Shaheed Sukhdev College of Business Studies

University of Delhi

Post Graduate Diploma in Cyber Security and Law

Sakshi Garg • Roll no-23726 • Subject-Web Applications • Semester-1

Insecure Design and Security Misconfiguration

It arises in the website, server when configuration is not properly configured. It is important to ensure that the application frameworks and server have secured settings We can access someones account information, unsecured files, unencrypted files

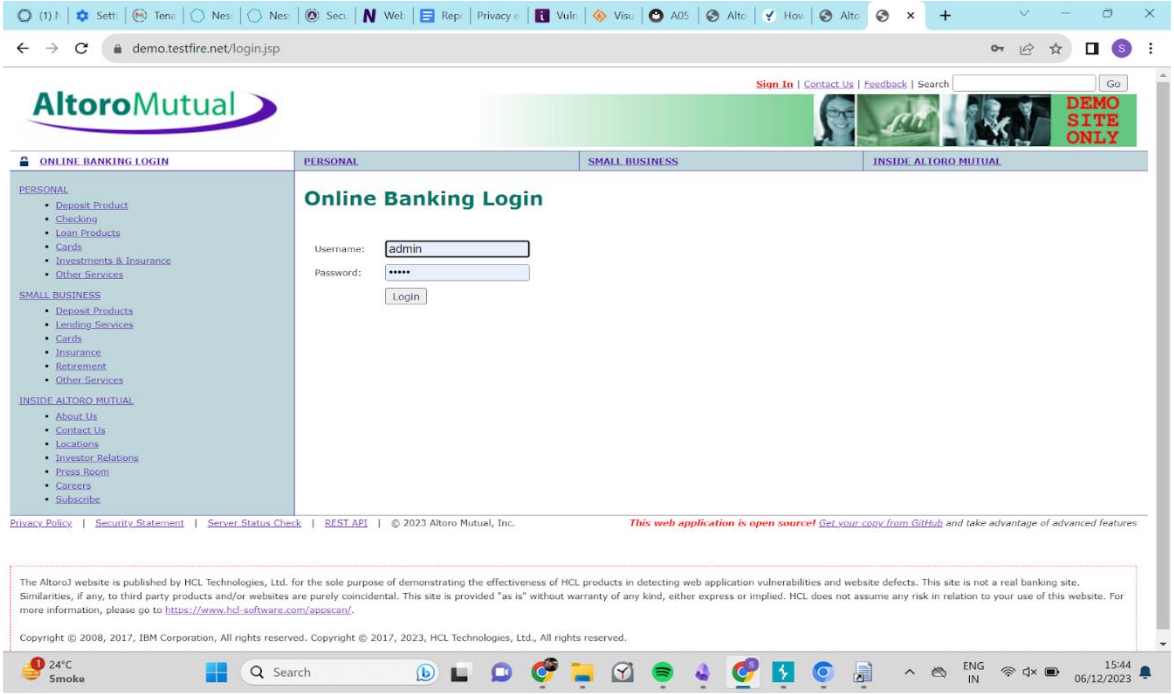
Preventions -
There should be a revealer test for the website security,there should be regular audits , we should avoid unused features

References-

1. https://www.aquasec.com/cloud-native-academy/supply-chain-security/security-misconfigurations/#:~:text=Prevent%20Security%20Misconfiguration-,What%20Is%20a%20Security%20Misconfiguration%3F,in%20cloud%20and%20network%20infrastructure.
2. https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

POC

Steps 1 - open demo.testfire.net -> login -> login as username & pass ‘admin’ .
On the dashboard right click inspect -> storage -> go on cookies -> view the site -> copy the session -> paste in notepad -> go on any other browser like chrome -> open demo.testfire.net -> right click on screen -> go on inspect element -> go on application -> click on cookie - >select the cookies present -> delete it and paste the session id present in notepad -> close the window and reload the site



demo.testfire.net/login.jsp

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

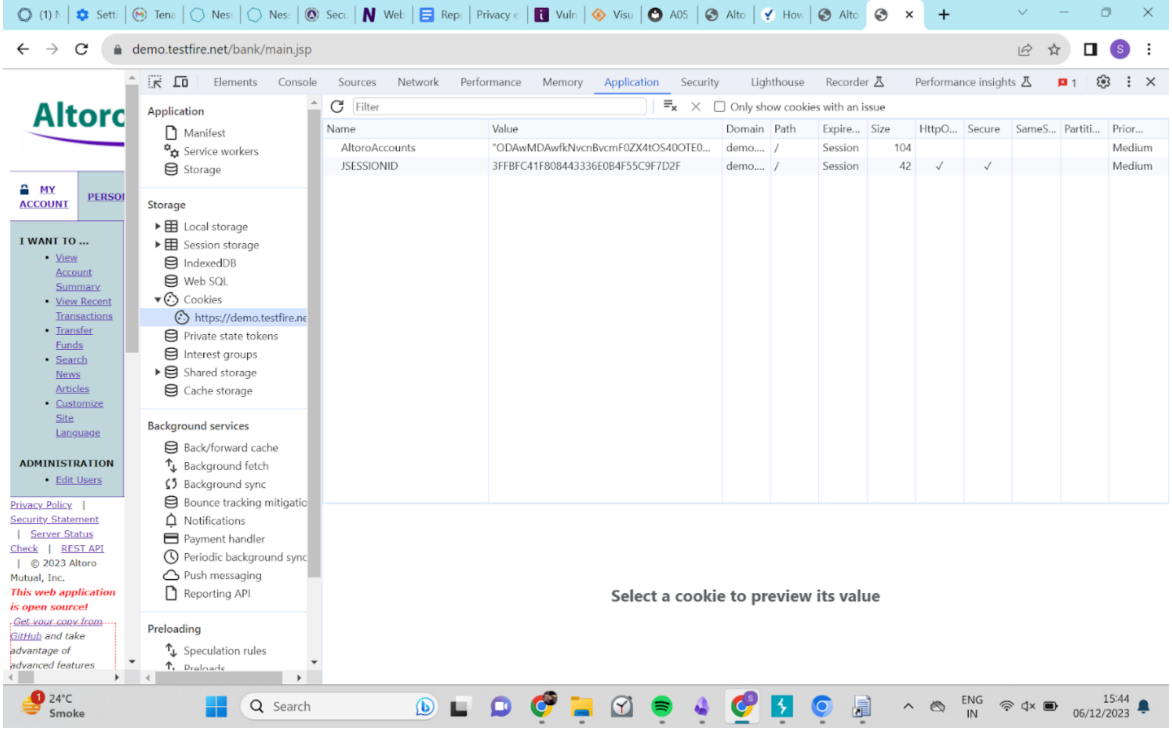
Password: •••••

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 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.hcl-software.com/appscan/.

Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2023, HCL Technologies, Ltd., All rights reserved.



demo.testfire.net/bank/main.jsp

MY ACCOUNT | PERSO

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

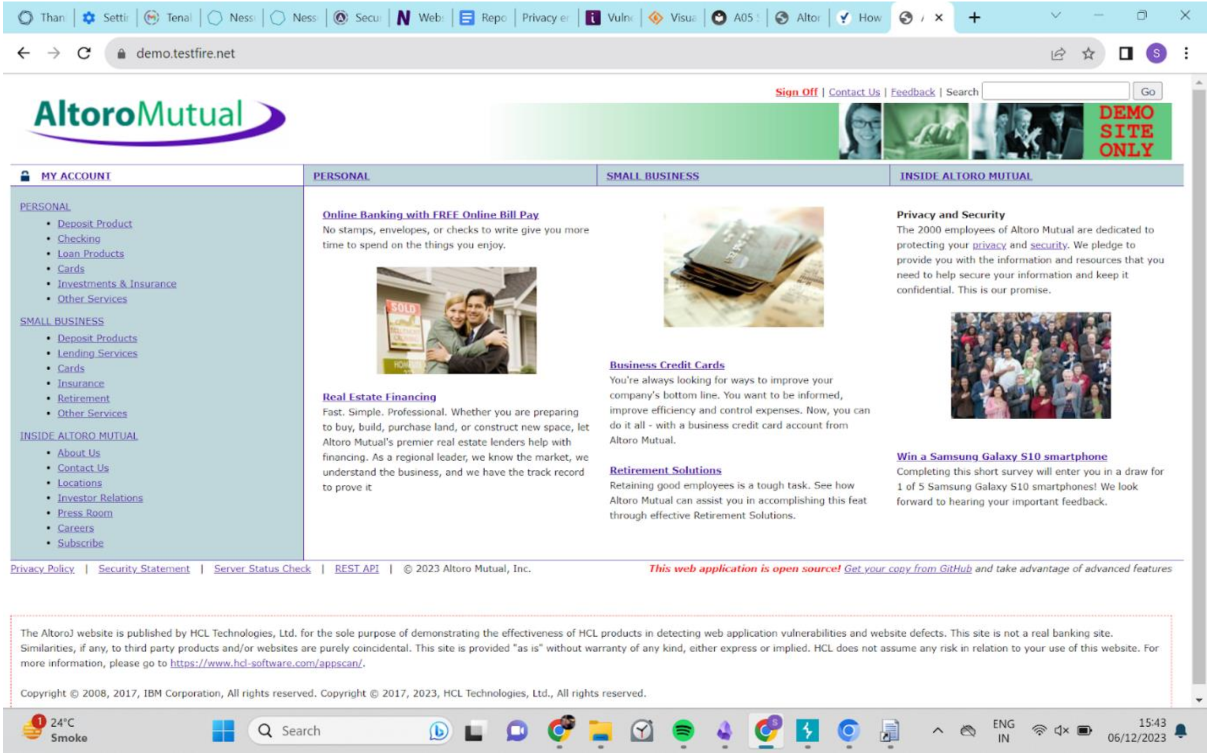
ADMINISTRATION
- Edit Users

Filter ☐ Only show cookies with an issue

Name	Value	Domain	Path	Expire...	Size	HttpO...	Secure	SameS...	Partiti...	Prior...
AltoroAccounts	"ODAwMDAwfkNvcnBvcmF0ZX4tOS40OTE0...	demo....	/	Session	104					Medium
JSESSIONID	3FFBFC41F808443336E0B4F55C9F7D2F	demo....	/	Session	42	✓	✓			Medium

Select a cookie to preview its value

Step 2 - login screen will present



Sign Off | Contact Us | Feedback | Search Go

MY ACCOUNT | 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 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

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.

Privacy and Security
The 2000 employees of 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 AltoroJ 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.hcl-software.com/appscan/.