Ride-hailing-website

Current Risk Summary report

Fri May 09 2025 04:58:16 GMT+0000 (Coordinated Universal Time)

Project description: *No description*

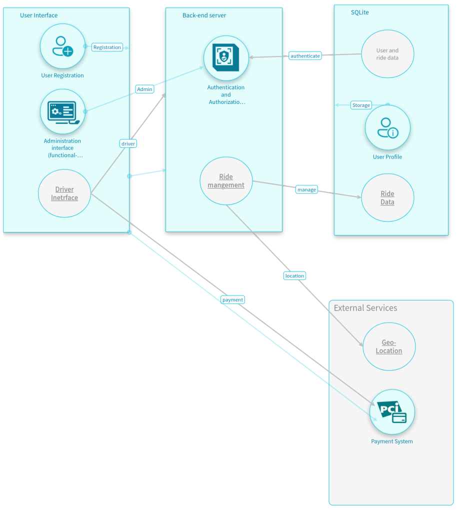
Filtered by: *No filters*

Unique ID: ride-hailing-website-1746764099620

Owner: Arsalan Khan

Workflow state: Draft

Tags: *No tags*



Content menu

Current Risk summary

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

- **Risk Rating:** 77% Critical

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:** 77% Critical

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

- **Risk Rating:** 74% High

Components

- Administration interface (functional-components)

  Model questionnaire information:
  - **Credit Card Data: How is it handled by this component?** Stored
  - **Customer Data: How is it handled by this component?** Stored
  - **Personally Identifiable Information: How is it handled by this component?** Sent from component
- Authentication and Authorization Module

  Model questionnaire information:
  - **Credit Card Data: How is it handled by this component?** Processed
  - **Customer Data: How is it handled by this component?** Processed
  - **Personally Identifiable Information: How is it handled by this component?** Processed
  - **Protected Health Information: How is it handled by this component?** Processed
- Back-end server

  Model questionnaire information:
  - **Credit Card Data: How is it handled by this component?** Stored
  - **Customer Data: How is it handled by this component?** Stored
  - **Personally Identifiable Information: How is it handled by this component?** Processed
  - **Protected Health Information: How is it handled by this component?** Processed
- Payment System

  Model questionnaire information:
  - **Credit Card Data: How is it handled by this component?** Processed
  - **Customer Data: How is it handled by this component?** Processed
  - **Personally Identifiable Information: How is it handled by this component?** Processed
  - **Protected Health Information: How is it handled by this component?** Processed
- SQLite

  Model questionnaire information:
  - **Credit Card Data: How is it handled by this component?** Stored
  - **Credit Card Data: How is it handled by this component?** Processed
  - **Customer Data: How is it handled by this component?** Stored
  - **Personally Identifiable Information: How is it handled by this component?** Stored
  - **Protected Health Information: How is it handled by this component?** Stored
- User Interface
- User Profile

  Model questionnaire information:
  - **Credit Card Data: How is it handled by this component?** Stored
  - **Customer Data: How is it handled by this component?** Stored
  - **Personally Identifiable Information: How is it handled by this component?** Stored
  - **Protected Health Information: How is it handled by this component?** Stored
- User Registration

  Model questionnaire information:
  - **Are you preventing user enumeration (a process where attackers attempt to discover valid usernames) and automated attacks (such as bots trying to gain unauthorized access)?** Not sure
  - **Are you using strong password policies and multi-factor authentication (an additional security step requiring more than just a password) for user registration and account protection?** No, but it is required
  - **Credit Card Data: How is it handled by this component?** Processed
  - **Customer Data: How is it handled by this component?** Processed
  - **Does this component handle personally identifiable information from citizens of the European Union?** No
  - **Does this component have to be CCPA-compliant?** No
  - **Personally Identifiable Information: How is it handled by this component?** Processed
  - **Protected Health Information: How is it handled by this component?** Processed

Accepted Risks

No data

Current Risks

Component: Administration interface (functional-components)

Use case: Elevation of Privilege

CRT1. Threat name: Attackers gain access to the system through an unprotected administration interface

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR1. Countermeasure name:** Restrict access to administrative functionality
  - **Status:** RECOMMENDED
- **CR2. Countermeasure name:** Restrict access to administrative interfaces
  - **Status:** RECOMMENDED

Component: Authentication and Authorization Module

Use case: Elevation of Privilege

CRT2. 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
- **CR3. Countermeasure name:** Use secure access control mechanisms
  - **Status:** RECOMMENDED

Use case: Tampering

CRT3. 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
- **CR4. Countermeasure name:** Input validation and sanitization
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT4. Threat name: Attackers intercept or eavesdrop on sensitive information during transmission

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR5. Countermeasure name:** Enforce secure configuration and encryption
  - **Status:** RECOMMENDED

Use case: Denial of Service

CRT5. 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
- **CR6. Countermeasure name:** Rate limiting and proper resource management
  - **Status:** RECOMMENDED

Use case: Repudiation

CRT6. Threat name: Lack of evidences of misuse due to insufficient logging

- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR7. Countermeasure name:** Create a policy and workflow for comprehensive logging and monitoring
  - **Status:** RECOMMENDED

Component: Back-end server

Use case: General

CRT7. Threat name: Back-end servers used as a means to attack a vehicle or extract data

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR8. Countermeasure name:** Prevent unauthorized access through system design
  - **Status:** RECOMMENDED
- **CR9. Countermeasure name:** Minimize unauthorized access
  - **Status:** RECOMMENDED
- **CR10. Countermeasure name:** Minimize the risk of insider attack
  - **Status:** RECOMMENDED

CRT8. Threat name: Services from back-end server being disrupted affecting the operation of a vehicle

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR11. Countermeasure name:** Prepare recovery measures in case of system outage
  - **Status:** RECOMMENDED

CRT9. Threat name: Vehicle related data held on back-end servers being lost or compromised

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR12. Countermeasure name:** Minimize risks associated with cloud computing
  - **Status:** RECOMMENDED
- **CR13. Countermeasure name:** Prevent data breaches
  - **Status:** RECOMMENDED

Component: Payment System

Use case: Information Disclosure

CRT10. Threat name: Attackers can compromise third-party vendors, leading to a breach of the payment system

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR14. Countermeasure name:** Conduct thorough security assessments and due diligence before engaging with third-party vendors
  - **Status:** RECOMMENDED

CRT11. Threat name: Attackers can intercept sensitive payment data, such as credit card information

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR15. Countermeasure name:** Implement end-to-end encryption
  - **Status:** RECOMMENDED

CRT12. Threat name: Attackers may attempt to gain unauthorized access to the payment system

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR16. Countermeasure name:** Use role-based access controls (RBAC)
  - **Status:** RECOMMENDED
- **CR17. Countermeasure name:** Implement strong authentication mechanisms
  - **Status:** RECOMMENDED

Use case: Denial of Service

CRT13. Threat name: Attackers may attempt to overload the payment system with excessive requests

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR18. Countermeasure name:** Deploy anti-DoS measures such as rate limiting, traffic filtering, and the use of web application firewalls (WAF)
  - **Status:** RECOMMENDED

Use case: Repudiation

CRT14. Threat name: Employees or other insiders may intentionally or unintentionally compromise the security of the payment system

- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR19. Countermeasure name:** Use logging and auditing to detect unauthorized access or suspicious behavior
  - **Status:** RECOMMENDED

Component: SQLite

Use case: Tampering

CRT15. Threat name: Attackers exploit outdated SQLite vulnerabilities

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR20. Countermeasure name:** Regularly update SQLite to the latest secure version
  - **Status:** RECOMMENDED

CRT16. Threat name: Attackers inject malicious SQL commands via SQL injection

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR21. Countermeasure name:** Use parameterized queries and input validation
  - **Status:** RECOMMENDED

CRT17. Threat name: Attackers tamper with data due to physical access to the database file

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR22. Countermeasure name:** Use full disk encryption and secure backup mechanisms
  - **Status:** RECOMMENDED

Use case: Elevation of Privilege

CRT18. Threat name: Attackers gain unauthorized access due to insecure file permissions

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR23. Countermeasure name:** Enforce secure file permissions on the database file
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT19. Threat name: Data exposure through insecure backup of the SQLite database

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR24. Countermeasure name:** Implement secure backup procedures with encryption and access controls
  - **Status:** RECOMMENDED

CRT20. Threat name: Data leakage due to unencrypted SQLite database file

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR25. Countermeasure name:** Encrypt the SQLite database file (e.g., using SQLCipher)
  - **Status:** RECOMMENDED

Component: User Interface

Use case: Spoofing

CRT21. Threat name: An attacker can perform clickjacking attacks

- **Inherent risk:** Critical
- **Current risk:** Critical

- **Projected risk:** Critical
- **State:** Expose
- **CR26. Countermeasure name:** Implement frame busting techniques
  - **Status:** RECOMMENDED
- **CR27. Countermeasure name:** Use X-Frame-Options header
  - **Status:** RECOMMENDED

CRT22. Threat name: An attacker can perform UI redressing attacks

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR28. Countermeasure name:** Use multi-factor authentication
  - **Status:** RECOMMENDED
- **CR29. Countermeasure name:** Implement visual cues and indicators
  - **Status:** RECOMMENDED

Use case: Tampering

CRT23. Threat name: An attacker can perform cross-site scripting (XSS) attacks

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR30. Countermeasure name:** Implement input validation and sanitization
  - **Status:** RECOMMENDED
- **CR31. Countermeasure name:** Use Content Security Policy (CSP)
  - **Status:** RECOMMENDED

Use case: Denial of Service

CRT24. Threat name: An attacker can perform denial-of-service (DoS) attacks on the user interface

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR32. Countermeasure name:** Use load balancing and scaling
  - **Status:** RECOMMENDED
- **CR33. Countermeasure name:** Implement rate limiting
  - **Status:** RECOMMENDED

Component: User Profile

Use case: Spoofing

CRT25. Threat name: Attackers exploit flaws in access control systems

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR34. Countermeasure name:** Implement Multi-Factor Authentication (MFA)
  - **Status:** RECOMMENDED

Use case: Tampering

CRT26. Threat name: Attackers inject malicious code into systems by exploiting security weaknesses

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR35. Countermeasure name:** Sanitize all input to avoid injection attacks
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT27. Threat name: Attackers take advantage of exposed sensitive data

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR36. Countermeasure name:** Implement secure session management

  - **Status:** RECOMMENDED

Component: User Registration

Use case: Spoofing

CRT28. Threat name: Attackers assume the identity of legitimate users

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Very Low
- **State:** Expose
- **CR37. Countermeasure name:** Ensure the integrity and security of the registration process and user accounts
  - **Status:** REQUIRED

CRT29. Threat name: Attackers create malicious or fake accounts

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR38. Countermeasure name:** Harden the registration process
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT30. Threat name: Attackers enumerate users

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR39. Countermeasure name:** Prevent user enumeration and other automated attacks
  - **Status:** RECOMMENDED

CRT31. Threat name: Insecure data storage, e.g., passwords

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR40. Countermeasure name:** Handle secrets and user data securely
  - **Status:** RECOMMENDED

Use case: Tampering

CRT32. Threat name: Attackers inject malicious code through input fields

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR41. Countermeasure name:** Sanitize and validate all user inputs
  - **Status:** RECOMMENDED

Use case: Repudiation

CRT33. Threat name: Insufficient logging and monitoring

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR42. Countermeasure name:** Implement comprehensive logging and monitoring
  - **Status:** RECOMMENDED

End of Current Risk Report