Assignment 4
Using Burp suite to execute OS command injection

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.

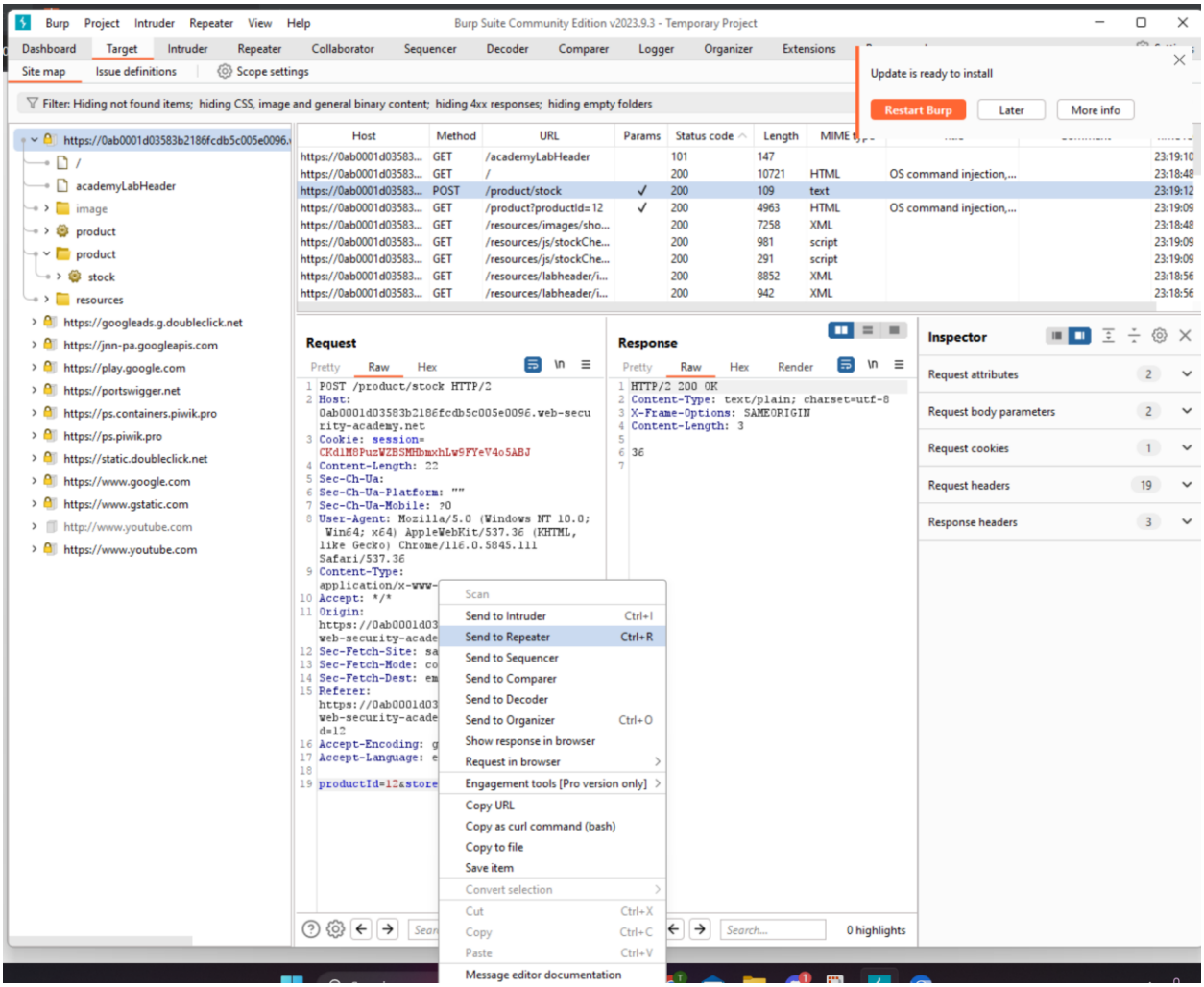
Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you.

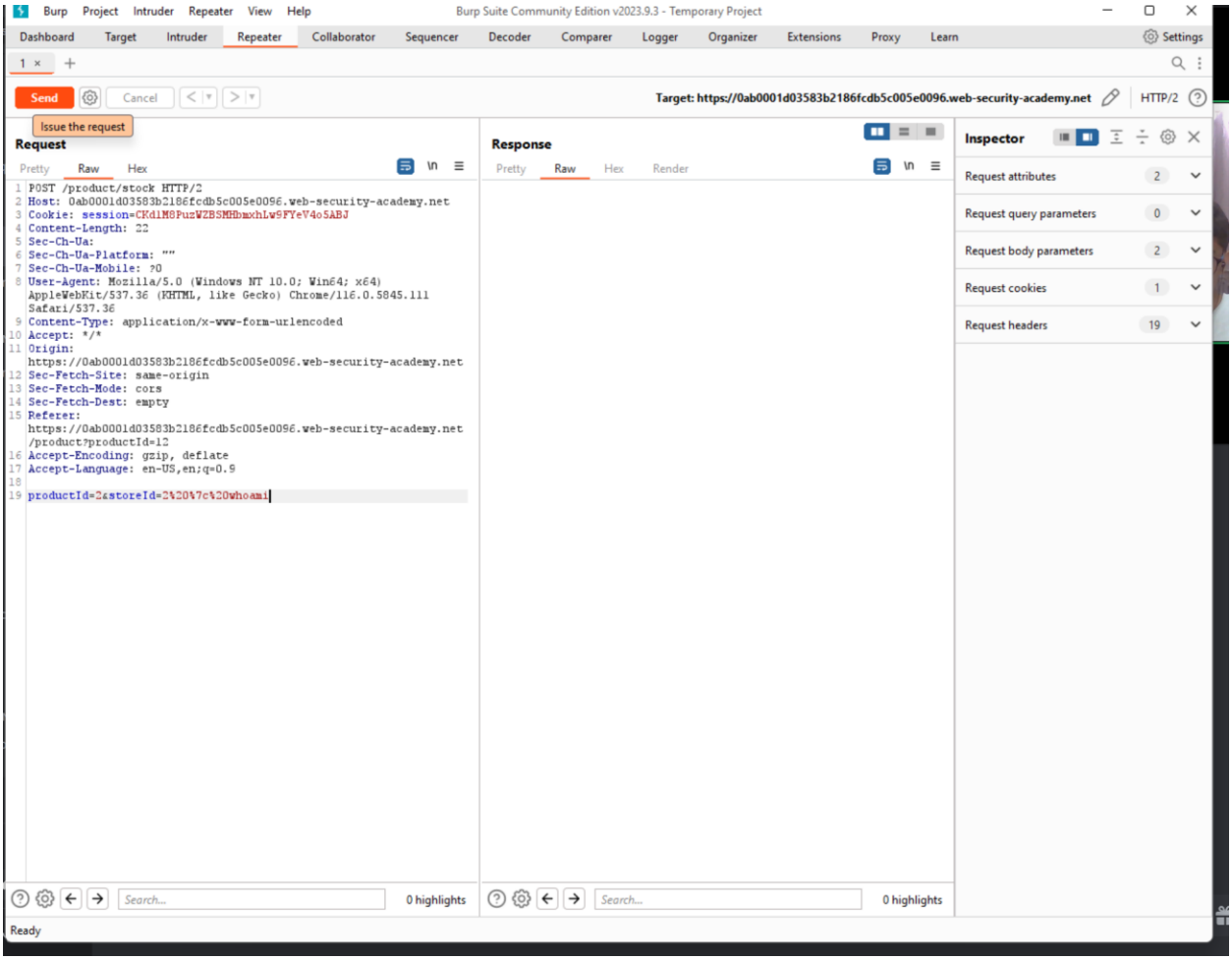
Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.

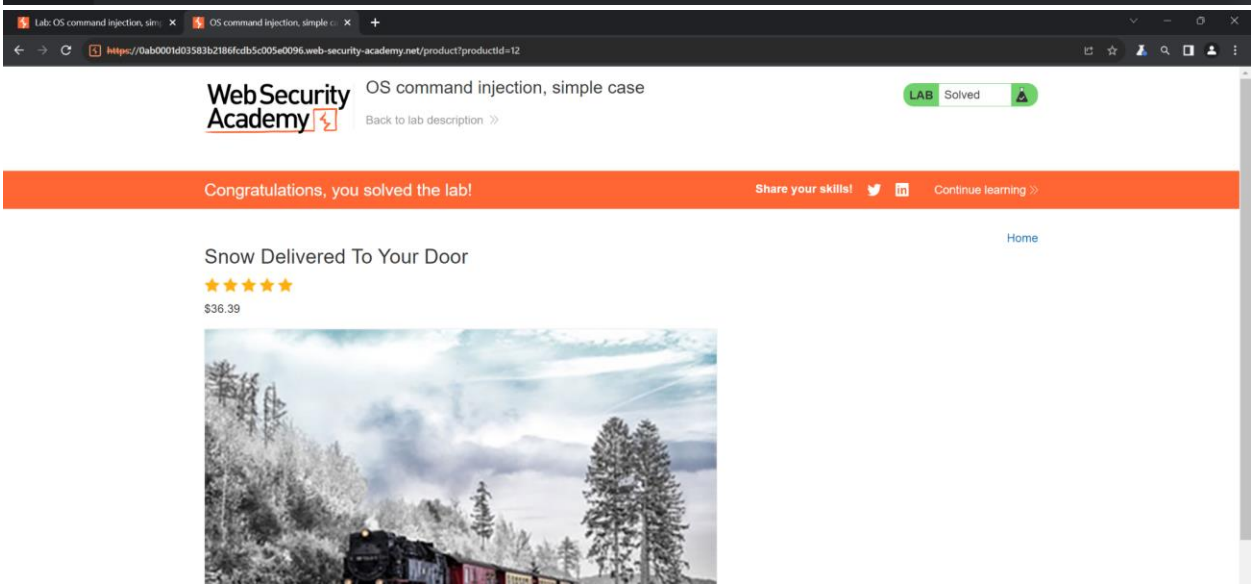
London Check stock

36 units

< Return to list


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.9.3 - Temporary Project
Dashboard Target Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
Site map Issue definitions Scope settings
Update is ready to install
Restart Burp Later More info
Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
Host Method URL Params Status code Length MIME type
https://0ab0001d03583b2186fcdb5c005e0096.
/
academyLabHeader
image
product
product
stock
resources
https://googleads.g.doubleclick.net
https://jnn-pa.googleapis.com
https://play.google.com
https://portswigger.net
https://ps.containers.piwik.pro
https://ps.piwik.pro
https://static.doubleclick.net
https://www.google.com
https://www.gstatic.com
http://www.youtube.com
https://www.youtube.com
https://0ab0001d03583... GET /academyLabHeader 101 147 23:19:10
https://0ab0001d03583... GET / 200 10721 HTML OS command injection,... 23:18:48
https://0ab0001d03583... POST /product/stock ✓ 200 109 text 23:19:12
https://0ab0001d03583... GET /product?productId=12 ✓ 200 4963 HTML OS command injection,... 23:19:09
https://0ab0001d03583... GET /resources/images/sho... 200 7258 XML 23:18:48
https://0ab0001d03583... GET /resources/js/stockChe... 200 981 script 23:19:09
https://0ab0001d03583... GET /resources/js/stockChe... 200 291 script 23:19:09
https://0ab0001d03583... GET /resources/labheader/i... 200 8852 XML 23:18:56
https://0ab0001d03583... GET /resources/labheader/i... 200 942 XML 23:18:56
Request
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0ab0001d03583b2186fcdb5c005e0096.web-security-academy.net
3 Cookie: session=CKdlM8PuzWZB5MHbmxhLw9FYeV4o5ABJ
4 Content-Length: 22
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/116.0.5845.111 Safari/537.36
9 Content-Type: application/x-www-
10 Accept: */*
11 Origin: https://0ab0001d03
web-security-acade
12 Sec-Fetch-Site: sa
13 Sec-Fetch-Mode: co
14 Sec-Fetch-Dest: em
15 Referer: https://0ab0001d03
web-security-acade
d=12
16 Accept-Encoding: g
17 Accept-Language: e
18
19 productId=12&store
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/plain; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 3
5
6 36
7
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Show response in browser
Request in browser
Engagement tools [Pro version only]
Copy URL
Copy as curl command (bash)
Copy to file
Save item
Convert selection
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Inspector
Request attributes 2
Request body parameters 2
Request cookies 1
Request headers 19
Response headers 3
Search...
0 highlights





Functions of burp suite

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.

Collaboration: Burp Suite Pro offers collaboration features that enable multiple security professionals to work together on the same project, share findings, and track progress.