Letter of Attestation for Sonatype

August 15, 2022

Executive Summary

Sonatype, solicited Axxum to perform a vulnerability assessment and penetration testing (VAPT) on its Hosted Data Service (HDS) REST application. The goal of the assessment was to identify vulnerabilities and their associated risks on the Sonatype applications.

The external vulnerability scanning and penetration testing, post assessment analyses, and the assessment and testing reports development and documentation were performed remotely from May 16, 2022, through August 1, 2022.

This letter of attestation covers an overview and outcome of the external vulnerability assessment and penetration testing of the aforementioned Sonatype's application using both automated testing tools and manual testing methods. The security assessment engagement included an in-depth penetration test of the Sonatype application, with the objective of identifying common web application security vulnerabilities. The Axxum security assessment team evaluated security weaknesses and their potential impact on any of the security objectives (e.g., Confidentiality, Integrity, and Availability) of the application, interaction with the product components, and the data stored in it. During testing, the Axxum assessment security team found that the design and implementation of the overall architecture of the Sonatype solution was carried out with security best practices in mind. The objective of the penetration testing was to verify that the components of Sonatype's HDS application, and its supporting infrastructure are adequately protected with the appropriate controls and that the organization adhere to industry information technology (IT) security standards, regulations, laws, and guidance.

Findings Summary

A summary of the identified finding and its categorized risk level from the HDS REST security assessment engagement is illustrated in the table below:

Application Assessed & Tested	Critical	High	Medium	Low
Hosted Data Service (HDS)	0	0	0	1

Conclusion

During the testing, Axxum Technologies, LLC discovered that the Sonatype HDS web application was resilient to most of the attacks that were performed during the penetration test. Axxum has determined that the security controls selected and implemented to protect HDS are adequate and within the industry standards for securing web applications. This is based on our experience of

testing a large variety of applications over the years as IT security consultants.

Holistic security for web applications requires the underlying infrastructure to also be secure. Vulnerabilities and weaknesses in networks, operating systems, and security policies, procedures, 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 public facing infrastructure, Axxum discovered zero critical risk findings, which speaks to the diligence that Sonatype places in the security of their IT assets, network, and environment.

It is important to note that Axxum Technologies, LLC believes that the statements made in this document provide an accurate representation of the assessment conducted on Sonatype's current security posture as it pertains to their assessed web applications. However, as the environment changes, and new vulnerabilities and risks are discovered and made public, an organization's overall security posture will change. Such changes may affect the validity of this letter. Therefore, the conclusion reached from our analysis only represents a "snap-shot" in time.

Furthermore, it should be noted that an organization's overall security posture is dependent upon many factors and security is only as strong as the weakest link. Therefore, Sonatype has prioritized the remediation of the discovered findings based on the severity of the associated risk(s), and the risk mitigation activities which align with the organizational vulnerability management plan and process are currently in progress.

Use of this Document

This document has been prepared solely for Sonatype and its owners, leadership team, officers, directors, and employees. Sonatype shall own all right, title, and interest in any written reports, analyses, information, or documentation prepared for Sonatype in connection with the web applications' vulnerability assessment and penetration testing services provided to Sonatype. Completion of this security assessment does not guarantee, nor does Axxum Technologies, LLC warrant for Sonatype that it will:

- Receive favorable results in any future audits by third parties.
- Be safe from all future information security risks or vulnerabilities.
- Adhere to any third party compliance program or any regulatory compliance requirements.