



Web Application Security Assessment Summary Report

May 23, 2022 (v1.0)

Prepared for:
Kagi Inc.

By Matija Siljak



Table of Contents

Executive Summary4
 Assessment Components4
 Conclusion4
 Summary of Findings5
About Illumant.....6

May 23rd 2022

Vladimir Prelovac
CEO, Founder
Kagi Inc.
Palo Alto, CA

Dear Vladimir,

In May of 2022, Illumant completed a comprehensive web application security assessment of a search application developed by Kagi Inc. ("Kagi"). The purpose of the assessment was to attempt to identify vulnerabilities and weaknesses, to assess their criticality through attempted exploitation, and to provide recommendations for remediation where applicable.

The assessment component performed can be summarized as follows:

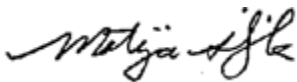
- Credentialed and uncredentialed penetration testing of Kagi's web-based application

Based on the results of our assessment, while we found some security issues that deserve consideration, as we do for just about every organization and application we assess, **we believe that overall Kagi's application and underlying data are reasonably secure**. Reasonably secure means that, the security issues discovered present a low risk, and it would require a hacker with rare skills and sophisticated tools, and/or the identification of new, as yet undiscovered vulnerabilities to compromise the security of the assessed application.

In comparison with other applications from organizations of similar size and profile, we find Kagi's application to be more secure than average, which is not to say that it could not become the target of a successful security breach before others, but that the information security risk to the application is lower than that of applications from comparable organizations.

Thank you for the opportunity to provide you with this assessment. Some additional summary information is provided on the following pages. Full details are provided in separate assessment reports.

Sincerely,



Matija Siljak
Director of Advisory Services
Illumant

Executive Summary

In May of 2022, Illumant completed a web application security assessment primary product application belonging to Kagi. The scope included a technical security assessment from an external (or hacker's) perspective with and without credentials. This report summarizes our findings.

Assessment Components

Based on the findings we arrived at a security rating for Kagi's application as "**Reasonably Secure**". The definitions of each classification rating are as follows:

Assessment Component	Description	Rating
Web Application Security Assessment (WASA)	Vulnerability analysis and penetration testing of applications with and without credentials (including comparison with OWASP's application security top 10)	Reasonably Secure

Conclusion

Based on the security assessment components above, we assess Kagi's application security rating as "**Reasonably Secure.**" The definitions of each classification rating are as follows:

Rating	Definition
Highly Secure	There were no findings of material significance. This indicates that the organization's applications, systems, networks and data are well protected.
Reasonably Secure	While there may be recommendations for improving the security of the applications, systems, networks and data under review, appropriate action has been taken in the past to ensure the security of the organization
Marginally Secure	The security findings identified are significant enough to suggest a heightened risk of a successful attack or intrusion if remediation actions are not taken.
Not Reasonably Secure	Appropriate actions necessary to secure the applications, systems, networks, applications and data have not been taken

A **reasonably secure** rating implies that the organization has done a good job securing applications and associated information, relative to organizations of similar size and profile. Kagi is above average in comparison with other organizations we have reviewed.

This does not mean, however, that the organization is not exposed to some risk of successful cyber-attack. Vulnerabilities we may not have identified, and potential future vulnerabilities, separately or in combination, could be exploited to successfully compromise the security of the application and/or other systems. The likelihood of this, however, is much lower than average compared to similar organizations (same industry vertical, similar size and complexity).

Still, it behooves Kagi to continue to improve its security posture by addressing the lower risk issues described in the detailed reports to further improve its security posture.

Summary of Findings

The key findings for each component are listed below:

Web Application Security Assessment (WASA):

- Cross Site Scripting (XSS). Authenticated attackers can inject arbitrary JavaScript in the context of the user. These scripts fail to execute due to CSP protections implemented correctly, however, HTML injection is still possible.
- Sessions remain active until logout without any observed inactivity timeout.
- Session tokens are passed via insecure methods. This makes it easier for an attacker to steal the tokens and impersonate a valid user.
- The application uses a weak password policy. This increases the chances for an attacker to obtain valid credentials via other attacks such as brute forcing.
- Insufficient Brute Force Protection. It is possible to perform brute force attacks against certain infrastructure unabated.
- Username enumeration. It was possible to enumerate valid user accounts. With enough time and attempts, an attacker may be able to successfully brute force a matching password and gain access to the internal network.

About Illumant

We're one of the best – We are not just making this up. Our clients often tell us that we're the best pen-testing firm they've worked with. And we have some great clients.

Hall of fame bug hunters – Became 1st ranked on Alibaba's Bug Bounty Hall of Fame for 2018 after only a month.

Awesome deliverables – We take a lot of pride in our reporting. Our reports are super informative and look great – and following our recommendations improves your security.

Zero-days – We don't just find the vulnerabilities that everyone already knows about, we find new and undiscovered vulnerabilities as well – meaning with us you are ahead of the hackers. Check out our latest, here: www.owndigo.com.

Friendly, expert hackers – We have some of the top hacking talent around, with the best skills and certifications, as well (OSCE, OSCP, GPEN, etc.) But we're not just great at hacking, our people are great at presenting and discussing, too.

Great clients – here are a few:





About Illuminant

Delivering confidence in all aspects of information security through assessment and penetration testing.

Illuminant is a trusted strategic and tactical information security risk management advisor to companies of all sizes across all industry verticals. We partner with our clients to help them navigate the security and threat landscape to become more secure, less of a target, and more compliant.