

# AI FOR CYBERSECURITY WITH IBM QURADAR

## ASSIGNMENT – 1

### PERFORMING VULNERABILITIES ON WEBSITES

NAME: SHIVANSHU TIWARI

BRANCH: CSE – DATA SCIENCE

COLLEGE: VIT – VELLORE

- **BROKEN ACCESS CONTROL**

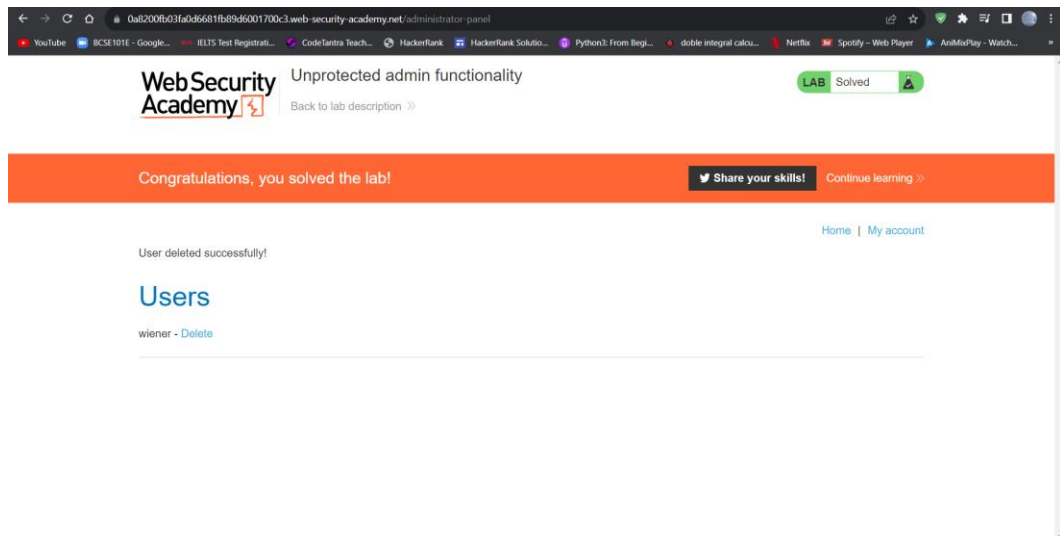
A broken access control vulnerability refers to a security weakness that permits an individual without proper authorization to gain entry to limited sections of a website. This compromise can encompass confidential data like financial details, clientele records, or intellectual assets. Malicious actors exploit these vulnerabilities to purloin information, engage in deceitful activities, or hinder regular operations.

i) **Unprotected Admin Funtionality**

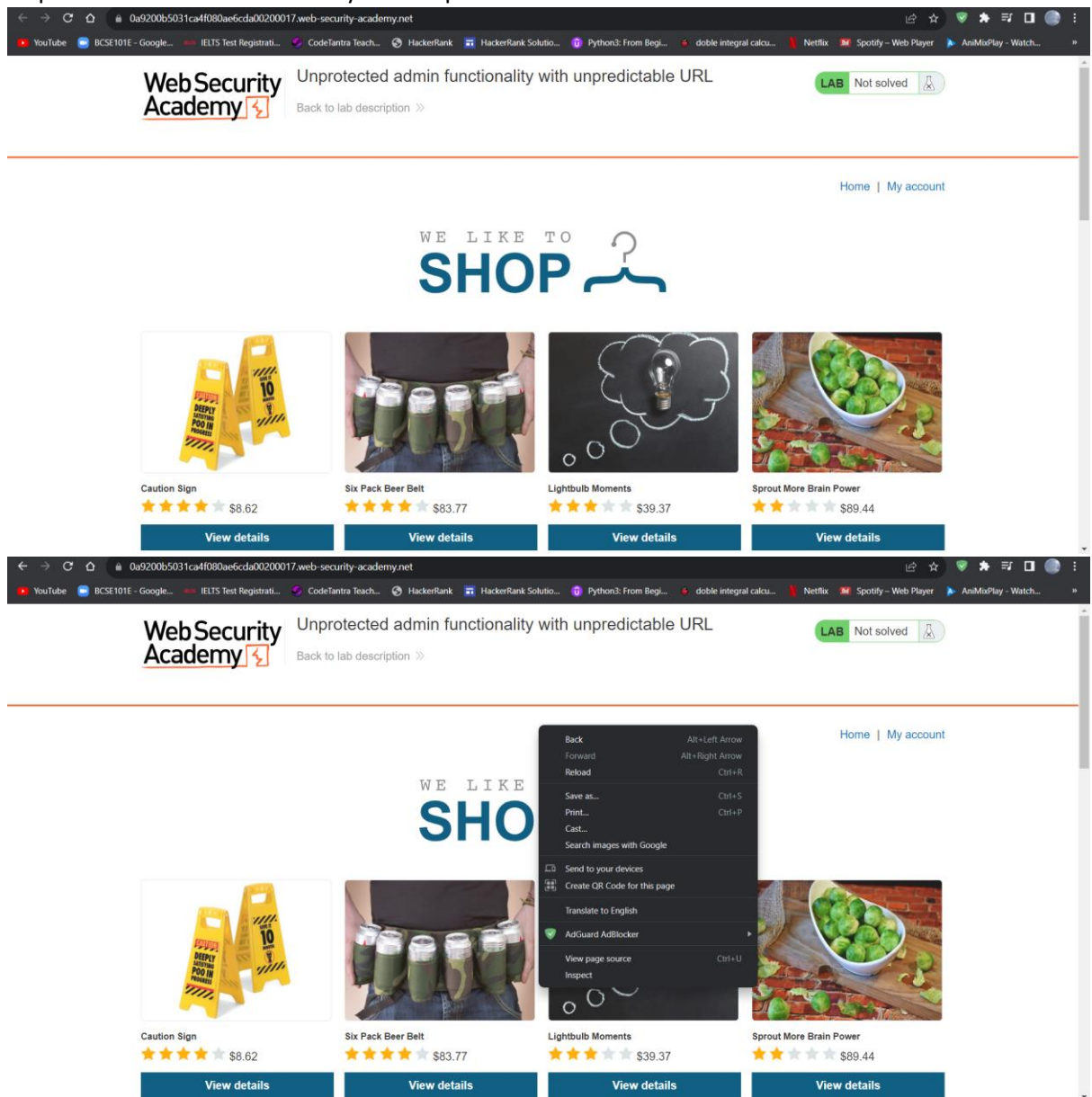
The image displays two screenshots of the WebSecurity Academy interface during a lab exercise titled "Unprotected admin functionality".

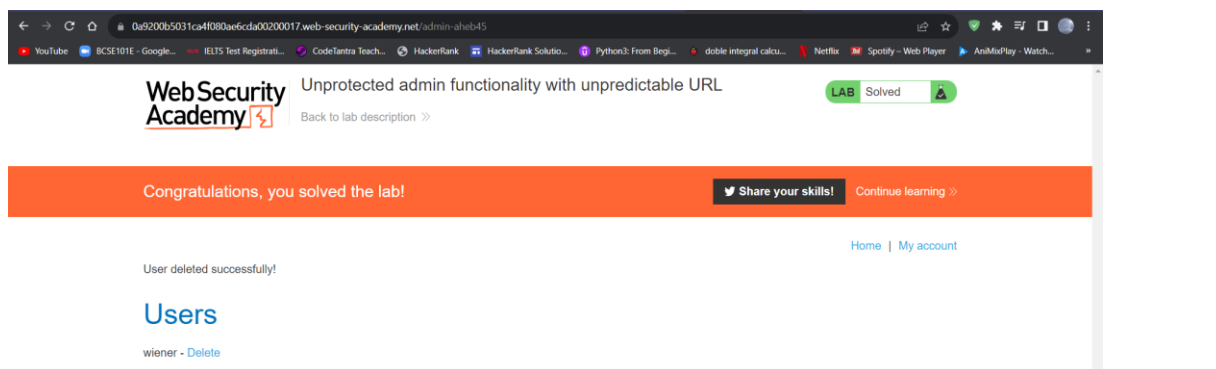
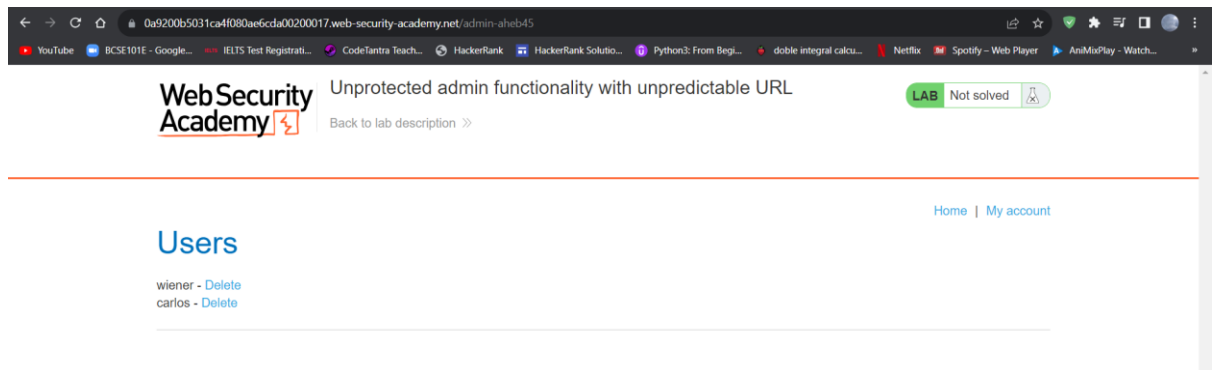
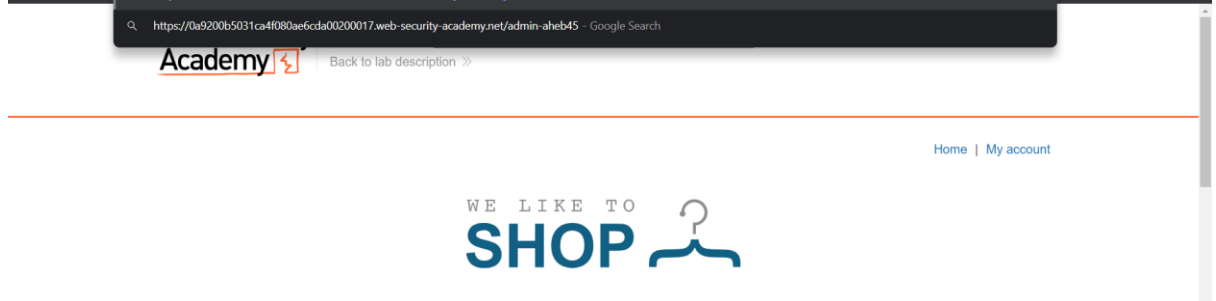
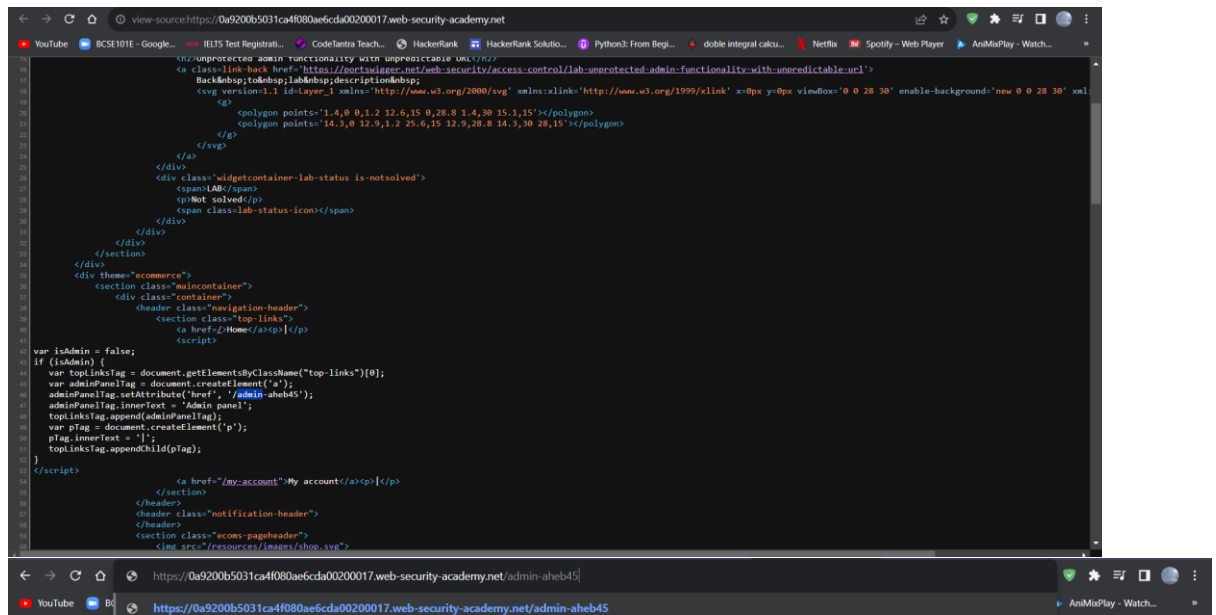
**Top Screenshot:** Shows the lab page with a green "LAB Solved" status. Below the lab title, a congratulatory message reads "Congratulations, you solved the lab!". The main content area displays a "WE LIKE TO SHOP" banner with four product listings: "Padding Pool Shoes" (\$71.65), "Couple's Umbrella" (\$40.20), "The Giant Enter Key" (\$98.36), and "Photobomb Backdrops" (\$97.54). The bottom navigation bar includes "Home" and "My account" links.

**Bottom Screenshot:** Shows the "Unprotected admin functionality" lab page with a green "LAB Not solved" status. Below the lab title, a "Back to lab description" link is visible. The main content area displays a "Users" section with a list of users: "wiener" (with a "Delete" link) and "carlos" (with a "Delete" link). The bottom navigation bar includes "Home" and "My account" links.



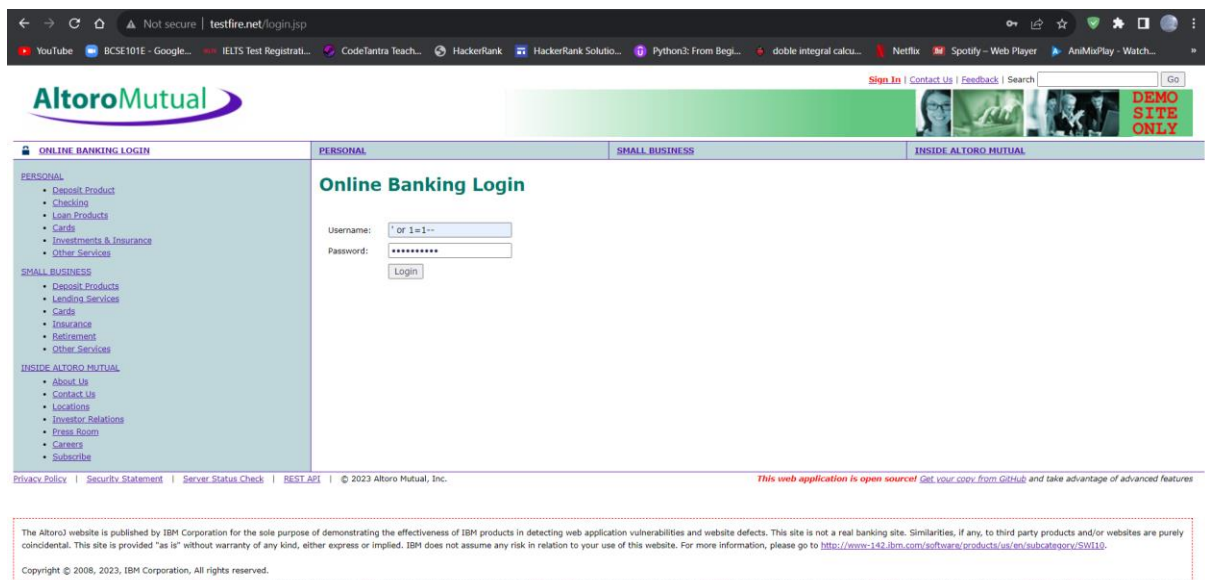
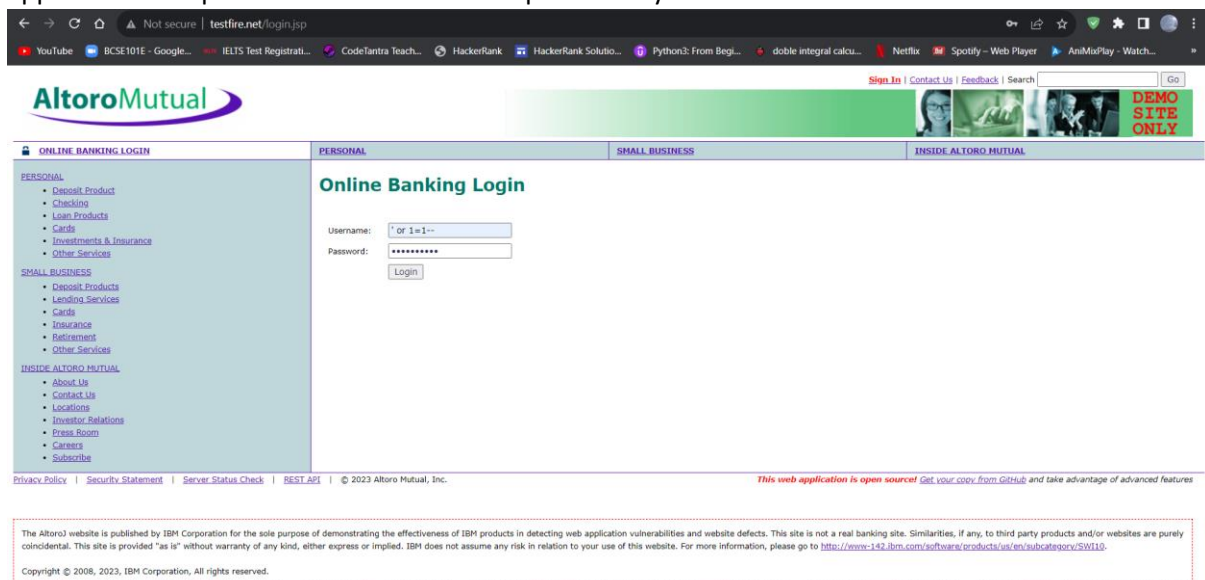
ii) Unprotected admin functionality with unpredicted URL





## • SQL INJECTION

SQL injection is a form of attack that takes advantage of weaknesses in web applications utilizing SQL databases. This technique enables a malicious actor to insert harmful code into a database query, subsequently enabling data theft, data manipulation, or potential commandeering of the database server. SQL injection vulnerabilities can manifest through different avenues, but they are most prevalent when a web application accepts user input and employs this input directly within a database query, neglecting prior validation. As an instance, a vulnerable scenario could arise in a web application that permits users to search for products by their names.



## • CROSS SITE SCRIPTING VULNERABILITY ASSESSMENT

The process of cross-site scripting (XSS) vulnerability assessment involves recognizing and resolving susceptibilities within a website that could be abused by malicious individuals to insert harmful code into the site. XSS vulnerabilities are detectable across various locations, including:

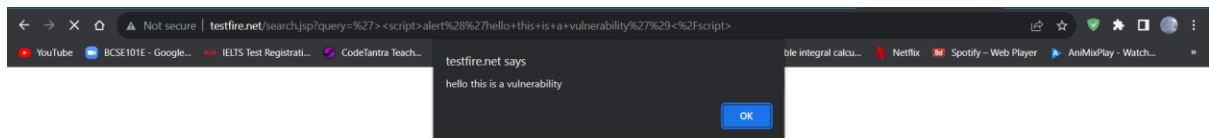
1. Form input fields
2. URL parameters
3. HTTP headers
4. Comment sections
5. Error prompts

Once an XSS vulnerability is pinpointed, attackers can capitalize on it to pilfer cookies, session tokens, or other sensitive data. Moreover, they can exploit it to reroute users to malevolent websites or to execute arbitrary JavaScript code within the victim's web browser.

The screenshot shows the AltoroMutual website with a search bar at the top right. The search bar contains the payload `<script>alert('hacked')</script>`. An alert box is visible on the right side of the page, displaying the text "hacked". The website layout includes a navigation bar with links like "Sign In", "Contact Us", and "Feedback". The main content area is divided into sections for "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The footer contains a disclaimer: "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/30110>. Copyright © 2008, 2023, IBM Corporation, All rights reserved."

This screenshot shows a different view of the AltoroMutual website, specifically the "INSIDE ALTORO MUTUAL" section. The search bar at the top right still contains the payload `<script>alert('hacked')</script>`. The page layout includes a navigation bar with links like "Sign In", "Contact Us", and "Feedback". The main content area is divided into sections for "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The footer contains a disclaimer: "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/30110>. Copyright © 2008, 2023, IBM Corporation, All rights reserved."

This screenshot shows the "Privacy and Security" page of the AltoroMutual website. The search bar at the top right still contains the payload `<script>alert('hacked')</script>`. The page layout includes a navigation bar with links like "Sign In", "Contact Us", and "Feedback". The main content area is divided into sections for "PERSONAL", "SMALL BUSINESS", and "INSIDE ALTORO MUTUAL". The footer contains a disclaimer: "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/30110>. Copyright © 2008, 2023, IBM Corporation, All rights reserved."



- **AUTHENTICATION FLAWS**

Authentication flaws denote vulnerabilities present in websites or web applications that permit a malicious actor to masquerade as an authorized user. These vulnerabilities arise from weaknesses in the authentication procedures, such as frail passwords, substandard session management, or insecure password reset processes.

Several prevalent instances of broken authentication vulnerabilities encompass:

1. **Weak passwords:** Passwords that are brief, easily guessed, or reused across multiple platforms pose substantial security threats. Adversaries can readily decipher these passwords using tactics like brute-force or dictionary attacks.
2. **Inadequate session management:** Poorly implemented session management opens the door for attackers to purloin session cookies or tokens, enabling them to impersonate valid users. This scenario can unfold if sessions remain valid even after users log out, or if session cookies lack encryption.
3. **Unsecure password reset mechanisms:** If password reset mechanisms lack robust security measures, wrongdoers can exploit them to access user accounts. This vulnerability can be exploited if password reset emails are dispatched without verification, or if safeguards for password reset tokens



are insufficiently established.

The image shows two screenshots of the AltoroMutual website. The top screenshot is the 'Online Banking Login' page. It features a navigation bar with 'PERSONAL', 'SMALL BUSINESS', and 'INSIDE ALTORO MUTUAL' tabs. The 'PERSONAL' tab is active, showing a sidebar with links to 'Deposit Products', 'Checking', 'Loan Products', 'Cards', 'Investments & Insurance', and 'Other Services'. The main content area has a 'Hello Jane Doe' greeting and a login form with fields for 'Username' (containing 'jdoe') and 'Password' (masked with dots), and a 'Login' button. The bottom of the page includes a footer with 'Privacy Policy', 'Security Statement', 'Server Status Check', 'BEST API', and '© 2023 Altoro Mutual, Inc.'. A red banner at the bottom states 'This web application is open source! Get your copy from GitHub and take advantage of advanced features'. The bottom screenshot is the 'MY ACCOUNT' page. It shows the same navigation bar and sidebar. The main content area has a 'Hello Jane Doe' greeting and a 'View Account Details' section with a dropdown menu showing '800004 Savings' and a 'GO' button. Below this, it says 'Congratulations!' and 'You have been pre-approved for an Altoro Gold Visa with a credit limit of \$10000!'. The footer is identical to the top screenshot, but the red banner is absent. A small disclaimer at the bottom states '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-147.ibm.com/software/products/us/en/subcategory/50110>. Copyright © 2008, 2023, IBM Corporation. All rights reserved.'


- EXPOSURE OF SENSITIVE DATA (DUE TO ACCESS CONTROL BREACH)

A vulnerability involving the exposure of sensitive data within a website refers to a security weakness that enables an unauthorized individual to retrieve confidential information not meant for public access. This data can encompass:



1. Personally identifiable information (PII), such as names, addresses, and Social Security numbers
2. Financial particulars, including credit card numbers and bank account details
3. Login credentials, like passwords and API keys
4. Intellectual assets, such as trade secrets and product blueprints

The repercussions of sensitive data exposure vulnerabilities can be grave for both enterprises and individuals. When an attacker gains entry to sensitive information, they could exploit it

for identity theft, fraudulent activities, or other unlawful acts. This data could also be sold to other wrongdoers or leveraged for purposes of extortion against the victim.



[Sign Off](#) | [Contact Us](#) | [Feedback](#) |



[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](#)

## Hello Jane Doe

Welcome to Altoro Mutual Online.

View Account Details:

**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](#) | [BEST 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-152.ibm.com/software/products/us/en/subcategory/50W10>.

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



[Sign Off](#) | [Contact Us](#) | [Feedback](#) |



[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](#)

## Account History - 800004 Savings

Balance Detail	
<input type="text" value="800004 Savings"/>	<input type="button" value="Select Account"/>
Amount	
Ending balance as of 8/28/23 5:20 AM	-\$18446744078004150000.00
Available balance	-\$18446744078004150000.00

### 10 Most Recent Transactions

Date	Description	Amount
2023-08-28	Withdrawal	-\$8888.00
2023-08-28	Withdrawal	-\$8888.00
2023-08-28	Withdrawal	-\$18446744073709552000.00
2023-08-28	Withdrawal	-\$4294967297.00
2023-08-28	Withdrawal	\$10000000000000000000.00
2023-08-28	Withdrawal	-\$10000000000000000000.00
2023-08-28	Withdrawal	-\$8888.00

### Credits

Account	Date	Description	Amount
1001160140	12/29/2004	Paycheck	1200
1001160140	01/12/2005	Paycheck	1200
1001160140	01/29/2005	Paycheck	1200
1001160140	02/12/2005	Paycheck	1200