HALBORN

Truffles - Backend / Frontend Whitebox

Executive Summary

Prepared by: **Halborn**

Date of Engagement: **April 17th, 2023 - May 22nd, 2023**

Visit: **Halborn.com**

DOCUMENT REVISION HISTORY

VERSION	MODIFICATION	DATE	AUTHOR
0.1	Document Creation	05/16/2023	Alvaro Macias
0.2	Draft Review	05/23/2023	Carlos Polop
0.3	Draft Review	05/23/2023	Gabi Urrutia
1.0	Remediation Plan	06/06/2023	Alvaro Macias
1.1	Remediation Plan Review	06/08/2023	Carlos Polop
1.2	Remediation Plan Review	06/09/2023	Gabi Urrutia

CONTACTS

CONTACT	COMPANY	EMAIL
Rob Behnke	Halborn	Rob.Behnke@halborn.com
Steven Walbroehl	Halborn	Steven.Walbroehl@halborn.com
Gabi Urrutia	Halborn	Gabi.Urrutia@halborn.com
Carlos Polop	Halborn	Carlos.Polop@halborn.com
Alvaro Macias	Halborn	Alvaro.Macias@halborn.com

EXECUTIVE OVERVIEW

1.1 INTRODUCTION

Truffles engaged Halborn to conduct a white-box pentest of their staging app: https://stagingapp.truffles.one beginning on April 17th, 2023 and ending on May 22nd, 2023. The security assessment was scoped to GitHub source code to the Halborn team.

1.2 ASSESSMENT SUMMARY

The team at Halborn was provided four weeks for the white-box pentest and assigned a full-time security engineer to verify the security of the staging's web applications. The security engineer is a penetration testing expert with advanced knowledge in web, recon, discovery & infrastructure penetration testing.

The goals of our security assessments are to improve the quality of systems by testing this as white-box approach to have an attacker perspective of targeting the staging web application.

In summary, Halborn identified security risks that were mostly addressed by the Truffles team. The security assessment of the web application revealed several vulnerabilities that could potentially compromise user accounts and expose sensitive information. The findings are as follows:

- Broken Access Control on KYC Verification:
  This issue refers to a flaw in the system's access control mechanisms related to the "Know Your Customer" (KYC) verification process. It allows unauthorized individuals to perform actions they should not have permissions for due to their KYC process not yet approved. It is mitigated successfully now.
- Broken Access Control on Organization ID Parameter:
  By leveraging a vulnerability, it was possible to chain an attack and obtain the organization ID (orgId) information. Subsequently, a GET request could be sent to any organization that did not belong to the user. This chain of exploitation allowed for the retrieval

of sensitive information, such as personal IDs, from the targeted organization. It is already fixed by the team after the report.

- OTP Bypass on Transfer Funds Mechanism:
  The One-Time Password (OTP) verification mechanism used for transferring funds has a vulnerability that allows attackers to bypass this security step and initiate unauthorized transfers. It is also remediated successfully.
- Mail Server Misconfiguration:
  The mail server contained multiple misconfigurations, allowing an attacker to impersonate emails as Truffles.one and performing scams/fraud/phishing users, which may result in financial and customer loss. Furthermore, an attacker could exploit the aforementioned vulnerability in conjunction with another exploit to execute a specifically targeted attack against corporate users. It was an infrastructure issue, which was fixed, and Truffles team also started moving to a more secured environment to stop this kind of issue in future
- Malicious Upload Documents for KYC Process:
  Attackers could exploit vulnerabilities in the KYC document upload process to submit malicious files that might compromise the system, steal sensitive data. It is fixed now by the team
- Account Impersonation:
  This issue relates to a security weakness that enables attackers to impersonate legitimate users, gaining unauthorized access to their accounts and potentially engaging in fraudulent activities. That is fixed now.
- Clickjacking:
  Clickjacking is a technique where attackers trick users into clicking on hidden or disguised elements on a web page, leading them to perform unintended actions, potentially compromising sensitive data or executing malicious operations. It is already fixed from Infrastructure side .
- Failed to Invalidate Session after a Logout:
  A failure to invalidate user sessions properly after logout can expose users to session hijacking attacks, allowing unauthorized access to user accounts even after they have logged out. Secured measure implemented to stop that issue in future.

- Private Access Token in URL:
  Including private access tokens in URLs can be a security risk as URLs may get logged in various systems, leading to unauthorized access if the token is exposed.
- Improper Input Handling:
  During the assessment, it was discovered multiple instances of client-side exception errors within the system. These errors occur on the client side, typically within the user's web browser or application, and can negatively impact the user experience and the overall functionality of the system.
- Vulnerable Third Party Dependencies:
  Using third-party libraries or components with known security vulnerabilities can expose the system to potential attacks or compromises. Team implemented SAST (Static application security testing) to prevent future issues with code and third party libraries.
- Lack of Prevention against Brute Force Mechanisms on Register:
  The authentication page of the web application features a registration form; however, it lacks a captcha validation mechanism. Consequently, this absence of captcha verification allowed users to submit an excessive number of requests, leading to an overload of new user creations on the support. It is prevented using rate limit and WAF together now.

Lastly, several low severity issues were found. While these issues pose a lower risk, they still present potential security concerns. Team is going through fixing all of them one by one and will be completed soon.

1.3 SCOPE

The following endpoints were in scope:

- https://stagingapp.truffles.one
- https://stagadmin.truffles.one

1.4 TEST APPROACH & METHODOLOGY

Halborn followed a white-box approach and performed a combination of manual and automated security testing to balance efficiency, timeliness, practicality, and accuracy regarding the scope of the pentest. While manual testing is recommended to uncover flaws in logic, process and implementation; automated testing techniques assist enhance coverage of the infrastructure and can quickly identify flaws in it. The following phases and associated tools were used throughout the term of the assessment:

- Mapping Content and Functionality
- Logic Flaws
- Access Handling
- Authentication/Authorization Flaws
- Rate Limitations Tests
- Brute Force Attempts
- Input Handling
- Response Manipulation
- Source Code Review
- Fuzzing of all input parameters
- Multiple Type of Injection (SQL/JSON/HTML/Command)

Halborn's findings, descriptions and remediations have been redacted at the request of Truffles.

RISK METHODOLOGY:

Vulnerabilities or issues observed by Halborn are ranked based on the risk assessment methodology by measuring the **LIKELIHOOD** of a security incident and the **IMPACT** should an incident occur. This framework works for communicating the

characteristics and impacts of technology vulnerabilities. The quantitative model ensures repeatable and accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the Risk scores. For every vulnerability, a risk level will be calculated on a scale of 5 to 1 with 5 being the highest likelihood or impact.

RISK SCALE - LIKELIHOOD

5 - Almost certain an incident will occur.
4 - High probability of an incident occurring.
3 - Potential of a security incident in the long term.
2 - Low probability of an incident occurring.
1 - Very unlikely issue will cause an incident.

RISK SCALE - IMPACT

5 - May cause devastating and unrecoverable impact or loss.
4 - May cause a significant level of impact or loss.
3 - May cause a partial impact or loss to many.
2 - May cause temporary impact or loss.
1 - May cause minimal or un-noticeable impact.

The risk level is then calculated using a sum of these two values, creating a value of 10 to 1 with 10 being the highest level of security risk.

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL

10 - CRITICAL
9 - 8 - HIGH

7 - 6 - MEDIUM

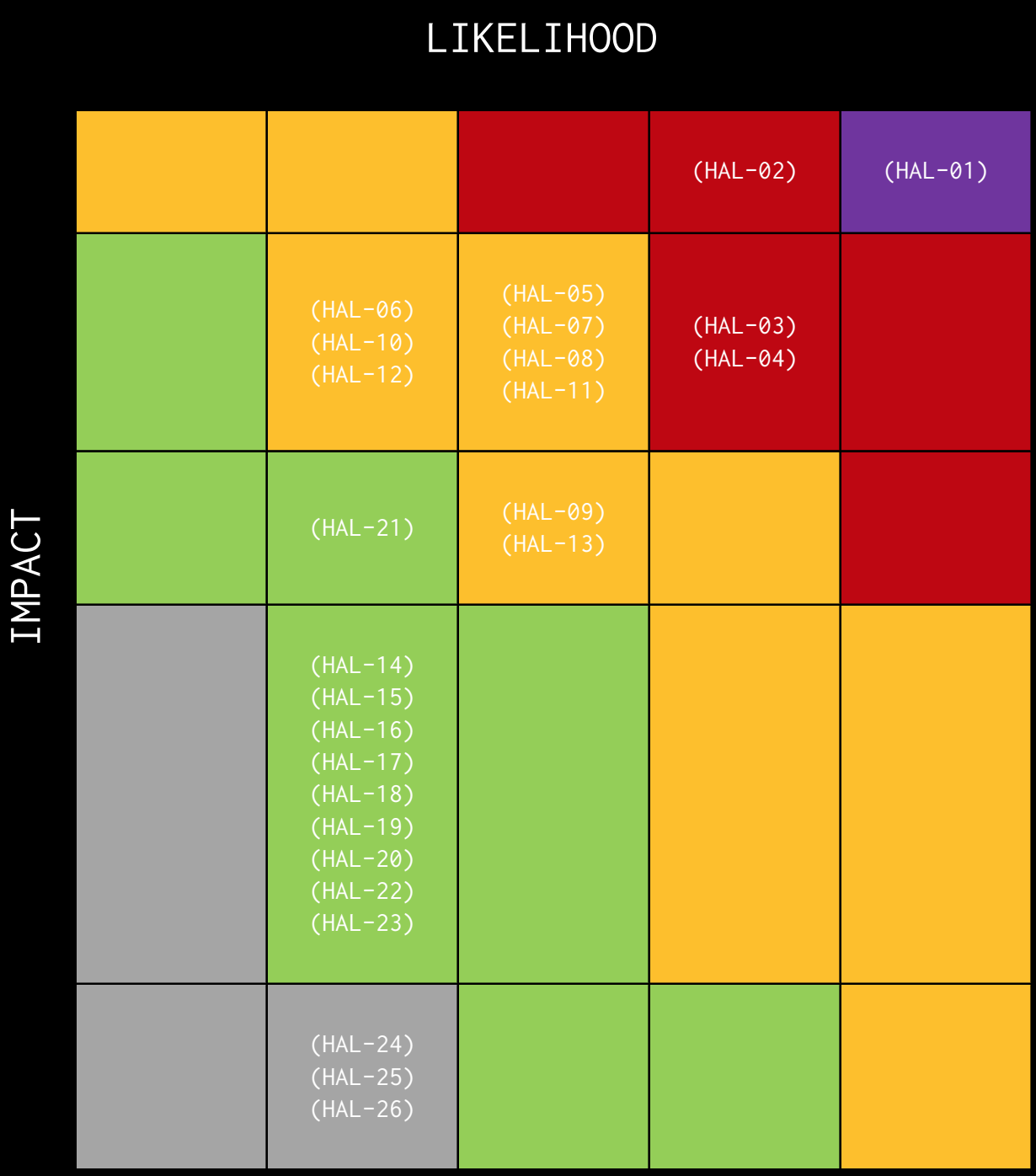
5 - 4 - LOW

3 - 1 - VERY LOW AND INFORMATIONAL

2. ASSESSMENT SUMMARY & FINDINGS OVERVIEW

CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
1	4	9	10	3

EXECUTIVE OVERVIEW



EXECUTIVE OVERVIEW

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION DATE
(HAL-01) BROKEN ACCESS CONTROL ON KYC VERIFICATION	Critical	SOLVED
(HAL-02) BROKEN ACCESS CONTROL ON ORGANIZATION ID	High	SOLVED
(HAL-03) OTP BYPASS ON TRANSFER	High	SOLVED
(HAL-04) MAIL SERVER MISCONFIGURATION	High	SOLVED
(HAL-05) MALICIOUS UPLOAD DOCUMENTS FOR KYC PROCESS	Medium	SOLVED
(HAL-06) ACCOUNT IMPERSONATION	Medium	SOLVED
(HAL-07) NO FILE VALIDATION ON UPLOAD DOCUMENTS FOR KYC PROCESS	Medium	SOLVED
(HAL-08) CLICKJACKING	Medium	SOLVED
(HAL-09) FAILED TO INVALIDATE SESSION AFTER A LOGOUT	Medium	SOLVED
(HAL-10) PRIVATE ACCESS TOKEN IN URL	Medium	FUTURE RELEASE
(HAL-11) IMPROPER INPUT HANDLING	Medium	SOLVED
(HAL-12) VULNERABLE THIRD PARTY DEPENDENCIES	Medium	RISK ACCEPTED
(HAL-13) LACK OF PREVENTION AGAINST BRUTE FORCE MECHANISMS ON REGISTER	Medium	SOLVED
(HAL-14) SIMILAR HASHES ON ORGANIZATION AND USER ID	Low	SOLVED
(HAL-15) MULTIPLE ACCOUNTS USING ONE EMAIL	Low	SOLVED
(HAL-16) SENSITIVE DATA EXPOSURE IN LOCALSTORAGE	Low	SOLVED
(HAL-17) PREFIX MOBILE NUMBER NEVER COULD BE UPDATED	Low	SOLVED

(HAL-18) RESPONSE MANIPULATION	Low	SOLVED
(HAL-19) USE OF INSECURE RANDOM FUNCTION GENERATION	Low	SOLVED
(HAL-20) FAILED TO INVALIDATE TOKEN ON REQUEST NEW JWT	Low	SOLVED
(HAL-21) LACK OF PREVENTION AGAINST BRUTE FORCE MECHANISMS	Low	SOLVED
(HAL-22) DEPENDENCIES SHOULD BE PINNED TO EXACT VERSIONS	Low	SOLVED
(HAL-23) NEGATIVE VALUES ON TRANSFER	Low	SOLVED
(HAL-24) POOR AUTHENTICATION MECHANISM	Informational	ACKNOWLEDGED
(HAL-25) REGISTER USING DISPOSABLE EMAILS	Informational	SOLVED
(HAL-26) HARDCODED WALLEX API KEY	Informational	SOLVED

THANK YOU FOR CHOOSING

// HALBORN