Secureworks

IAGON

Web Application Security Assessment Report

January 3, 2025

Presented To:

Nils I

Iagon

Submitted By:

Secureworks

Report Disclaimer Statement

Customer shall own all right, title, and interest in and to any written summaries, reports, analyses, and findings or other information or documentation prepared for Customer in connection with Secureworks' provision of the Consulting Services to Customer (the "Customer Reports"). The provision by Customer of any Customer Report or any information therein to any unaffiliated third party shall not entitle such third party to rely on the Customer Report or the contents thereof in any manner or for any purpose whatsoever, and Secureworks specifically disclaims all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary or punitive) arising from or related to reliance by any third party on any Customer Report or any contents thereof.

This document has been prepared solely for the use of the Customer and its officers, directors, and employees. No other third party shall be entitled to rely upon this document. The provision of this document or information herein to the parties other than the Customer shall not entitle such parties to rely on this report or the contents thereof in any manner or for any purpose whatsoever, and Secureworks Inc. specifically disclaims all liability for any damages whatsoever (whether foreseen or unforeseen, direct, indirect, consequential, incidental, special, exemplary, or punitive) arising from or related to provision of such report or information to such parties.

Our opinions are based on controls and data we evaluated as of this report date. Any projection of such information to the future is subject to the risk that, because of changes within the environment, our evaluation may be based on controls and a system no longer in existence. The potential effectiveness of specific controls is subject to inherent limitations and, accordingly, errors or fraud may occur and not have been detected. Furthermore, the projection of any conclusions to future events, based on our findings, is subject to the risk that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of our conclusions.

Copyrights and Trademarks

Technical Team

Jared M
Managing Principal Consultant
jr @secureworks.com

Chris S
Principal Consultant
c @secureworks.com

Table of Contents

1. Executive Overview

Iagon contracted with Secureworks to perform the following security assessment task:

- Web Application Assessment

The security engagement occurred during the period from December 16, 2024 to December 20, 2024. The objective of this engagement was to identify vulnerabilities in Iagon's application security that both internal and external adversaries could exploit.

Secureworks assessment activities included testing of the Iagon app during the course of the engagement. All aspects of the target were considered in scope.

NOTE: Staking and node storage features were not tested as they were not implemented during the test. These should be implemented prior to future tests.

[REDACTED DETAILS]

The following High-Severity issue contributed to the information disclosure and data modification issue:

[REDACTED DETAILS]

Secureworks recommends the following high-level actions:

[REDACTED DETAILS]

It is important to note that this report is not an objective measure but is solely based upon observation and experience; it does not cover areas deemed out of scope or issues beyond the capabilities of this methodology.

2. Technical Overview

One high-severity issue was discovered during the assessment.

[REDACTED DETAILS]

Four low-severity issues were discovered during the assessment.

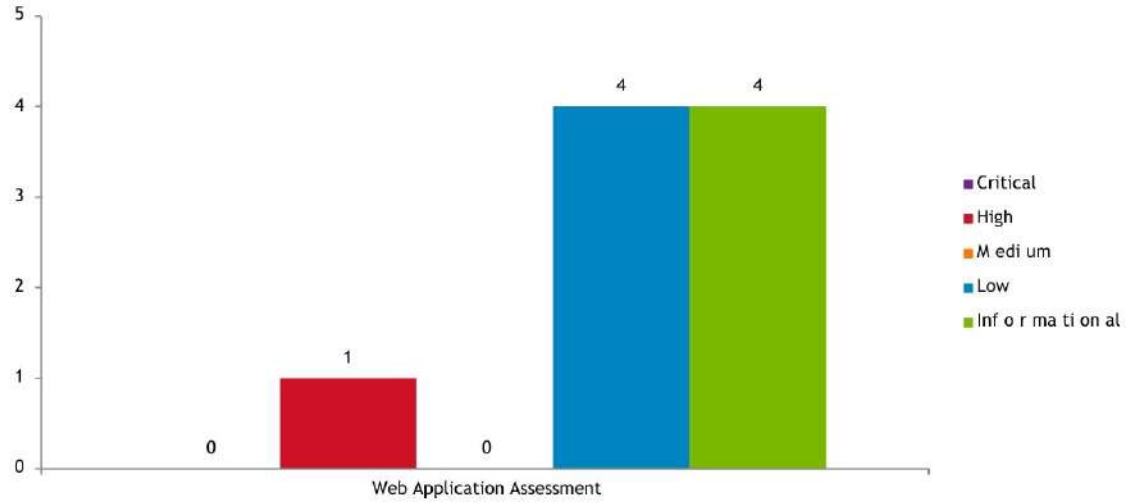
[REDACTED DETAILS]

Four informational-severity issues were discovered during the assessment.

[REDACTED DETAILS]

2.1. Summary of Findings

A high-level overview of the results is presented below. Detailed results can be found in subsequent sections of this document.



- **Web Application Assessment:** Secureworks identified zero (0) critical-severity findings, one (1) high-severity finding, zero (0) medium-severity findings, four (4) low-severity findings, and four (4) informational-severity findings.

2.2. Summary of Recommendations

Secureworks provides the following recommendations to help maintain and improve upon Iagon's current security level:

[REDACTED DETAILS]

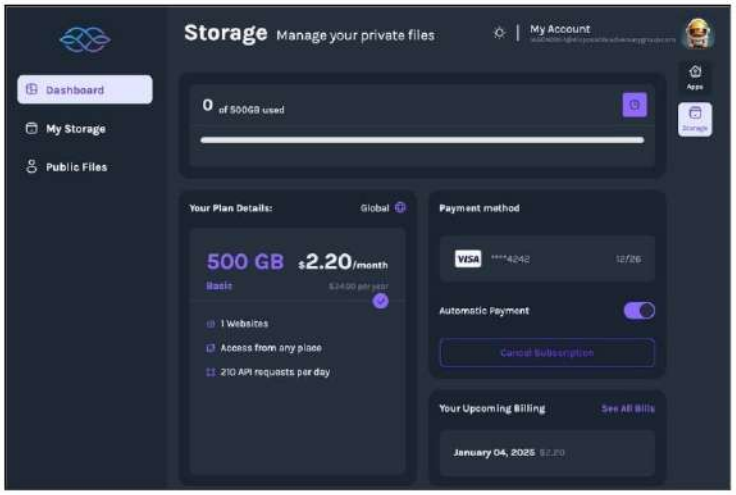
3. Web Application Assessment

During the period from December 16, 2024, to December 20, 2024, Secureworks performed a web application assessment against the following public application(s):

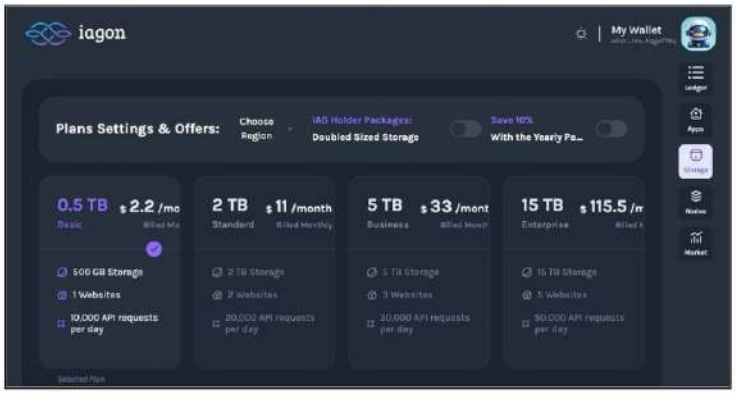
Targets

~~https://[REDACTED]~~

[email account – storage requests only]



[wallet account – hosting and storage requests]



3.1. Application Autopsy

The target application is written using React, Next.js, and the Express framework. It runs on an nginx web server. Blockchain technology is used to verify hosting transactions. Wallet management is handled separately via browser plugins--Eternl was used during this examination. The application has the following characteristics:

- File upload and download.
- Decentralized storage hosting.
- Payments.
- Node, ledger search.
- App hosting.
- Account management.

The test was conducted against a staging environment with limited data. The following accounts and respective roles were provided for authenticated testing:

[REDACTED DETAILS]

3.2. Methodology

The assessment consisted of several phases, each detailed below along with the methodology, associated findings, and subsequent recommendations:

3.2.1. Scope Validation

The first phase of testing is focused on identifying in-scope hosts through various methods of reconnaissance, such as spiders, robots, and crawlers; search engine discovery/reconnaissance; identification of application entry points; web application fingerprint; application discovery; and analysis of error codes.

3.2.2. Automated Testing

Automated web application scanners are limited in their scope, but are effective at identifying the most common issues, including those in the OWASP Top 10. The scanner can be configured to execute with or without a valid account on the web application; this has a major effect on the type and depth of testing it can provide.

3.2.3. Manual Verification

One issue with automated scanning is the high risk of false positives. The manual verification process reduces, as much as possible, the occurrence of 'false positives,' thereby improving the accuracy of testing results.

3.2.3.1. Multi-Stage Process

Automated scanners are not suitable for testing multi-stage processes, such as account registration or payment processes. This phase focuses the tester on these multi-stage processes and aims to identify persistent Cross-Site Scripting (XSS) flaws, downstream database injection flaws, etc.

3.2.3.2. Privilege escalation

To be comprehensive in testing, the capabilities of an authenticated user must be considered. As such, valid credentials are used to test what an authenticated user may accomplish. This is a manual exercise to attempt to verify an authenticated user's access is appropriate to the role, and that the ability to elevate privileges, view, or modify other user or account data is limited.

3.2.3.3. Business logic flaws

Business logic is a process or workflow built into a web application. Flaws in this logic can circumvent certain controls that would affect your business but would not result in a technical penetration of your environment—for example, modifying the price of an item from $100 to $1, or skipping the payment process and going straight to shipping. Testing identifies critical business logic flaws, as appropriate for the invasiveness and time allotted for testing.

3.3. Rules of Engagement

Systems were assessed and exploited to the extent described in the methodology. Any deviations from the stated methodology are noted in this section.

3.4. Key Findings and Recommendations

The following set of tables lists key findings identified during the assessment, describes their severity, provides a remediation plan, and lists additional information where applicable.

3.4.1. Critical-Severity Findings

During the period of the assessment, no critical-severity vulnerabilities were identified.

Appendix A: Key Terms

A.1 OWASP Top Ten

Secureworks captures the characteristics of web application vulnerabilities, as defined by the OWASP (Open Worldwide Application Security Project) Top-Ten categories (http://www.owasp.org). OWASP Top Ten is a list of the top-ten, most critical web application security vulnerabilities. Top-ten vulnerabilities affecting your web application are identified and assigned, allowing you to prioritize your remediation efforts. OWASP Top Ten will often reference CVSSv2 vulnerability information, which provides consistent severity reporting. OWASP Top Ten categories are prefaced with an A.

A.2 Definitions

The following terms and ratings are used to describe each vulnerability that was found:

Systems/URLs Affected: Describes by name, URL, or Internet Protocol (IP) Address the systems which are affected by the named vulnerability.

Description: A detailed explanation of the vulnerability and possible consequences of its successful exploitation.

Remediation: Describes possible or suggested steps to take to resolve the vulnerability.

Reference: If additional outside information is available, such as that found on websites, it will be listed here.

Notes: Where applicable, additional detail or clarifying information is included.

A.3 Severity Ratings

The following table defines Secureworks Severity Ratings as used throughout this report.