E commerce website

Current Risk Summary report

Wed Apr 23 2025 14:31:00 GMT+0000 (Coordinated Universal Time)

Project description:
A secure e commerce website for secure user interaction

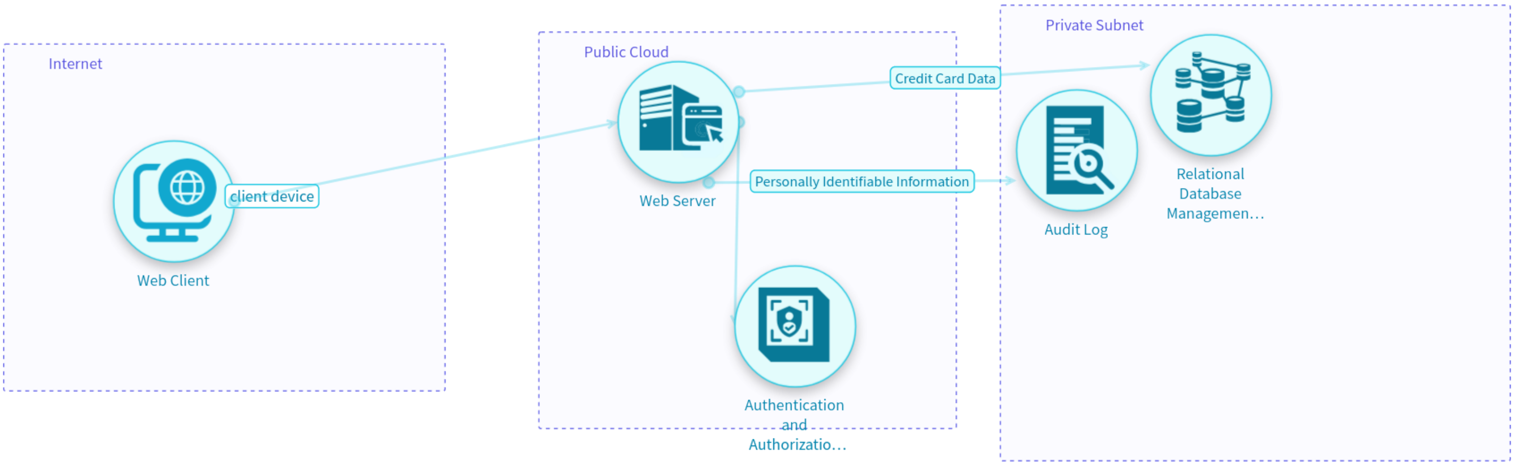
Filtered by: *No filters*

Unique ID: e-commerce-website-1745415526788

Owner: Muhammad Aurangzaib Bhatti

Workflow state: Draft

Tags: *No tags*


Internet
Web Client
client device
Public Cloud
Web Server
Credit Card Data
Personally Identifiable Information
Authentication and Authorizatio…
Private Subnet
Audit Log
Relational Database Managemen…

Content menu

Current Risk summary

Inherent risk description: The Inherent Risk before countermeasures were applied.

- **Risk Rating:** 63% ^ High

The Current Risk description (the risk we are at now): The Current Risk is based on the current implementation status of the countermeasures and test results.

- **Risk Rating:** 63% ^ High

Projected Risk description: The Projected Risk is the level of risk that would be reached should the required countermeasures be implemented.

- **Risk Rating:** 63% ^ High

Components

- Audit Log

  Model questionnaire information:

  - **Personally Identifiable Information: How is it handled by this component?** Received by component

- Authentication and Authorization Module
- Relational Database Management System (RDBMS)

  Model questionnaire information:

  - **Credit Card Data: How is it handled by this component?** Received by component

- Web Client
- Web Server

  Model questionnaire information:

  - **Credit Card Data: How is it handled by this component?** Sent from component
  - **Personally Identifiable Information: How is it handled by this component?** Sent from component

Accepted Risks

No data

Current Risks

Component: Audit Log

Use case: Repudiation

CRT1. Threat name: Attackers rely on the lack of monitoring and timely response to achieve their goals without being detected

- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR1. Countermeasure name:** Ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion
  - **Status:** RECOMMENDED
- **CR2. Countermeasure name:** Log and reject all data validation failures
  - **Status:** RECOMMENDED
- **CR3. Countermeasure name:** Ensure that logs are generated in a format that log management solutions can easily consume
  - **Status:** RECOMMENDED

Use case: Tampering

CRT2. Threat name: The attacker injects, manipulates or forges malicious log entries in the log file, allowing them to mislead a log audit, cover traces of attack, or perform log injection attacks

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR4. Countermeasure name:** Develop a log retention policy
  - **Status:** RECOMMENDED
- **CR5. Countermeasure name:** Log details of user actions within the system
  - **Status:** RECOMMENDED

Component: Authentication and Authorization Module

Use case: Elevation of Privilege

CRT3. Threat name: Attackers gain unauthorized access or elevated privileges, e.g., via stolen credentials, cookies, or tokens

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR6. Countermeasure name:** Use secure access control mechanisms
  - **Status:** RECOMMENDED

Use case: Tampering

CRT4. Threat name: Attackers inject malicious content, e.g., SQL queries, to manipulate or access data

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR7. Countermeasure name:** Input validation and sanitization
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT5. Threat name: Attackers intercept or eavesdrop on sensitive information during transmission

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR8. Countermeasure name:** Enforce secure configuration and encryption
  - **Status:** RECOMMENDED

Use case: Denial of Service

CRT6. Threat name: Attackers use enumeration to discover valid user identifiers, potentially creating a Denial of Service (DoS) condition

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR9. Countermeasure name:** Rate limiting and proper resource management

  - **Status:** RECOMMENDED

Use case: Repudiation

CRT7. Threat name: Lack of evidences of misuse due to insufficient logging

- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR10. Countermeasure name:** Create a policy and workflow for comprehensive logging and monitoring
  - **Status:** RECOMMENDED

Component: Relational Database Management System (RDBMS)

Use case: Tampering

CRT8. Threat name: An attacker can exploit SQL injection vulnerabilities

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR11. Countermeasure name:** Use parameterized queries
  - **Status:** RECOMMENDED

Use case: Elevation of Privilege

CRT9. Threat name: An attacker can gain unauthorized access to the database

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR12. Countermeasure name:** Implement strong authentication mechanisms
  - **Status:** RECOMMENDED

CRT10. Threat name: An attacker can perform database privilege escalation

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR13. Countermeasure name:** Adopt the principle of least privilege
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT11. Threat name: An attacker can perform data exfiltration through insecure backups

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR14. Countermeasure name:** Secure backup storage and access controls
  - **Status:** RECOMMENDED

Component: Web Client

Use case: Spoofing

CRT12. Threat name: Clickjacking

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR15. Countermeasure name:** Detect and block UI redressing attempts
  - **Status:** RECOMMENDED

Use case: Tampering

CRT13. Threat name: Client-side insecure data storage

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose

- **CR16. Countermeasure name:** Prevent storage of sensitive data on the client
  - **Status:** RECOMMENDED

CRT14. Threat name: Cross-site scripting

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR17. Countermeasure name:** Avoid unsafe DOM manipulation and isolate untrusted scripts
  - **Status:** RECOMMENDED

CRT15. Threat name: Man-in-the-middle attacks

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR18. Countermeasure name:** Ensure secure communication and validate external resources
  - **Status:** RECOMMENDED

Component: Web Server

Use case: Elevation of Privilege

CRT16. Threat name: Attackers carry out cross-service attacks

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR19. Countermeasure name:** Use virtualization/containerization to isolate servers and services
  - **Status:** RECOMMENDED

Use case: Denial of Service

CRT17. Threat name: Attackers cause a service disruption, e.g., DoS

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR20. Countermeasure name:** Protect the system and application against resource abuse
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT18. Threat name: Attackers gain access to information about the server, e.g., verbose errors or misconfiguration

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR21. Countermeasure name:** Secure configuration and server hardening
  - **Status:** RECOMMENDED

CRT19. Threat name: Insufficient logging

- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR22. Countermeasure name:** Ensure proper logging and monitoring
  - **Status:** RECOMMENDED

Use case: Spoofing

CRT20. Threat name: Attackers intercept and tamper with data

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR23. Countermeasure name:** Ensure the use of a secure form of communication, e.g. TLSv1.2 and above
  - **Status:** RECOMMENDED

Use case: Tampering

CRT21. Threat name: Attackers manipulate SSL/TLS weaknesses, e.g., Heartbleed

- **Inherent risk:** ^ High
- **Current risk:** ^ High
- **Projected risk:** ^ High
- **State:** Expose
- **CR24. Countermeasure name:** Implement strong and up-to-date cipher suites
  - **Status:** RECOMMENDED

CRT22. Threat name: Attackers manipulate the server in unintended ways, e.g., injection attacks

- **Inherent risk:** ^ High
- **Current risk:** ^ High
- **Projected risk:** ^ High
- **State:** Expose
- **CR25. Countermeasure name:** Ensure proper resources and system manipulation prevention
  - **Status:** RECOMMENDED

End of Current Risk Report