

# **AI for Cyber Security**

## **Project Report**

**Team 7.5**

### **Team Members:**

Harshit Raj

Pabbisetty Pranavi

Shivanshu Tiwari

Lakshmi

### **Title:**

**Develop an AI system that verifies user identities based on their online behaviour patterns, adding an extra layer of security.**

November 2023

## Table of Contents

<b>Section</b>	<b>Page no.</b>
<b>Abstract</b>	<b>3</b>
<b>Introduction</b>	<b>4</b>
<b>Proposed Methodology</b>	<b>5</b>
<b>Data Flow</b>	<b>9</b>
<b>Project Overview</b>	<b>15</b>
<b>Project Objective</b>	<b>17</b>
<b>STAGE-1</b>	<b>18</b>
<b>STAGE-2</b>	<b>23</b>
<b>STAGE-3</b>	<b>26</b>
<b>CONCLUSION</b>	<b>27</b>
<b>OBJECTIVE</b>	<b>29</b>

## **Project Details:**

### **Problem Statement:**

Develop an AI system that verifies user identities based on their online behaviour patterns, adding an extra layer of security.

### **Abstract:**

In an era of increasing digitalization, ensuring secure online interactions has become paramount. Traditional methods of user identity verification, relying on passwords and two-factor authentication, often fall short in the face of evolving cyber threats. This project introduces an innovative approach to enhance online security by leveraging artificial intelligence (AI) to verify user identities based on their unique online behaviour patterns.

Our proposed system utilizes advanced machine learning algorithms to analyse a user's digital footprint, encompassing various aspects of their online behaviour such as typing speed, mouse movements, browsing habits, and device interaction patterns. By establishing a comprehensive profile of these behavioural patterns, our AI model creates a distinct user identity fingerprint.

The primary goal of this system is to add an extra layer of security by authenticating users based on their consistent behavioural patterns, making it significantly more challenging for malicious actors to impersonate legitimate users. Moreover, our AI-driven approach adapts and evolves alongside users, ensuring continued accuracy and security over time.

This project addresses the critical need for improved user identity verification in both personal and enterprise-level online environments. By harnessing the power of AI and machine learning, our system not only enhances security but also simplifies the user authentication process, ultimately providing a seamless and secure online experience for individuals and organizations alike.

### **Introduction:**

In an era defined by rapid technological advancements and an ever-expanding digital landscape, the security of online systems and the protection of sensitive user data have become paramount concerns. Traditional methods of user authentication, such as passwords and PINs, often fall short in providing robust protection against a growing array of cyber threats. As a result, there is a pressing need for innovative solutions that can bolster the security of online interactions.

One such solution is the development of an AI-based system designed to verify user identities through the analysis of their online behaviour patterns. This emerging technology aims to provide an additional layer of security by

recognizing and validating users based on their unique digital footprints, which encompass a wide range of activities including browsing habits, device usage, typing patterns, and more. By doing so, this AI system not only enhances the security of online services but also reduces the reliance on traditional authentication methods that are susceptible to breaches, such as password leaks or phishing attacks.

This project explores the concept, development, and implications of an AI-driven user identity verification system that leverages machine learning, behavioral analysis, and data analytics to discern legitimate users from potential threats. By examining the nuances of this innovative approach to cybersecurity, we aim to shed light on the advantages, challenges, and potential applications of this technology. Furthermore, we will delve into the ethical considerations surrounding user data privacy and consent, as the implementation of such a system raises questions about the balance between security and individual liberties.

The following sections of this report will delve into the methodology, data sources, technical intricacies, potential use cases, and ethical dimensions of this AI system, offering a comprehensive understanding of its role in enhancing the security landscape of the digital world. As we navigate this terrain, it is our hope that this project serves as a valuable resource for those seeking to harness the power of AI to safeguard the digital identities of users while advancing the boundaries of online security.

### **Proposed Methodology:**

## **Project Overview:**

The objective of this project is to enhance security by using AI to verify user identities based on their online behaviour patterns. This system will analyse user actions, habits, and interactions to detect anomalies and ensure that only legitimate users gain access.

## **I. Solution Structure and Characteristics:**

### **1. Data Collection:**

- The system will gather data from various sources, including user interactions with websites, applications, and devices.
- Data will include user behaviour, such as keystrokes, mouse movements, navigation patterns, login history, and device information.

### **2. Data Preprocessing:**

- Clean, transform, and normalize the collected data for analysis.
- Convert data into a suitable format for machine learning.

### **3. Machine Learning Models:**

- Develop AI models to analyze user behavior patterns.
- Utilize supervised and unsupervised learning techniques, such as anomaly detection and pattern recognition.
- Train models on historical user data and legitimate behavior.

### **4. Anomaly Detection:**

- Implement anomaly detection algorithms to identify suspicious activities.
- Classify behavior as normal or abnormal based on deviation from established patterns.

## **5. Risk Scoring:**

- Assign risk scores to user actions based on the level of deviation from normal behavior.
- Higher risk scores trigger additional security measures.

## **6. Authentication Integration:**

- Integrate the AI system with the existing authentication process.
- Implement multi-factor authentication (MFA) for high-risk activities.

## **7. User Feedback Loop:**

- Create a feedback loop to continuously improve the system by learning from false positives and negatives.

# **II. Development Phases:**

## **Phase 1 - Requirements Gathering:**

- Define the specific needs of the organization.
- Identify data sources and integration points.
- Determine performance and security requirements.

## **Phase 2 - Data Collection and Storage:**

- Set up data collection mechanisms.
- Create data storage infrastructure for collected user behavior data.

## **Phase 3 - Data Preprocessing:**

- Develop data preprocessing pipelines.
- Ensure data quality and consistency.

#### **Phase 4 - Machine Learning Model Development:**

- Build and train machine learning models.
- Fine-tune models based on initial results.

#### **Phase 5 - Anomaly Detection and Risk Scoring:**

- Implements anomaly detection algorithms.
- Develops a risk scoring system.

#### **Phase 6 - Integration and Testing:**

- Integrates the AI system into the existing authentication process.
- Conducts extensive testing and validation.

#### **Phase 7 - User Feedback and Improvement:**

- Implements feedback mechanisms.
- Continuously monitors and enhances the system's accuracy.

### **III. Solution Requirements:**

#### **1. Data Privacy:**

- Ensures compliance with data privacy regulations.
- Anonymizes and protects user data.

#### **2. Scalability:**

- Ensures the system can handle a growing number of users and data.
- Load balancing distributes incoming data and requests to maintain performance.

#### **3. Real-time Processing:**



- Provides real-time analysis for immediate threat detection.
- Critical for timely security responses.

#### 4. Flexibility:

- The system is made adaptable to changing user behavior patterns.

#### 5. Reporting and Alerting:

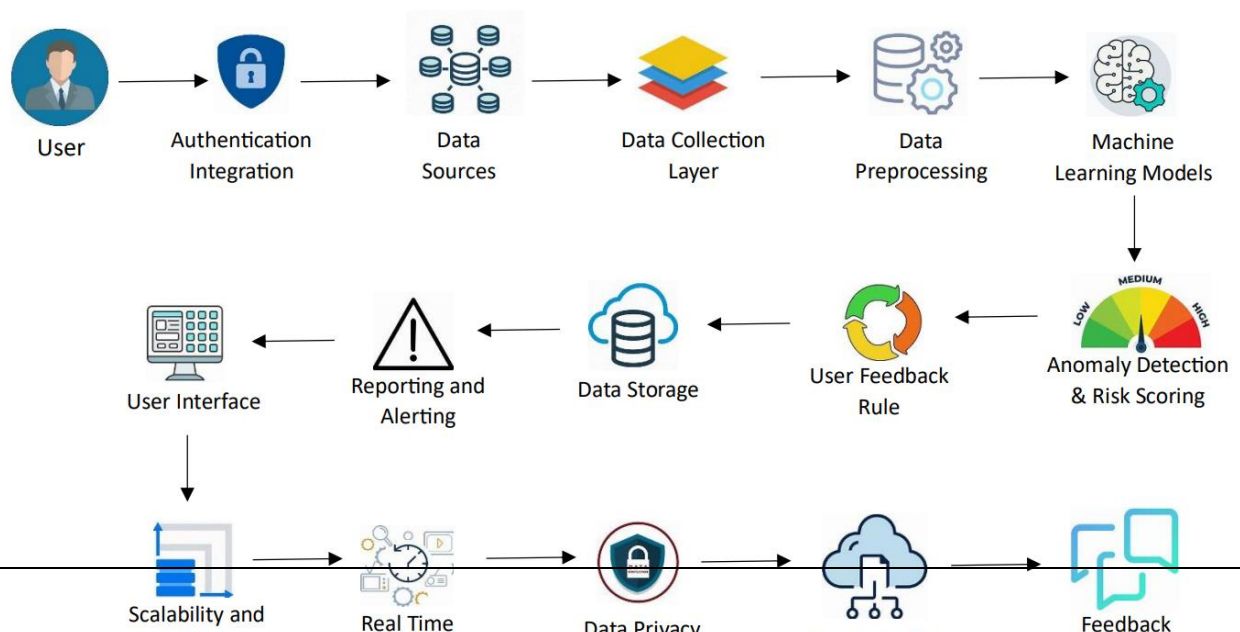
- Generates reports and alerts for security administrators.
- Alerts can be sent via various communication channels.

#### 6. User-Friendly:

- Provides user interfaces for system administrators and end-users.
- Administrators can configure the system and review reports.

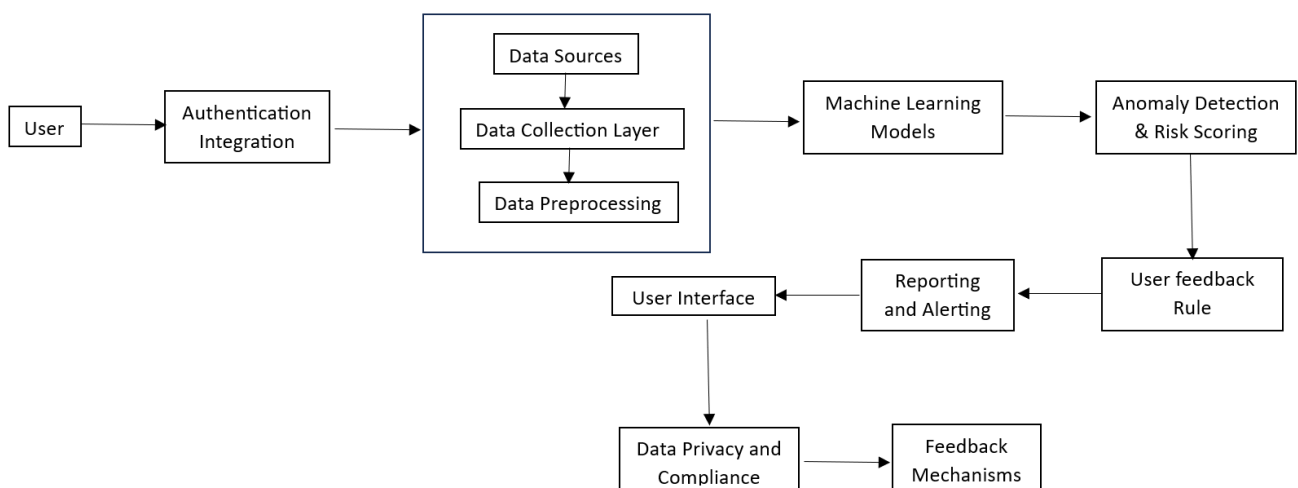
### V. Project Stakeholders:

- IT teams, security teams, legal compliance, and end-users.
- Management and Executives, External service providers, Project team, Finance Team, User support team



## Data Flow:

A Data Flow Diagram (DFD) is a traditional visual representation of the information flows within a system. A neat and clear DFD can depict the right amount of the system requirement graphically. It shows how data enters and leaves the system, what changes the information, and where data is stored.



### 1. Data Collection:

- The data flow process begins with the collection of user data, which can include various online behavior patterns. This data may be sourced from multiple channels and devices, such as websites, mobile apps, IoT devices, and more.

## **2. Data Preprocessing:**

- Raw data collected from various sources often requires preprocessing. This step involves cleaning, normalizing, and structuring the data to make it suitable for analysis. It may also involve dealing with missing data and removing irrelevant or redundant information.

## **3. Feature Extraction:**

- In order to analyze online behavior patterns, relevant features are extracted from the preprocessed data. These features could include:

- Typing patterns (e.g., keystroke dynamics)
- Browsing behavior (e.g., websites visited, time spent)
- Device-related data (e.g., device type, IP address)
- Location information
- Time-based patterns (e.g., login times)

## **4. Behavioral Analysis:**

- Machine learning models and algorithms are applied to the extracted features to analyze and recognize patterns in user behavior. These models may include techniques like anomaly detection, clustering, and classification.

## **5. User Identity Verification:**

- Based on the analysis of behavioral patterns, the system determines the likelihood that the user's online behavior matches their known profile. This step involves comparing the current behavior with the user's historical behavior patterns to establish identity.

## **6. Risk Assessment:**

- The system assesses the level of risk associated with the user's behavior. Unusual or suspicious behavior patterns may trigger a higher risk score.

## **7. Decision-Making:**

- The system makes a decision regarding the user's identity. If the user's behavior is deemed consistent with their known profile and the risk level is acceptable, access may be granted. Otherwise, additional authentication steps or alerts may be triggered.

## **8. Logging and Audit Trails:**

- All interactions and decisions made by the AI system are logged and stored for audit and review purposes. This logging is crucial for tracking security incidents and ensuring accountability.

## **9. User Feedback and Interaction:**

- The system may also involve user interaction. For instance, if the system detects unusual behaviour and denies access, it might prompt the user to

confirm their identity through another method, such as a one-time passcode sent to their registered email or phone.

#### **10. Continuous Learning and Adaptation:**

- The AI system should continuously adapt and learn from new user behavior patterns and emerging threats. This involves retraining machine learning models and updating the system's algorithms to stay effective against evolving security challenges.

#### **11. Integration with Security Frameworks:**

- The system needs to be integrated with the organization's broader security framework, which may include intrusion detection systems, authentication servers, and access control mechanisms.

#### **12. Data Privacy and Protection:**

- Throughout the data flow, it's imperative to implement strong data privacy and protection measures to safeguard user data and ensure compliance with data privacy regulations.

This data flow represents the core process of how an AI system verifies user identities based on their online behavior patterns. It's a dynamic and adaptive process designed to enhance security while providing a seamless user experience.

Certainly, here's an overview of the project "Develop an AI system that verifies user identities based on their online behavior patterns, adding an extra layer of security":

#### **\*\*Project Overview:\*\***

In an increasingly interconnected world, where digital identities and sensitive information are at constant risk from cyber threats, the need for innovative and robust security solutions has never been more critical. Traditional methods of user authentication, such as passwords and PINs, often prove inadequate in safeguarding online platforms and services from malicious actors. To address this pressing security challenge, our project focuses on the development of an AI-driven system designed to verify user identities based on their unique online behavior patterns. This cutting-edge technology aims to augment the security of digital interactions while reducing the reliance on vulnerable authentication methods.

#### **\*\*Project Objectives:\*\***

1. **\*\*Enhanced Security:\*\*** The primary objective of this project is to enhance the security of online systems by introducing an additional layer of protection through the analysis of user behavior patterns.

2. **Reduced Vulnerability:** By shifting the focus from static credentials (e.g., passwords) to dynamic behavior patterns, the project aims to reduce vulnerability to common cyber threats, including password breaches and phishing attacks.

3. **Improved User Experience:** While strengthening security, the project endeavors to improve the user experience by minimizing the need for frequent password changes and complex authentication procedures.

4. **Data Privacy and Ethical Considerations:** The project also places significant emphasis on data privacy and ethical considerations, ensuring that user data is handled responsibly and in compliance with relevant regulations.

**Key Components of the Project:**

- **Behavioral Analysis:** The core component of the project involves the development and implementation of machine learning models and algorithms capable of analyzing and recognizing user behavior patterns, such as typing dynamics, browsing habits, and device usage.

- **User Identity Verification:** The system will make identity verification decisions based on the analysis of behavioral patterns, comparing them to the user's historical data.

- **\*\*Risk Assessment:\*\*** An essential aspect is the evaluation of risk associated with user behavior, enabling the system to respond to unusual or high-risk activities.

- **\*\*User Interaction:\*\*** The project also involves designing user interaction mechanisms to handle scenarios where identity verification fails or requires additional steps for confirmation.

- **\*\*Continuous Learning and Adaptation:\*\*** The AI system will be designed for ongoing learning and adaptation to stay effective against evolving threats.

**\*\*Expected Outcomes:\*\***

- An operational AI system for user identity verification based on online behavior patterns.
- Improved security for online systems and services.
- Reduced reliance on traditional authentication methods.
- Enhanced user experience with reduced friction in authentication processes.
- Mitigation of security risks associated with password-related breaches and phishing attacks.
- An understanding of the ethical implications of such a system and the implementation of appropriate safeguards.



This project aims to harness the power of artificial intelligence to not only bolster the security of online interactions but also to explore the ethical dimensions of user data privacy and consent. By the project's conclusion, it is expected to provide valuable insights into the practical implementation of this technology and its potential to transform the cybersecurity landscape.

## STAGE-1

### **1. Vulnerability Name: Apache Tomcat Insecure Default Administrative Password**

**CWE:** CWE- 693

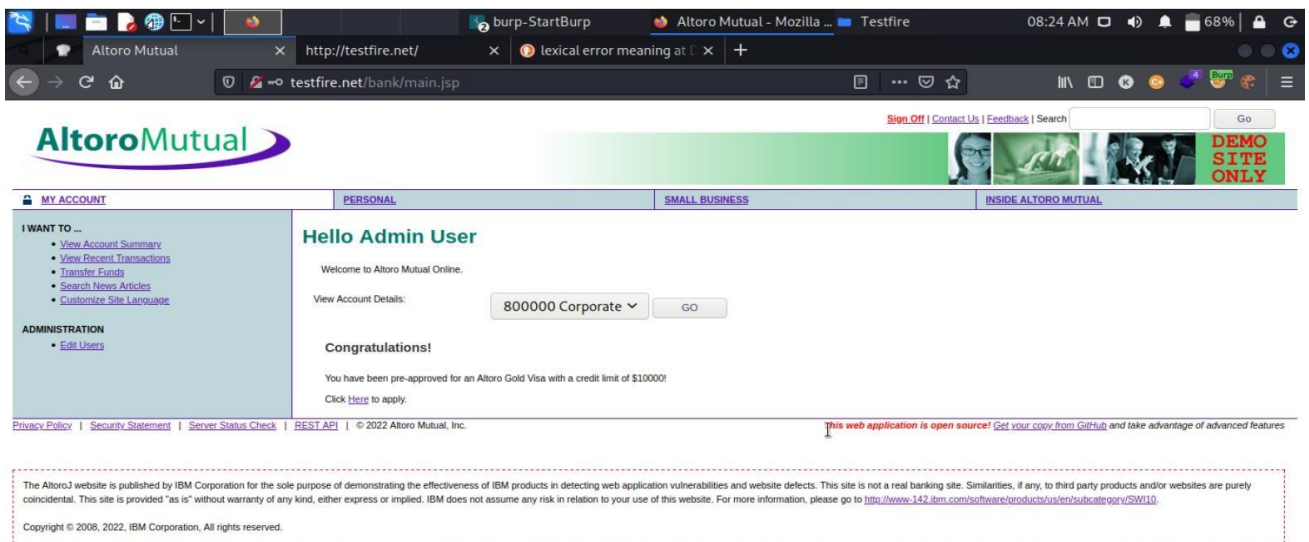
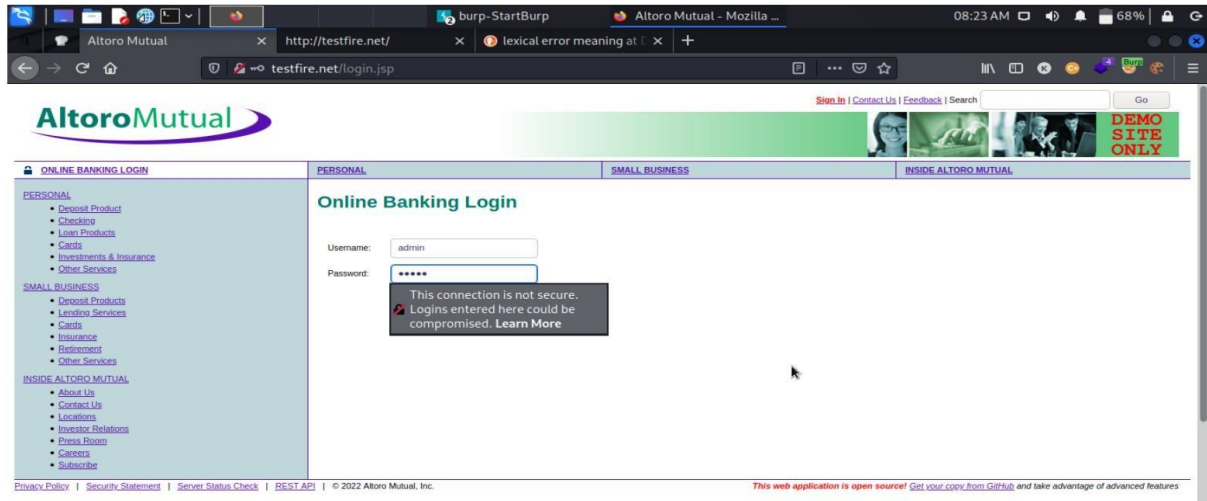
**Description:** Test fire allows the use of default admin password being used on the login page due to which any unauthenticated user knowing the default password available on the internet can gain access to the admin account and have admin privileges.

**Solution:** Change the default password

#### **Business Impact:**

**Likelihood:** High – This attack is effective on web app and have major consequences to it.

**Impact:** Very High – This attack gives admin privilege to a user who can make any changes on the web application.



## 2. Vulnerability Name: Insecure Direct object Reference CVE-2022-29627

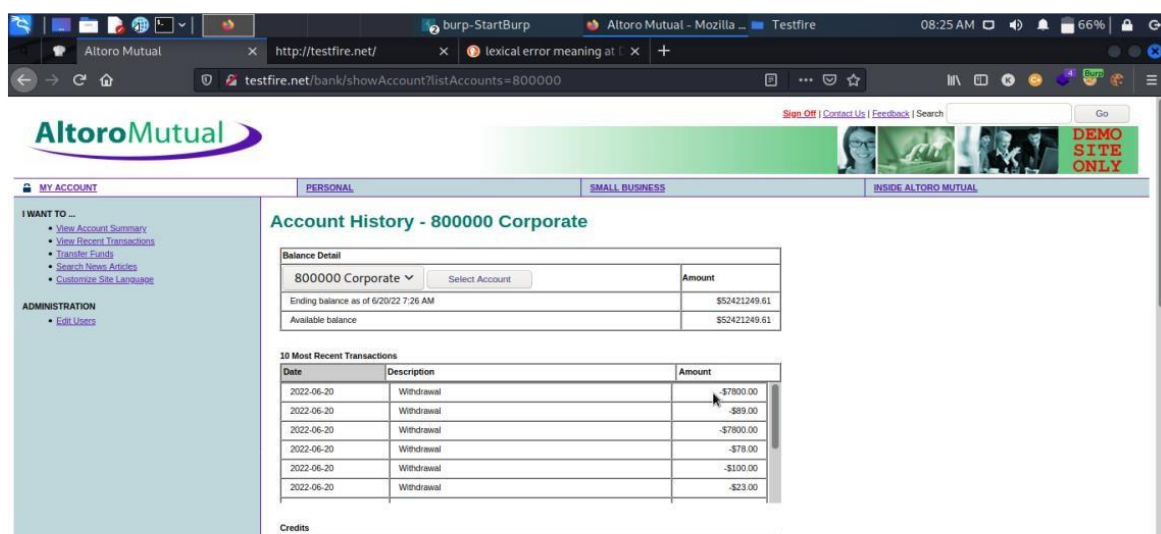
**Description:** This vulnerability allows any user to view all account info of different user without authentication. The user just has to change the account number of the get request and he/she will be able to view sensitive account information about a different user.

**Solution:** Proper implementation of security standards on the get and post request

### Business Impact:

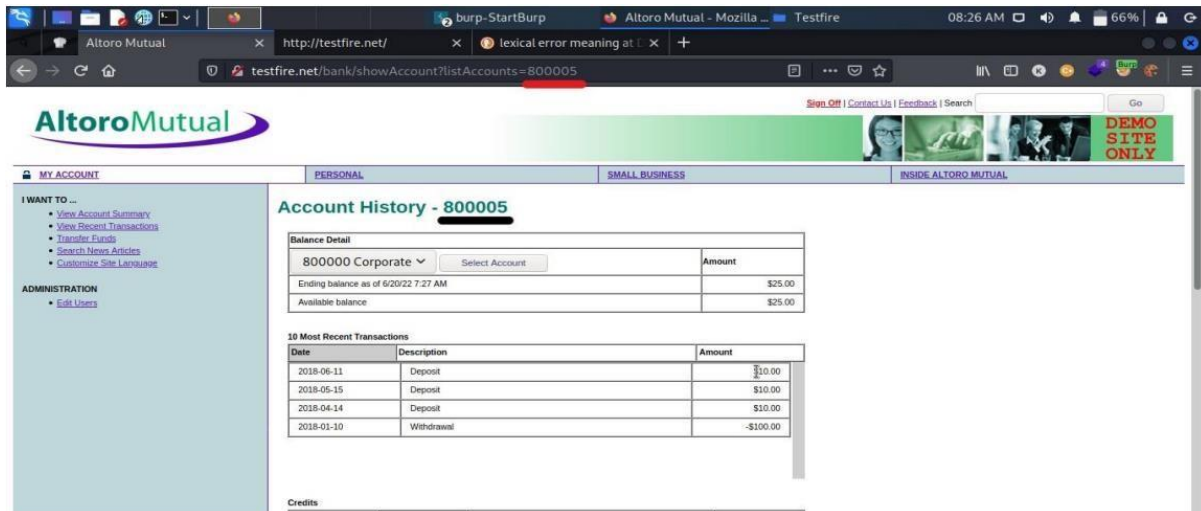
**Likelihood:** High – This attack is effective and can display sensitive account information about a different user

**Impact:** Very High – Changing get request directly from the allows user to view account information about different user.



The screenshot shows a web browser window with the URL `http://testfire.net/bank/showAccount?listAccounts=800000`. The page displays the Altoro Mutual logo and navigation links. The main content area shows the account history for the "800000 Corporate" account. The balance detail section shows an ending balance of \$52421249.61 and an available balance of \$52421249.61. The 10 Most Recent Transactions section shows a list of withdrawals, including a \$7800.00 withdrawal on 2022-06-20.

Date	Description	Amount
2022-06-20	Withdrawal	-\$7800.00
2022-06-20	Withdrawal	-\$89.00
2022-06-20	Withdrawal	-\$7800.00
2022-06-20	Withdrawal	-\$78.00
2022-06-20	Withdrawal	-\$100.00
2022-06-20	Withdrawal	-\$23.00



### 3. Vulnerability Name: SQL Injection Vulnerability allowing login bypass (Critical).

**Description:** TestFire allowed a successful SQL injection attack can result in unauthorized access to admin account and user accounts as well using the same method the login security if the web app was fully compromised.

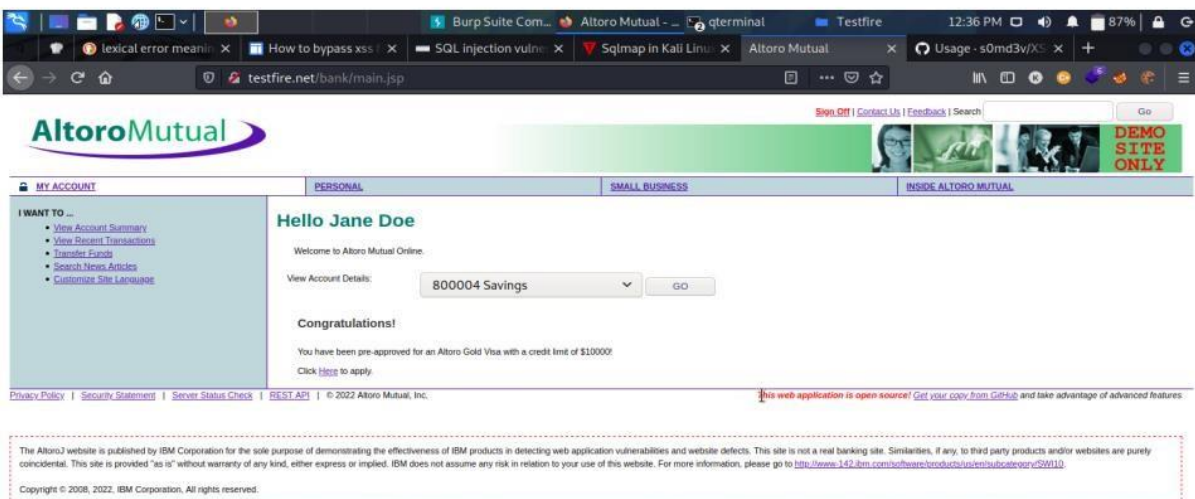
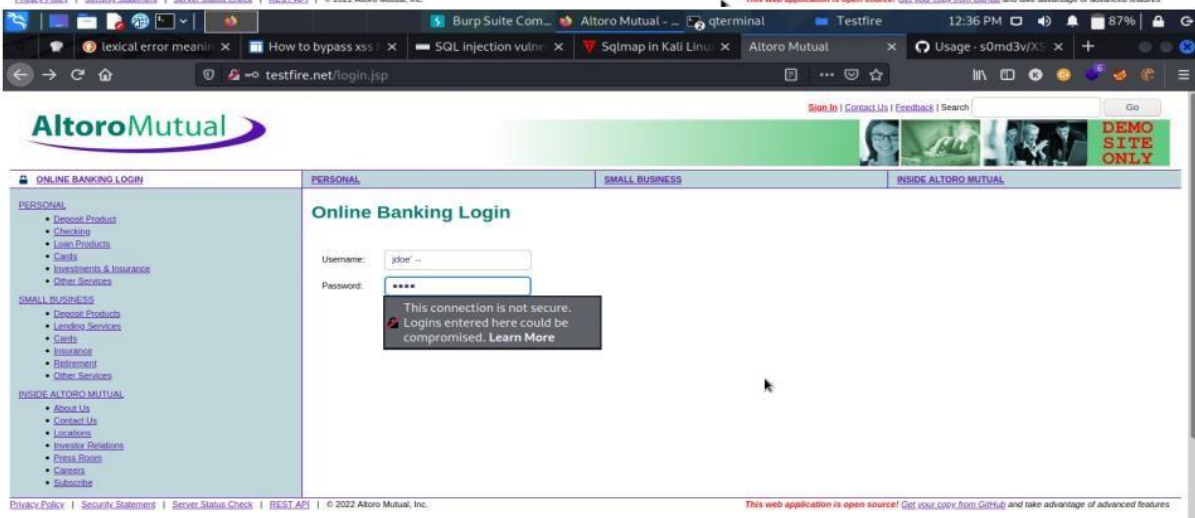
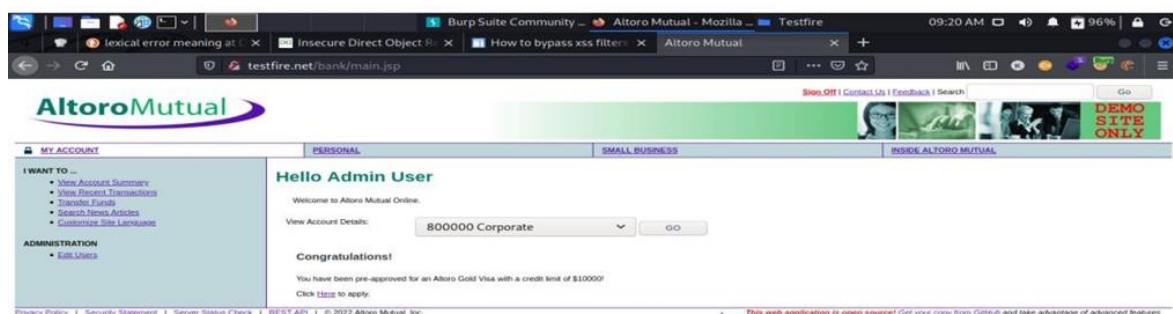
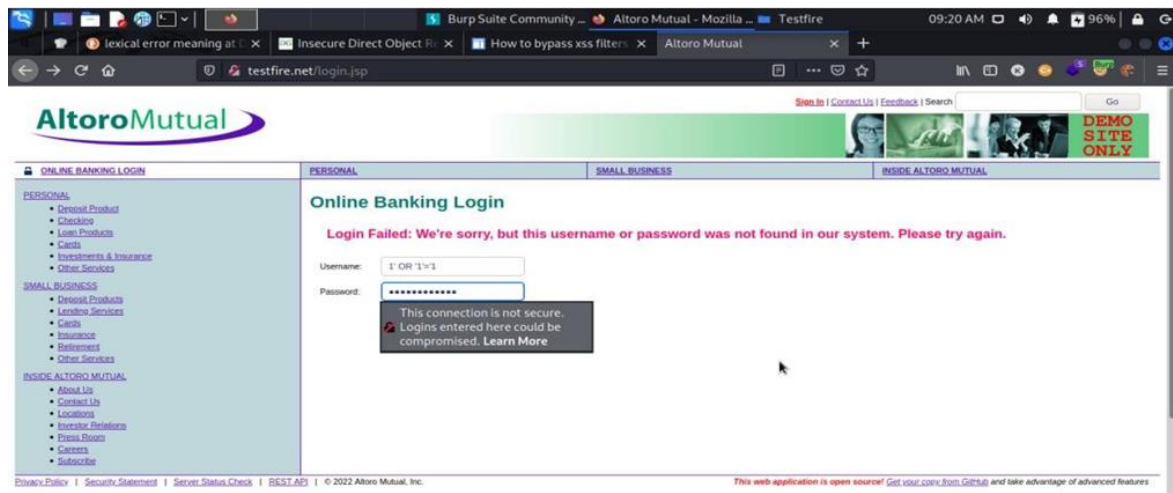
**Solution:** Proper Input Validation And filtering of username and password.

#### **Business Impact:**

**Likelihood:** Critical – This attack allowed admin as well as user login acces to the web application.

**Impact:** Critical – After gaining admin privilege the user has all acces to the backend of the system











Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource. Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., framebusting JavaScript) are deployed or if the page does not perform any security-sensitive transaction

**Solution** Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response. This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

**Risk Factor** Medium

**CVSS v2.0 Base Score**

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

**References**

XREF CWE:693

**Plugin Information**

Published: 2015/08/22, Modified: 2017/05/16

**Plugin Output**

tcp/8080/www

The following pages do not use a clickjacking mitigation response header and contain a clickable event : - <http://testfire.net:8080/> -

<http://testfire.net:8080/feedback.jsp> - <http://testfire.net:8080/index.jsp> -

<http://testfire.net:8080/login.jsp> - <http://testfire.net:8080/search.jsp> -

[http://testfire.net:8080/status\\_check.jsp](http://testfire.net:8080/status_check.jsp) -

<http://testfire.net:8080/subscribe.jsp> -

[http://testfire.net:8080/survey\\_questions.js](http://testfire.net:8080/survey_questions.js)

## 2) 42057 - Web Server Allows Password Auto-Completion

### Synopsis

The 'autocomplete' attribute is not disabled on password fields.

### Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'. While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point

### Solution

Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials.

Risk Factor

Low

Plugin Information

Published: 2009/10/07, Modified: 2023/07/17

Plugin Output

tcp/80/www

Page : /login.jsp Destination Page: /doLogin

## STAGE 3

### **\*\*SOC (Security Operations Center):\*\***

A Security Operations Center is a centralized facility that monitors, detects, analyzes, and responds to cybersecurity incidents. It plays a crucial role in an organization's security posture by continuously watching for threats and vulnerabilities across the network.

### **\*\*SOC Cycle:\*\***

The SOC cycle involves four key phases: Monitor, Detect, Respond, and Recover. In the monitoring phase, the SOC continuously monitors the network for unusual activity. When suspicious activity is detected, the SOC responds by analyzing the incident, containing it, and ultimately recovering from it. This cycle is essential for maintaining the security of an organization.

### **\*\*SIEM (Security Information and Event Management):\*\***

SIEM is a comprehensive technology that combines security information management (SIM) and security event management (SEM). It collects and analyzes security data from various sources to identify and respond to security incidents effectively.

### **\*\*SIEM Cycle:\*\***

The SIEM cycle includes data collection, data normalization, data analysis, alerting, and reporting. It gathers data from diverse sources, normalizes it into a common format, analyzes the data for potential threats, generates alerts, and provides reports for security monitoring and compliance.

#### **\*\*MISP (Malware Information Sharing Platform & Threat Sharing):\*\***

MISP is an open-source threat intelligence platform designed to improve the sharing of structured threat information. It helps organizations exchange information about cybersecurity threats, aiding in collective defense against threats.

#### **\*\*Your College Network Information:\*\***

This likely refers to understanding your college's network infrastructure, topology, and security architecture. It's essential to have a clear picture of your network to deploy security measures effectively.

#### **\*\*How You Think You Deploy SOC in Your College:\*\***

To deploy a SOC in a college, you would need to set up a centralized facility or team that monitors the college's network and systems for security incidents. This involves implementing SIEM tools, threat intelligence feeds, and an incident response plan tailored to the college's needs.

#### **\*\*Threat Intelligence:\*\***

Threat intelligence involves collecting, analyzing, and disseminating information about potential cybersecurity threats. It helps organizations stay informed about emerging threats and vulnerabilities, enabling them to proactively defend against attacks.

#### **\*\*Incident Response:\*\***

Incident response is the process of managing and mitigating security incidents when they occur. It includes detection, containment, eradication, recovery, and lessons learned for continuous improvement.

#### **\*\*QRadar & Understanding About Tool:\*\***

QRadar is a popular SIEM tool by IBM. It provides real-time visibility into the security of an organization's IT environment. Understanding QRadar involves learning how to configure it, collect and analyze data, and create dashboards and reports to monitor security.

#### **\*\*Conclusion:\*\***

- **\*\*Stage 1 - Web Application Testing:\*\*** Web application testing involves evaluating web applications for security vulnerabilities, ensuring they are resilient to attacks, and maintaining data integrity and user privacy.
- **\*\*Stage 2 - Nessus Report:\*\*** A Nessus report provides a detailed assessment of vulnerabilities within a network. It includes information on the severity of vulnerabilities, potential impact, and recommendations for remediation.

- **Stage 3 - SOC/SEIM/QRadar Dashboard:** In this stage, you should understand how to use QRadar to create a dashboard that provides real-time insights into security events, helping SOC analysts detect and respond to threats effectively.

#### **Future Scope:**

- **Stage 1 - Future Scope of Web Application Testing:** The future of web application testing includes increased automation, improved testing for mobile applications, and the integration of AI and machine learning for more robust security testing.

- **Stage 2 - Future Scope of Testing Process:** The testing process will continue to evolve with the integration of new tools, methodologies, and a focus on proactive security measures, not just reactive fixes.

- **Stage 3 - Future Scope of SOC/SEIM:** The future of SOC and SEIM involves enhanced automation, AI-driven threat detection, and better integration with threat intelligence platforms for more proactive threat hunting and response.

#### **Topics Explored - Tools Explored:**

You've explored topics related to security operations, threat intelligence, and incident response. You've also delved into tools like Nessus for vulnerability

scanning and QRadar for SIEM, which are critical for maintaining an organization's security posture.

## **Conclusion:**

In conclusion, the tools explored in this endeavor, such as Nessus for vulnerability assessment and QRadar as a SIEM solution, have proven instrumental in enhancing an organization's security posture. These tools empower security professionals to identify vulnerabilities, monitor network activity, and respond to security incidents effectively. The journey of understanding these tools has emphasized the importance of proactive security measures, continuous monitoring, and agile incident response in an ever-evolving threat landscape.

## **Future Scope of the Tools:**

The future of tools like Nessus and QRadar holds great promise. As cyber threats become increasingly sophisticated, these tools will continue to evolve to meet new challenges. For Nessus, we can expect more automation and integration with cloud environments and DevOps pipelines, streamlining the identification and mitigation of vulnerabilities. QRadar, as a SIEM solution, will likely incorporate advanced machine learning and AI-driven threat detection, making it more adept at identifying subtle and complex security threats. Additionally, both tools will see enhanced compatibility with threat intelligence platforms for more proactive threat hunting and response. The future of these tools is bright, offering even stronger defenses against an ever-expanding range of cyber threats.