Public Report

Whistlelink Web Application and API Security Assessment

Title	Whistlelink Web Application and API Security Assessment Public Report
Version	1.0
Reporting Date	Monday, March 4, 2024
Prepared by	CT Defense
Prepared for	Whistleblowing Solutions AB
CT Defense Contact	Razvan Furdui, Cyber Operations Manager
Classification	Public

Document Control

Version	Date	Author	Change Description
0.1	Monday, September 04, 2023	Cyber Security Team	Security Assessment Start
0.2	Friday, September 08, 2023	Quality Control Manager	Security Assessment Report Delivery
0.3	Friday, February 16, 2024	Cyber Security Team	Vulnerability Remediation Verification Completed
1.0	Monday, March 4, 2024	Quality Control Manager	Public Report Delivery

CYBER THREAT DEFENSE
TURNING CYBER THREATS INTO ACTIONABLE INSIGHTS

Legal name: CT DEFENSE SRL	
Fiscal Code: RO38412840	**Phone**: 0040 752607204
Email: info@CTDefense.com	**Website**: CTDefense.com

CREST

CT Defense is a CREST Accredited Company in Penetration Testing.

Independent Security Assessment Report

CT Defense LTD (“CT Defense”) has performed the Web Application Security Assessment for Whistleblowing Solutions AB, (“Client”) while acting as an independent security assessor. This assessment was performed with the intent of evaluating the security and resiliency of the client’s Web Application and API Security Assessment scoped assets.

The methodology utilized during this assessment is detailed in Methodology. CT Defense developed this methodology based on extensive professional experience and information system security assessment best practices gathered from the NIST Risk Management Framework, Open Source Security Testing Methodology Manual ("OSSTMM"), the National Institute of Standards and Technology ("NIST") Special Publication 800-115: Technical Guide to Information Security Testing and Assessment, the Penetration Testing Execution Standard ("PTES"), NIST Guide Details Forensic Practices, various CIS Benchmarks, and the Open Web Application Security Project ("OWASP") Testing Guide.

While this type of assessment is intended to mimic a real-world attack scenario or identify the capacity of the existing controls, CT Defense is bound by rules of engagement, defined scope, allocated time, and additional related constraints. CT Defense has made every effort to perform a thorough analysis and to provide appropriate remedial advice. However, inherent limitations, errors, misrepresentations, and changes to the Client environment may have prevented CT Defense from identifying every security issue that was present in the Client environment at the time of testing. Therefore, the findings included in this report should be considered to be representative of what a similarly skilled attacker could achieve with comparable resources, constraints, and time frame.

Additionally, it is worth emphasizing that the findings and remediation recommendations are the result of a point-in-time assessment based on the state of the Client environment as of Friday, February 16, 2024. CT Defense therefore does not provide any assurance related to configuration or control modifications in the Client environment, changes in regulatory or compliance requirements, discoveries of new vulnerabilities and attack techniques, or any other future event that may impact the Client’s security posture.

The information contained in this report represents a fair and unbiased assessment of the Client’s environment based on the agreed-upon criteria as defined in the Statement of Work. This report is provided to the Client as notification of outstanding security risks that threaten the confidentiality, integrity, and availability of sensitive information, as well as to provide assistance and direction with remediation. The evidence and references provided for each finding serve as the basis for our qualified opinions in this report.

CT Defense has provided this report solely for private and internal use by the Client, and it may not be shared or redistributed without CT Defense’s express written consent. CT Defense’s assessments focus exclusively on information security and the conclusions arrived at in this report should not be considered to be a representation or endorsement of the Client’s products or services.

Razvan Furdui
Cyber Operations Manager

Scope of Work

Background Information

CT Defense performed a security audit following the Web Application Security Assessment methodology to assess the risk that a real-life, targeted attacker poses to the security and integrity of the client's assets. Understanding the current vulnerabilities is the first step in remediating and ultimately enhancing Whistleblowing Solutions AB's overall security maturity.

The purpose of the assignment was to identify and evaluate any risks or potential issues that could impact the Confidentiality, Integrity, or Availability of the systems in scope. In this assessment, both automated and manual security testing techniques were used to identify weaknesses in the systems in scope from an attacker's perspective.

CT Defense performed testing from both unauthenticated (anonymous) and authenticated perspectives. Unauthenticated testing identifies vulnerabilities and weaknesses available to anyone who possesses network connectivity to the Whistlelink Web Application and API environment. Authenticated testing identifies vulnerabilities and weaknesses in functionality that are only available to valid, authenticated users. Since most applications commonly limit anonymous access and provide the majority of their functionality to authenticated users, authenticated testing often provides the best insight into the security posture of the systems in scope.

Remediation Verification

Remediation verification was performed using an updated system version. All previously identified findings from the initial assessment were validated to confirm if successful remediation had occurred.

Scope Overview

The scope of the assessment included the following assets as authorized by Whistleblowing Solutions AB:

```
https://clients.preprod.wltoolbox.com
https://admin.preprod.wltoolbox.com
https://clients-api.preprod.wltoolbox.com
https://cyberthreatdefense1.preprod.wltoolbox.com
https://cyberthreatdefense2.preprod.wltoolbox.com
```

Timeframe

The Web Application Security Assessment was performed on the dates between **Monday, September 04, 2023** and **Friday, September 08, 2023.**

Remediation Verification was performed on **Friday, February 16, 2024.**

Limitations

This was a time-boxed security testing engagement. During a time-boxed engagement, the CTDefense team prioritizes testing to assess the most sensitive portions and functions of the application.

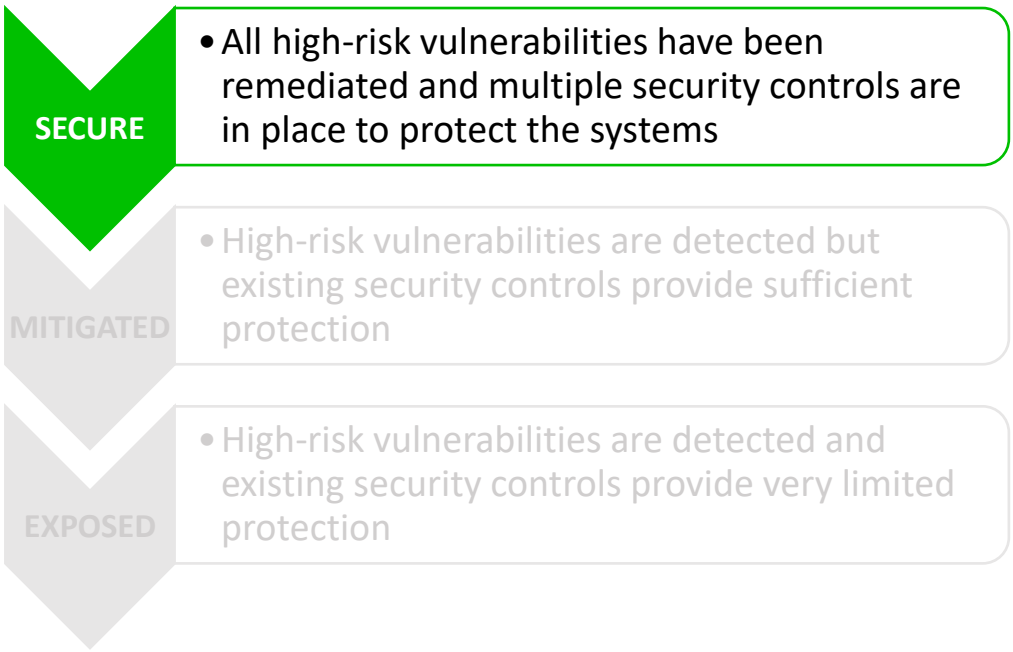
No other specific limitations were defined in the scoping phase by the client.

Summary of Findings

This section documents the results of the Web Application Security Assessment and remediation verification conducted for Whistleblowing Solutions AB. The security assessment was conducted by CT Defense's certified security engineers.

The Security team identified several security vulnerabilities and provided remediation advice to Whistleblowing Solutions AB.

After being notified by Whistleblowing Solutions AB that all vulnerabilities had been remediated, CT Defense performed a remediation test on Friday, February 16, 2024 and confirmed that the vast majority of findings identified were either corrected or had been adequately addressed through other controls.



Identified Security Controls

Security Control in place	State
Client-side controls denying client-side attacks	Good Practice
Rate-limiting mechanism is performing accordingly	Good Practice
Sensitive information is not sent via GET requests	Good Practice
Sensitive Information Enumeration is not possible anymore	Good Practice
Malicious Files are not accepted by the application	Good Practice
CORS Header follows a custom scheme	Good Practice
NO SSL/TLS Weak Ciphers are in use anymore	Good Practice
Multiple security-centred HTTP Response Headers are now in use	Good Practice

Final Statement

As a result of conducting this engagement and remediation verification, CT Defense has determined that cumulatively the vulnerabilities identified pose a **Low** risk to Whistlelink. While no application or

system can be 100% secure, all the security findings were corrected or addressed and it is confirmed that the systems in scope are reasonably well written from a security perspective and the supporting systems are deployed, configured, and implemented securely.