

ASSIGNMENT – 1

CHECKING THE TOP 5 CWE VULNERABILITIES 2021

Name: Harsh Pravin Gharlute

Email: harshpravin.gharlute2021@vitstudent.ac.in

BROKEN ACCESS CONTROL:

The screenshot shows a web browser displaying a store interface. The URL is aca21f9f1fde09fcc0ac32670078008f.web-security-academy.net. The page features a large "SHOP" logo at the top. Below it, there are eight product cards arranged in two rows of four. Each card includes an image, a title, a rating, a price, and a "View details" button.

Product	Rating	Price
Eggstastic, Fun, Food Eggcessories	★ ★ ★ ★ ★	\$20.22
Laser Tag	★ ★ ★ ★ ★	\$91.01
Six Pack Beer Belt	★ ★ ★ ★ ★	\$45.61
Pest Control Umbrella	★ ★ ★ ★ ★	\$32.23
Couple's Umbrella	★ ★ ★ ★ ★	\$62.50
Sprout More Brain Power	★ ★ ★ ★ ★	\$50.11
Weird Crushes Game	★ ★ ★ ★ ★	\$89.43
Cheshire Cat Grin	★ ★ ★ ★ ★	\$59.05

The screenshot shows a web browser displaying a robots.txt file. The URL is aca21f9f1fde09fcc0ac32670078008f.web-security-academy.net/robots.txt. The page contains a single line of text: "User-Agent: *\nDisallow: /administrator-panel".

i.e., the site has a vulnerability of broken access control. Because we can use the Admin panel URL is given in the .txt URL

aca21f9f1fde09fcc0ac32670078008f.web-security-academy.net/administrator-panel

YouTube Channel dashboard... Translate Python Tutorials Fo... My learning Dashboard < Hackin... harsh-bohra/Secur... learn365/day2.md a... The Hacker News ... TCM Security, Inc.

Web Security Academy Unprotected admin functionality

Back to lab description >

LAB Not solved

Home | My account

Users

carlos -	Delete
wiener -	Delete

carlos wiener

Therefore, this website has a broken access control vulnerability.

CRYPTOGRAPHIC FAILURES:

Visit a website.

Source code disclosure via backup files

Submit solution Back to lab description »

WE LIKE TO SHOP

Snow Delivered To Your Door Cheshire Cat Grin Sprout More Brain Power The Bucket of Doom

View details View details View details View details

Type here to search

14:02 29-10-2022

Change the URL of the website and add /robots.txt to find if there is some description.

The screenshot shows a browser window with the URL <https://0adc007b030f67bec0951972004f0087.web-security-academy.net/robots.txt>. The page content is:

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

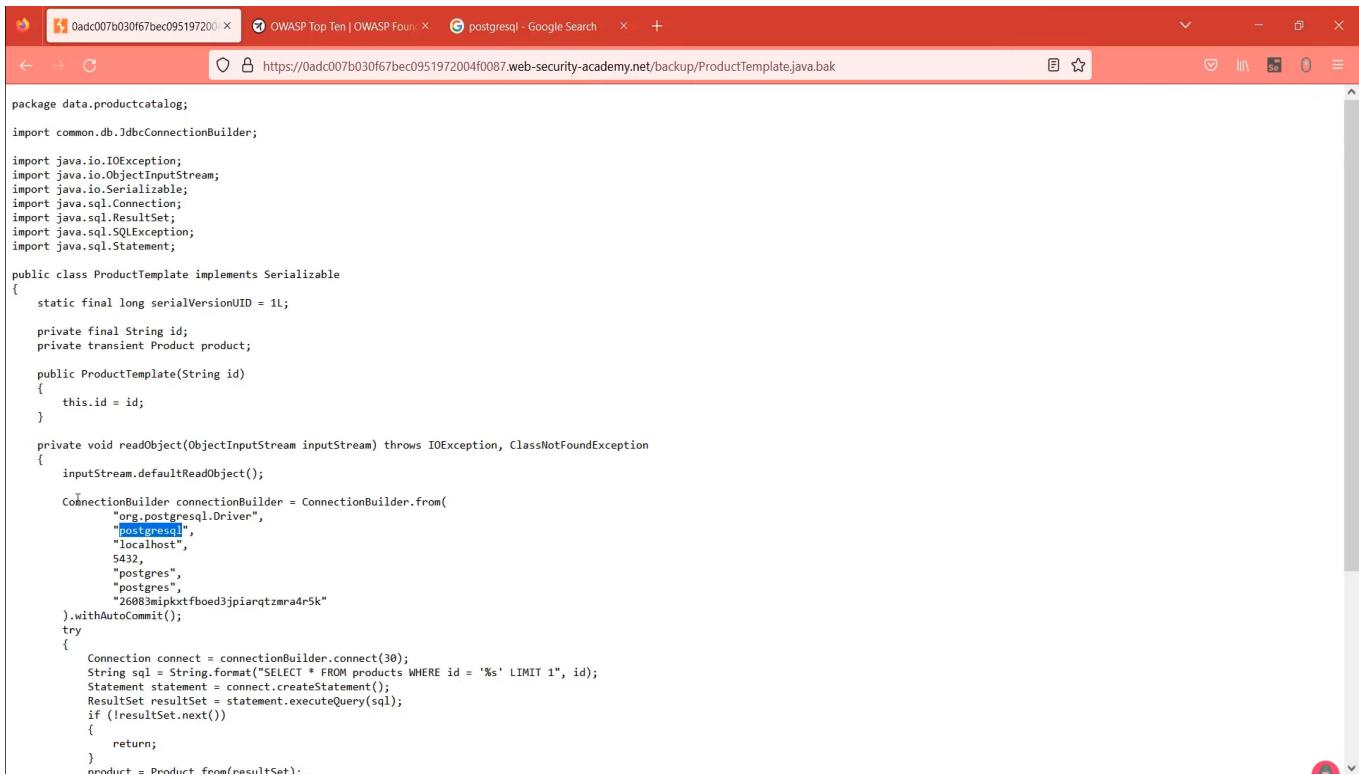
We get a disallowed URL containing a link of backup file.

The screenshot shows a browser window with the URL <https://0adc007b030f67bec0951972004f0087.web-security-academy.net/backup>. The page title is "Index of /backup". The content is:

Index of /backup

Name	Size
ProductTemplate.java.bak	1647B

We use the URL in the SITE and get the decrypted password for the backup storage of website.



The screenshot shows a Microsoft Edge browser window with the URL <https://0adc007b030f67bec0951972004f0087.web-security-academy.net/backup/ProductTemplate.java.bak>. The page content is a large block of Java code, specifically a class named ProductTemplate. The code includes imports for various Java.sql and java.io packages, a constructor taking a String id, and a readObject method that uses a ConnectionBuilder to establish a connection to a PostgreSQL database at localhost:5432, using the org.postgresql.Driver. It then executes a SELECT query to retrieve a product by its ID. The password '26083m1pkxtfb0ed3jpiarqtzmr4r5k' is stored in plain text within the SQL query.

```
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",
            "26083m1pkxtfb0ed3jpiarqtzmr4r5k"
        ).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);
        }
    }
}
```

Therefore, we can say that the website has vulnerability in cryptographic failures as the password was not stored in encrypted manner.

INJECTION:

Visit a website. E.g. AltotoMutual

(47) SQL Injections are scary! (hacking) Altoro Mutual demo.testfire.net/index.jsp

ONLINE BANKING LOGIN

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

PERSONAL

Online Banking with FREE Online Bill Pay

No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing

Fast, Simple, Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

SMALL BUSINESS

Business Credit Cards

You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions

Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

INSIDE ALTORO MUTUAL

Privacy and Security

The 2000 employees at Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

Win a Samsung Galaxy S10 smartphone

Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

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 Altoro 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/SW110>.

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

Type here to search 35°C Haze 15:24 27-08-2023

Go to the log in page:

Altoro Mutual demo.testfire.net/login.jsp

ONLINE BANKING LOGIN

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:

Password:

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 Altoro 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/SW110>.

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

Type here to search 35°C Haze 15:24 27-08-2023

Altoro Mutual demo.testfire.net/login.jsp

AltoroMutual

PERSONAL

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

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Risk Management
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

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

Sign Off | Contact Us | Feedback | Search | Go | DEMO SITE ONLY

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

The Altoro 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/SW110>.

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



We get error saying wrong username and password.

Altoro Mutual demo.testfire.net/login.jsp

AltoroMutual

PERSONAL

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

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Risk Management
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

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

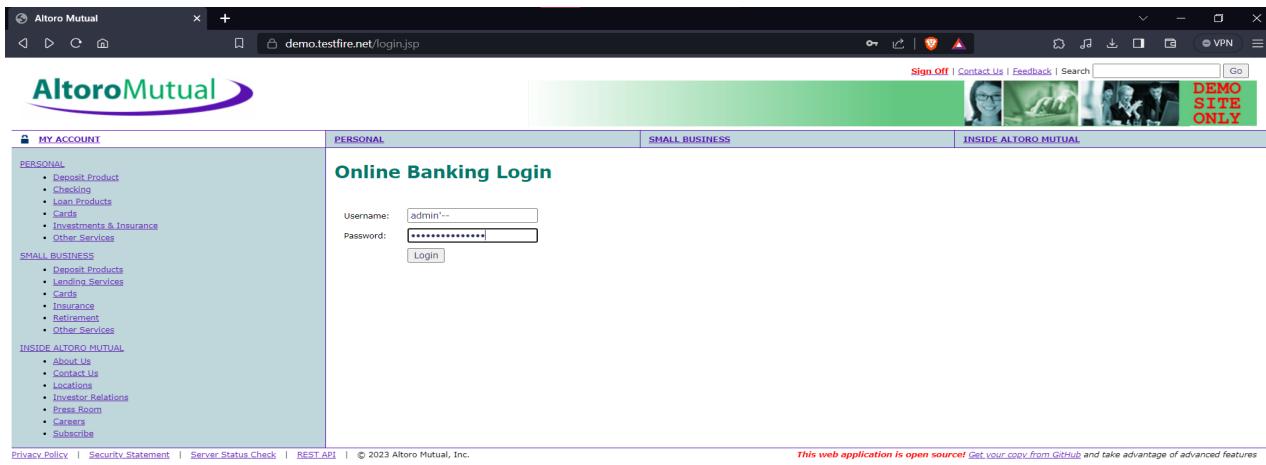
Sign Off | Contact Us | Feedback | Search | Go | DEMO SITE ONLY

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

The Altoro 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/SW110>.

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





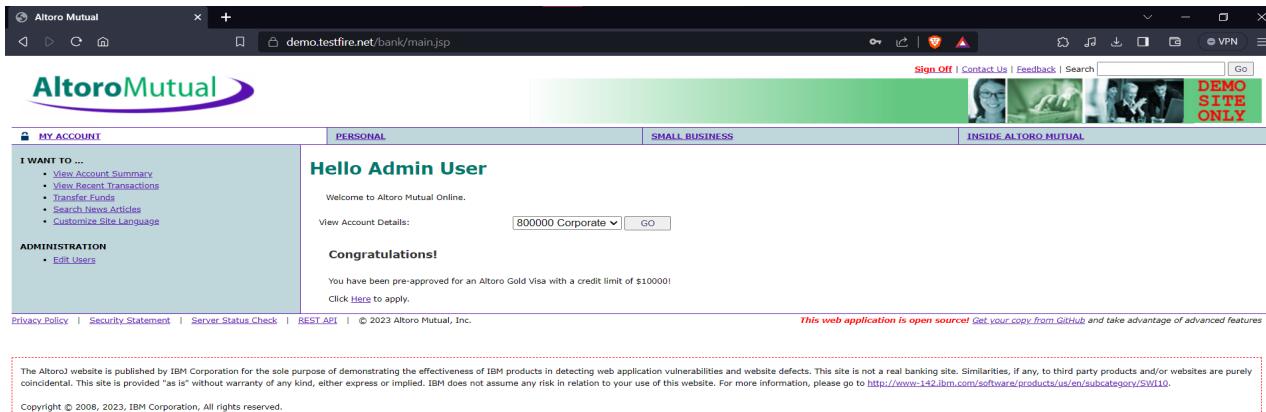
This web application is open source! Get your copy from GitHub and take advantage of advanced features.

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/SW110>.

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



We successfully log in!!



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/SW110>.

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

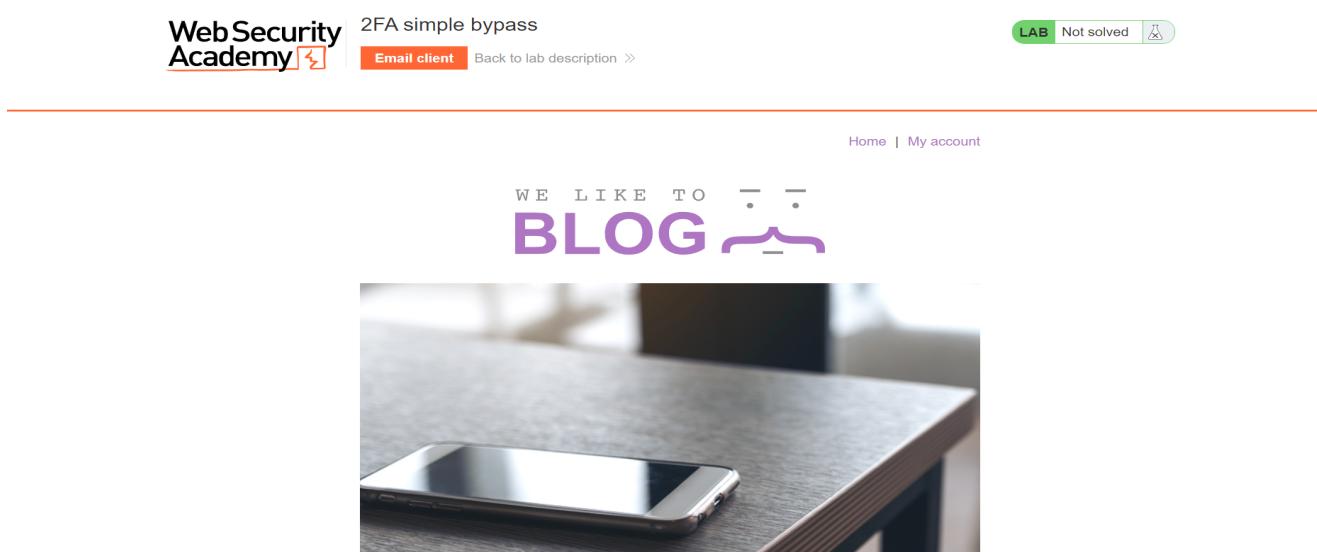


Therefore, this website has SQL injection vulnerabilities.

INSECURE DESIGN:

SECURITY MISCONFIGURATION:

We got to a Blog wesbiste:



LOG IN USING THE GIVEN CREDENTIALS:

A screenshot of a 'Login' form from 'Web Security Academy'. The top navigation bar is identical to the previous screenshot. The main form has 'Username' and 'weiner' in the input field, 'Password' and '****' in the input field, and a 'Log in' button at the bottom.

Enter the OTP given in the email:

The screenshot shows the '2FA simple bypass' lab from the Web Security Academy. At the top, there are navigation links: 'Back to lab home', 'Email client', and 'Back to lab description >'. A green 'LAB' button indicates it's not solved yet. The main area contains a form with a placeholder 'Please enter your 4-digit security code' and a text input field containing '1313'. Below the input is a green 'Login' button.

We logged in successfully.

Now we notice the URL of the logged in account.

The screenshot shows a browser window with the URL <https://ac0a1f441fc4fb1c076774a002e00da.web-security-academy.net/my-account>. The page title is 'My Account'. It displays the user's information: 'Your username is: wiener' and 'Your email is: wiener@exploit-ac351fa11fd4fa8c0d27767014800c2.web-security-academy.net'. There is a form with an 'Email' input field containing the same email address and a green 'Update email' button.

Now we log in with victim's credentials,

Congratulations, you solved the lab!

[Share your skills!](#) [Continue learning >](#)

Login

Username
carlos

Password

Log in

we change the URL to the same URL of that of the logged in account.

The screenshot shows a browser window with the following details:

- Address Bar:** https://ac0af441f1c4fb1c076774a002e00da.web-security-academy.net/my-account
- Toolbar:** Shows various browser extensions and icons.
- Status Bar:** Not solved (with a refresh icon).
- Content Area:** A login form with a placeholder "Please enter your 4-digit security code" and a "Login" button.

WE LOG IN SUCCESSFULLY !!!

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

Email

 Update email

Therefore, this website has Security misconfiguration vulnerability.