

## What is Burp Suite?

Burp Suite is a robust cybersecurity tool primarily designed for testing the security of web applications. It is utilized to uncover and address security weaknesses in web applications and is available in two versions: Burp Suite Community (free) and Burp Suite Professional (paid, with advanced features).

## Why Choose Burp Suite?

Reasons to opt for Burp Suite include its versatility in handling a wide range of web security testing tasks, a user-friendly interface that simplifies the testing process, a potent automated scanner for detecting vulnerabilities, and its ability to act as a proxy for intercepting and modifying web traffic. Additionally, users can extend its capabilities through custom extensions, and it receives regular updates to stay current with evolving security standards and threats.

## Key Features of Burp Suite:

Key features of Burp Suite encompass functions such as proxying web traffic, automated vulnerability scanning, automated attacks for vulnerability identification, manual testing capabilities, randomness analysis, data encoding and decoding, response comparison, extensibility through custom add-ons, detecting out-of-band vulnerabilities, pre-defined security checks, session management, and comprehensive reporting.

In essence, Burp Suite is a versatile and powerful tool for assessing the security of web applications, offering a range of features to facilitate effective testing and vulnerability identification.

## Testing Vulnerabilities on testfire.net:

```
(kali@kali)-[~]
$ sudo nikto -h http://testfire.net
[sudo] password for kali:
- Nikto v2.5.0

+ Target IP: 65.61.137.117
+ Target Hostname: testfire.net
+ Target Port: 80
+ Start Time: 2023-09-24 12:33:13 (GMT-4)

+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Name: Kamalnath R

Reg no: 21BCE2844