Penetration Testing Letter of Attestation

Thursday, August 22, 2024

For:

Modern Interpreters Inc. (Screenshotbot)

screenshotbot.io

Arnold Noronha

arnold@screenshotbot.io

By:

Pensive Security, LLC

pensivesecurity.io

Luke Wegryn, Security Engineer

865.964.0099

luke@pensivesecurity.io

1.0 Executive Summary

Penetration Testing

Pensive Security performed a penetration test of the Screenshotbot web application, concluding on Friday, November 10, 2023. Pensive Security identified one high, three medium, and two low-severity issues during the assessment. No critical issues were found. The findings from the penetration test are detailed in the Findings sections (3.0 and 4.0) of the original penetration testing report. Pensive Security delivered the penetration testing report, and the Screenshotbot team created a remediation plan to address the reported issues.

Remediation Verification Retest

On August 22, 2024, Pensive Security performed a remediation verification retest and found that **the Screenshotbot team fully remediated all reported security issues**. After the remediation effort, the estimated security risk of the Screenshotbot application was reduced to **low**.

Scope

This penetration test was performed against the following Screenshotbot resources.

Target Type	Resource Identifier
Web Application	screenshotbot.io api.screenshotbot.io

2.0 Application Penetration Testing Methodology

For web application-based testing and assessments, Pensive Security attempts a variety of simulated attacks, including those most commonly found in web applications, according to the OWASP Top 10.

Manual Penetration Testing

While Pensive Security performs some automated testing for application enumeration and identifying "low hanging fruit", the majority of testing performed by Pensive Security is manual. It involves creative and critical thinking by the tester. Manual pentesting for web applications involves reviewing client-side source code, testing application flows for business logic issues, verifying access controls between users and organizations, crafting application-specific input injection attacks, bypassing the application firewalls, and chaining vulnerabilities together in complex ways to gain deeper access to the application infrastructure.

Unauthenticated and Authenticated Testing

For web application penetration testing, Pensive Security first performs unauthenticated testing to assess the application from the perspective of an attacker who does not have access to a valid user account. During this stage of the engagement, activities typically include application directory and file mapping, brute-force login attempts, password stuffing attacks, application login flow review, password reset attacks, and input injection. Once Pensive Security has achieved good application coverage from an unauthenticated perspective, Pensive Security moves on to authenticated testing.

For authenticated testing, Pensive Security requests user credentials from the customer for each user role. Pensive Security also requests credentials in multiple organizations within the application. Lastly, Pensive Security creates a set of credentials using the registration or signup flow if possible. With access to these users, Pensive Security can properly test access controls both within each user organization and between different organizations ensuring that an attacker cannot privilege escalate or access other organizations' data. Since most of the application business logic is located behind authentication, a large amount of manual testing is required to test the logic flows and functionality of the application.

Tools Used during the Penetration Test

Pensive Security uses many different tools during a penetration test. Some tools are used on almost every engagement, while some are specific to certain application frameworks or infrastructure. The following table shows a few of the tools used during this engagement.

Tool Type	Tool Name
Open-source Intelligence (OSINT)	Spiderfoot, Amass, SandCastle
Vulnerability Scanning	OpenVAS and Nessus

Enumeration and Mapping	Nmap, BurpSuite Pro, Nuclei, Sn1per, Dirb, GoBuster, wpscan, Nikto, Fuzzdb
Exploitation	Metasploit Framework, ExploitDB, sqlmap, John the Ripper, Hydra

Common Attack Vectors

Pensive Security tests for many different types of attack vectors which vary widely between different applications; however, some appear often, such as those listed in the OWASP Top 10.

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery (SSRF)

In addition to these standard attacks, Pensive Security performed extensive enumeration and reconnaissance to identify areas that appear likely to contain vulnerabilities. Pensive Security follows the OWASP Web Security Testing Guide and Pensive Security also develops attacks specific to the customer's web applications.

3.0 About Pensive Security

Based in Asheville, North Carolina, Pensive Security has provided high-quality security testing, security reviews, architecture reviews, security assessments, and other cybersecurity services since 2017. Team members hold security testing certifications, including OSCP, OSCE, and BSCP.

Pensive Security's primary service offering is penetration testing. Pensive Security has provided hundreds of successful penetration tests to a wide range of customers in almost every industry, including heavily regulated industries such as healthcare and finance.

With new attack vectors constantly surfacing, Pensive Security is committed to keeping testing methods current. Pensive Security utilizes cutting-edge tools, cross-discipline expertise, and trusted security standards to ensure highest-quality results.

Pensive Security's custom reports are well-written and provide customers with a detailed description, proof of concept exploit, remediation, and severity rating for every vulnerability found, helping the customer understand and remediate reported issues. Pensive Security also provides a detailed executive summary and attack narrative, ensuring customers and stakeholders better understand the in-depth testing that was performed.

For more information about Pensive Security, please visit https://pensivesecurity.io/.