Letter of Attestation - Rapid7 Services Portal

10 February 2020

Executive Summary

Secure Ideas, LLC is a leading provider of security consulting and penetration testing services headquartered in Jacksonville, Florida, and has conducted an assessment for Rapid7. The objective of the penetration test was to verify that the components of the Rapid7 Services Portal application and its supporting infrastructure are adequately protected with the appropriate controls and based on industry information security standards and regulations.

Test Methodology

Our assessments are performed in accordance with an industry standard methodology, which incorporates widely available requirements from information security regulations and industry standards, to include the following:

- Open Web Application Security Project (OWASP) Guide to Building Secure Web Applications and Web Services
- Payment Card Industry (PCI) Data Security Standards v3.2.1 (Requirements 3 & 6 only)
- Center for Internet Security (CIS) Benchmarks for Amazon Web Services (AWS) environments.

The objectives of the assessment for the Services Portal application were as follows:

- Identify vulnerabilities and security weaknesses within the Internet-facing web applications.
- Assess the web application for business logic flaws that could be exploited to perform unauthorized transactions or actions.
- Exploit identified weaknesses with the Internet-facing web application to demonstrate the risks and potential business impacts to Rapid7 systems and operations.
- Recommend remediation and security controls to improve the security of Rapid7 systems.

Findings Summary

Secure Ideas LLC identified zero (0) critical risk findings, zero (0) high risk findings, one (1) medium risk finding, and one (3) low risk finding during the course of the assessment. An overview of the findings for this assessment is illustrated in the table below.

Application Assessed	Critical	HIgh	Medium	Low
Services Portal	0	0	1	3

Conclusion

During the testing, Secure Ideas discovered that the Services Portal web application developed by Rapid7 was resilient to all of the attacks that were performed during the penetration test. Secure Ideas has determined that the application's security controls are above the standards for securing web applications. This is based on experience testing a large variety of applications over our tenure as security consultants.

sales@secureideas.com
+1 (904) 639-6709

It is important to note that the assessment also focused on testing the surrounding environment of the Insight Cloud Platform. Holistic security for web applications requires the underlying infrastructure to also be secure. Vulnerabilities and weaknesses in networks, operating systems, and security policies and processes could lead to potential compromise, and security controls are required at all layers of the organization to mitigate these risks. During the assessment of the surrounding external facing infrastructure Secure Ideas discovered zero high risk findings, which speaks to the diligence that Rapid7 places in their security controls.

Use of this Document

This document has been prepared solely for Rapid7 and its officers, directors, and employees. Rapid7 shall own all right, title, and interest in any written reports, analyses, information or documentation prepared for Rapid7 in connection with the web application penetration services provided to Rapid7. Completion of said security assessment does not guarantee, nor does Secure Ideas, LLC warrant for Rapid7 that it, (i) will receive favorable results in any audits by third parties, (ii) will be safe from all information security risks or vulnerabilities, or (iii) is in compliance with any third party compliance program or any regulatory compliance requirements.

sales@secureideas.com
+1 (904) 639-6709