Anti Phishing Browser Extension

Current Risk Summary report

Sun Apr 20 2025 17:55:48 GMT+0000 (Coordinated Universal Time)

Project description: *No description*

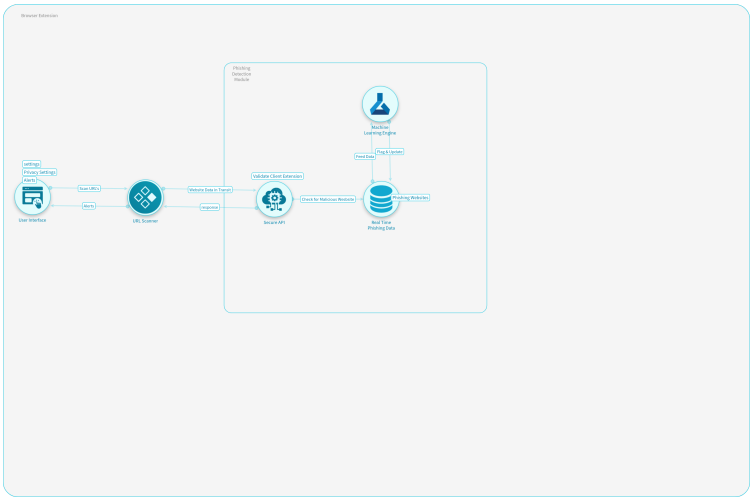
Filtered by: *No filters*

Unique ID: anti-phishing-browser-extension-1745167653042

Owner: Shameer Awais

Workflow state: Draft

Tags: *No tags*



Content menu

Current Risk summary

Inherent risk description: The Inherent Risk before countermeasures were applied.
- **Risk Rating:** 76% 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:** 76% Critical

Projected Risk description: The Projected Risk is the level of risk that would be reached should the required countermeasures be implemented.
- **Risk Rating:** 76% Critical

Components

- Machine Learning Engine
- Real Time Phishing Data
- Secure API
- URL Scanner
- User Interface

Accepted Risks

No data

Current Risks

Component: Machine Learning Engine

Use case: Information Disclosure

CRT1. Threat name: Improper storage and handling of credentials and secrets
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR1. Countermeasure name:** Restrict the exposure of credential and secrets
  - **Status:** RECOMMENDED
- **CR2. Countermeasure name:** Restrict resource access based on conditions
  - **Status:** RECOMMENDED
- **CR3. Countermeasure name:** Manage application identities securely and automatically
  - **Status:** RECOMMENDED

CRT2. Threat name: Unauthorized access to customer-managed encryption keys and data exfiltration
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR4. Countermeasure name:** Use a secure key management process
  - **Status:** RECOMMENDED
- **CR5. Countermeasure name:** Use customer-managed key option in data at rest encryption when required
  - **Status:** RECOMMENDED
- **CR6. Countermeasure name:** Monitor anomalies and threats targeting sensitive data
  - **Status:** RECOMMENDED
- **CR7. Countermeasure name:** Discover, classify, and label sensitive data
  - **Status:** RECOMMENDED

Use case: Elevation of Privilege

CRT3. Threat name: Pre-installed ClamAV can be used to bypass malware detection
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR8. Countermeasure name:** Ensure anti-malware software and signatures are updated
  - **Status:** RECOMMENDED
- **CR9. Countermeasure name:** Use modern anti-malware software
  - **Status:** RECOMMENDED

Use case: Tampering

CRT4. Threat name: Unauthorized configuration changes detected in Azure resources
- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR10. Countermeasure name:** Use only approved services
  - **Status:** RECOMMENDED

Component: Real Time Phishing Data

Use case: Information Disclosure

CRT5. Threat name: Attackers exfiltrate data due to insecure backup procedures
- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR11. Countermeasure name:** Implement secure backup procedures with encryption and access controls
  - **Status:** RECOMMENDED

CRT6. Threat name: Attackers exploit misconfigurations in database settings
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR12. Countermeasure name:** Harden configuration and restrict network access

- **Status:** RECOMMENDED

CRT7. Threat name: Attackers intercept data due to unencrypted communications
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR13. Countermeasure name:** Enforce TLS encryption for all connections
  - **Status:** RECOMMENDED

Use case: Elevation of Privilege

CRT8. Threat name: Attackers exploit outdated vulnerabilities
- **Inherent risk:** Medium
- **Current risk:** Medium
- **Projected risk:** Medium
- **State:** Expose
- **CR14. Countermeasure name:** Regularly update the database to the latest secure version
  - **Status:** RECOMMENDED

Use case: Tampering

CRT9. Threat name: Attackers exploit SQL injection vulnerabilities
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR15. Countermeasure name:** Use parameterized queries and validate inputs
  - **Status:** RECOMMENDED

Use case: Spoofing

CRT10. Threat name: Attackers gain unauthorized access due to weak authentication
- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR16. Countermeasure name:** Implement strong authentication and role-based access control
  - **Status:** RECOMMENDED

Component: Secure API

Use case: Tampering

CRT11. Threat name: Attackers compromise the system through inadequate input validation
- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR17. Countermeasure name:** Use Parameterized Queries and Input Validation
  - **Status:** RECOMMENDED

CRT12. Threat name: Attackers manipulate SSRF weaknesses to compromise the system
- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR18. Countermeasure name:** Validate Input and Implement Allowlists
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT13. Threat name: Attackers expose sensitive data
- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR19. Countermeasure name:** Apply Strong Encryption
  - **Status:** RECOMMENDED

Use case: Spoofing

CRT14. Threat name: Attackers gain control of users' accounts in the system by abusing poorly implemented API authentication

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR20. Countermeasure name:** Implement best practices for API authentication
  - **Status:** RECOMMENDED

Use case: Repudiation

CRT15. Threat name: Attackers go undetected by exploiting insufficient logging and monitoring

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR21. Countermeasure name:** Implement Comprehensive Logging and SIEM Integration
  - **Status:** RECOMMENDED

Use case: Elevation of Privilege

CRT16. Threat name: Attackers take advantage of weaknesses in access controls

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR22. Countermeasure name:** Implement a proper authorization mechanism that relies on the user policies and hierarchy
  - **Status:** RECOMMENDED

Use case: Denial of Service

CRT17. Threat name: Over consumption of the resources of the API server can render it inaccessible

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR23. Countermeasure name:** Use Rate Limiting and Throttling
  - **Status:** RECOMMENDED

Component: URL Scanner

Use case: Tampering

CRT18. Threat name: Attackers can alter or tamper with URLs to deceive users or exploit vulnerabilities in web applications

- **Inherent risk:** High
- **Current risk:** High
- **Projected risk:** High
- **State:** Expose
- **CR24. Countermeasure name:** Implement URL validation and sanitize user-provided URLs extracted from QR codes
  - **Status:** RECOMMENDED
- **CR25. Countermeasure name:** Verify the authenticity and integrity of the scanned URLs before processing or redirecting users
  - **Status:** RECOMMENDED

CRT19. Threat name: Attackers can create QR codes to deceive users by displaying false or misleading information

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR26. Countermeasure name:** Use unique QR code designs or cryptographic signatures to validate the authenticity of QR codes
  - **Status:** RECOMMENDED

CRT20. Threat name: Attackers can exploit vulnerabilities in QR code scanning software or deceive users into taking unintended actions

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR27. Countermeasure name:** Implement strict input validation and sanitization techniques to prevent malicious QR codes
  - **Status:** RECOMMENDED

Use case: Information Disclosure

CRT21. Threat name: Unauthorized or unintentional disclosure of sensitive or confidential information

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR28. Countermeasure name:** Minimize the amount of sensitive or personal information stored within QR codes
  - **Status:** RECOMMENDED
- **CR29. Countermeasure name:** Encrypt sensitive information before embedding it into the QR code
  - **Status:** RECOMMENDED

Component: User Interface

Use case: Spoofing

CRT22. Threat name: An attacker can perform clickjacking attacks

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR30. Countermeasure name:** Implement frame busting techniques
  - **Status:** RECOMMENDED
- **CR31. Countermeasure name:** Use X-Frame-Options header
  - **Status:** RECOMMENDED

CRT23. Threat name: An attacker can perform UI redressing attacks

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR32. Countermeasure name:** Implement visual cues and indicators
  - **Status:** RECOMMENDED
- **CR33. Countermeasure name:** Use multi-factor authentication
  - **Status:** RECOMMENDED

Use case: Tampering

CRT24. Threat name: An attacker can perform cross-site scripting (XSS) attacks

- **Inherent risk:** Critical
- **Current risk:** Critical
- **Projected risk:** Critical
- **State:** Expose
- **CR34. Countermeasure name:** Use Content Security Policy (CSP)
  - **Status:** RECOMMENDED
- **CR35. Countermeasure name:** Implement input validation and sanitization
  - **Status:** RECOMMENDED

Use case: Denial of Service

CRT25. 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
- **CR36. Countermeasure name:** Use load balancing and scaling
  - **Status:** RECOMMENDED
- **CR37. Countermeasure name:** Implement rate limiting
  - **Status:** RECOMMENDED

End of Current Risk Report