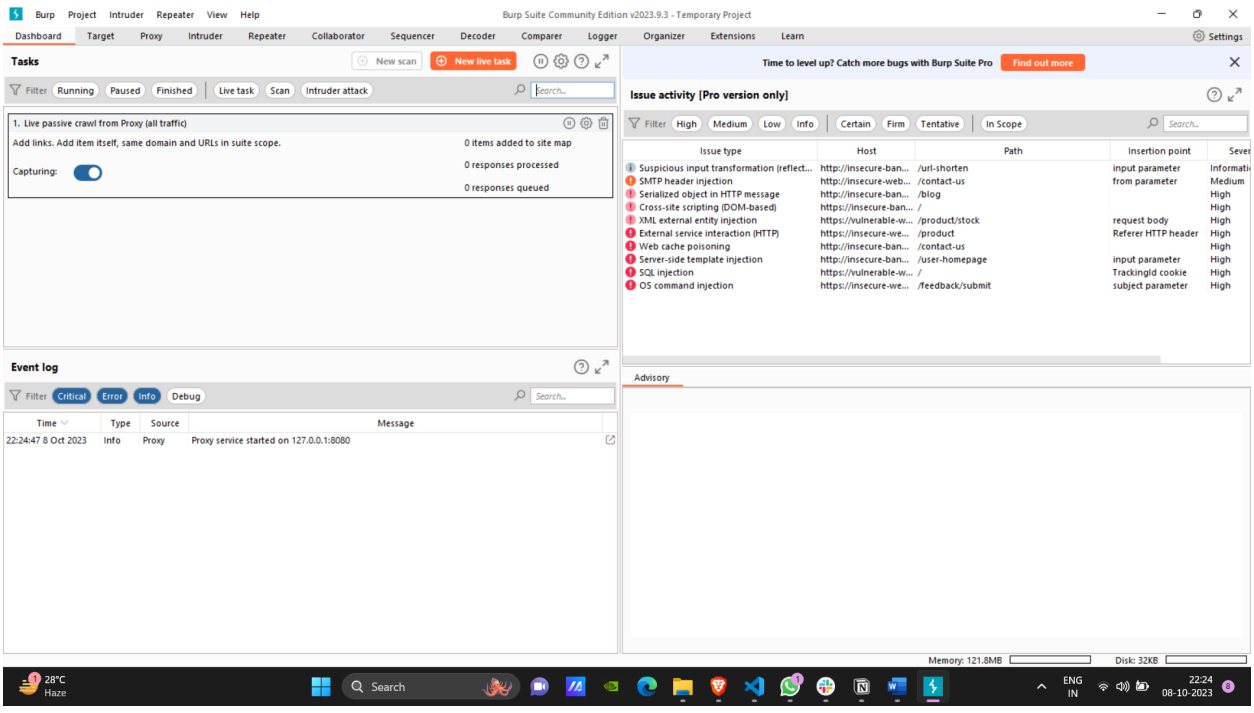
Week 4 - Assignment

Dev Mehta - 21BCE2888

Burp Suite

1. What is Burp suite?

Developed by PortSwigger, Burp Suite is a well-known web vulnerability scanner and testing tool for identifying security flaws in web applications. It is frequently used to find vulnerabilities in online applications throughout the development and testing phases by cybersecurity experts, penetration testers, and ethical hackers. Burp Suite offers a number of tools and capabilities that aid in identifying and using security flaws.



2. Why Burp suite?

- `User-Friendly Interface`

  Burp Suite offers a straightforward UI that is user-friendly for both novice and

seasoned users.

- `Extensive Features`
  It has several functions, such as crawling, session management, web vulnerability screening, and more.
- `Actively Maintained`
  Burp Suite is continuously updated and maintained by PortSwigger to keep it current with the most recent security threats and vulnerabilities.
- `Flexibility`
  Its extensibility capabilities enable customization and expansion, enabling users to include their own plugins and scripts.
- `Effective Reporting`
  Burp Suite offers extensive details on vulnerabilities discovered, making it simpler for developers to comprehend and address the problems.

3. What are the features of burp suite?

- `Spider`
  Burp Suite can map out the various pages and functionality of websites by crawling them.
- `Scanner`
  It contains a strong scanner that can instantly identify widespread online application vulnerabilities like SQL injection, cross-site scripting (XSS), and more.
- `Intruder`
  With the help of the Intruder tool from Burp Suite, users may automate targeted assaults to identify vulnerabilities by adjusting various settings.
- `Repeater`
  With the help of this tool, testers may manually test individual requests and alter and thoroughly examine them.
- `Sequencer`
  It evaluates the level of unpredictability in tokens created by applications, which is important for security measures like session tokens.

- `Decoder`
  Burp Suite's decoder feature enables testers to comprehend and alter many sorts of data, including URL and Base64 encoding. This data is transmitted between the client and the server.
- `Comparer`
  It compares server answers to find variations that may be a sign of possible security problems.
- `Collaborator`
  Burp Out-of-band vulnerabilities, which do not directly interact with the tester but can still be attacked, are found with the assistance of the collaborator.

Burp Suite is a *powerful and versatile tool* that can be *used to perform a wide range of WAST tasks.* It is a must-have tool for any security professional who *tests web applications for security vulnerabilities*.

4. Testing the vulnerabilities

SQL Injection

Lets try to login to Admin account in testfire.net

Try 1:

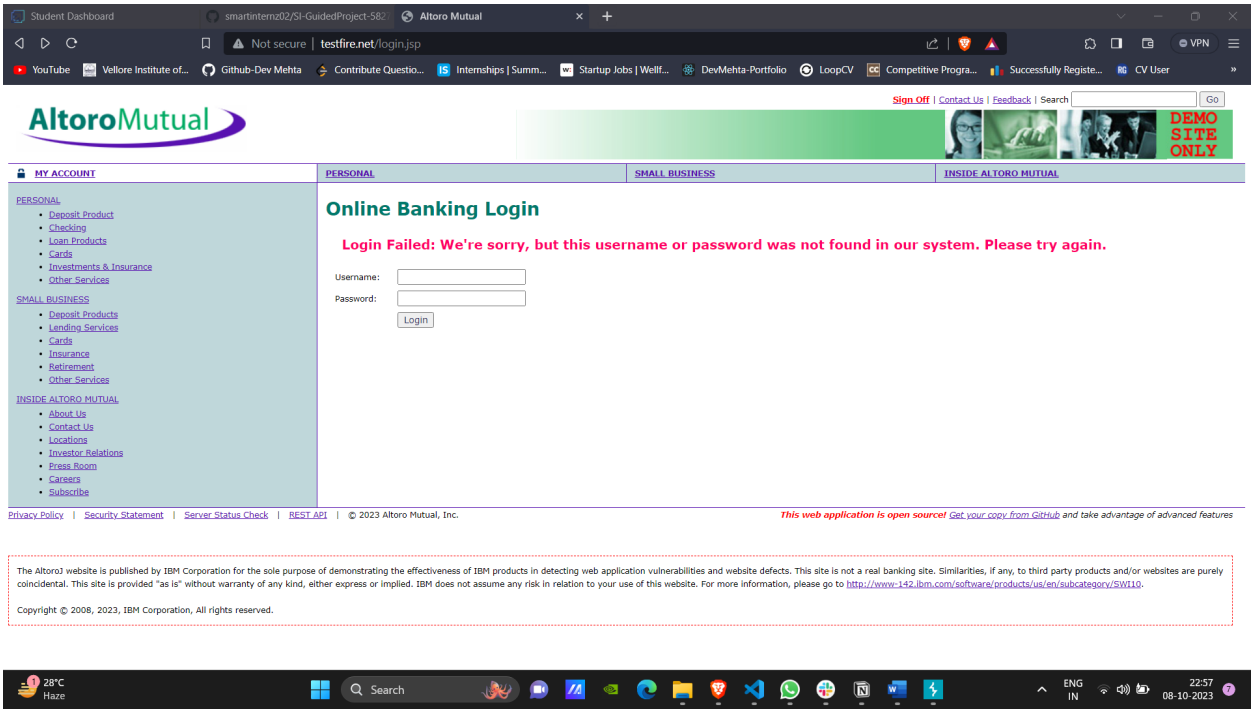
Username - admin

Password - 12345678

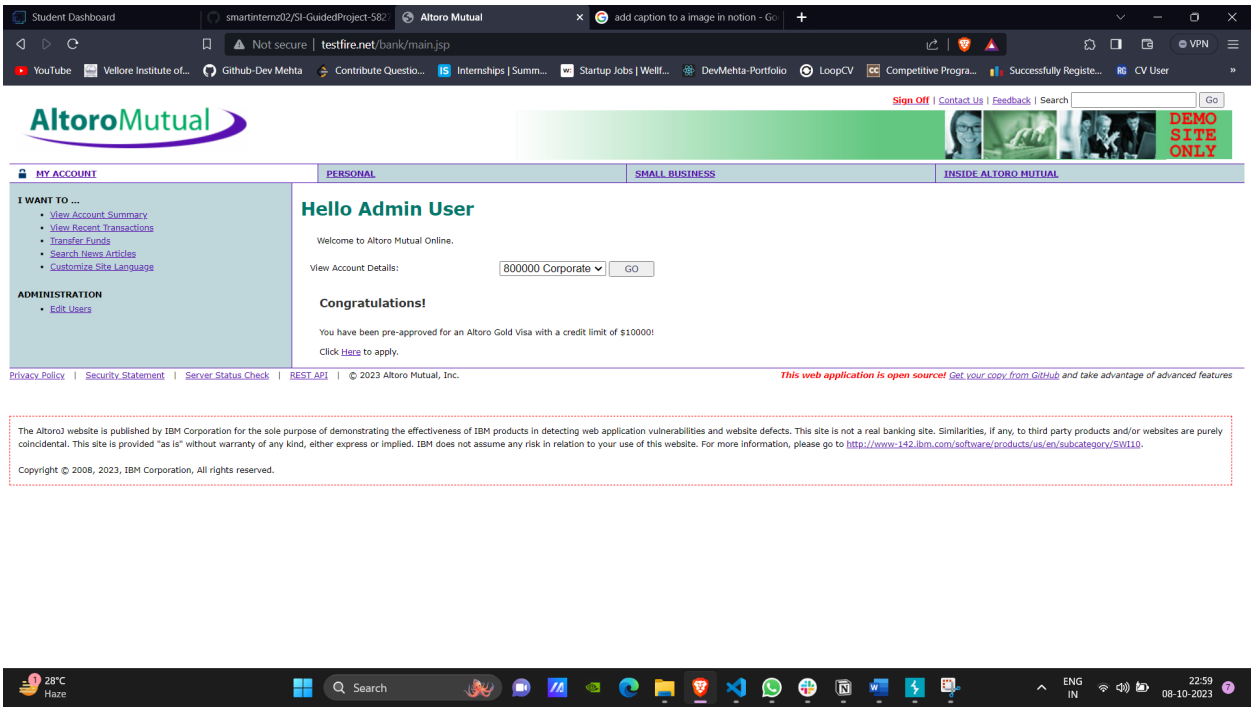
Try 2:

Username - admin'—

Password - 12345678


Student Dashboard
Altoro Mutual
Not secure | testfire.net/login.jsp
AltoroMutual
Sign Off | Contact Us | Feedback | Search
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
Online Banking Login
Login Failed: We're sorry, but this username or password was not found in our system. Please try again.
Username:
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 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.

Try 1


Student Dashboard
Altoro Mutual
Not secure | testfire.net/bank/main.jsp
AltoroMutual
Sign Off | Contact Us | Feedback | Search
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
Hello Admin User
Welcome to Altoro Mutual Online.
View Account Details:
800000 Corporate
GO
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 | 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 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.

Try 2