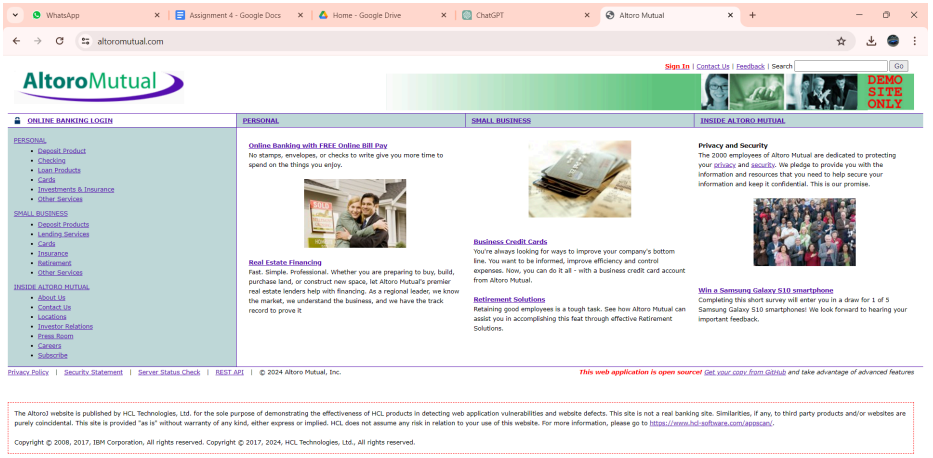
Assignment 4

Name: Chitrada Pavan
College: Dr.Lankapalli Bullayya college
Regd.No: 721128805304
Date: 15/03/2024

Step 1: OWASP Top 10 Vulnerabilities Overview:

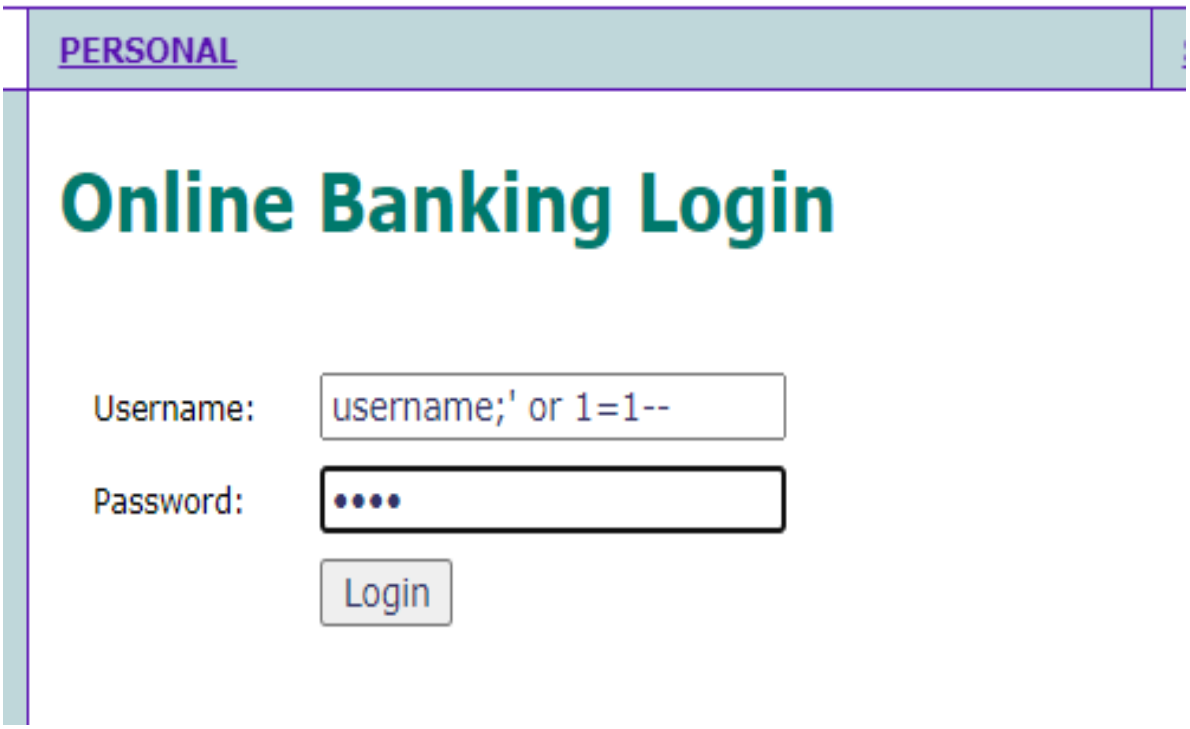
- Injection: Injection flaws occur when untrusted data is sent to an interpreter as part of a command or query. This can result in an attacker executing unintended commands or accessing unauthorized data.
- Broken Authentication: This vulnerability arises when an application does not correctly manage authentication and session management, allowing attackers to compromise passwords, keys, or session tokens.
- Sensitive Data Exposure: This occurs when an application fails to adequately protect sensitive data, such as financial information or personal identifiers. Attackers can exploit this vulnerability to access such data.
- XML External Entities (XXE): XXE vulnerabilities arise when an application parses XML input from untrusted sources. Attackers can exploit this to access sensitive data, execute remote code, or perform denial of service attacks.
- Broken Access Control: This vulnerability occurs when restrictions on what authenticated users can do are not properly enforced. Attackers can exploit this to access unauthorized functionality or data.
- Security Misconfiguration: Security misconfigurations happen when an application is not securely configured, leaving it vulnerable to attack. This could include default configurations, open cloud storage, or unnecessary features enabled.
- Cross-Site Scripting (XSS): XSS vulnerabilities occur when an application includes untrusted data in a web page without proper validation or escaping. Attackers can exploit this to execute scripts in the victim's browser, potentially stealing cookies or other sensitive information.
- Insecure Deserialization: Insecure deserialization vulnerabilities arise when untrusted data is used to abuse the logic of an application, leading to remote code execution or other attacks.
- Using Components with Known Vulnerabilities: This occurs when an application uses components (such as libraries or frameworks) with known vulnerabilities. Attackers can exploit these vulnerabilities to compromise the application.
- Insufficient Logging and Monitoring: When an application lacks sufficient logging and monitoring, it becomes difficult to detect and respond to security incidents. Attackers can exploit this to maintain persistence in the system or to cover their tracks.

Step 2: Altro Mutual Website Analysis:



Altoro Mutual is a subsidiary of Altoro, a multi-state holding company located in the heart of Massachusetts. Altoro Mutual has been serving Boston and surrounding communities for nearly 75 years.
Altoro Mutual offers a broad range of commercial, private, retail and mortgage banking services to small- and middle-market businesses and individuals. We pride ourselves on constantly surpassing the demands of our most loyal customers. And, we are determined to help you stay ahead of your expectations.

Step 3: Vulnerability Identification Report:



We have used invalid login credentials but it has logged in

PERSONAL | SMALL BUSINESS

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.

This vulnerability is called Broken Authentication

Account History - 800000 Corporate

Balance Detail

800000 Corporate Select Account	Amount
Ending balance as of 4/12/24 6:37 AM	-$10000000000000000000000000000000000000000000000000000000000000000000000000.00
Available balance	-$10000000000000000000000000000000000000000000000000000000000000000000000000.00

10 Most Recent Transactions

Date	Description	Amount
2024-04-12	Withdrawal	-$5000.00
2024-04-12	Withdrawal	-$800.00
2024-04-12	Deposit	$100000.00
2024-04-12	Deposit	$100000.00
2024-04-12	Withdrawal	-$1000.00
2024-04-12	Deposit	$1.00

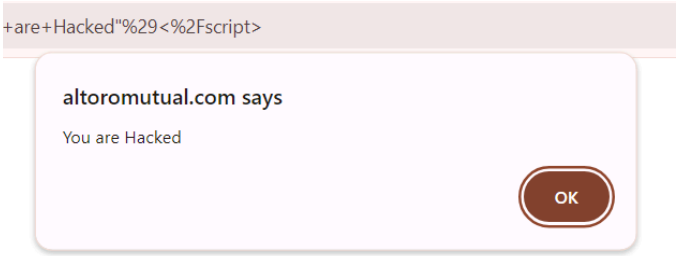
Credits

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
1001160140	03/01/2005	Paycheck	1200
1001160140	03/15/2005	Paycheck	1200

We also got access to account data, this vulnerability is called Sensitive Data Exposure.

Step 4: Vulnerability Exploitation Demonstration

To demonstrate this we inject a script to altoro mutual site
The script is , <script>alert(“You are hacked”)</script>



This is known as cross-site scripting .

Step 5: Mitigation Strategy Proposal:

Mitigations for the encountered vulnerabilities

Sensitive Data Exposure:

- Data Encryption: Encrypt sensitive data both at rest (stored data) and in transit (data transmitted over networks). Use strong encryption algorithms and ensure that encryption keys are managed securely.
- Access Controls: Implement role-based access controls (RBAC) to restrict access to sensitive data based on the principle of least privilege. Only authorized users should have access to sensitive information. Utilize access control lists (ACLs) or other access management mechanisms to enforce data access policies and prevent unauthorized access.
- Secure Data Storage: Store sensitive data securely, following industry best practices and compliance standards. This may include using secure databases, encrypting data fields, and protecting data backups. Regularly review and audit data storage mechanisms to ensure compliance with security policies and standards.
- Input Validation and Sanitization: Implement robust input validation and data sanitization techniques to prevent injection attacks, such as SQL injection, NoSQL injection, or XSS (Cross-Site Scripting) attacks. Use parameterized queries and prepared statements to mitigate SQL injection vulnerabilities.
- Secure Configuration: Follow secure configuration guidelines for web servers, application servers, databases, and other components involved in handling sensitive data. Disable unnecessary services, default accounts, and unnecessary features.

Broken Authentication:

- Strong Authentication Mechanisms:
    - Implement strong authentication mechanisms, such as multi-factor authentication (MFA) or biometric authentication, to enhance the security of user authentication.
    - Enforce complex password policies, including requirements for minimum length, complexity, and expiration.

- Session Management:
    - Implement secure session management practices, including session timeouts, session regeneration after authentication, and secure cookie attributes (e.g., HttpOnly, Secure).
    - Use secure protocols (e.g., HTTPS) to encrypt session data during transmission.
- Account Lockout and Brute Force Protection:
    - Implement account lockout mechanisms to prevent brute force attacks on user accounts. After a certain number of failed login attempts, temporarily lock the account or introduce delays between login attempts.
    - Implement CAPTCHA challenges or other mechanisms to differentiate between human users and automated bots during authentication attempts.
- Credential Handling:
    - Follow secure password storage practices, such as hashing passwords with strong and industry-standard hashing algorithms (e.g., bcrypt, Argon2).
    - Avoid storing sensitive authentication credentials (e.g., passwords) in clear text or weakly encrypted formats.
- User Education and Awareness:
    - Educate users about best practices for creating and managing secure passwords, recognizing phishing attempts, and protecting their accounts from unauthorized access.