a better option than free substitutes like OWASP ZAP because of how simple it is to use.

Key features of burp suite:

1. **Penetration Testing:** Burp Suite is an essential tool for penetration testers and ethical hackers. It allows them to simulate real-world attacks on web applications to assess their security posture. By doing so, security experts can provide valuable insights into the vulnerabilities and risks associated with a web application.
2. **Identifying Vulnerabilities:** One of the primary purposes of Burp Suite is to identify vulnerabilities and security weaknesses in web applications. It can detect issues like SQL injection, cross-site scripting (XSS), security misconfigurations, and more. By identifying these vulnerabilities, security professionals can help organizations address and mitigate potential threats before they can be exploited by malicious actors.
3. **Security Assessment:** Organizations use Burp Suite to conduct comprehensive security assessments of their web applications. This helps them proactively identify and remediate vulnerabilities to enhance their overall security posture.
4. **Manual Testing:** Burp Suite's various tools, such as the Proxy and Repeater, allow security professionals to manually interact with web applications, inspect requests and responses, and manipulate data. This is

particularly useful for uncovering hidden vulnerabilities that automated scanners might miss.

5. **Web Application Mapping:** The Spider tool in Burp Suite can automatically crawl a web application and create a map of its structure and functionality. This helps testers understand the application's architecture and identify potential entry points for attacks.

6. **Customization:** Burp Suite is highly customizable and extensible. Security professionals can create custom scripts and extensions to tailor the tool to specific testing requirements or to automate repetitive tasks.

7. **Collaboration:** Burp Suite's Collaborator feature aids in identifying out-of-band vulnerabilities and can be valuable for teams working on web application security assessments. It provides a unique domain that can be used to detect potential vulnerabilities that might not be apparent through regular interactions.

8. **Reporting:** Burp Suite offers reporting capabilities, allowing security testers to generate detailed reports that can be shared with stakeholders, including developers and management. These reports provide a clear overview of identified vulnerabilities and their severity, making it easier to prioritize and address them.

9. **Education and Training:** Burp Suite is commonly used in cybersecurity training and certification programs. It helps individuals learn about web application security, hands-on testing techniques, and the exploitation of vulnerabilities in a controlled environment.

## Vulnerabilities found using Burp Suite:

