Flock Safety web app - November 2020 Penetration Test Report

TARGET(S)

https://admin.flocksafety.com

https://users.flocksafety.com

https://camera-management.flocksafety.com

https://hotlist.flocksafety.com

https://planner.flocksafety.com

https://analytics.flocksafety.com/

https://search.flocksafety.com

TEST PERIOD

Nov 23, 2020 ⟶ Dec 7, 2020

STATUS

Final

Contents

Scope of Work 4

Methodology 7

- Pre Engagement | 1 Week 7
- Penetration Testing | 2~3 Weeks 7
- Post Engagement | On-demand 7
- Risk Factors 8
- Criticality Definitions 9

Terms 12

PDF created Mar 15, 2021 14:31 UTC
Cobalt Web App 2021
by Cobalt Labs • San Francisco, CA •
cobalt.io

Scope of Work

Coverage

This penetration test was a manual assessment of the security of the app's functionality, business logic, and vulnerabilities such as those cataloged in the OWASP Top 10. The assessment also included a review of security controls and requirements listed in the OWASP Application Security Verification Standard (ASVS). The pentesters conduct manual analysis assisted by tools.

The team had access to authenticated users, enabling them to test security controls across roles and permissions. This included attempting "vertical" privilege escalation (access to information not authorized within the container/project) and "horizontal" privilege escalation (access to information in other containers/projects without authorization).

The following is a brief summary of the main tests performed on the Web Application:

- Authenticated user testing for session and authentication issues
- Authorization testing for privilege escalation and access control issues
- Input injection tests (SQL injection, XSS, and others)
- Platform configuration and infrastructure tests
- OWASP Top 10 testing

The following is a brief summary of the main tests performed on the API:

- Authenticated endpoint testing for missing access control issues
- Authorization testing for privilege escalation and access control issues

- Input injection tests (SQL injection, XSS, and others)
- OWASP Top 10 testing

Below is the summary of methodologies used to assess the security at the mentioned endpoints:

Inventory of web service endpoints:

We inventoried the calls made by the Flock Safety web app during all user activities. We then proceeded to analyze requests and responses to observe the underlying technology and any possible vulnerabilities.

Manual and automated fuzzing of web service endpoints:

We proceeded to reverse engineer the endpoints and perform modified calls using manual and automated methods. We attempted the following:

- Parameter manipulation (adding / modifying parameters to perform new functions, horizontal privilege escalation, etc.)
- Code injection (SQL injection attempts, Template injection, Cross Site Scripting attacks, etc.).
- XML External Entity attacks
- Header manipulation
- Path traversal
- Malicious file upload

Test Cases that successfully thwarted exploitation

We successfully enumerated the attack surface, then fuzzed for XSS/SQLi and other input injection-related vulnerabilities. The results showed that successful security controls and/or design patterns were implemented

consistently throughout the enumerated attack surface - demonstrating a healthy SDLC and attention to security concepts/practices.

During testing many positive controls were observed the be in place within the application. A brief overview of these includes:

- The application is handling the injection attacks very well. The application is not vulnerable to XSS, SQL injection, XXE attacks.
- No CSRF attacks are found.
- The error messages are customized enough to not reveal the underlying technology.
- No LFI/RFI issues has been observed.
- Session Fixation for Concurrent Sessions is not possible.
- Session token is not predictable
- "Forgot Password" functionality is not vulnerable to Host Header injection

Target description

Application:

- https://admin.flocksafety.com
- https://users.flocksafety.com
- https://camera-management.flocksafety.com
- https://hotlist.flocksafety.com
- https://planner.flocksafety.com
- https://analytics.flocksafety.com/
- https://search.flocksafety.com

Environment:
Production

Methodology

The test was done according to penetration testing best practices. The flow from start to finish is listed below.

Pre Engagement

- Scoping
- Customer
- Documentation
- Information
- Discovery

Penetration Testing

- Tool assisted assessment
- Manual assessment of OWASP top 10 & business logic
- Exploitation
- Risk analysis
- Reporting

Post Engagement

- Prioritized remediation
- Best practice support
- Re-testing

Risk Factors

Each finding is assigned two factors to measure its risk. Factors are measured on a scale of 1 (very low) through 5 (very high).

Impact

This indicates the finding's effect on technical and business operations. It covers aspects such as the confidentiality, integrity, and availability of data or systems; and financial or reputational loss.

Likelihood

This indicates the finding's potential for exploitation. It takes into account aspects such as skill level required of an attacker and relative ease of exploitation.

Criticality Definitions

Findings are grouped into three criticality levels based on their risk as calculated by their business impact and likelihood of occurrence, `risk = impact * likelihood`. This follows the OWASP Risk Rating Methodology.

High

Vulnerabilities with a high or greater business impact and high or greater likelihood are considered High severity. Risk score minimum 16.

Medium

Vulnerabilities with a medium business impact and likelihood are considered Medium severity. This also includes vulnerabilities that have either very high business impact combined with a low likelihood or have a low business impact combined with a very high likelihood. Risk score between 5 and 15.

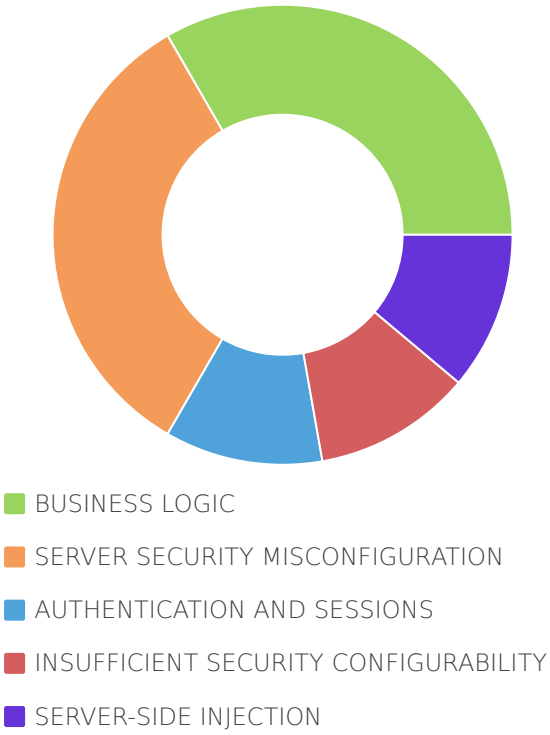
Low

Vulnerabilities that have either a very low business impact, maximum high likelihood, or very low likelihood, maximum high business impact, are considered Low severity. Also, vulnerabilities where both business impact and likelihood are low are considered Low severity. Risk score 1 through 4.

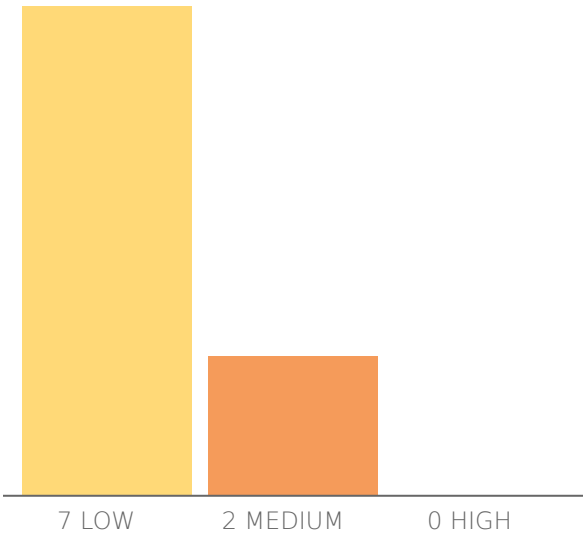
Summary of Findings

The following charts group discovered vulnerabilities by OWASP vulnerability type, and by overall estimated severity.

BY VULNERABILITY TYPE



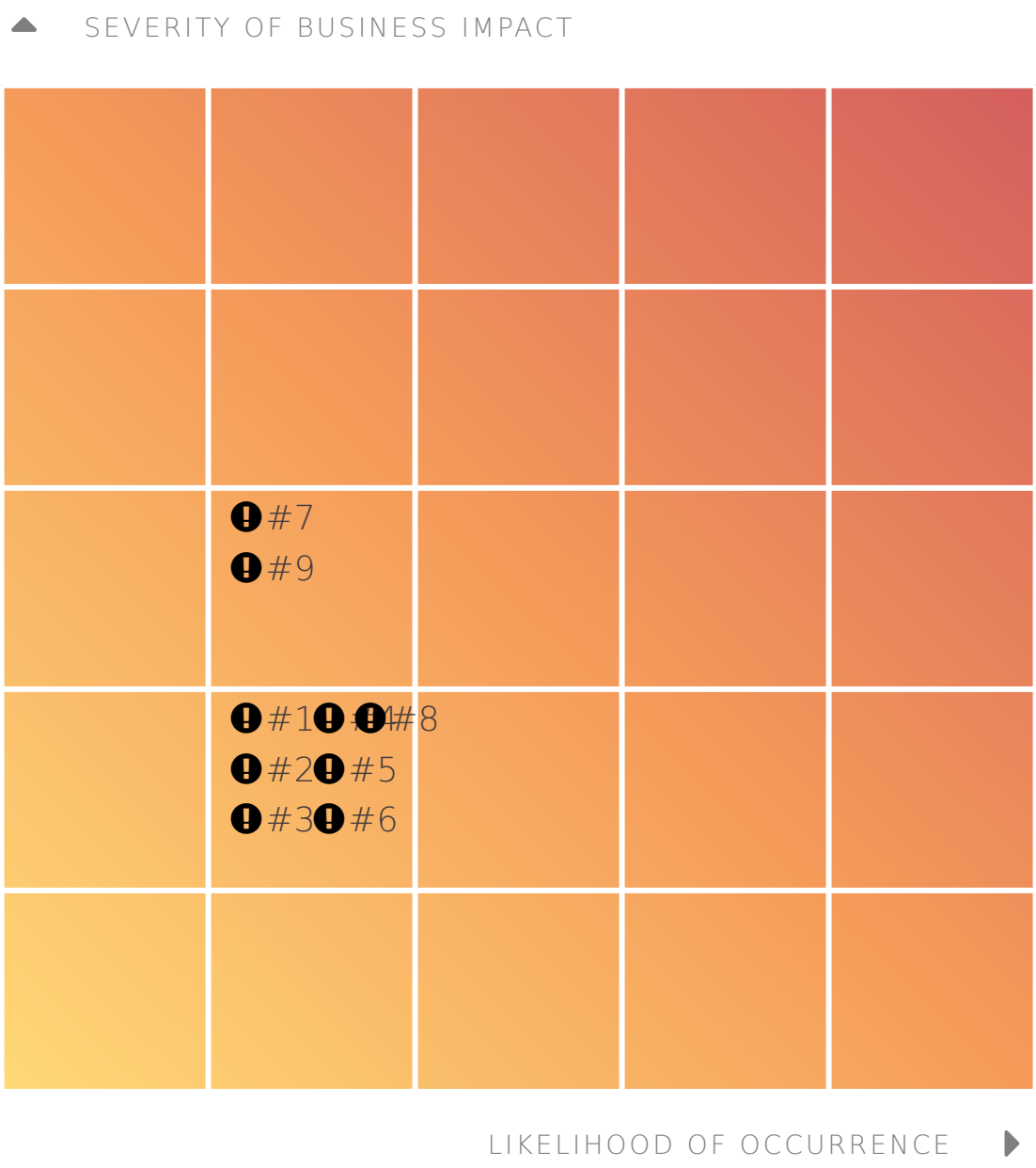
BY CRITICALITY



PDF created Mar 15, 2021 14:31 UTC
Cobalt Web App 2021
by Cobalt Labs • San Francisco, CA • cobalt.io

General Risk Profile

The chart below summarizes vulnerabilities according to business impact and likelihood, increasing to the top right.



PDF created Mar 15, 2021 14:31 UTC
Cobalt Web App 2021
by Cobalt Labs • San Francisco, CA •
cobalt.io

Terms

Please note that it is impossible to test networks, information systems and people for every potential security vulnerability. This report does not form a guarantee that your assets are secure from all threats. The tests performed and their resulting issues are only from the point of view of Cobalt Labs. Cobalt Labs is unable to ensure or guarantee that your assets are completely safe from every form of attack. With the ever-changing environment of information technology, tests performed will exclude vulnerabilities in software or systems that are unknown at the time of the penetration test.

PDF created Mar 15, 2021 14:31 UTC
Cobalt Web App 2021
by Cobalt Labs • San Francisco, CA •
cobalt.io