AI FOR CYBERSECURITY WITH IBM QURADAR

ASSIGNMENT – 1

PERFORMING VULNERABILITIES ON WEBSITES

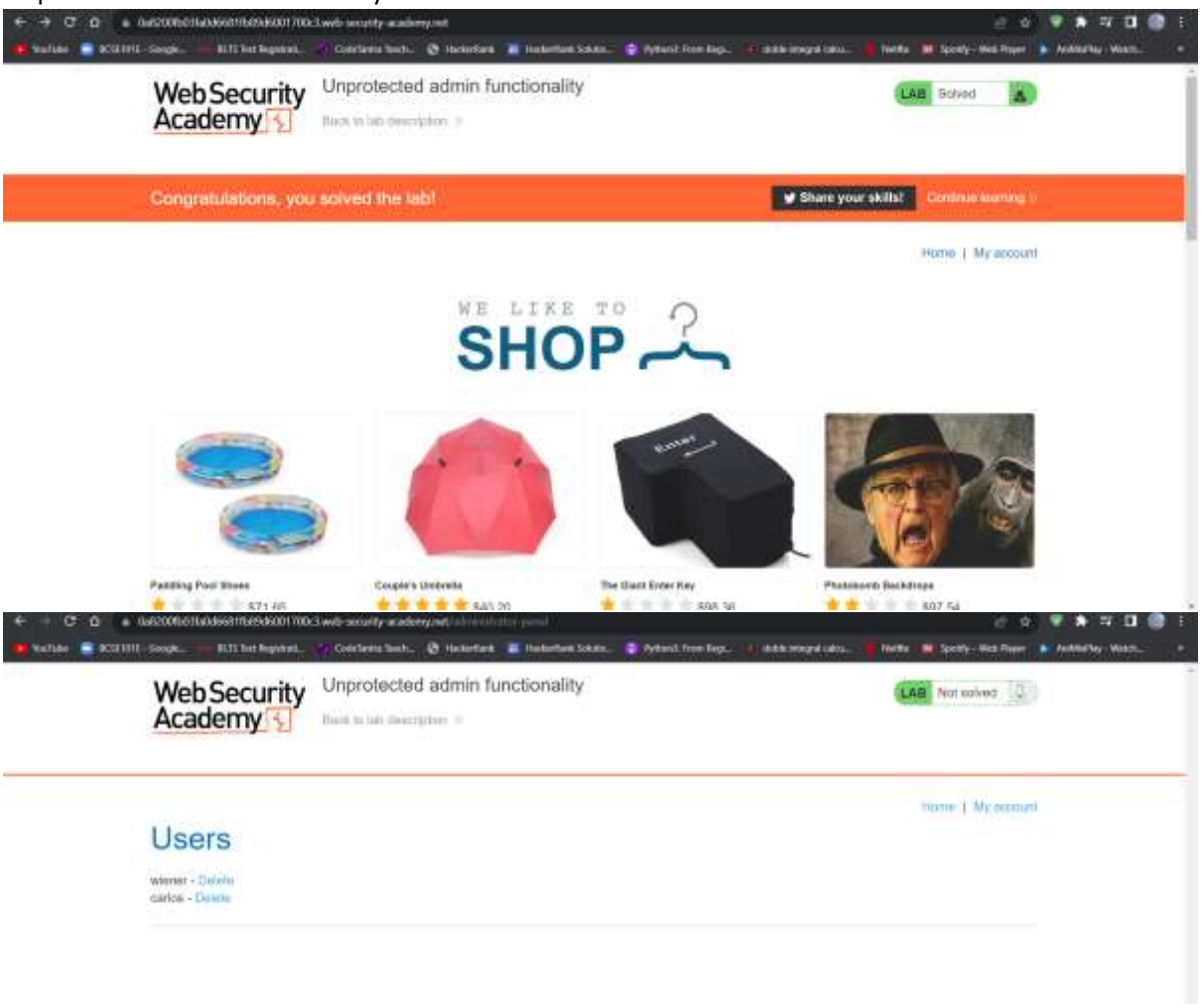
NAME: ORRA RAGHAVENDRA REDDY

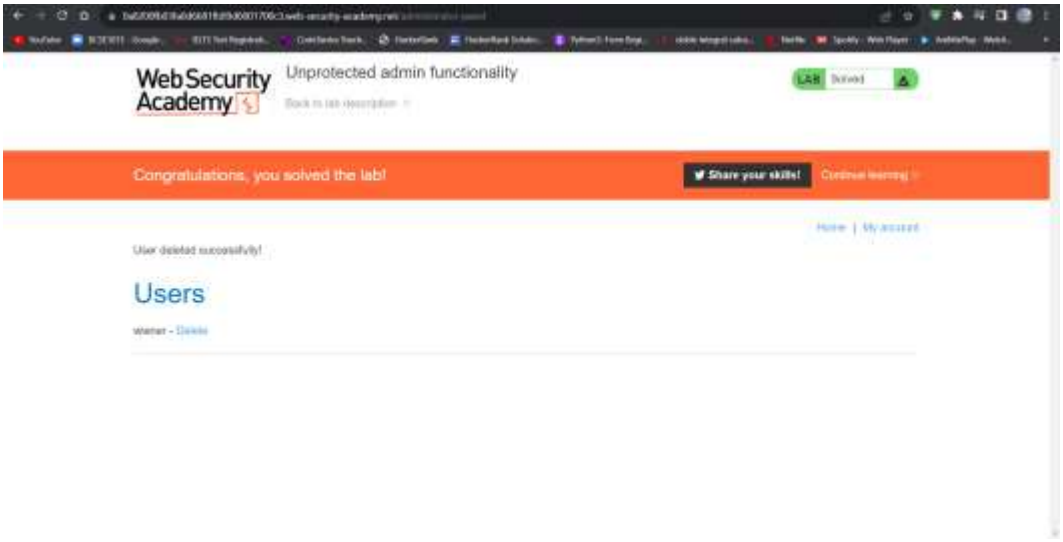
BRANCH: CSE – INFORMATIION SECURITY

COLLEGE: VIT – VELLORE

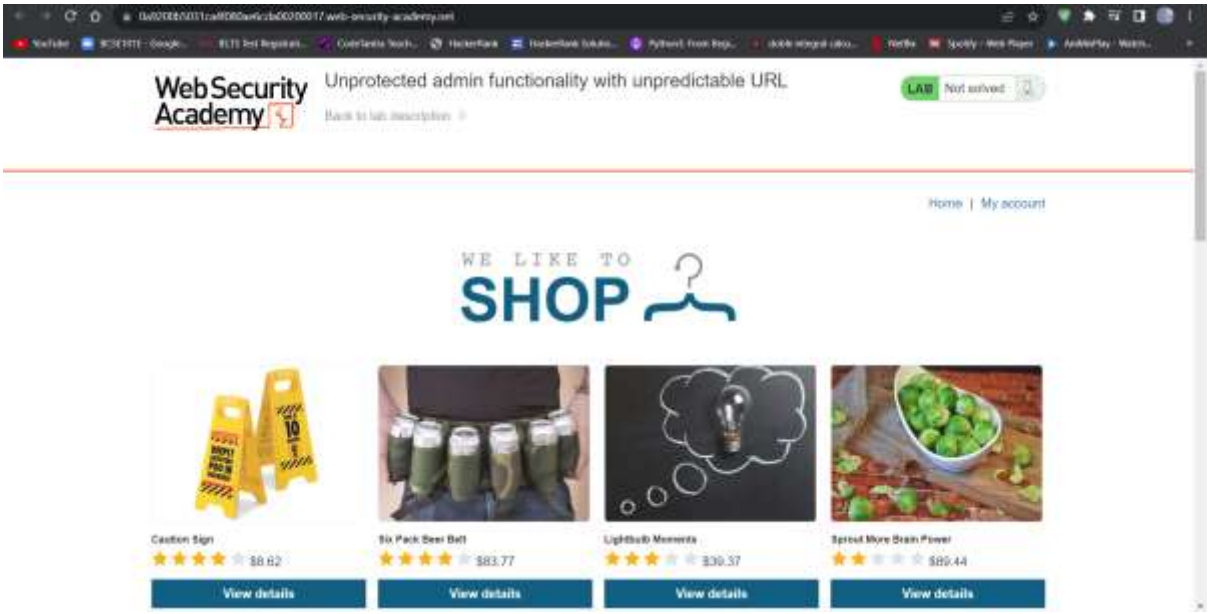
- BROKEN ACCESS CONTROL
  A broken access control vulnerability is a security flaw that allows an unauthorized user to access restricted resources on a website. This can include sensitive information such as financial data, customer records, or intellectual property. Broken access control vulnerabilities can be exploited by attackers to steal data, conduct fraud, or disrupt operations.

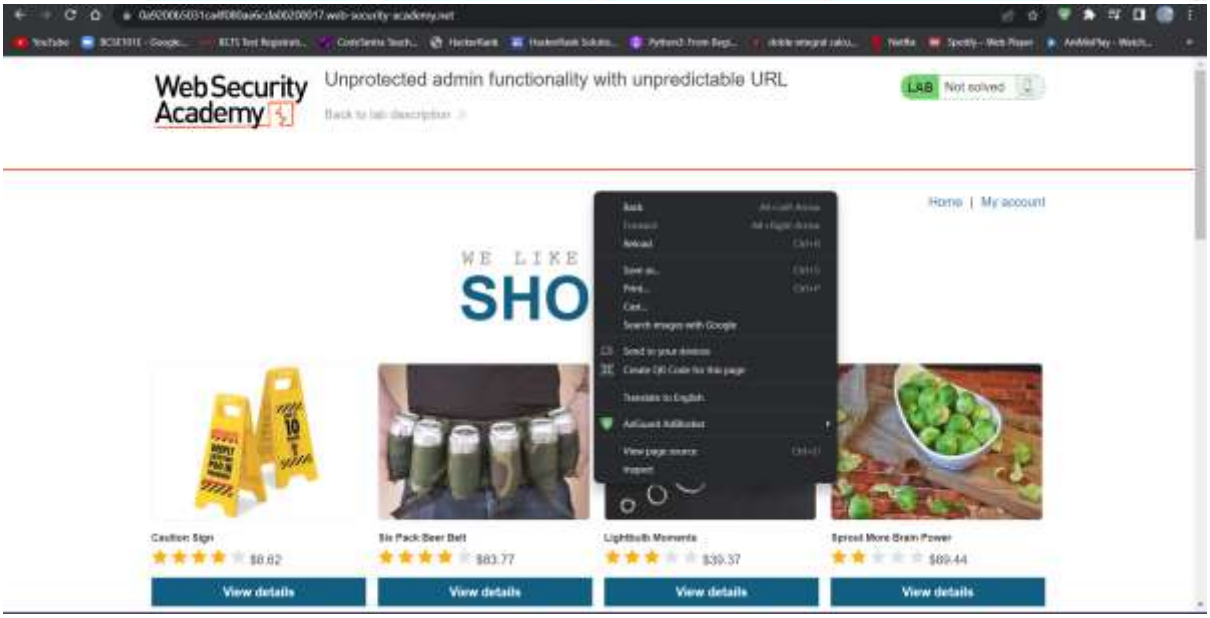
  i) Unprotected Admin Funtionality

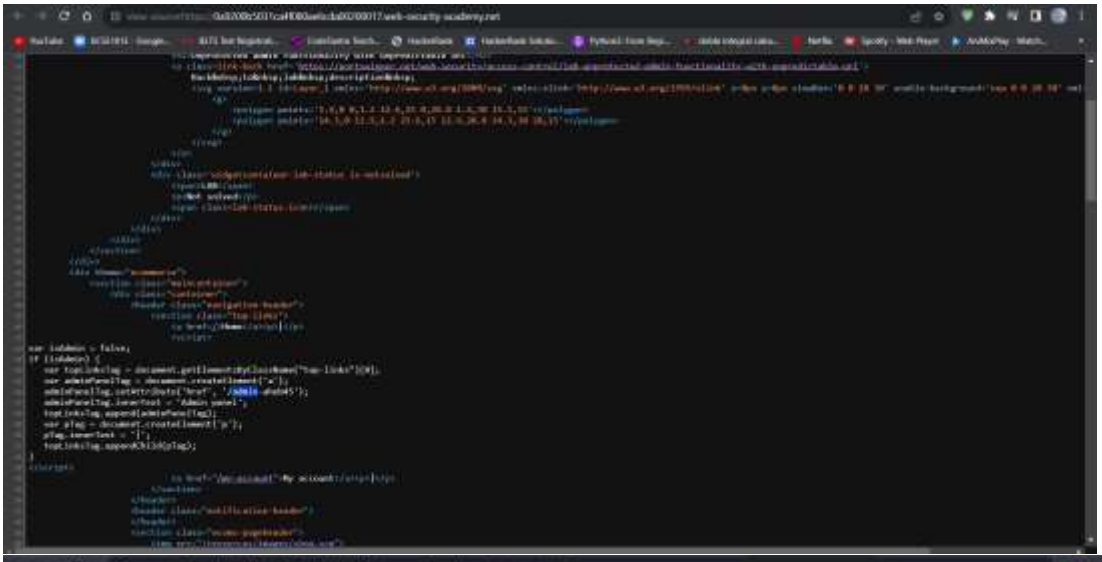




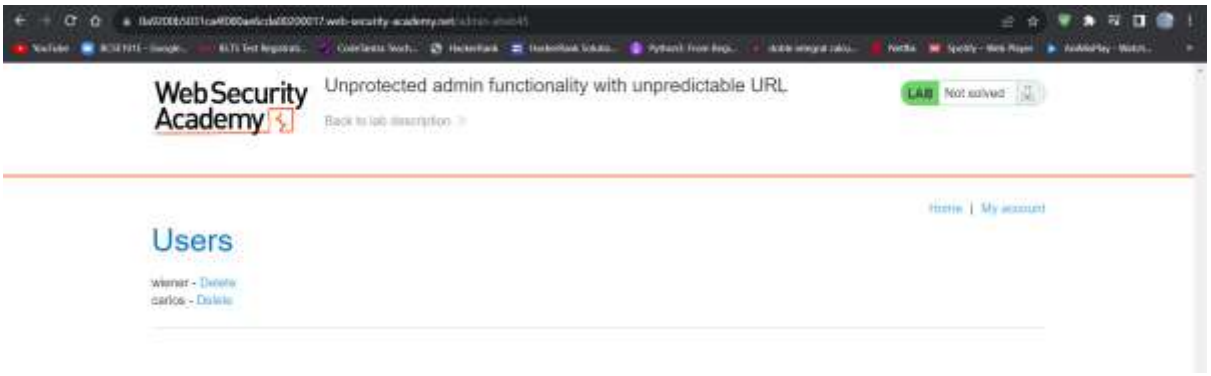
ii) Unprotected admin functionality with unpredicted URL

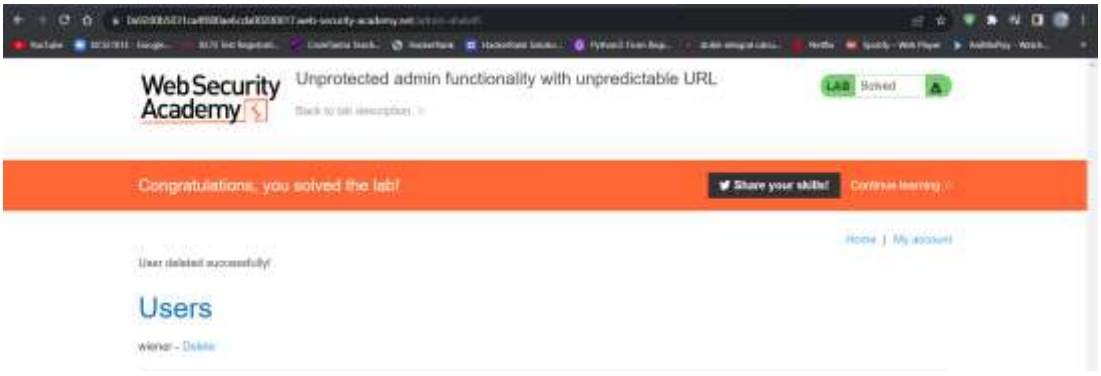




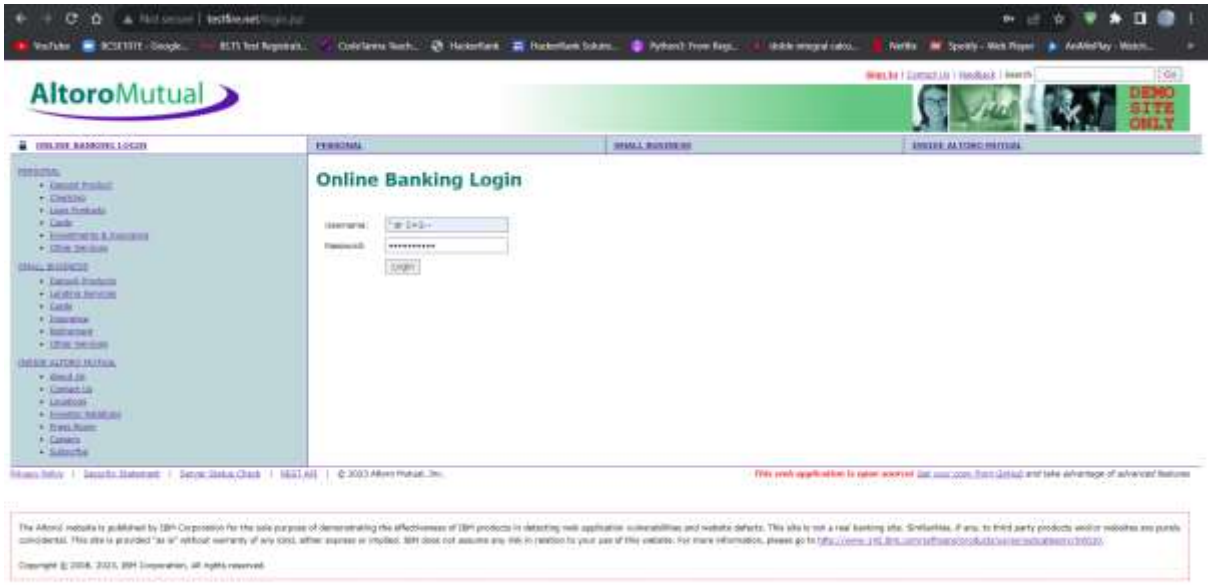


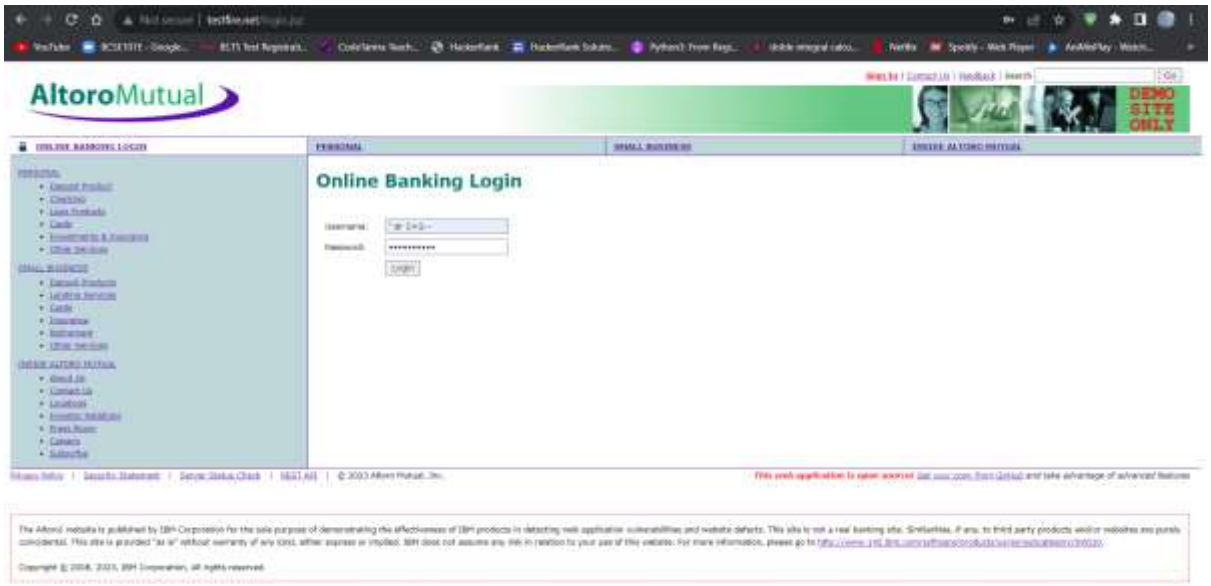

Academy
Back to lab description
Home | My account
WE LIKE TO
SHOP


Web Security
Academy
Unprotected admin functionality with unpredictable URL
Back to lab description
LAB Not solved
Home | My account
Users
wiener - Delete
carlos - Delete


Web Security
Academy
Unprotected admin functionality with unpredictable URL
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account
User deleted successfully!
Users
wiener - Delete

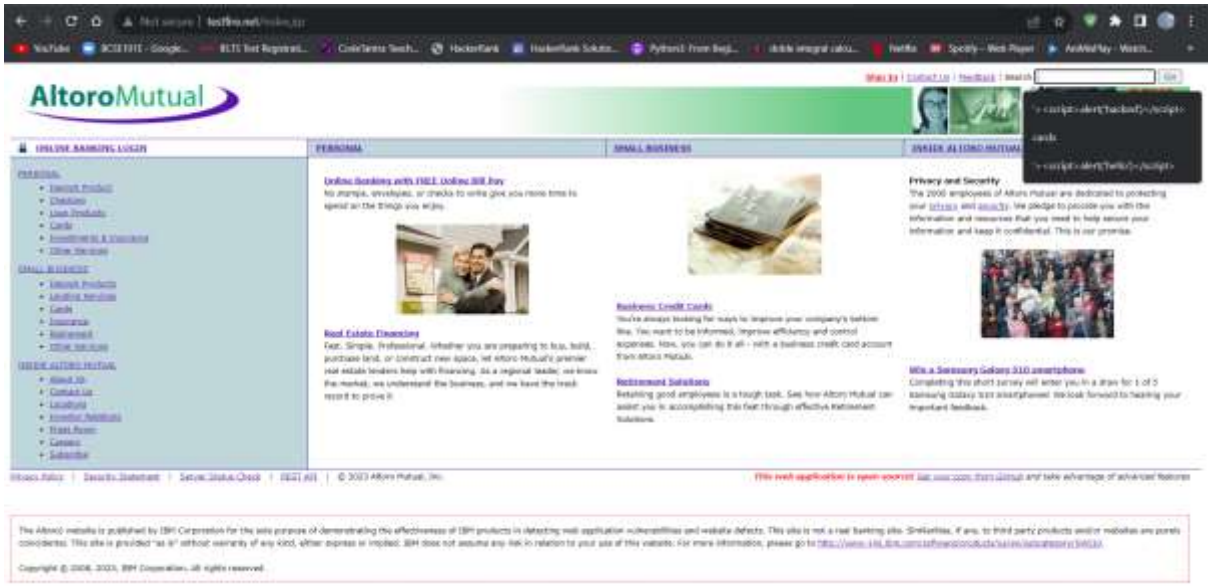
- SQL INJECTION
  SQL injection is a type of attack that exploits vulnerabilities in web applications that use SQL databases. It allows an attacker to inject malicious code into a database query, which can then be used to steal data, modify data, or even take control of the database server. SQL injection vulnerabilities can occur in a variety of ways, but they most commonly occur when a web application accepts user input and then uses that input directly in a database query without validating it first. For example, a web application that allows users to search for products by name might be vulnerable to SQL injection.





- CROSS SITE SCRIPTING VULNERABILITY CHECKING
  Cross-site scripting (XSS) vulnerability checking is the process of identifying and mitigating vulnerabilities in a website that could be exploited by attackers to inject malicious code into the website. XSS vulnerabilities can be found in a variety of places, such as:
  1. Input fields in forms
  2. URL parameters
  3. HTTP headers
  4. Comments
  5. Error messages

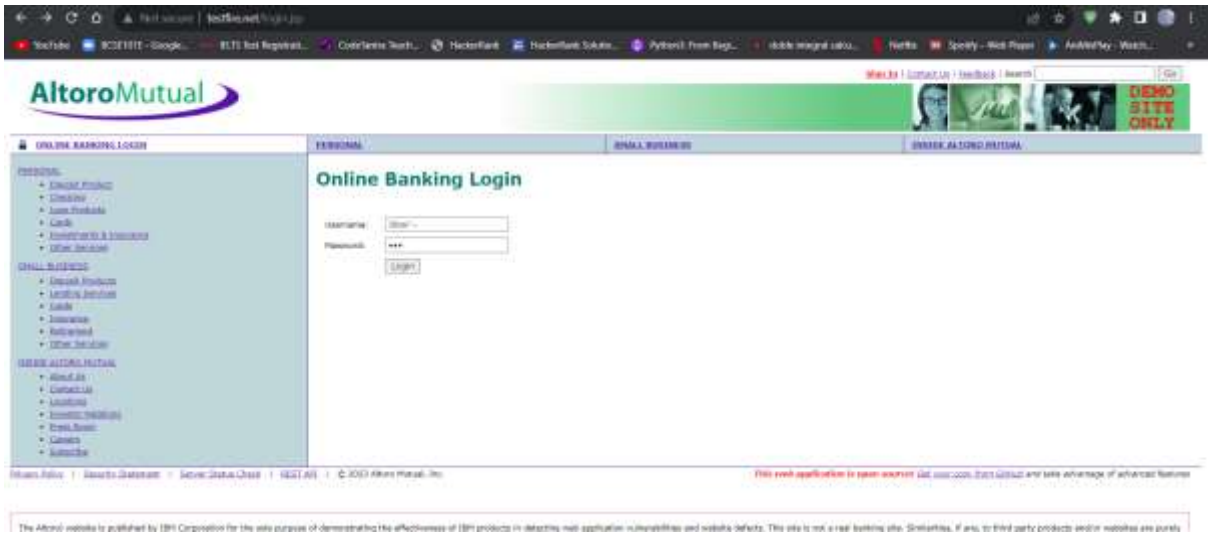
  Once an XSS vulnerability is found, it can be exploited by an attacker to steal cookies, session tokens, or other sensitive information. They can also use it to redirect users to malicious websites, or to execute arbitrary JavaScript code in the victim's browser.

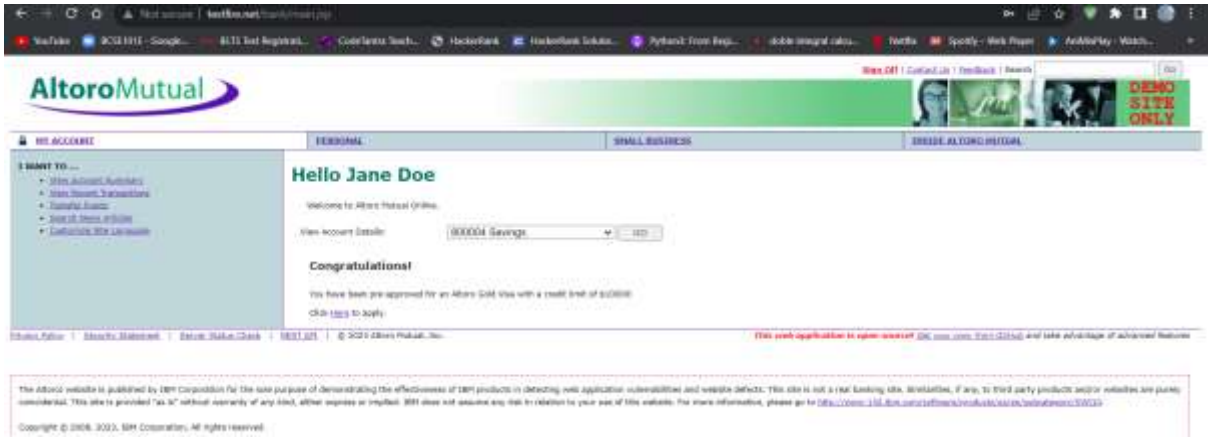


- BROKEN AUTHENTICATION
  Broken authentication is a vulnerability in a website or web application that allows an attacker to impersonate a legitimate user. This can be done by exploiting weaknesses in the authentication process, such as weak passwords, poor session management, or insecure password reset mechanisms.

  Some of the most common broken authentication vulnerabilities include:

  1. Weak passwords: Passwords that are too short, easy to guess, or reused across multiple websites are a major security risk. Attackers can easily crack these passwords using brute-force attacks or dictionary attacks.
  2. Poor session management: When session management is not implemented properly, attackers can steal session cookies or tokens and impersonate a legitimate user. This can happen if sessions are not properly invalidated when users log out, or if session cookies are not encrypted.
  3. Insecure password reset mechanisms: If password reset mechanisms are not secure, attackers can use them to gain access to user accounts. This can happen if password reset emails are sent to the user's email address without any verification, or if password reset tokens are not properly protected.



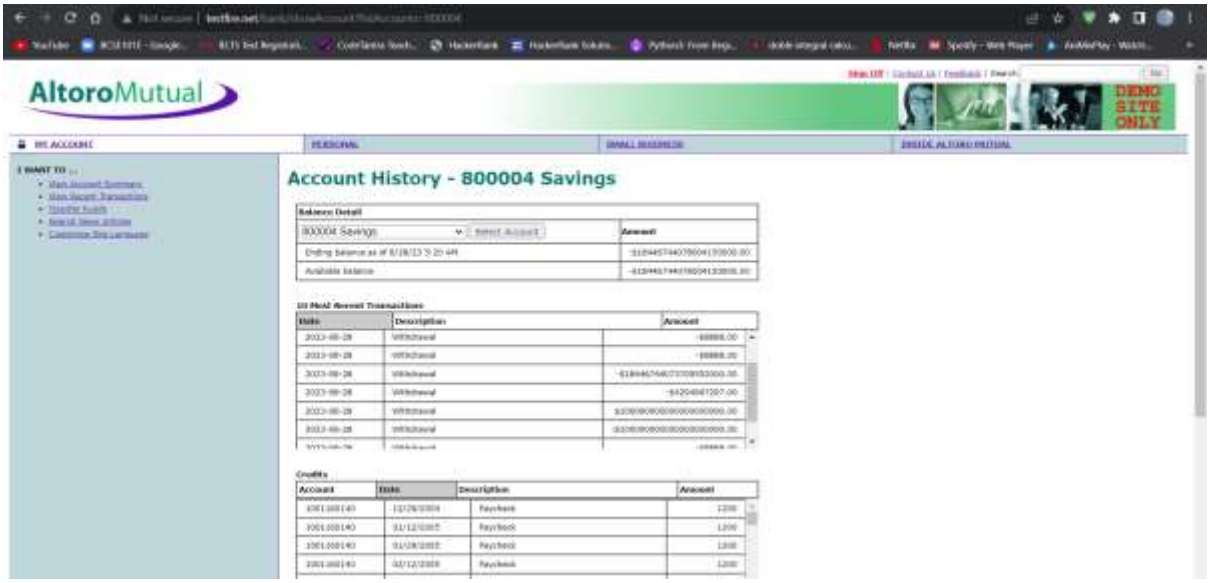


- SENSITIVE DATA EXPOSURE (DUE TO BROKEN ACCESS CONTROL)

  A sensitive data exposure vulnerability in a website is a security flaw that allows an attacker to access sensitive information that is not intended to be publicly accessible. This information can include things like:

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

  Sensitive data exposure vulnerabilities can have a serious impact on businesses and individuals. If an attacker gains access to sensitive information, they could use it to commit identity theft, fraud, or other crimes. They could also sell the information to other criminals or use it to blackmail the victim.


AltoroMutual
DEMO SITE ONLY
Account History - 800004 Savings