Vulnerability Report

HTC Global – Automated Security Report Tool

Report Date: 16-Sep-2025
Generated By: Automated Security Tool

Confidential

Table of Contents

Security Misconfiguration

OWASP Category	A05:2021 – Security Misconfiguration
Severity	High
Affected Component	Web servers, application servers, databases, APIs, cloud services, network infrastructure
Status	Active / Needs Remediation

Description

Security Misconfiguration occurs when security settings are missing, misconfigured, or left at insecure defaults, including unnecessary services, outdated software, verbose error messages, default credentials, or open cloud storage.

Proof of Concept

- Accessing /.git/ directory reveals source code
- Login with default admin:admin credentials
- Directory listing enabled at /uploads/

Steps to Reproduce

1. Enumerate server/software versions using Nmap or Nikto.
2. Attempt login with default credentials.
3. Check cloud storage for public read/write access.
4. Review HTTP headers for missing security configurations.
5. Attempt directory listing or access to sensitive files.

Recommendation

Disable unused services, update/patch software, remove default credentials, implement secure headers, use automated config management, conduct regular audits.

Risk Rating

Metric	Value
Base Score	6.5–9.0

Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None

References

- https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
- https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/09-Configuration_and_Deployment_Management_Testing.html
- https://cwe.mitre.org/data/definitions/16.html

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

Report Summary

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

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