natural-row-bece1e61

Current Risk Summary report

Tue Apr 01 2025 11:06:01 GMT+0000 (Coordinated Universal Time)

Project description: *No description*

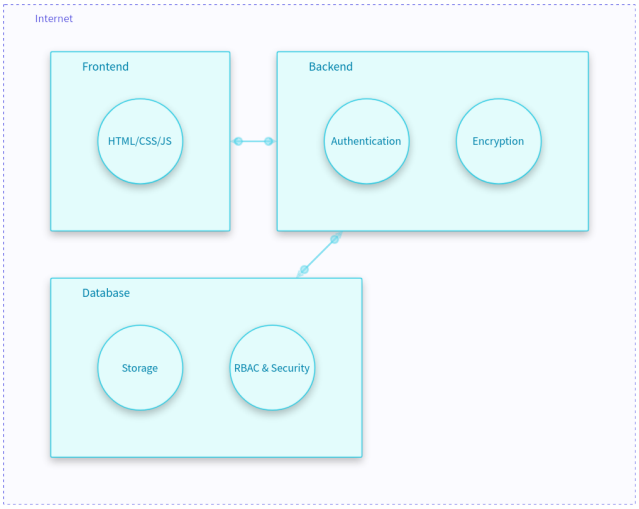
Filtered by: No filters

Unique ID: bcc75c44-9515-490a-ac4b-715bcd56cfa0

Owner: sohaib khan

Workflow state: Draft

Tags: *No tags*



Content menu

Current Risk summary

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

- **Risk Rating:** 64% 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:** 64% High

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

- **Risk Rating:** 64% High

Components

- Authentication
- Backend
- Database
- Encryption
- Frontend
- HTML/CSS/JS
- RBAC & Security
- Storage

Accepted Risks

No data

Current Risks

Component: Authentication

Use case: Elevation of Privilege

CRT1. Threat name: Attackers access the system taking advantage of broken authentication
- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR1. Countermeasure name:** Implement server-side access control checks
  - **Status:** RECOMMENDED

CRT2. Threat name: Attackers exploit flaws in access control systems
- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR2. Countermeasure name:** Implement secure session management
  - **Status:** RECOMMENDED
- **CR3. Countermeasure name:** Implement Multi-Factor Authentication (MFA)
  - **Status:** RECOMMENDED

Use case: Tampering

CRT3. Threat name: Attackers capitalize on security misconfigurations
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR4. Countermeasure name:** Conduct regular security audits and reviews
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT4. Threat name: Attackers get access to sensitive data
- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR5. Countermeasure name:** Use encryption to protect sensitive data
  - **Status:** RECOMMENDED

Component: Backend

Use case: Tampering

CRT5. Threat name: Attacker exploit misconfiguration and Vulnerable Third-Party
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR6. Countermeasure name:** Comprehensive Configuration Hardening and Dependency Auditing
  - **Status:** RECOMMENDED

CRT6. Threat name: Attackers execute Injection Attacks
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR7. Countermeasure name:** Use Parameterized Queries and Input Validation
  - **Status:** RECOMMENDED

Use case: Spoofing

CRT7. Threat name: Attackers gain elevated privileges or unauthorized access
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose

- **CR8. Countermeasure name:** Implement Multi-layered Security for Authentication and Access Control
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT8. Threat name: Attackers gather useful information from inadequate Error Handling
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR9. Countermeasure name:** Implement Generic Error Messages and Proper Exception Handling
  - **Status:** RECOMMENDED

CRT9. Threat name: Attackers take advantage of insecure communication channels and unprotected sessions
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR10. Countermeasure name:** Implement Comprehensive Secure Communication and Session Management Protocols
  - **Status:** RECOMMENDED

CRT10. Threat name: Attackers take advantage of weak encryption of sensitive Data
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR11. Countermeasure name:** Implement and Maintain Advanced Encryption Standards with Effective Key Management
  - **Status:** RECOMMENDED

Use case: Denial of Service

CRT11. Threat name: Attackers perform a Denial of Service (DoS)
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR12. Countermeasure name:** Implement Rate Limiting and Resource Allocation
  - **Status:** RECOMMENDED

Use case: Repudiation

CRT12. Threat name: Lack of evidences of misuse due to insufficient Auditing and Logging and poor log protection
- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR13. Countermeasure name:** Implement Comprehensive Logging and Monitoring with Log Integrity Measures
  - **Status:** RECOMMENDED

Component: Database

Use case: Denial of Service

CRT13. Threat name: Attackers cause denial of service through resource exhaustion
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR14. Countermeasure name:** Implement rate limiting and resource throttling
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT14. Threat name: Attackers exfiltrate data due to insecure backup procedures
- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR15. Countermeasure name:** Implement secure backup procedures with encryption and access controls
  - **Status:** RECOMMENDED

CRT15. Threat name: Attackers exploit misconfigurations in postgresql settings

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR16. Countermeasure name:** Harden postgresql configuration and restrict network access
  - **Status:** RECOMMENDED

CRT16. Threat name: Attackers exploit sql injection vulnerabilities
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR17. Countermeasure name:** Use parameterized queries and validate inputs
  - **Status:** RECOMMENDED

CRT17. Threat name: Attackers intercept data due to unencrypted communications
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR18. Countermeasure name:** Enforce TLS encryption for all connections
  - **Status:** RECOMMENDED

Use case: Tampering

CRT18. Threat name: Attackers exploit outdated postgresql vulnerabilities
- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR19. Countermeasure name:** Regularly update postgresql to the latest secure version
  - **Status:** RECOMMENDED

CRT19. Threat name: Attackers tamper with data due to insecure file permissions
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR20. Countermeasure name:** Enforce secure file permissions on PostgreSQL database files
  - **Status:** RECOMMENDED

Use case: Spoofing

CRT20. Threat name: Attackers gain unauthorized access due to weak authentication
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR21. Countermeasure name:** Implement robust authentication and role-based access control
  - **Status:** RECOMMENDED

Component: Encryption

Use case: Tampering

CRT21. Threat name: Attacker exploit misconfiguration and Vulnerable Third-Party
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR22. Countermeasure name:** Comprehensive Configuration Hardening and Dependency Auditing
  - **Status:** RECOMMENDED

CRT22. Threat name: Attackers execute Injection Attacks
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR23. Countermeasure name:** Use Parameterized Queries and Input Validation
  - **Status:** RECOMMENDED

Use case: Spoofing

CRT23. Threat name: Attackers gain elevated privileges or unauthorized access
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR24. Countermeasure name:** Implement Multi-layered Security for Authentication and Access Control
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT24. Threat name: Attackers gather useful information from inadequate Error Handling
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR25. Countermeasure name:** Implement Generic Error Messages and Proper Exception Handling
  - **Status:** RECOMMENDED

CRT25. Threat name: Attackers take advantage of insecure communication channels and unprotected sessions
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR26. Countermeasure name:** Implement Comprehensive Secure Communication and Session Management Protocols
  - **Status:** RECOMMENDED

CRT26. Threat name: Attackers take advantage of weak encryption of sensitive Data
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR27. Countermeasure name:** Implement and Maintain Advanced Encryption Standards with Effective Key Management
  - **Status:** RECOMMENDED

Use case: Denial of Service

CRT27. Threat name: Attackers perform a Denial of Service (DoS)
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR28. Countermeasure name:** Implement Rate Limiting and Resource Allocation
  - **Status:** RECOMMENDED

Use case: Repudiation

CRT28. Threat name: Lack of evidences of misuse due to insufficient Auditing and Logging and poor log protection
- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR29. Countermeasure name:** Implement Comprehensive Logging and Monitoring with Log Integrity Measures
  - **Status:** RECOMMENDED

Component: Frontend

Use case: Spoofing

CRT29. Threat name: Attackers can deceive users into clicking on hidden elements
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR30. Countermeasure name:** Employ frame-busting scripts, set X-Frame-Options header, and enforce Content Security Policy
  - **Status:** RECOMMENDED

Use case: Tampering

CRT30. Threat name: Attackers can exploit vulnerabilities in third-party dependencies leading to security breaches
- **Inherent risk:** High
- **Current risk:** High
-

- **Projected risk:** High
- **State:** Expose
- **CR31. Countermeasure name:** Regularly update dependencies, use dependency scanning tools, and follow best practices for secure coding
  - **Status:** RECOMMENDED

CRT31. Threat name: Attackers can inject malicious scripts into web pages viewed by other users
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR32. Countermeasure name:** Implement input validation, output encoding, and enforce Content Security Policy (CSP)
  - **Status:** RECOMMENDED

Use case: Elevation of Privilege

CRT32. Threat name: Attackers may exploit weaknesses in authentication and authorization mechanisms
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR33. Countermeasure name:** Implement strong authentication mechanisms and follow the least privilege principle
  - **Status:** RECOMMENDED

Component: HTML/CSS/JS

Use case: Spoofing

CRT33. Threat name: Attackers can deceive users into clicking on hidden elements
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR34. Countermeasure name:** Employ frame-busting scripts, set X-Frame-Options header, and enforce Content Security Policy
  - **Status:** RECOMMENDED

Use case: Tampering

CRT34. Threat name: Attackers can exploit vulnerabilities in third-party dependencies leading to security breaches
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR35. Countermeasure name:** Regularly update dependencies, use dependency scanning tools, and follow best practices for secure coding
  - **Status:** RECOMMENDED

CRT35. Threat name: Attackers can inject malicious scripts into web pages viewed by other users
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR36. Countermeasure name:** Implement input validation, output encoding, and enforce Content Security Policy (CSP)
  - **Status:** RECOMMENDED

Use case: Elevation of Privilege

CRT36. Threat name: Attackers may exploit weaknesses in authentication and authorization mechanisms
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR37. Countermeasure name:** Implement strong authentication mechanisms and follow the least privilege principle
  - **Status:** RECOMMENDED

Component: RBAC & Security

Use case: Elevation of Privilege

CRT37. 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

- **CR38. Countermeasure name:** Use secure access control mechanisms
  - **Status:** RECOMMENDED

Use case: Tampering

CRT38. 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
- **CR39. Countermeasure name:** Input validation and sanitization
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT39. Threat name: Attackers intercept or eavesdrop on sensitive information during transmission
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR40. Countermeasure name:** Enforce secure configuration and encryption
  - **Status:** RECOMMENDED

Use case: Denial of Service

CRT40. 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
- **CR41. Countermeasure name:** Rate limiting and proper resource management
  - **Status:** RECOMMENDED

Use case: Repudiation

CRT41. Threat name: Lack of evidences of misuse due to insufficient logging
- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR42. Countermeasure name:** Create a policy and workflow for comprehensive logging and monitoring
  - **Status:** RECOMMENDED

Component: Storage

Use case: Information Disclosure

CRT42. Threat name: An attacker exploits weak access controls to retrieve sensitive secrets
- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR43. Countermeasure name:** Implement strict access control policies
  - **Status:** RECOMMENDED

CRT43. Threat name: Compromised systems reuse leaked or old secrets
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR44. Countermeasure name:** Implement automatic secret rotation
  - **Status:** RECOMMENDED

CRT44. Threat name: Overly permissive secrets sharing between services leads to data leakage
- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR45. Countermeasure name:** Restrict secret sharing based on least privilege
  - **Status:** RECOMMENDED

CRT45. Threat name: Secrets are stored without encryption, leading to potential exposure

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR46. Countermeasure name:** Enforce encryption of secrets at rest and in transit
  - **Status:** RECOMMENDED

Use case: Elevation of Privilege

CRT46. Threat name: Attackers exploit vulnerabilities in the Secrets Manager API

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR47. Countermeasure name:** Secure the API with strong authentication and input validation
  - **Status:** RECOMMENDED

End of Current Risk Report