Assignment-4

Hiya Sharma
21BCY10078

Burp Suite

Burp Suite is an integrated platform/graphical tool for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

Key features and functionalities of Burp Suite:

Web Application Scanning: Burp Suite can crawl websites and web applications, mapping out their structure and identifying potential security issues such as cross-site scripting (XSS), SQL injection, and other vulnerabilities.

Proxy Server: It acts as a proxy server, allowing users to intercept and inspect HTTP requests and responses between a web browser and a web server. This enables security professionals to analyze and manipulate web traffic for testing purposes.

Automated Scanning: Burp Suite offers automated scanning tools that can help identify common vulnerabilities in web applications, such as scanning for SQL injection, cross-site scripting, and more.

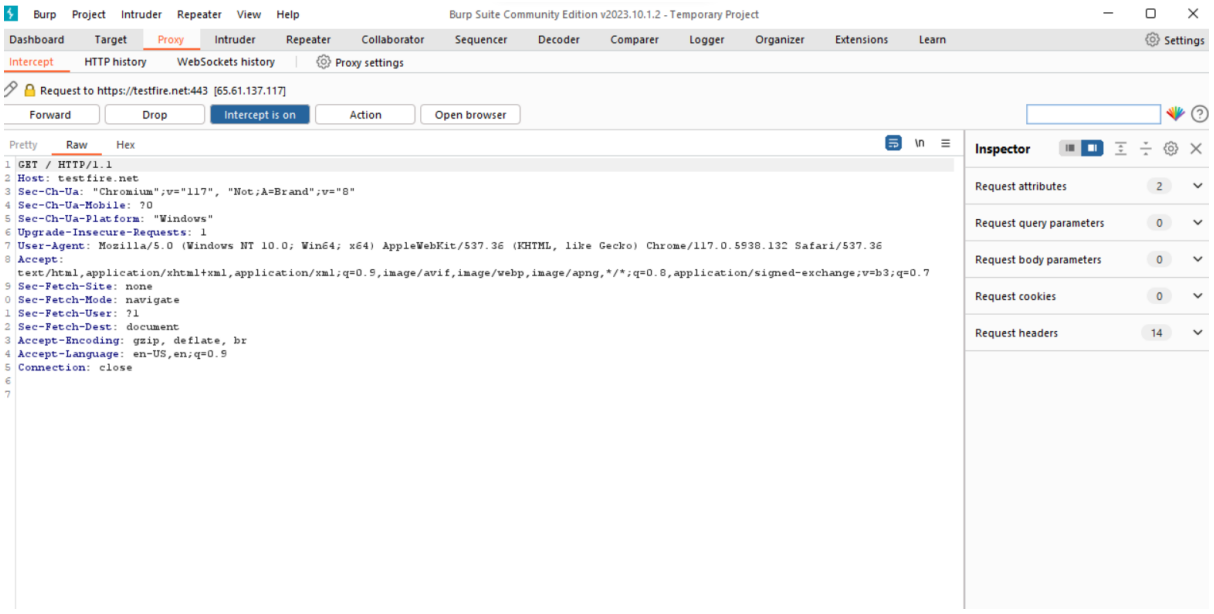
Manual Testing: Security professionals can use Burp Suite to manually test web applications by intercepting and modifying requests and responses, making it a powerful tool for discovering vulnerabilities that automated scanners might miss.

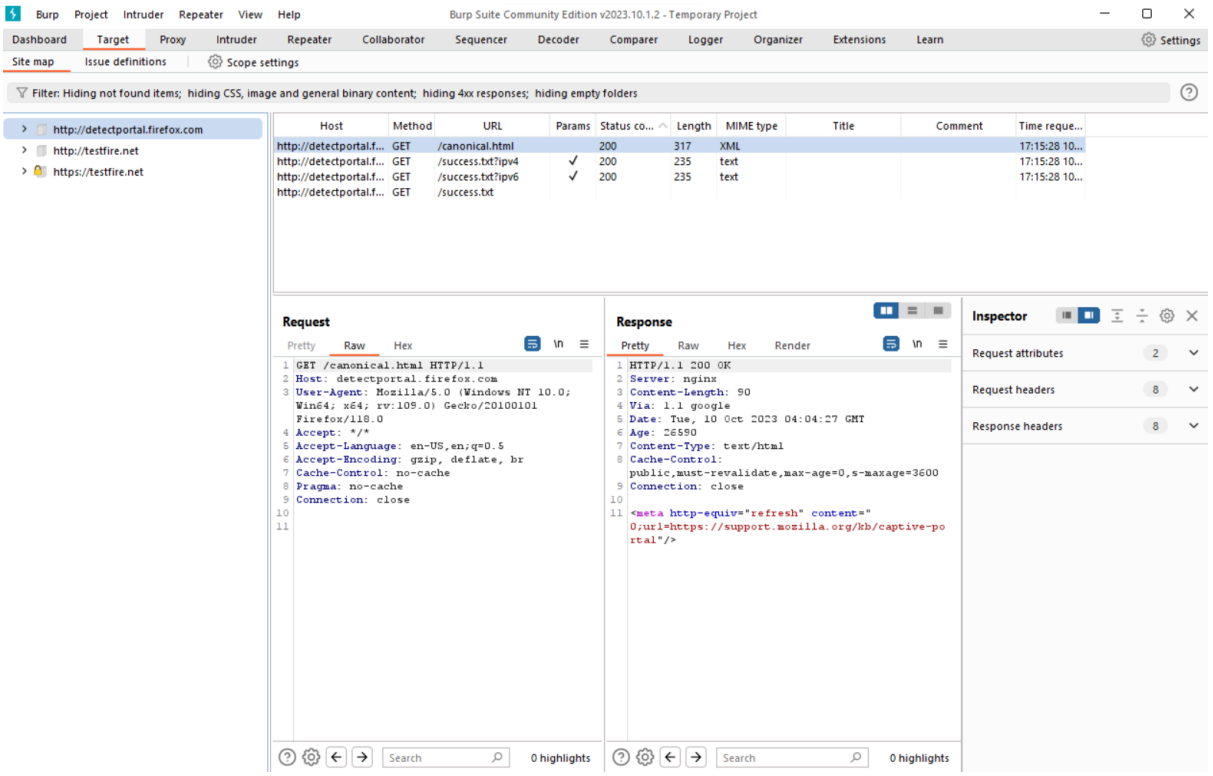
Intruder: This tool within Burp Suite allows for automated and customizable attacks on web applications to test for vulnerabilities like SQL injection, brute-force attacks, and more.

Repeater: It permits users to resend individual requests to a web application, making it easier to modify and test different parameters and payloads.
Sequencer: Burp Suite's Sequencer tool analyzes the randomness and unpredictability of tokens generated by a web application, which can be useful for identifying weaknesses in session management or token generation.

Extensibility: Burp Suite can be extended using its extensive API and supports the development of custom extensions and plugins. This makes it highly adaptable to specific testing requirements.

Reporting: The tool provides reporting features to document and share findings, making it easier to communicate vulnerabilities to developers and stakeholders.




Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.2 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Site map Issue definitions Scope settings
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
http://detectportal.firefox.com
http://testfire.net
https://testfire.net
Host Method URL Params Status co... Length MIME type Title Comment Time reque...
http://detectportal.f... GET /canonical.html 200 317 XML 17:15:28 10...
http://detectportal.f... GET /success.txt?ipv4 ✓ 200 235 text 17:15:28 10...
http://detectportal.f... GET /success.txt?ipv6 ✓ 200 235 text 17:15:28 10...
http://detectportal.f... GET /success.txt
Request
Pretty Raw Hex
1 GET /canonical.html HTTP/1.1
2 Host: detectportal.firefox.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Cache-Control: no-cache
8 Pragma: no-cache
9 Connection: close
10
11
Search 0 highlights
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx
3 Content-Length: 90
4 Via: 1.1 google
5 Date: Tue, 10 Oct 2023 04:04:27 GMT
6 Age: 26590
7 Content-Type: text/html
8 Cache-Control: public,must-revalidate,max-age=0,s-maxage=3600
9 Connection: close
10
11 <meta http-equiv="refresh" content="0;url=https://support.mozilla.org/kb/captive-portal"/>
Search 0 highlights
Inspector
Request attributes 2
Request headers 8
Response headers 8