DAVID MAK, M.S. CYBERSECURITY
CYBERSECURITY CONSULTANT • BOSTON, MA
MAK.D@NORTHEASTERN.EDU • 617-331-5165

28 April 2023

Penetration Test Report

LiveShopper SassieShop : uat.sassieshop.com/2_qa/

Change Log

28 April 2023 Initial Draft
XX April 2023 Final Version

Executive Summary

This report is authored by David Mak, an independent contractor with experience in the INFOSEC and Cybersecurity realm serving in software engineer, application administrator, and systems integrator roles in a career spanning from 1993 to the present. I, David Mak, was contracted by LiveShopper, LLC via Tony Felos, CISO, to perform a penetration test of the Unit Test/QA application entry point identified by LiveShopper as a suitable test application entry point that has the same production software installed, allowing for tests to not impact production traffic and availability. This report summarizes the findings from this test executed on 28 April 2023.

Primarily utilizing the Docker container image of the stable release of OWASP ZAProxy tool,[1] coupled with a configuration file determined to be appropriate for the LiveShopper Sassie web application, a black-box penetration test was performed with active scan, brute-force modes to generate information relevant to the UAT/QA application entry-point representative of the production instance. Coordination with LiveShopper consisted of receiving the entry-point: http://uat.sassieshop.com/2_qa/ and notifying LiveShopper the time for the start of scans so that operational monitoring staff at LiveShopper were informed and aware that any alerts generated are part of the contracted scanning. This is an engagement with LiveShopper following previous projects starting in 2021 to provide consultation for their ISO27001 certification along with penetration tests.

Application security is built around the concept of layered defenses, with integration of controls implemented by the application infrastructure, and the application itself. The results of the different scans may identify some controls that are not implemented, but the criticality of this should be considered in conjunction with other controls or application design that may lower or raise the reported risk when taken into account with other variables. It is the conclusion for this analyst, to find that the results of the most recent penetration tests do not identify any significant application flaws that can be trivially exploited. LiveShopper may wish to consider more detailed technical analysis of the impact of implementing any of the low alert controls identified as missing, with specific Sassie and client needs determining the relevance of such work. The low risk alerts are isolated to browser cookie and HTTP header settings that may provide some additional security or privacy protections that may serve to augment the existing layered defense system of controls, so long as they do not result in functional limitations or breaks that would represent a regression in service.

Vulnerability Scans

OWASP ZAProxy

Execution

The ZAP tool was utilized, via a command-line interface utilizing Docker to download, install, and perform an active scan on the http://uat.sassieshop.com/2_qa/ entry point, with the following command:

```
docker run -v $(pwd):/zap/wrk/:rw -t owasp/zap2docker-stable:2.12.0
zap-full-scan.py -c config.yml -t http://uat.sassieshop.com/2_qa/ -r
20230428_qa.sassieshop.com.html
```

The report generation tool was utilized to create a detailed summary of the results in a HTML rendered report. This report will be supplied to LiveShopper for full detailed analysis by their technical team, with the results summarized in this report based on the expert opinion of this report's author, in the following analysis section.

Analysis

The summary results from the ZAP test flagged zero (0) high risk, zero (0) medium classified, four (4) low risk, and four (4) informational alerts:

Alerts

Name	Risk Level	Number of Instances
Cookie No HttpOnly Flag	Low	1
Cookie without SameSite Attribute	Low	1
Permissions Policy Header Not Set	Low	8
X-Content-Type-Options Header Missing	Low	3
Non-Storable Content	Informational	3
Re-examine Cache-control Directives	Informational	2
Storable and Cacheable Content	Informational	9
User Agent Fuzzer	Informational	120

In a detailed analysis of the alerts, one can verify the first two low risk cookie alerts are correctly classified as low, relating primarily to system level PHP session cookies detailing a lack of HttpOnly and SameSite attributes/flags. Resolving these likely depends on the underlying PHP engine upon which Sassie is built, and would have minimal application impact. The next low risk level alert, “Permissions Policy Header Not Set” relates to the Sassie web application not setting HTTP headers that would restrict various browser permissions for functionality that end-users normally would be able to control themselves, such as camera, microphone, location, et al. The final low risk alert is only relevant for older browser versions of Internet Explorer (deprecated by Microsoft) and Chrome which might allow them to display page content with a different content type. Firefox is not affected by this setting. The informational alerts relate to headers or response content having proxy or cache settings that may help with response and performance of a website by taking advantage of content caching services such as provided by Akamai, et al. The final informational alert is a test that allows

web application operators to validate various browser/user agent values against the Sassie application to determine if they would affect the response.

Summary

Regular scans with a test tool such as ZAProxy, utilizing a controlled configuration tailored for the LiveShopper Sassie web application allows for monitoring of risks as the Sassie software evolves over time, and known vulnerabilities are discovered by the Cybersecurity community. This most recent test, with evolved parameters allowing for automation of such tests with easy change control shows that LiveShopper has successfully improved both the Sassie application and their processes over time. Previous tests had resulted in medium to low risks that have been addressed as evidence by this latest test report when compared to reports from previous years. Continued testing as LiveShopper Sassie, ZAProxy, and known vulnerabilities databases are updated over time is critical in maintaining a secure Sassie application.

References

1. OWASP Zed Attack Proxy (ZAP) Docker Image owasp/zap2docker-stable:2.12.0 https://www.zaproxy.org/