Let's make digital change happen

Vulnerability Report

HTC Global – Automated Security Report Tool

Report Title	Vulnerability Assessment Report
Organization	HTC Global
Generated By	Automated Security Tool
Report Date	17-Sep-2025
Classification	Confidential – Internal Use Only

This automated report provides an overview of security vulnerabilities identified during the assessment. The findings are mapped to the OWASP Top 10 categories and include detailed descriptions, proofs of concept, and remediation steps.

Table of Contents

Cryptographic Failures

OWASP Category	A02:2021 – Cryptographic Failures
Severity	High
Affected Component	Data storage, communication channels, authentication mechanisms, encryption/decryption functions
Status	Active / Needs Remediation

Description

Cryptographic Failures occur when sensitive data is not properly protected using strong cryptography, including weak algorithms, poor key management, improper TLS/SSL usage, or storing secrets insecurely.

Proof of Concept

- Intercept traffic via Burp Suite and observe credentials in plaintext HTTP
- Decrypt MD5 hashed password using public rainbow tables
- Check TLS configuration: accepts SSLv3 and weak ciphers

Steps to Reproduce

1. Intercept network traffic using Burp Suite or Wireshark.
2. Check if sensitive data is transmitted in plaintext.
3. Review stored data and attempt decryption with weak algorithms.
4. Search code for hardcoded encryption keys.
5. Test TLS configuration for weak ciphers or outdated protocols.

Recommendation

Use strong encryption algorithms, proper key management, enforce HTTPS/TLS 1.2+, avoid storing sensitive data in plaintext, use modern password hashing, review cryptographic implementations.

Risk Rating

Metric	Value
Base Score	7.5–9.0
Attack Vector	Network or Physical
Attack Complexity	Low to Medium
Privileges Required	None to Low
User Interaction	None

References

- https://owasp.org/Top10/A02_2021-Cryptographic_Failures/
- https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/10-Input_Validation_Testing/06-Cryptography_Testing.html
- https://cwe.mitre.org/data/definitions/310.html

Injection

OWASP Category	A03:2021 – Injection
Severity	High
Affected Component	Web applications, APIs, database queries, OS commands, LDAP, XML parsers
Status	Active / Needs Remediation

Description

Injection flaws occur when untrusted data is sent to an interpreter as part of a command or query, allowing attackers to execute unintended commands or access data without authorization.

Proof of Concept

- SQLi: ' OR '1'='1 --
- Command Injection: ; cat /etc/passwd
- LDAP Injection: (|(uid=*)(userPassword=*))
- XML Injection:

Steps to Reproduce

1. Identify all input points (forms, URL parameters, headers, APIs).
2. Test SQL Injection with payloads like `' OR '1'='1`.
3. Test Command Injection with OS commands in parameters.
4. Test LDAP Injection with malicious search filters.
5. Test XML Injection by modifying XML payloads.

Recommendation

Use parameterized queries, validate and sanitize input, enforce least privilege, avoid dynamic queries with untrusted data, consider WAF, perform automated and manual testing.

Risk Rating

Metric	Value
Base Score	8.0–9.0
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None

References

- https://owasp.org/Top10/A03_2021-Injection/
- https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/09-Injection_Testing.html
- https://cwe.mitre.org/data/definitions/89.html

Report Summary

This report contains details of 2 security vulnerabilities identified during the assessment.

This is a system-generated report. For internal use only.