Web Application Security Assessment Executive Summary Report

August 26, 2022 (v1.0)

Prepared for:

Kagi Inc.

By Matija Siljak

Illumant
431 Florence Street, Suite 210
Palo Alto, CA 94301
www.illumant.com
650-961-5911

Table of Contents

August 26th, 2022

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

Dear Vladimir,

In August 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, the findings we identified were very low severity, and **we believe that overall Kagi's application and underlying data are highly secure**. Highly secure means that, the security issues discovered present a very 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 much 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

Summary

In August 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 "**Highly 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)	Highly Secure

Conclusion

Based on the security assessment components above, we assess Kagi's application security rating as "**Highly 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 **highly secure** rating implies that the organization has done a very 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.

Methodology

Web Application Security Assessment (WASA)

Description

Credentialed and non-credentialed vulnerability assessment and penetration testing of web-based and intranet applications to validate security and protection against outside attackers, malware, privilege escalation and account hijacking.

Highlights

Web service/application testing

With and/or without **credentials**

Testing with cross section of **best-of-breed tools**

Manual validation and penetration testing using expert, state-of-the art techniques and methodologies

Vulnerability targets:

- **Logic flaws**
- Lateral and vertical **privilege escalation**
- **Injection** (**SQL**, LDAP, URL …)
- Authentication
- Session management (**Session Hijacking**)
- **XSS/CSRF**
- Misconfigurations
- Vulnerable components
- Forged forward and redirects
- **Malware**
- more

Test against **OWASP Top 10**

Remediation **recommendations**

Targets

Web applications

- Users from all permissions categories
- Registration processes
- Login pages
- All links/URLs
- All input fields
- All application workflows

Privileged objects and functionality

Methodology

Scoping:

- Client provides in-scope target applications/URLs
- Testing may be performed on production systems, or in a sandbox/development environment
- For production systems, testing is performed outside of peak hours and tests are limited to non-destructive testing
- Credentials/test accounts to be provided if credentialed testing is required. Accounts should represent sample of all user accounts/permissions types/privilege levels.

Vulnerability Analysis/Harvesting:

- Automated scanning of in scope target applications using best-of-breed commercial and open-source application security analysis tools
- Multiple tools are used to provide a maximally broad initial baseline for subsequent analysis
- Vulnerabilities identified in the following areas: Injection, authentication, session management, XSS/CSRF, misconfigurations, vulnerable components, forged forwards and redirects

- Automated testing performed with and without credentials to baseline public- and private-side app functionality. Tests for unauthorized access, lateral and vertical privilege escalation, session hijacking and lateral account traversal

Manual validation and manual testing:

- Manual validation of results of automated testing to discard false positives and test the severity of confirmed vulnerabilities.
- For confirmed vulnerabilities, Illumant runs known and custom designed exploits and attempts to propagate attacks to retrieve sensitive information or verify possibility of pivoting to other targets
- Illumant follows a separate thorough manual testing plan to test each application for vulnerabilities. This step is performed to uncover vulnerabilities missed by automated tools. This happens frequently particularly with custom or internally developed apps.
- Illumant's manual testing plan draws from best-practices standards (e.g. OWASP) as well as years of experience.
- Manual testing includes walkthrough of all workflows, including registration and login, and other application specific workflows
- All links, URLs, input fields are tested for logic flaws that could expose sensitive information, or allow for lateral or vertical escalation of privileges.

Reporting:

- Findings are described in the report including full technical details of each vulnerability and exploit.
- Findings are summarized to provide a high-level overview of the security posture and security rating of the target systems. Ratings are benchmarked against thousands of previous assessments.

Standards

OWASP, WAHH

Tools

Nessus, Qualys Web Application Scanner, ZAP, Nikto, Nexpose, Metasploit, internal tools

Notes

Testing assesses against OWASP Top 10 and beyond to ensure baseline coverage and more. For production systems, Illumant takes care not to run potentially destructive exploits.

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.

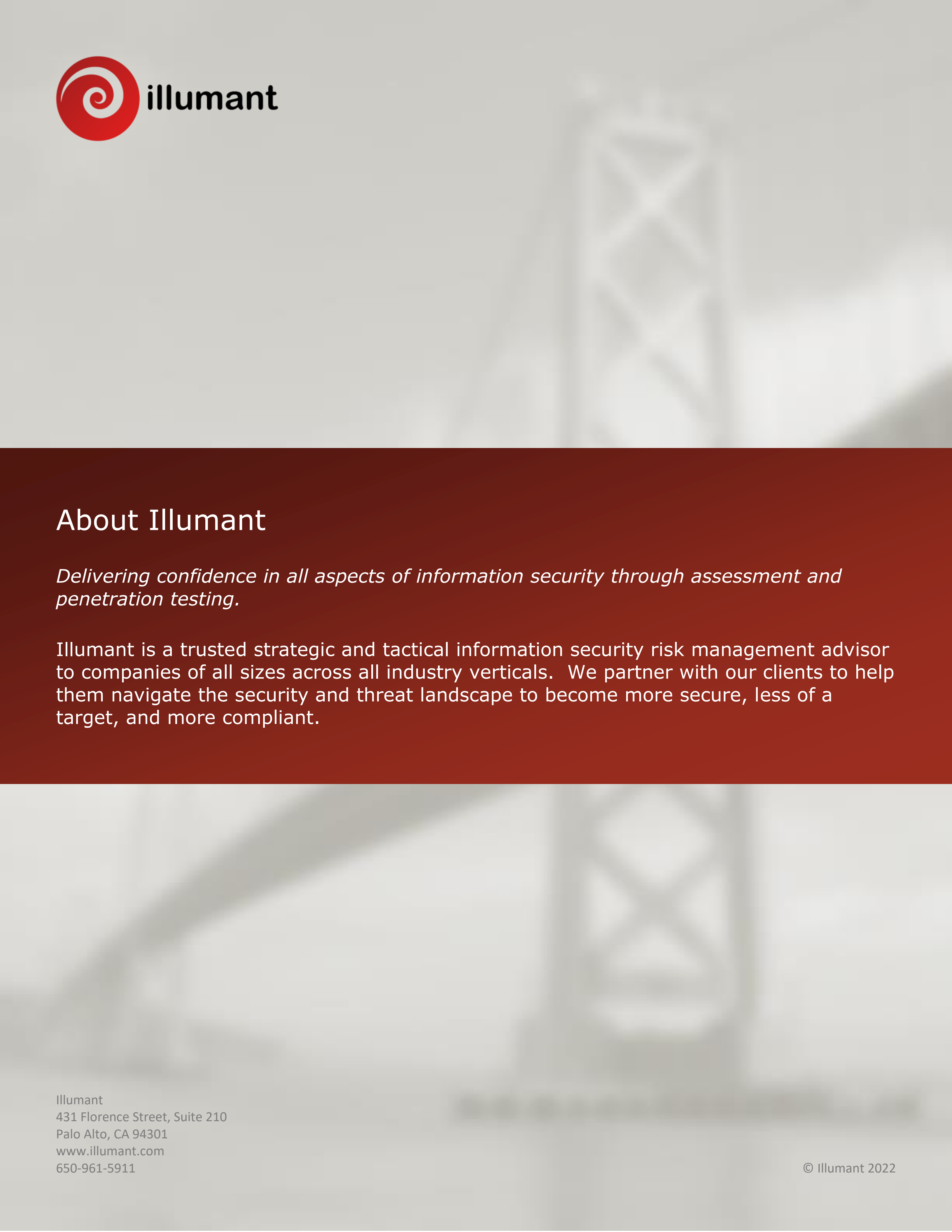
Awesome deliverables – We take a lot of pride in our reporting. Our reports are super informative and look great – and following our recommendations improves your security.

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 our great at presenting and discussing, too.

Great clients – here are a few:

Adobe
ARIEL INVESTMENTS
ARRIS
BESSEMER TRUST
Bloomberg
Bloomenergy
BROCADE
ch2m
COHERENT
COLAS
CollabNet
Cornell University
Duke UNIVERSITY
ebay
edp renewables
EllieMae Compliance. Quality. Efficiency.
EMC2
Harry&David
JUNIPER NETWORKS
K·SWISS
Panasonic
salesforce
Stanford University
Synaptics
tw telecom
tyco
Valley Health System



About Illumant

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

Illumant 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.

Illumant
431 Florence Street, Suite 210
Palo Alto, CA 94301
www.illumant.com
650-961-5911