LIFARS
your digital world, **secured**

Divi Project MOBILE PENETRATION TEST REPORT

Prepared for : The Divi Project
Prepared by: LIFARS LLC, Offensive Security Department
Date(report): DRAFT – 04/09/2021

This document and its content represent confidential information between LIFARS, LLC and CLIENT. As such, this document may not be shared with any outside party without the expressed consent of LIFARS, LLC and CLIENT.

Table of Contents

Table of Contents **1**

Executive Summary **2**

Overview 2
Document Objective 2
Project Scope 2
Rules of Engagement and Assumptions 3
CVSS Score 3
Legend - Severity rating scale 3
Methodology 4
Penetration Testing Phases 5
Findings Summary 6
Limiting factors 6

Disclaimer **7**

Executive Summary

LIFARS was engaged by The Divi Project (Company) on March 23rd, 2021 to conduct a Mobile Application Penetration Test encompassing both Android and iOS apps, as demonstrated in the Project Scope section of this report.

This report describes any findings discovered during the testing.

Overview

The main objective of this penetration testing engagement was to evaluate The Divi Project's security posture to known security vulnerabilities, logic flaws, Open Web Application Security Project (OWASP) mobile testing guidelines and other methodologies to determine the extent to which the targeted apps and APIs could be compromised. This was a white box mobile penetration test and executed in a manner that simulated a malicious threat actor engaged in a targeted attack against The Divi Project's mobile apps. This security testing effort was conducted with emphasis on the actual state of the systems examined, with support from provided documentation.

This penetration testing found no vulnerabilities of note. We reviewed the mobile apps for inappropriate local data storage local to the device, SSL/TLS implementation errors or weaknesses, weak or misconfigured inter-app and intra-app communication mechanisms, unnecessary permissions, and app configuration issues. We additionally tested API endpoints for authentication and authorization bypasses, JWT vulnerabilities, and incorrectly exposed or configured API endpoints.

This report reflects a snapshot in time. LIFARS recommends continuous security assessments such as periodic Penetration Test, Vulnerability Assessment, and Red Team Exercises to ensure optimal security.

Document Objective

This document provides a detailed technical analysis of the security and risk exposures found during the penetration test, as well as recommendations and solutions where applicable.

Penetration test is a form of a technical audit of overall cybersecurity resiliency and current cyber maturity of the enterprise systems. LIFARS reports reflect findings and their representation in industry standard testing methodology, and provides an allotted time view into posture from a potential vulnerability point of view.

Project Scope

The client requested for LIFARS to perform the tests on specified iOS and Android applications. No restrictive testing conditions were specified.

Apps tested:

- Android App v1.0.6
- iOS App v1.0.0 (49)
  - Via TestFlight

Rules of Engagement and Assumptions

Accounts/wallets were provided by the client for the purpose of testing.

CVSS Score

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score. The numerical score can then be translated into a qualitative representation (such as low/informational, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

In case there is no CVSS already associated with any of the finding identified during the assessment, LIFARS will provide its interpretation of the CVSS based on possible impact.

Legend - Severity rating scale

Rating:	CVSS Score:	
None/Informational	0.0	🟦
Low	0.1 – 3.9	🟩
Medium	4.0 – 6.9	🟧
High	7.0 – 8.9	🟥
Critical	9.0 – 10.0	🟪

Legend - Severity rating scale

Rating:	Definition:
None/Informational	No risk or exploitability potential.
Low	Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local, physical system access or a high, out of proportion, step(s) to be successful.
Medium	Medium vulnerabilities usually have some of the following characteristics: • Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. • Denial of service vulnerabilities that are difficult to set up. • Exploits that require an attacker to reside on the same local network as the victim. • Vulnerabilities where exploitation provides only very limited access. • Vulnerabilities that require user privileges for successful exploitation.

Rating:	Definition:
High	High vulnerabilities usually have some of the following characteristics: • Vulnerabilities found can be easily and immediately exploited. • Exploitation could result in elevated privileges. • Exploitation could result in a significant data loss or downtime. • An attacker can gain administrator privileges on a device, service or at the same level, compromise the confidentiality, integrity, and availability of data.
Critical	Critical vulnerabilities usually have most of the following characteristics: • Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices. • Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims, and does not need to persuade a target user, for example via social engineering, into performing any special functions. LIFARS advises to remediate the critical findings as soon as possible, unless other mitigating measures are already set in place.

Derived from NIST: https://nvd.nist.gov/.

Along with numerical score and qualitative representation for base CVSS score, LIFARS will provide environmental CVSS score, which takes into account known aspects of related environment and infrastructure and tester's professional judgment, which might increase or decrease the severity of a vulnerability.

Please note that combination of several specific lower risk findings could sometimes work in tandem. A chain of such vulnerabilities if misused effectively poses a higher risk finding.

Methodology

LIFARS deploys various methodologies for Penetration Testing and Red Team engagements that are enhanced by its own proprietary methods and tools as well as an experiential approach that is continually informed by current industry knowledge. Some of these methodologies include:

- NATO Cooperative Cyber Defense Center of Excellence (CCDCOE)
- US Army Red Teaming Handbook v7
- Penetration Testing Execution Standard (PTES)
- Safeguarding Information Operations, Article 8, CIA.gov, Retrieved 2008-06-27
- The Open Source Security Testing Methodology
- Open Web Application Security Project (OWASP)
- ISO 27001 Best practices, BS 7799
- Industry Frameworks (BITS/FSTC/NIST SP 800-30)
- National Institute of Standards and Technology (NIST) Special Publication 800-115, Technical Guide to Information Security Testing and Assessment

- Compliance and regulatory frameworks (HIPAA, PCI DSS, SOX)
- DoD Strategy for Operating in Cyberspace
- Cyber Defense Exercise, Nsa.gov. 2009-01-15. Retrieved 2012-01-08

LIFARS undertakes strict reviews in compliance with ISO 9001, OWASP Top 10 and ISO 27001 requirements. All of our vulnerability assessments also focus on the SANS/FBI Top Twenty list of the most critical vulnerabilities on the Internet.

Vulnerabilities are usually compared with industry standard databases such as CVE, MITRE, security focus, and internal lists in case of the specific exposure.

We use semi-automated vulnerability scanning using professional and open-source tools to detect potential vulnerabilities within the scope of the engagement. The report will outline all the vulnerabilities found, remediation steps, and more.

Phases

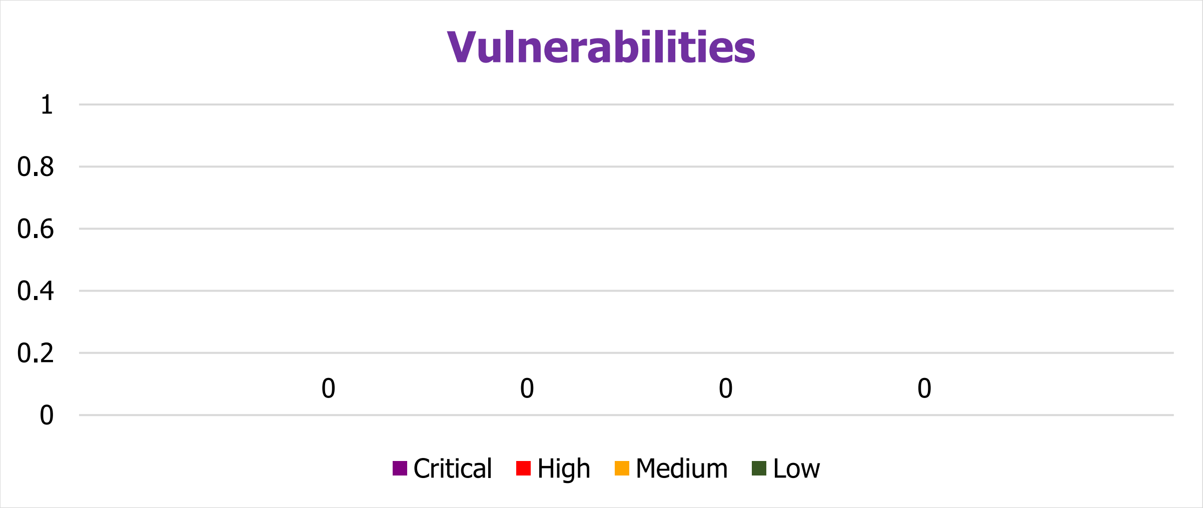
Penetration Testing Phases

The following are the main phases defined by the OWASP Mobile App Security Guide (MASG) as the basis for Mobile Penetration Testing execution:

1) Architecture, Design, and Threat Modelling
2) Data Storage and Privacy
3) Cryptography
4) Authentication and Session Management
5) Network Communication
6) Platform Interaction
7) Code Quality and Build Settings

Findings Summary

This section provides a summary of the vulnerabilities discovered during this assessment



Critical Risk

- None

High Risk

- None

Medium Risk

- None

Low Risk

- None

Limiting factors

- The wallets of the accounts we used were limited in funds, so certain API endpoints (such as those used to stand up master nodes) were not exercised in a valid context.

Limiting factors may prevent exploitation and verification of certain vulnerabilities. In any such cases, where the existence of vulnerability is highly probable, we include the vulnerability in the report as "identified, not verified".

Disclaimer

This report presents the results of an offensive security service that LIFARS performed under the direction of the Company. This report is designed for the reader to understand the activities performed by LIFARS and relevant findings.

Penetration Testing Engagements, Vulnerability Assessments and Red Teaming Exercises adhere to a defined methodology based upon industry best practices and LIFARS experience. It should be recognized that all information systems are vulnerable to some degree and subject to malicious attacks. Even if all known vulnerabilities are resolved, log files are reviewed, and people interviewed, there could be events or vulnerabilities which were not identified or that could emerge in the future. Therefore, while LIFARS has reviewed several issues which could contribute to an incident, there can be no assurance that any exercise of this nature will identify all possible vulnerabilities, indicators, or propose exhaustive and operationally viable recommendations to mitigate all exposures.

For the avoidance of doubt, and notwithstanding anything to the contrary in this report or in any agreement with the Company, LIFARS disclaims all representations and warranties, express, implied, statutory and otherwise, with respect to this report and the information and findings contained herein, all of which are provided "as is" and without warranty. LIFARS expressly disclaims the implied warranties of title, merchantability, fitness for a particular purpose and non-infringement.

The content of this report should be redacted before sharing or publishing.

End of Document