HyperPay APP Security Audit Report

Project Overview

This security audit project aims at a fast and comprehensive security audit for HyperPay to detect potential threats and further improve the security of HyperPay. The utmost efforts are made along with the HyperPay Team to safeguard the security of users and their funds in particular.

Foreword

We extend our gratitude for HyperPay 's recognition of SlowMist and hard work and support of relevant staff.

Audit Information

Audit Period: 15 working days

Audit Team: SlowMist Security Team

Audit Duration: January 13, 2020 - January 31, 2020

File Information

URL: https://hyperpay.me/download?lang=zh-cn

iOS File Information

File Name: HyperPay.ipa

MD5： 79c71fa89aa739040ecff9b27fcb0dde

HASH： 6b605471fa78eedccef99ef7c80fb024905773e4

Android File Information

File Name: HyperPay.apk

MD5: 135a2c06f4037f767f4fec4b773ab4a3

HASH: 90c10b1771befa4a95d3deb409f6301b570be702

Project Profile

HYPERPAY is a technology company that aims to bring inclusive financial services to the world.

Audit Results

(Other unknown security vulnerabilities are not included in the scope of this audit)

No.	Audit Category	Audit Subclass	Audit Results
1	Open-source intelligence collection	Whois domain information collection	Passed
		Discovery of real IP	Passed
		Subdomain detection	Passed
		Email service detection	Passed
		Certificate information collection	Passed
		Web service component fingerprint collection	Passed
		C-segment service collection	Passed
		Collection of personnel and organization structure	Passed
		GitHub source code leakage detection	Passed
		Privacy leakage detection	Passed
2	Server security	CDN service detection	Passed

	configuration audit	Resolution test of filename extension	Passed
		Backup / unlinked file testing	Passed
		HTTP method testing	Passed
		HTTP Strict Transport Security (HSTS) testing	Passed
		CORS testing	Passed
		Testing for Web Security Response headers	Passed
		Weak password and default password detection	Passed
		Management background discovery	Passed
3	Identity management audit	Testing for role definition	Passed
		Testing for user registration process	Passed
		Testing for account permission change	Passed
		Testing for account enumeration	Passed
		Testing for weak username policy	Passed
4	Certification and authorization audit	Testing for Sensitive information sent via unencrypted channels	Passed
		Testing for default password	Passed
		Testing for certification bypass	Passed
		Testing for remember password functionality	Passed

		Testing for browser cache	Passed
		Testing for password policy	Passed
		Testing for password reset functionality	Passed
		Testing for privilege escalation	Passed
		Testing for IDOR	Passed
		Testing for two-factor authentication bypass	Passed
		Testing for Hash robustness	Passed
5	Session management audit	Testing for session management bypass	Passed
		Testing for cookies attributes	Passed
		Testing for session fixation	Passed
		Testing for session token leakage	Passed
		Testing for cross-site request forgery	Passed
		Testing for logout functionality	Passed
		Session timeout testing	Passed
		Testing for session token refresh	Passed
6	Input security audit	Testing for cross site scripting	Passed
		Testing for template injection	Passed

		Vulnerability testing for third-party components	Passed
		Testing for HTTP parameter pollution	Passed
		Testing for SQL injection	Passed
		Testing for XML External Entity (XXE) injection	Passed
		Deserialization vulnerability testing	Passed
		Testing for Server-Side Request Forgery (SSRF) vulnerabilities	Passed
		Testing for code injection	Passed
		Testing for local file inclusion	Passed
		Testing for remote file inclusion	Passed
		Testing for command injection	Passed
7	Business logic audit	Testing for trading business logic	Passed
		Data integrity testing	Passed
		Request forgery testing	Passed
		Interface security testing	Passed
		Testing for interface frequency band	Passed
		Testing for workflow bypass	Passed

		Testing for upload of unexpected file types	Passed
		Testing for upload of malicious files	Passed
8	Cryptographic security audit	Testing for weak SSL/TLS ciphers, insufficient transport layer protection	Passed
		Testing for SSL Pinning security deployment	Passed
		Testing for sensitive information sent via unencrypted channels	Passed
9	Mobile App audit	Wallet security	Passed
		Operating environment security	Passed
		Disable code decompilation	Passed
		File storage security	Passed
		Communication encryption	Passed
		Permission security	Passed
		Interface security	Passed
		Business security	Passed
		WebKit security	Passed
		APP cache security	Passed
		APP Webview DOM security	Passed
		APP SQLite storage security audit	Passed

		APP code obfuscation	Passed
Comprehensive Audit Results			Passed

Final rating : Excellent

Disclaimer

SlowMist only issues this report based on the fact that has occurred or existed before the report is issued, and bears the corresponding responsibility in this regard. For the facts that occur or exist later after the report, SlowMist cannot judge the security status of theits smart contract. SlowMist, and is not responsible for it.

The security audit analysis and other contents of this report are based on the documents and materials provided by the information provider to SlowMist as of the date of this report (referred to as "the provided information"). SlowMist assumes that: there has been no information missing, tampered with, deleted, or concealed. If the information provided has been missinged, modified, deleted, concealed or reflected andor is inconsistent with the actual situation, SlowMist will not bear any responsibility for the resulting loss and adverse effects. SlowMist will not bear any responsibility for the background or other circumstances of the project.

Official Website

www.slowmist.com

E-mail

team@slowmist.com

Twitter

@SlowMist_Team

WeChat Official Account