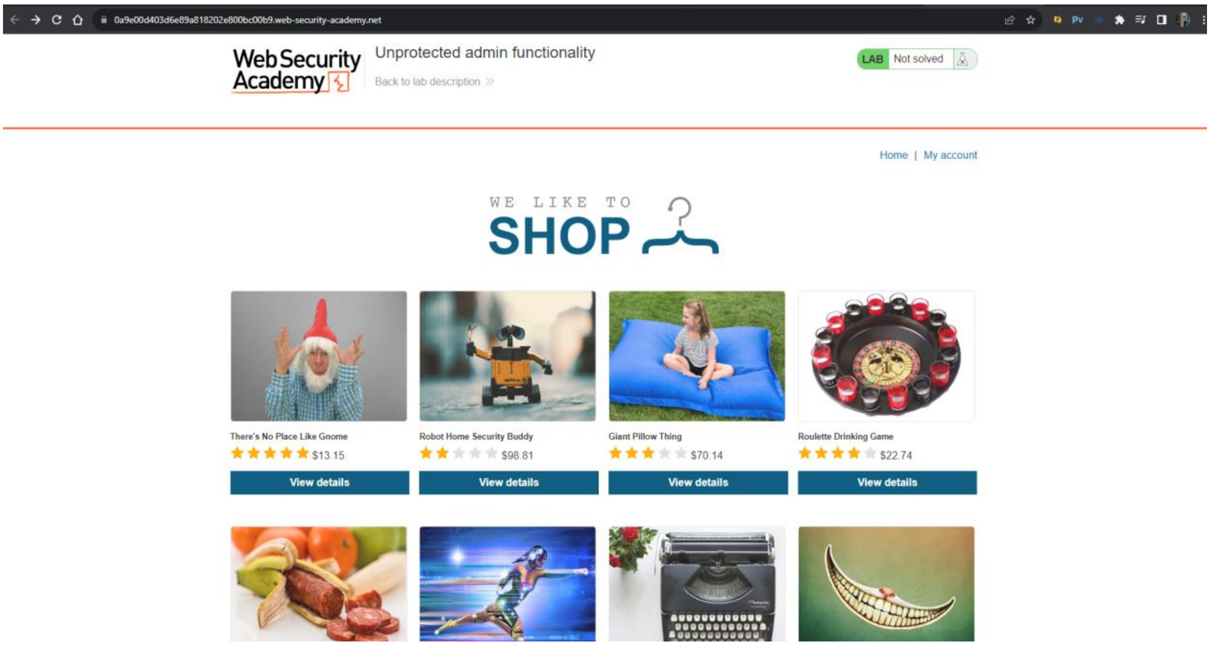
ASSIGNMENT 1

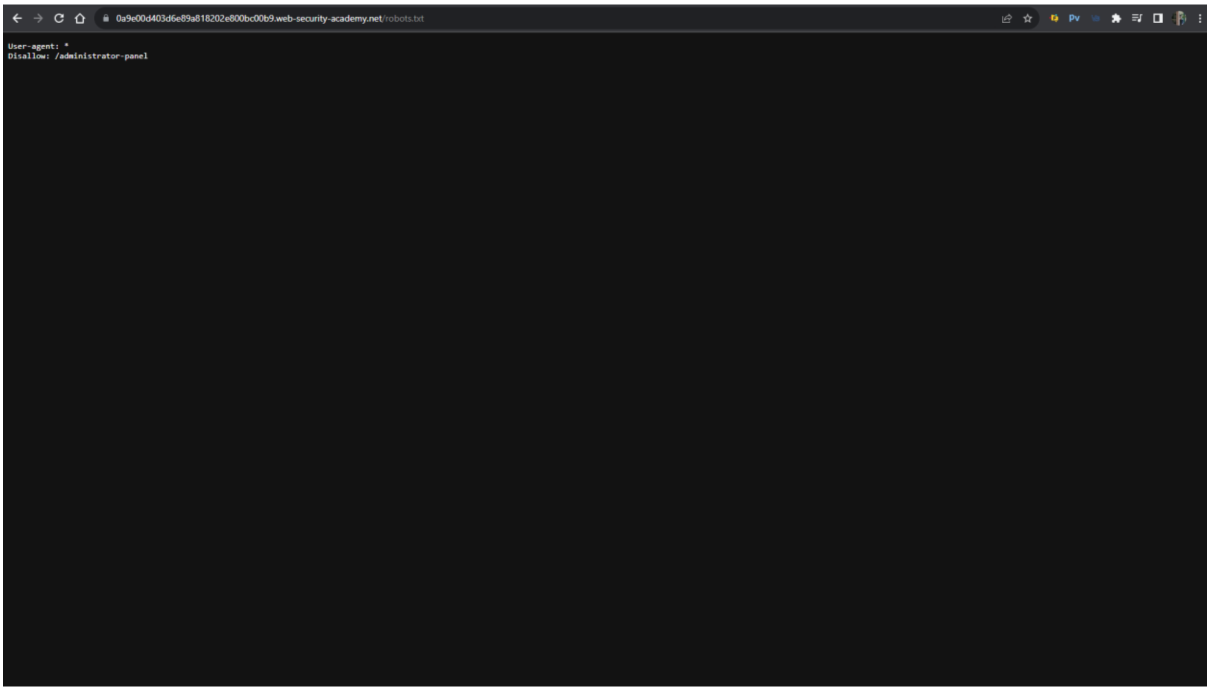
CHECKING THE TOP 5 CWE VULNERABILITIES

BROKEN ACCESS CONTROL:

Access the website

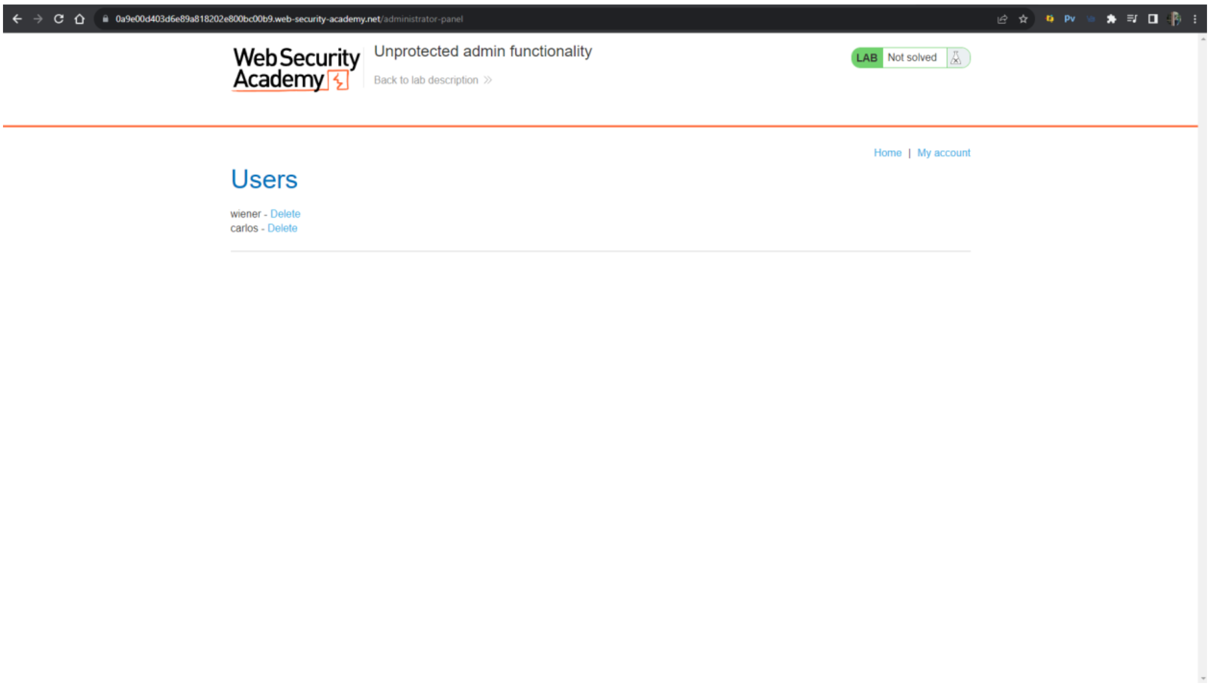


In the url add /robots.txt


0a9e00d403d6e89a818202e800bc00b9.web-security-academy.net/robots.txt

```
User-agent: *
Disallow: /administrator-panel
```

Add /administrator-panel



0a9e00d403d6e89a818202e800bc00b9.web-security-academy.net/administrator-panel

Unprotected admin functionality

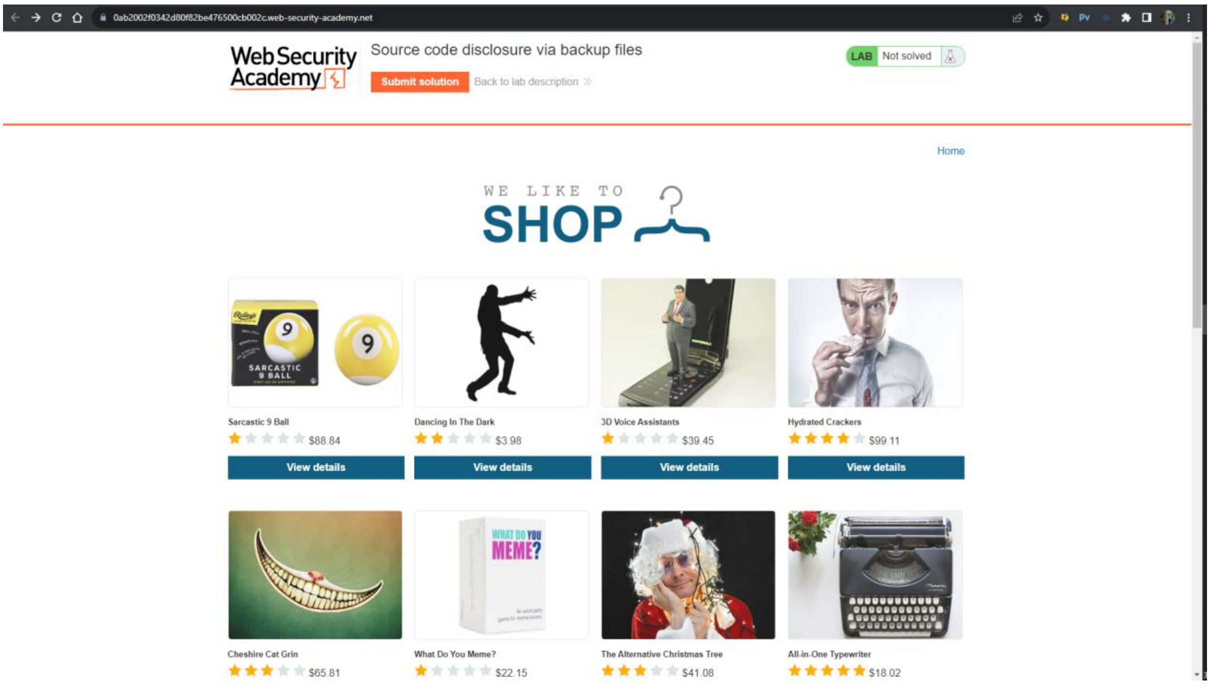
Users

wiener - Delete
carlos - Delete

hence this website has a broken access vulnerability

CRYPTOGRAPHIC FAILURES

Access the website

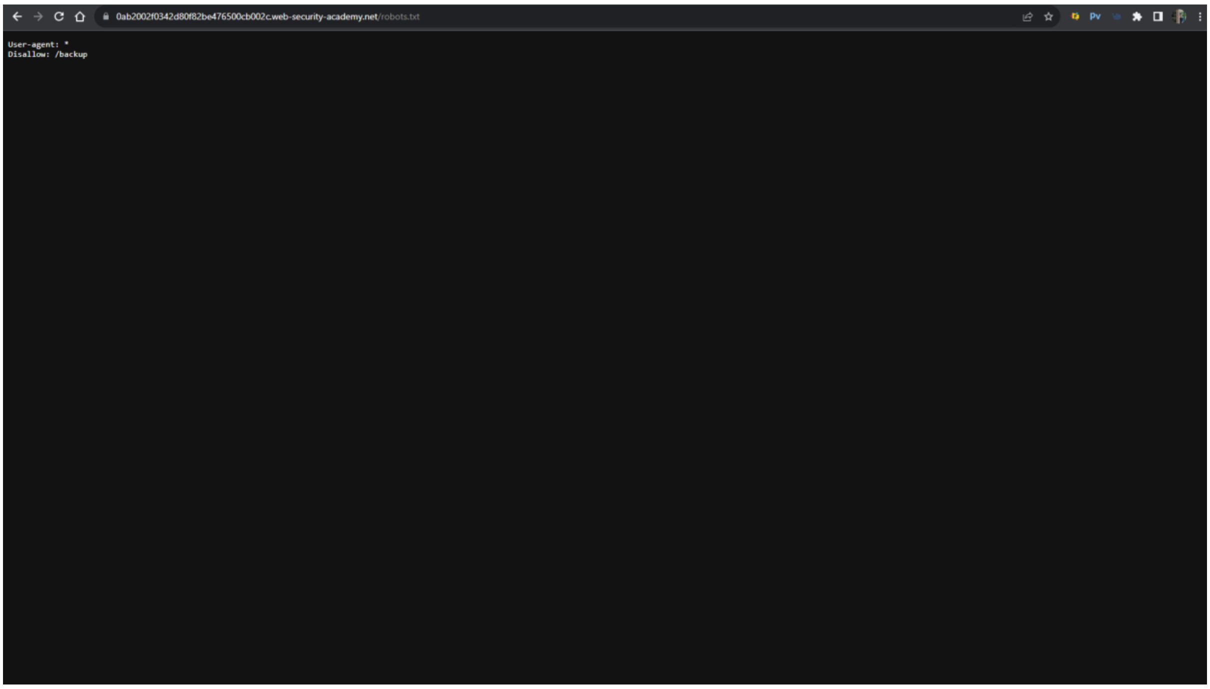


0ab2002f0342d80f82be476500cb002c.web-security-academy.net

Source code disclosure via backup files

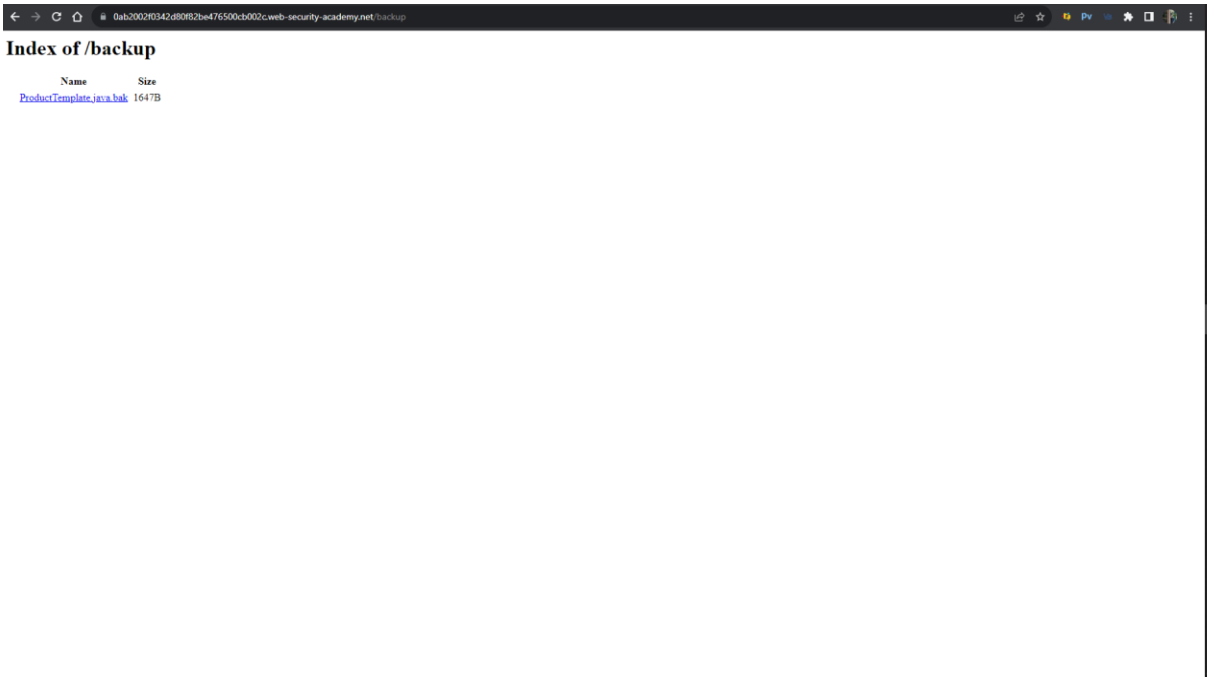
Sarcastic 9 Ball $88.84
Dancing In The Dark $3.98
3D Voice Assistants $39.45
Hydrated Crackers $99.11
Cheshire Cat Grin $65.81
What Do You Meme? $22.15
The Alternative Christmas Tree $41.08
All-in-One Typewriter $18.02

Add /robots.txt


0ab2002f0342d80f82be476500cb002c.web-security-academy.net/robots.txt

```
User-agent: *
Disallow: /backup
```

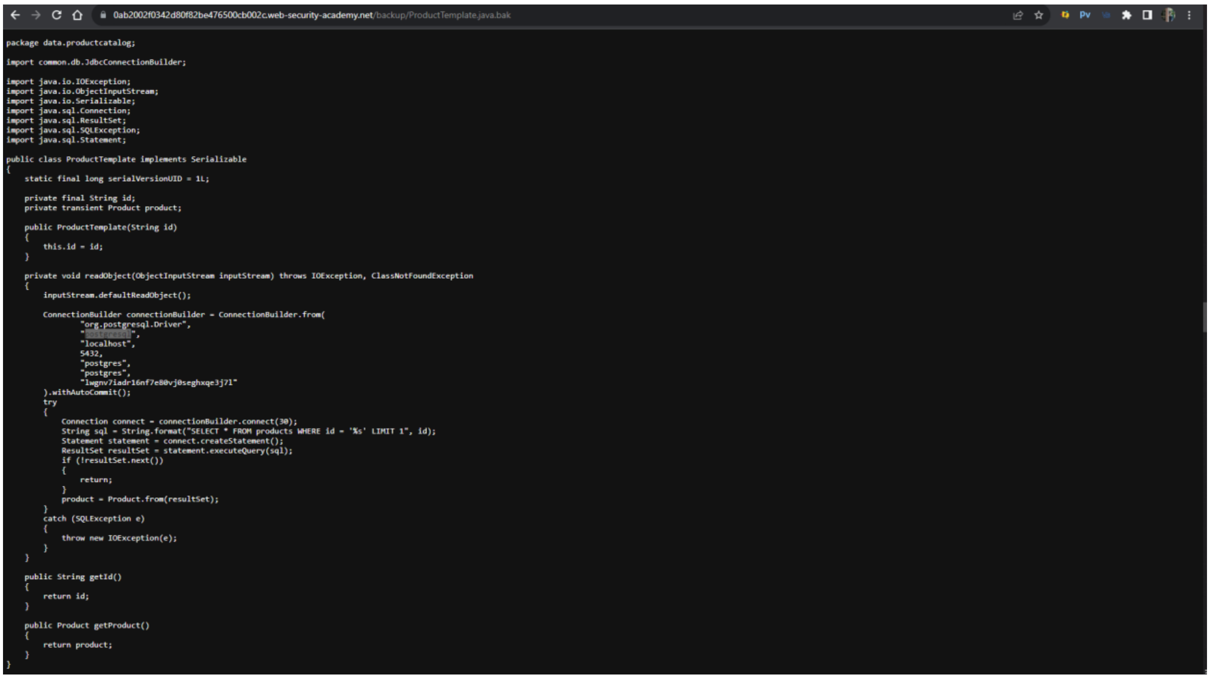
Add /backup in the url


0ab2002f0342d80f82be476500cb002c.web-security-academy.net/backup

Index of /backup

Name	Size
ProductTemplate.java.bak	1647B

We add ProductTemplate.java.bak in url


0ab2002f0342d80f82be476500cb002c.web-security-academy.net/backup/ProductTemplate.java.bak

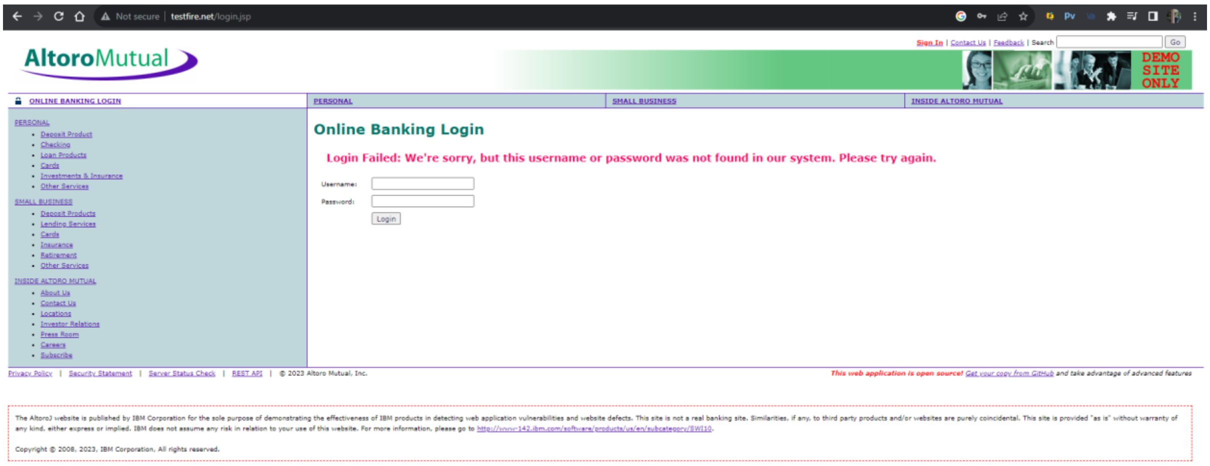
```
package data.productcatalog;

import common.db.JdbcConnectionBuilder;

import java.io.IOException;
import java.io.ObjectInputStream;
import java.io.Serializable;
import java.sql.Connection;
import java.sql.ResultSet;
import java.sql.SQLException;
import java.sql.Statement;

public class ProductTemplate implements Serializable
{
    static final long serialVersionUID = 1L;

    private final String id;
    private transient Product product;

    public ProductTemplate(String id)
    {
        this.id = id;
    }

    private void readObject(ObjectInputStream inputStream) throws IOException, ClassNotFoundException
    {
        inputStream.defaultReadObject();

        ConnectionBuilder connectionBuilder = ConnectionBuilder.from(
                "org.postgresql.Driver",
                "postgresql",
                "localhost",
                5432,
                "postgres",
                "postgres",
                "lwgnv7iadr16nf7e80vj0seghxqe3j7l"
        ).withAutoCommit();
        try
        {
            Connection connect = connectionBuilder.connect(30);
            String sql = String.format("SELECT * FROM products WHERE id = '%s' LIMIT 1", id);
            Statement statement = connect.createStatement();
            ResultSet resultSet = statement.executeQuery(sql);
            if (!resultSet.next())
            {
                return;
            }
            product = Product.from(resultSet);
        }
        catch (SQLException e)
        {
            throw new IOException(e);
        }
    }

    public String getId()
    {
        return id;
    }

    public Product getProduct()
    {
        return product;
    }
}
```

Hence the site is vulnerable to cryptographic failures

INJECTION FAILURES

VISIT WEBSITE

ADD ADMIN AND PASSWORD



Online Banking Login

Login Failed: We're sorry, but this username or password was not found in our system. Please try again.

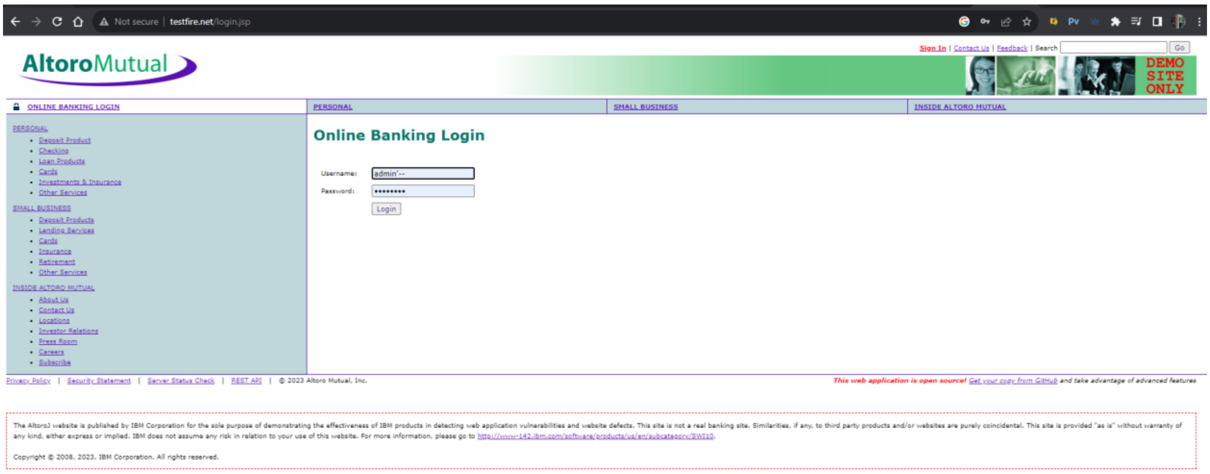
Username:

Password:

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.



Not secure | testfire.net/login.jsp

AltoroMutual

Sign In | Contact Us | Feedback | Search [ ] Go

DEMO SITE ONLY

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

Username: admin'--

Password: ••••••••

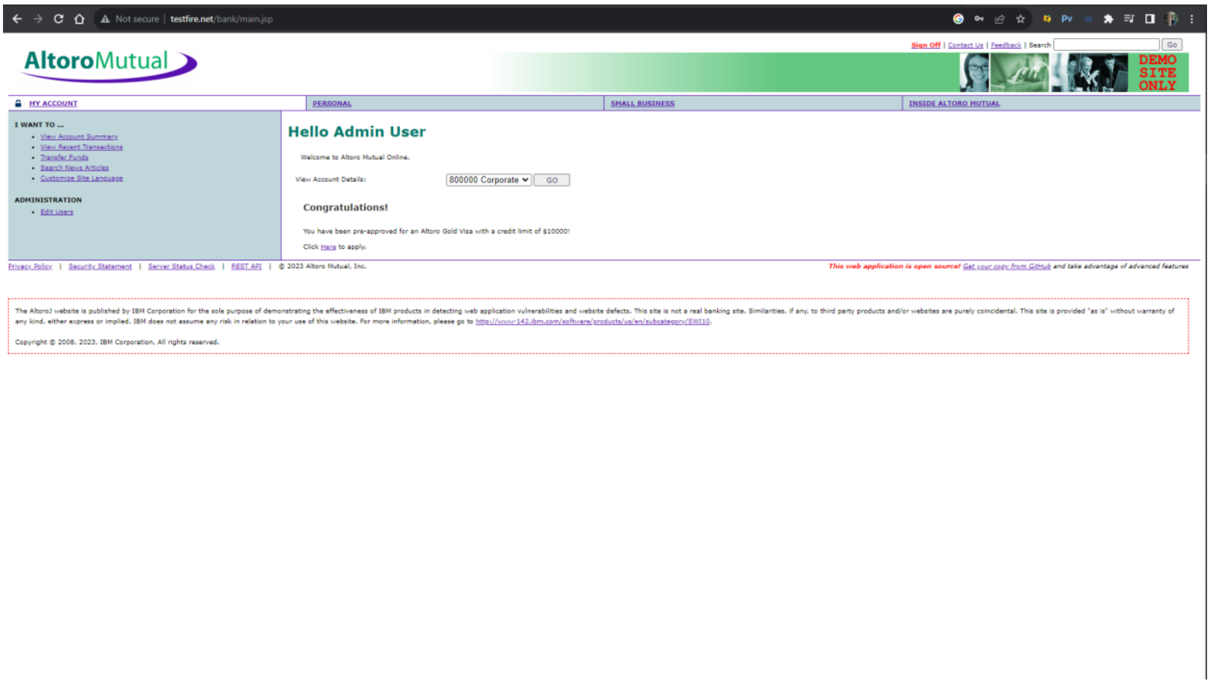
Login

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.



Not secure | testfire.net/bank/main.jsp

AltoroMutual

Sign Off | Contact Us | Feedback | Search [ ] Go

DEMO SITE ONLY

MY ACCOUNT | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

I WANT TO ...
- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION
- Edit Users

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of advanced features

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

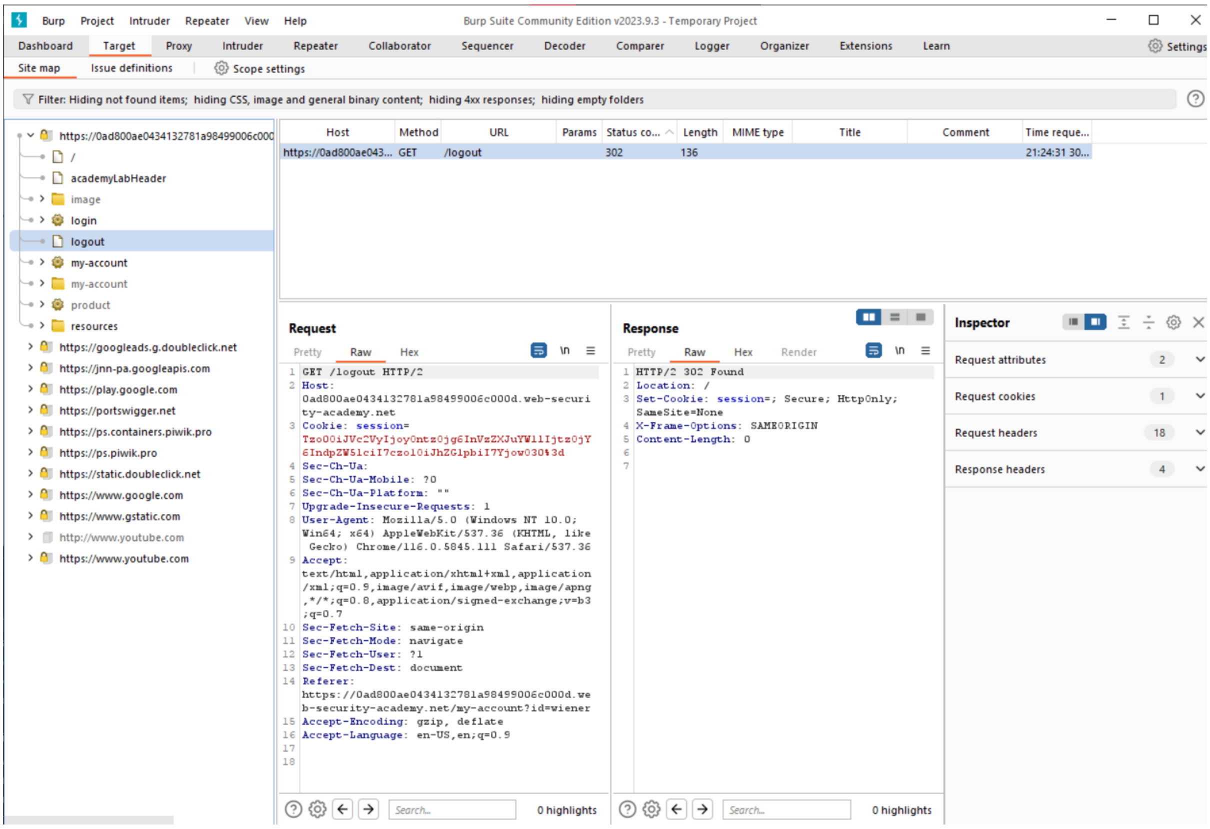
Copyright © 2008, 2023, IBM Corporation, All rights reserved.

Hence this website has SQL injection Vulnerabilities

INSECURE DESIGN

Access the website

Open burp suite access cookie layer



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- https://0ad800ae0434132781a98499006c000
  - /
  - academyLabHeader
  - image
  - login
  - logout
  - my-account
  - my-account
  - product
  - resources
- https://googleads.g.doubleclick.net
- https://jnn-pa.googleapis.com
- https://play.google.com
- https://portswigger.net
- https://ps.containers.piwik.pro
- https://ps.piwik.pro
- https://static.doubleclick.net
- https://www.google.com
- https://www.gstatic.com
- http://www.youtube.com
- https://www.youtube.com

Host	Method	URL	Params	Status co...	Length	MIME type	Title	Comment	Time reque...
https://0ad800ae043...	GET	/logout		302	136				21:24:31 30...

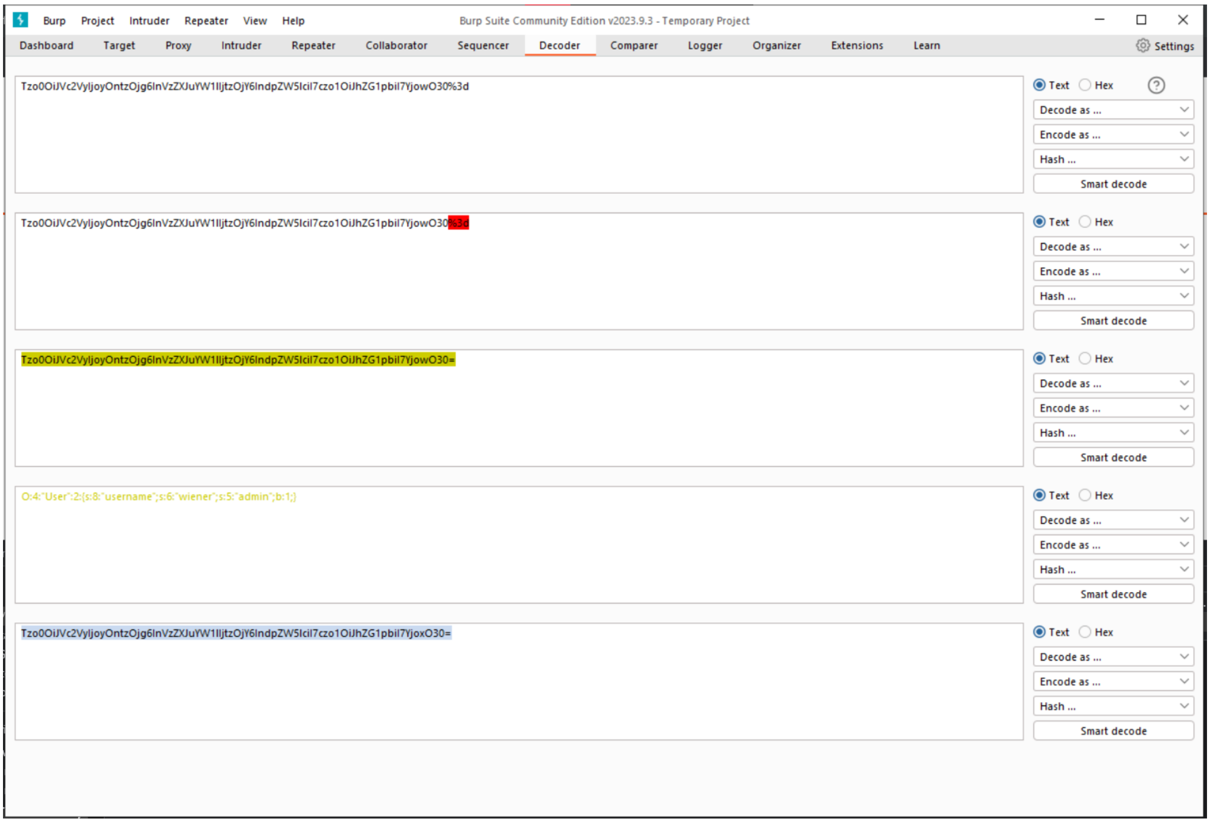
Request

```
GET /logout HTTP/2
Host:
0ad800ae0434132781a98499006c000d.web-securi
ty-academy.net
Cookie: session=
Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY
6IndpZW5lciI7czo1OiJhZG1pbiI7Yjow030%3d
Sec-Ch-Ua:
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0;
Win64; x64) AppleWebKit/537.36 (KHTML, like
 Gecko) Chrome/116.0.5845.111 Safari/537.36
Accept:
text/html,application/xhtml+xml,application
/xml;q=0.9,image/avif,image/webp,image/apng
,*/*;q=0.8,application/signed-exchange;v=b3
;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0ad800ae0434132781a98499006c000d.we
b-security-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

Response

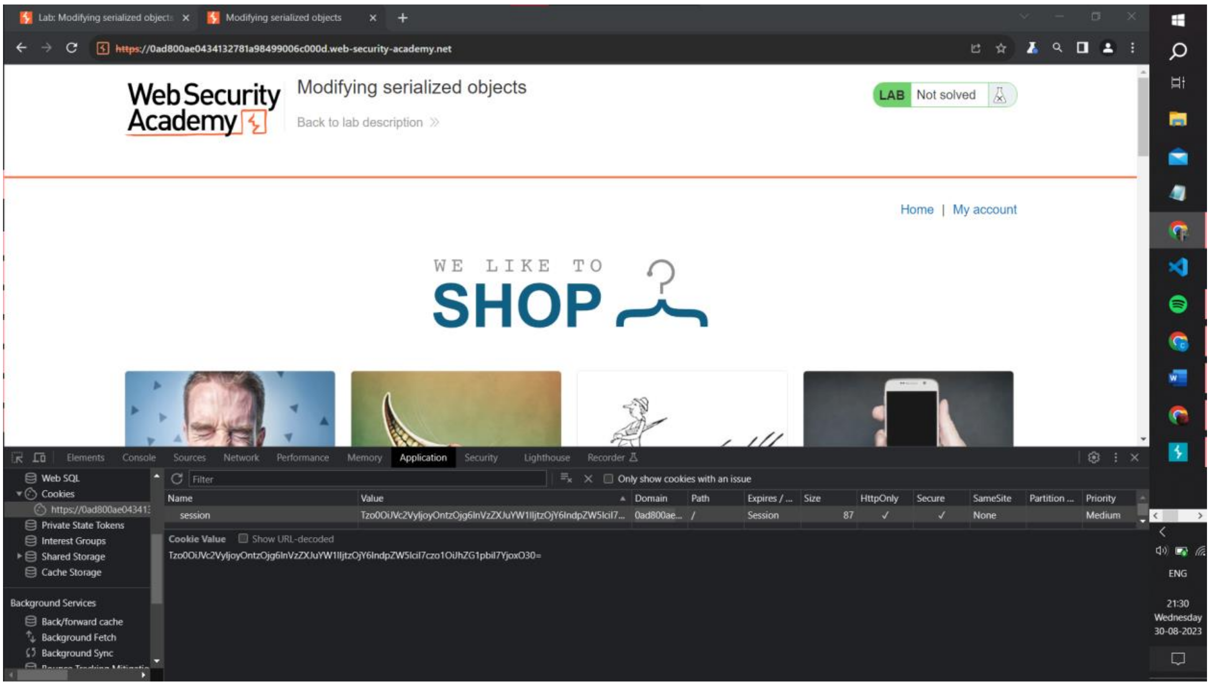
```
HTTP/2 302 Found
Location: /
Set-Cookie: session=; Secure; HttpOnly;
SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

Go to decoder change b=1 to access the admin portal



```
Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czo1OiJhZG1pbiI7YjowO30%3d

Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czo1OiJhZG1pbiI7YjowO30%3d

Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czo1OiJhZG1pbiI7YjowO30=

O:4:"User":2:{s:8:"username";s:6:"wiener";s:5:"admin";b:1;}

Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czo1OiJhZG1pbiI7YjoxO30=
```

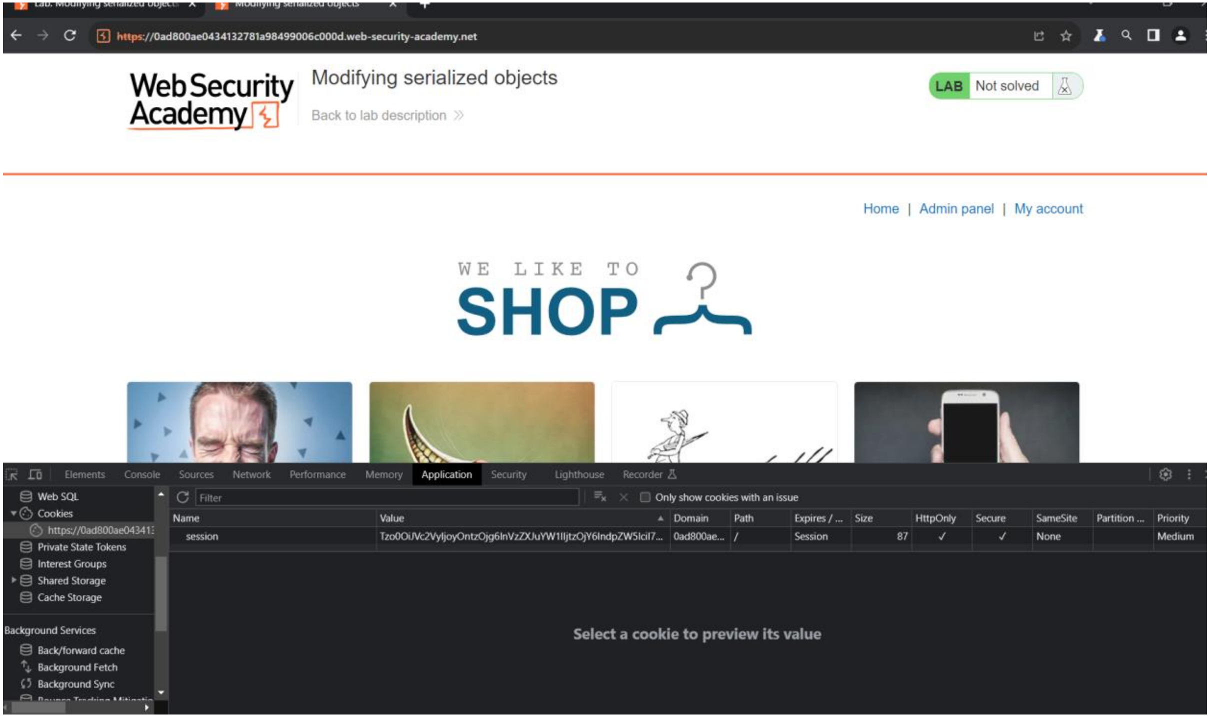
Change value in cookie layer of website



Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition ...	Priority
session	Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7...	0ad800ae...	/	Session	87	✓	✓	None		Medium

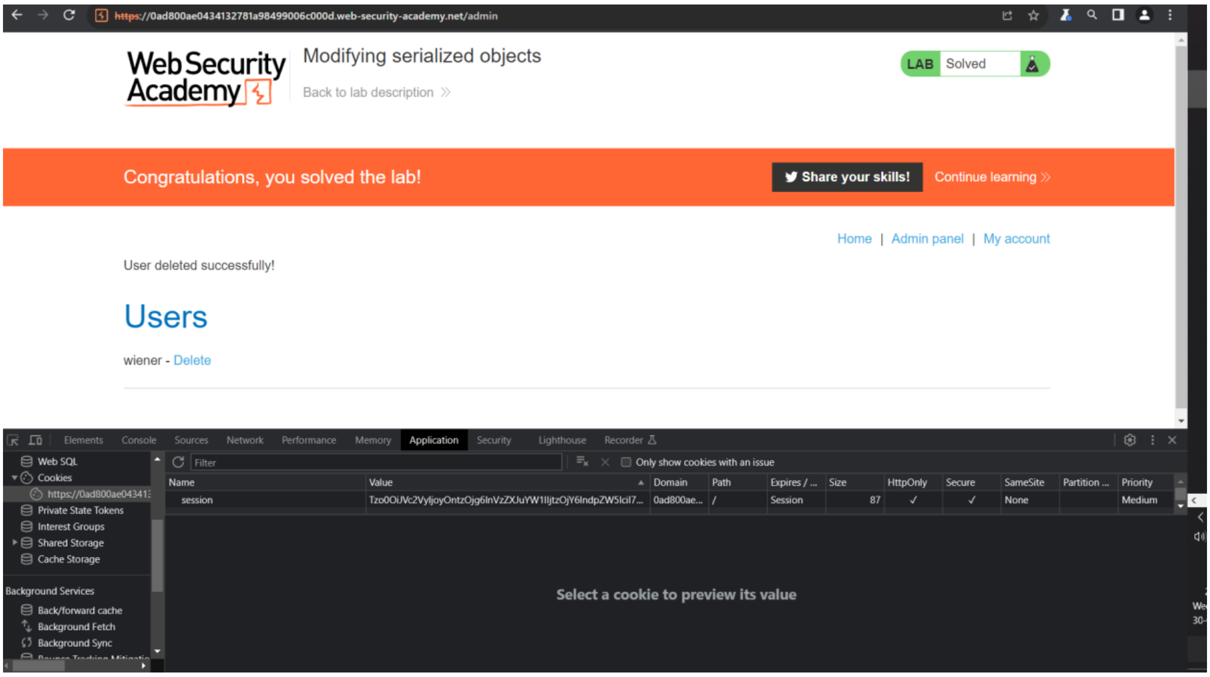
Cookie Value □ Show URL-decoded

Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czo1OiJhZG1pbiI7YjoxO30=



Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition ...	Priority
session	Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7...	0ad800ae...	/	Session	87	✓	✓	None		Medium

Select a cookie to preview its value



https://0ad800ae0434132781a98499006c000d.web-security-academy.net/admin

Modifying serialized objects

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | Admin panel | My account

User deleted successfully!

Users

wiener - Delete

Select a cookie to preview its value

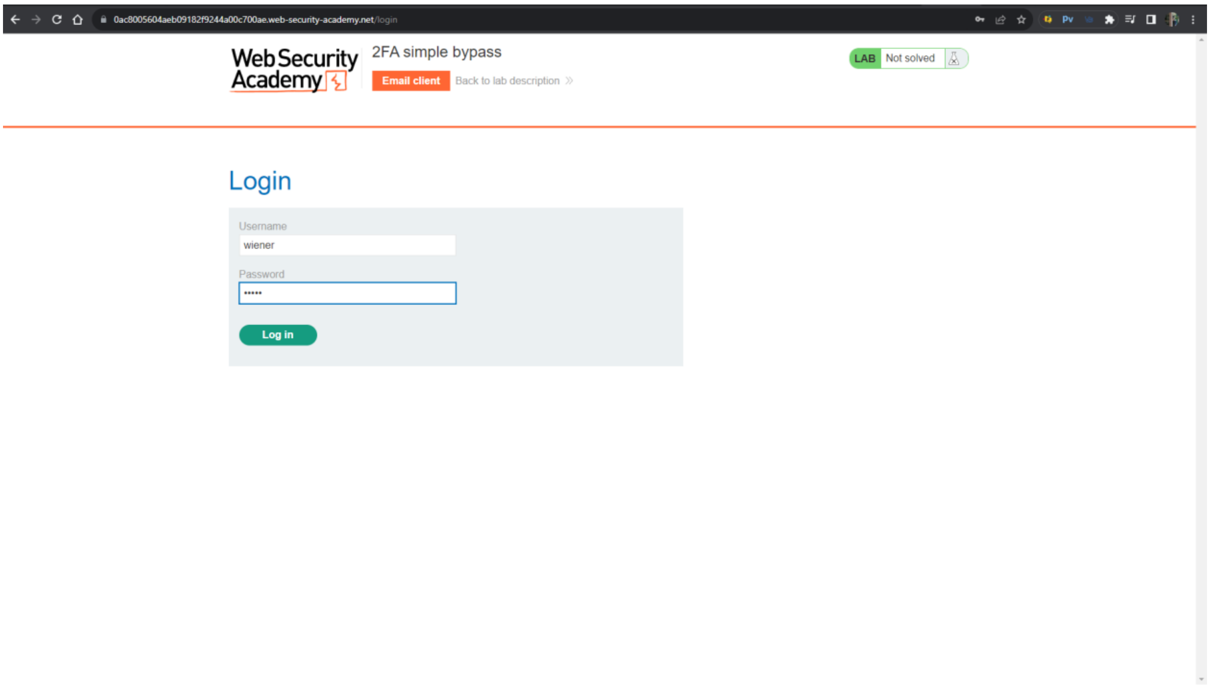
Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition ...	Priority
session	Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7...	0ad800ae...	/	Session	87	✓	✓	None		Medium

Delete user

hence website is vulnerable to insecure design

SECURITY MISCONFIG

ACCESS THE WEBSITE AND LOGIN



0ac8005604aeb09182f9244a00c700ae.web-security-academy.net/login

2FA simple bypass

Email client Back to lab description »

LAB Not solved

Login

Username

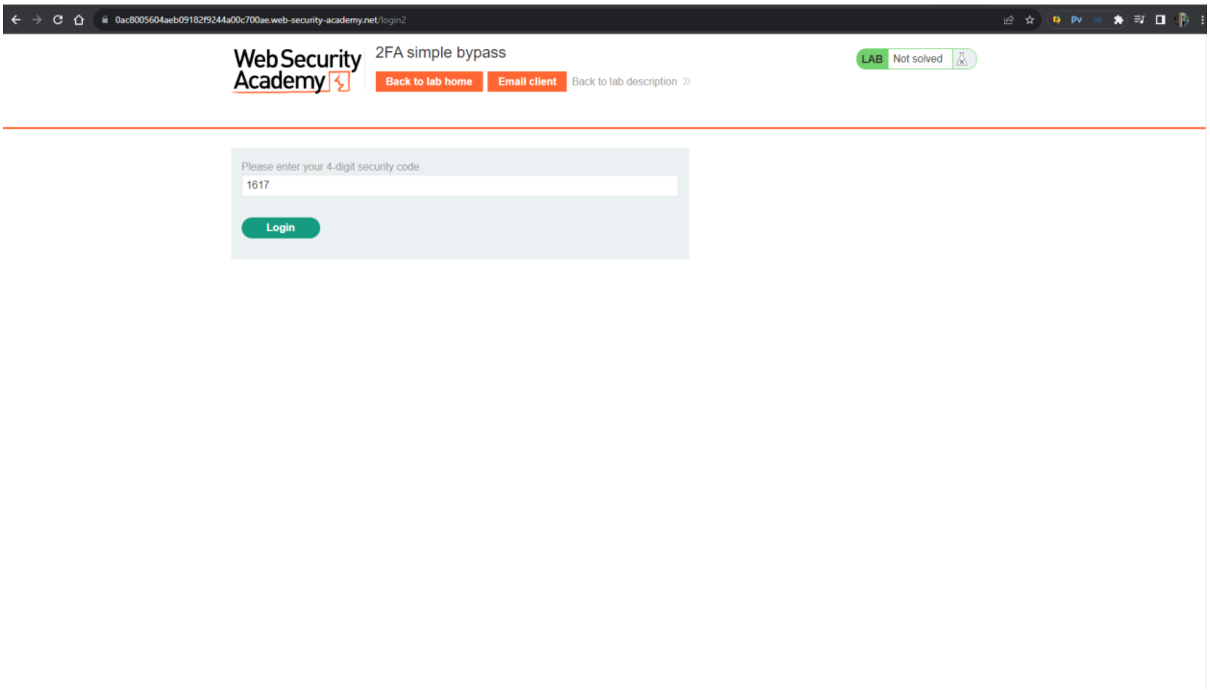
wiener

Password

•••••

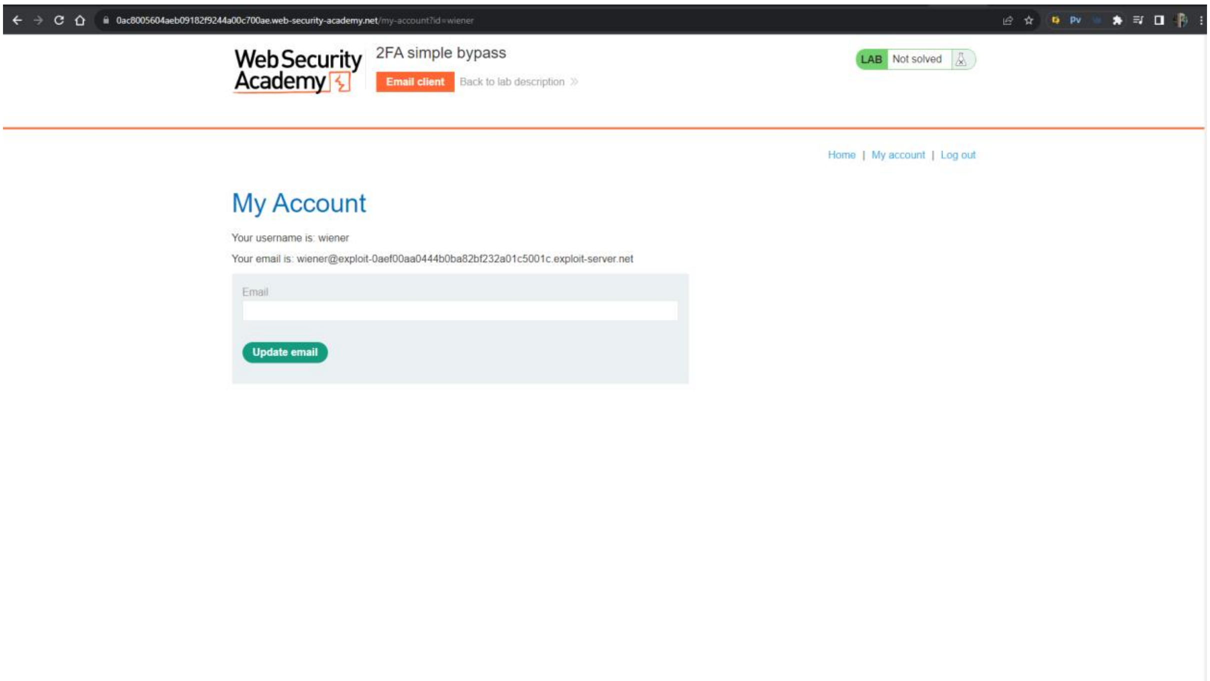
Log in

ENTER OTP



0ac8005604aeb09182f9244a00c700ae.web-security-academy.net/login2

Please enter your 4-digit security code: 1617



0ac8005604aeb09182f9244a00c700ae.web-security-academy.net/my-account?id=wiener

My Account

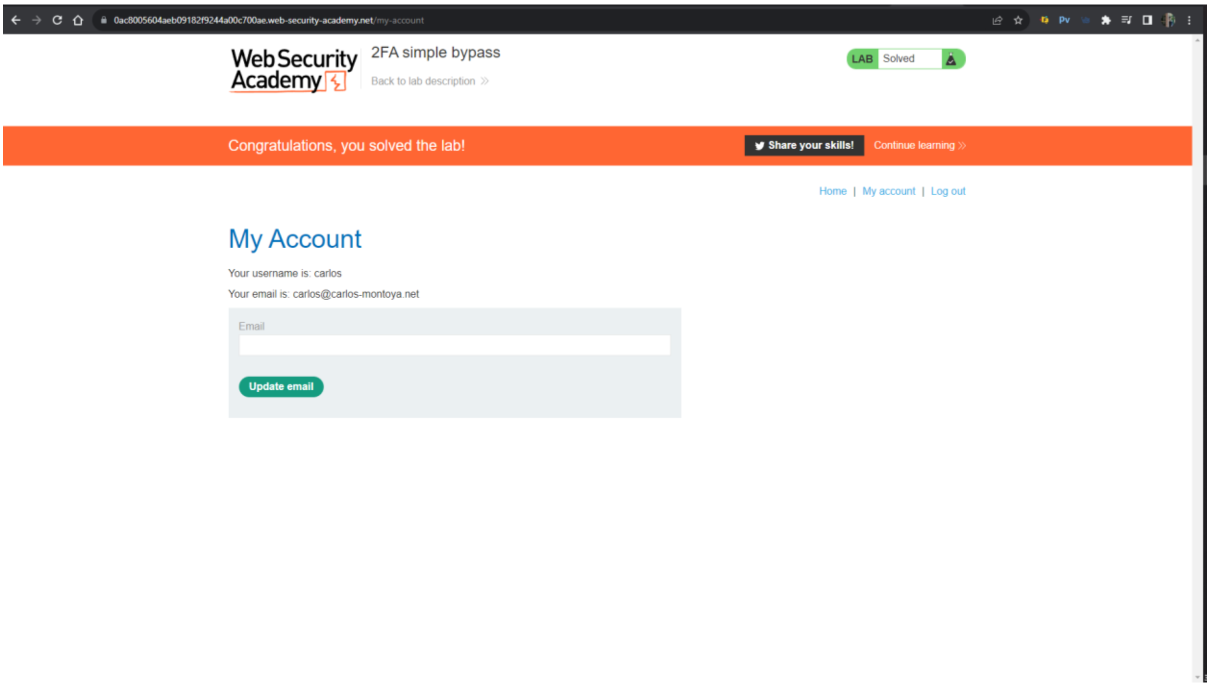
Your username is: wiener

Your email is: wiener@exploit-0aef00aa0444b0ba82bf232a01c5001c.exploit-server.net

Email:

Now we login into victims credentials

When askes for otp simply change the url to already loggen in account


0ac8005604aeb09182f9244a00c700ae.web-security-academy.net/my-account
WebSecurity Academy
2FA simple bypass
Back to lab description »
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning »
Home | My account | Log out

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Therefore this website has Security misconfiguration vulnerability