WhiteHat™

Security Audit Report

SaneBox

Report As Of	Wednesday, June 12, 2024
Prepared By	WhiteHat Security [redacted]
Report Description	The Security Audit report provides an overview of open vulnerabilities discovered in the assessment, including summaries, metrics, and conclusions. For those customers using both Sentinel and Sentinel Source, this report will cover both dynamic and static test results. Note that detailed vulnerability information is available in the vulnerability detail reports.
Notes	Sites are assessed using dynamic analysis, and vulnerabilities are rated by their severity levels. For descriptions of dynamic analysis and severity levels, please see the Appendix.
Assets	Sites: 1
NOTICE	This document contains sensitive and confidential information regarding information security at SaneBox. Appropriate care should be taken to secure this document from unauthorized access.

The Index of Content can be found on the last page

WhiteHat has performed an independent assessment on site(s) using the Sentinel Standard Edition Service (SE) to examine compliance with common security standards including the OWASP Top 10, the Web Application Security Consortium's Threat Classification (WASC) and industry practices for web application security.
This level of service includes custom scanner configuration by the WhiteHat Threat Research Center to ensure comprehensive coverage of applications, including those employing technologies such as Flash, JavaScript, and multi-part forms.
All vulnerabilities are verified for accuracy by the operations team to ensure accurate and actionable results.

Issue Summary – Open Vulnerabilities

This table displays a breakdown of each site's vulnerabilities.

Sites: Vulnerability Count							
Site Name	**Site Priority**	**Urgent**	**Critical**	**High**	**Medium**	**Low**	**Informational**
SaneBox	1	0	1	0	1	1	2
Total		**0**	**1**	**0**	**1**	**1**	**2**

Issue Summary – Open Vulnerabilities

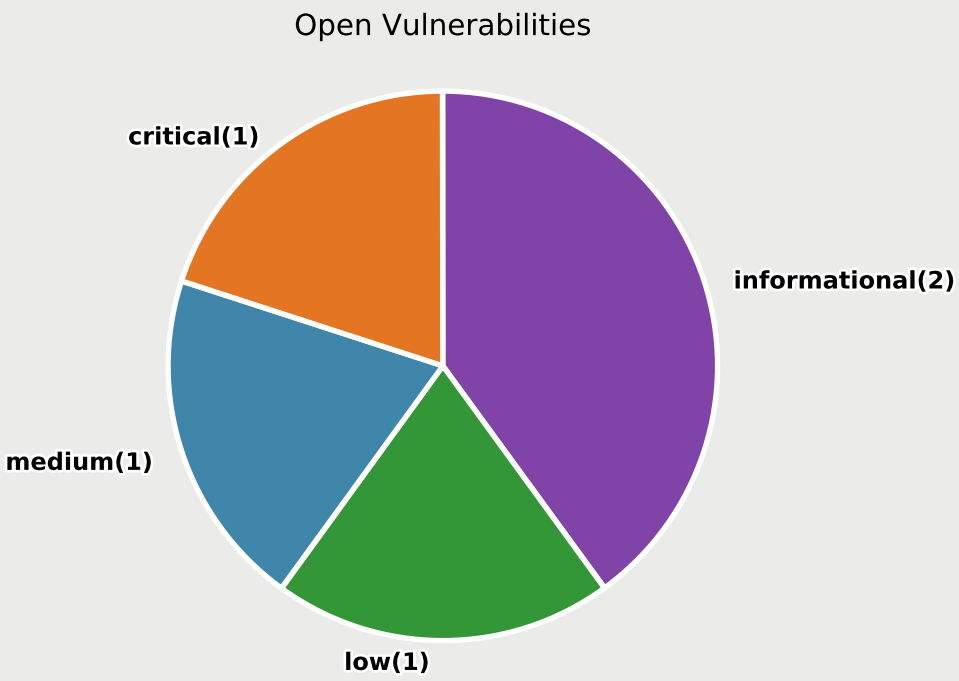
The following table summarizes the vulnerabilities found by WhiteHat that also fall into the OWASP Top 10 Categories. Not all WhiteHat vulnerability classes are represented in the OWASP Top 10 Categories, so not all identified on your asset(s) may be accounted for in this table. It is also possible that the vulnerabilities may fall into more than one OWASP Top 10 category, so one vulnerability may be represented under multiple OWASP classes.

Sites: Vulnerability Count							
Vulnerability Category	**No. of Occurrences**	**Urgent**	**Critical**	**High**	**Medium**	**Low**	**Informational**
A1 - 2021 - Broken Access Control	0	0	0	0	0	0	0
A2 - 2021 - Cryptographic Failures	0	0	0	0	0	0	0
A3 - 2021 - Injection	0	0	0	0	0	0	0
A4 - 2021 - Insecure Design	0	0	0	0	0	0	0
A5 - 2021 - Security Misconfiguration	5	0	1	0	1	1	2
A6 - 2021 - Vulnerable and Outdated Components	0	0	0	0	0	0	0
A7 - 2021 - Identification and Authentication Failures	0	0	0	0	0	0	0
A8 - 2021 - Software and Data Integrity Failures	0	0	0	0	0	0	0
A9 - 2021 - Security Logging and Monitoring Failures	0	0	0	0	0	0	0
A10 - 2021 - Server-Side Request Forgery	0	0	0	0	0	0	0
Total	**5**	**0**	**1**	**0**	**1**	**1**	**2**

Issue Summary

This graph summarizes your sites' vulnerabilities and includes the vulnerability count for each vulnerability level.

Sites: Summary of Vulnerabilities



Sentinel Standard Edition Testing Checklist

The Sentinel Standard Edition service level tests for the following list of WASC classes of Web vulnerabilities:

Client-side Attack Tests

1. Content Spoofing

Content Spoofing is an attack technique used to trick a user into believing that certain content appearing on a web site is legitimate and not from an external source.

2. Cross-site Scripting

Cross-site Scripting (XSS) is an attack technique that forces a web site to echo attacker-supplied executable code, which loads in a user's browser.

3. HTTP Response Splitting

HTTP Response Splitting is a technique allowing the attacker to send a single HTTP request that forces the Web server to send two HTTP responses instead of one response, in the normal case. The attacker completely controls the second response.

Command Execution Tests

4. Buffer Overflow

Buffer Overflow exploits are attacks that alter the flow of an application by overwriting parts of memory.

5. Format String Attack

Format String Attacks alter the flow of an application by using string formatting library features to access other memory space.

6. LDAP Injection

LDAP Injection is an attack technique used to exploit web sites that construct LDAP statements from user-supplied input.

7. OS Commanding

OS Commanding is an attack technique used to exploit web sites by executing Operating System commands through manipulation of application input.

8. SQL Injection

SQL Injection is an attack technique used to exploit web sites that construct SQL statements from user-supplied input.

9. SSI Injection

SSI Injection (Server-side Include) is a server-side exploit technique that allows an attacker to send code into a web application, which will later be executed locally by the web server.

10. XPath Injection

XPath Injection is an attack technique used to exploit web sites that construct XPath queries from user-supplied input.

Information Disclosure Tests

11. Directory Indexing

Automatic directory listing/indexing is a web server function that lists all of the files within a requested directory if the normal base file is not present.

12. Information Leakage

Information Leakage is when a web site reveals sensitive data, such as developer comments or error messages, which may aid an attacker in exploiting the system.

13. Path Traversal

The Path Traversal attack technique forces access to files, directories, and commands that potentially reside outside the web document root directory.

14. Predictable Resource Location

Predictable Resource Location is an attack technique used to uncover hidden web site content and functionality.

Appendix - Vulnerability Level Definitions (by Severity)

Severity is defined as the potential business impact if a specific vulnerability is exploited. The levels of severity are based on the same conditions factored into the PCI Security Scan report ratings, but the definitions below are clarified for Web application security concerns.

The Severity is scored between 0 and 5:

Urgent	Critical	High	Medium	Low	Informational
5	4	3	2	1	0

Severity ratings are defined below:

Rating	Description
Urgent	Attacker can assume remote root or remote administrator roles; exposes entire host to attacker; backend database, personally identifiable records, credit card data; full read and write access, remote execution of commands; example Weakness Class: Insufficient Authorization; example Attack Classes: SQL Injection, Directory/Path Traversal
Critical	Attacker can assume remote user only, not root or admin; exposes internal IP addresses, source code; partial file-system access (full read access without full write access); example Weakness Class: Insufficient Authentication; example Attack Classes: Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Abuse of Functionality
High	Exposes security settings, software distributions and versions, database names; example Weakness Classes: Information Leakage, Predictable Resource Location; example Attack Class: Content Spoofing
Medium	Exposes precise versions of applications; sensitive configuration information may be used to research potential attacks against host
Low	General information may be exposed to attackers, such as developer comments
Informational	No actual exposure: a failure to comply with best practices for security.

Appendix - Assessment Methodology for Dynamic Analysis

WhiteHat Security combines a proprietary vulnerability scanning engine with human intelligence and analysis from its Threat Research Center to deliver thorough and accurate assessments of web applications with its Sentinel Service.

WhiteHat Sentinel dynamic scanning services are all based on a continuously evolving top of class scanning engine with manual verification of all vulnerabilities to ensure quality results. WhiteHat's model allows customers to keep all sites covered at all times with minimal investment of personnel, while having access to the worlds largest team of web application security experts who keep on top of the latest web security issues, manage security assessments for customers, and provide support and information. With Premium service the security experts in the Threat Research Center also perform business logic assessments of sites, which may uncover additional issues which cannot be found through automatic scanning. This combination provides the highest quality of security assessments in the industry with high scalability and ease of use, to keep customers on top of their risk posture and help them secure their assets.

About WhiteHat by Synopsys

Synopsys provides integrated solutions that transform the way you build and deliver software, accelerating innovation while addressing business risk. WhiteHat is the leading solution for application risk assessment and management services that enable customers to protect critical data, ensure compliance, and narrow windows of risk. With Synopsys, your security teams can proactively manage risk and focus remediation efforts on what matters most to your organization. Our unmatched expertise helps you plan and execute any security initiative. Only Synopsys offers everything you need to build trust in your software.

Contents