Assignment 4

Step 1: OWASP Top 10 Vulnerabilities Overview:

- OWASP Top 10 vulnerabilities represent the most critical security risks to web applications, including injection attacks, broken authentication, sensitive data exposure, XML external entities (XXE), etc.
- Discuss the potential impact of these vulnerabilities on web application security and the importance of addressing them to prevent exploitation by attackers.

Step 2: Altro Mutual Website Analysis:

- Students should explore various sections of the Altro Mutual website, including the login page, user registration, payment portal, contact forms, and any other interactive features.
- They should identify vulnerabilities such as SQL injection, cross-site scripting (XSS), insecure authentication mechanisms, insecure direct object references, etc., based on their understanding of the OWASP Top 10 list.

Step 3: Vulnerability Identification Report:

- The report should include a detailed description of Altro Mutual's website structure and functionality, including potential areas of vulnerability.
- For each identified vulnerability, students should provide an explanation of how it could be exploited by attackers and the potential impact on Altro Mutual's business operations and users.
- Recommendations for mitigating each vulnerability should be provided, such as implementing input validation, using parameterized queries to prevent SQL injection, implementing secure authentication mechanisms like multi-factor authentication (MFA), etc.

Step 4: Vulnerability Exploitation Demonstration

- Students can demonstrate how each identified vulnerability could be exploited using proof-of-concept attacks or simulation tools.
- For example, they could demonstrate how SQL injection attacks can be used to extract sensitive information from the database or how cross-site scripting (XSS) attacks can be used to execute malicious scripts in users' browsers.

Step 5: Mitigation Strategy Proposal:

- The mitigation strategy should prioritize addressing high-risk vulnerabilities identified in the vulnerability identification report.

Step 6: Documenting the Exploit Process:

- Document the exploit process, including the commands used, the output received, and any challenges encountered.