HackenProof

Expert crowdsourced security provider

REPORT

Penetration Testing

for **Test company**

PREPARED BY

HackenProof

REPORT CREATED

20.03.2026

AUDIT DURATION

21.02.26-19.03.26

AUDIT TYPE

Web & Mobile

TABLE OF CONTENTS

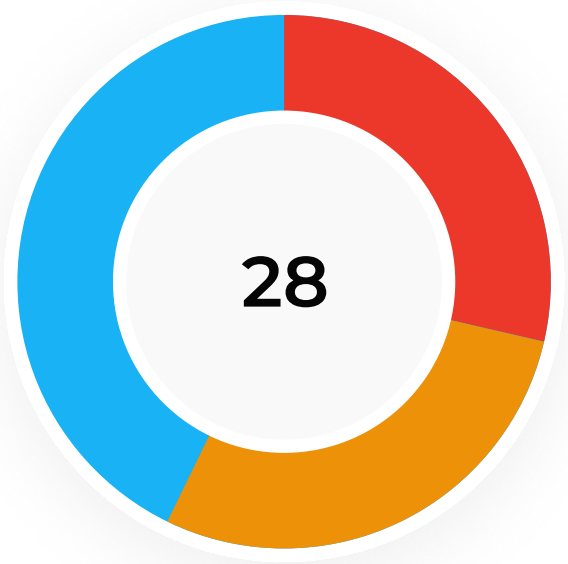
INTRODUCTION

HackenProof Audit is your solution to maximize cybersecurity through the involvement of the industry's most skilled and experienced community security researchers.

Name	Test company
Website	https://www.test.com/
Type	Penetration testing
Date	21.02.26 - 19.03.26
Scope	https://www.test.com http://futures.test.com https://h5.test.com https://api.test.com/api wss://ws.test.com/s/ws https://futures.test.com/api ws-futures.test.com/notification/v3 ws-futures.test.com/v1/market https://apps.apple.com/app/id154892 https://play.google.com/store/apps/details?id=com.io.test
Approved by	HackenProof team
Audited by	 @xaleraf4ra  @Marius-dp  @frodan  @jinxorder

AUDIT SUMMARY

28	28	0
Total Findings	Resolved	Informative



Critical	0
High	8
Medium	8
Low	12
None	0

FINDINGS LIST

HIGH

TEST-30	Active API Credentials Exposed in Public SDK Sample Enable Unauthorized Account Access and Trading	Resolved
TEST-25	IDOR Vulnerability Allows Unauthorized Bonus Recovery via bonusId Parameter Manipulation	Resolved
TEST-22	Cross-Site Scripting via JavaScript Bridge Callback Injection	Resolved
TEST-20	Debug/Test Credentials in Production Code	Resolved
TEST-12	Auth Token Exposure via Exported Activity and WebView JS Bridge → Session Hijacking & Potential Account Takeover	Resolved

TEST-6	Cross-Site Scripting in WebView	Resolved
TEST-5	API Server Address Hijacking via External Storage Domain Configuration File	Resolved
TEST-4	Hardcoded Third-Party Service Credentials (Zendesk) in Application	Resolved

MEDIUM

TEST-21	OS Command Injection via Unsanitized User Input	Resolved
TEST-19	Logging Authentication Token to System Log	Resolved
TEST-16	DoS via Malformed BigDecimal + Information Disclosure	Resolved
TEST-14	Logging Sensitive Financial Data	Resolved
TEST-13	Plaintext Password and Token Storage on Device	Resolved
TEST-7	Storing sensitive data on the SD card	Resolved
TEST-2	Domain Validation Bypass via Exception Handling Logic Flaw in Deep Link Router	Resolved
TEST-1	Plaintext Gesture Password Storage in SharedPreferences	Resolved

LOW

TEST-29	Pre-2FA Endpoint Exposes Authentication-Related Secret Value	Resolved
TEST-28	Potential Exposure of Sensitive Configuration Value via Public API	Resolved
TEST-27	Unauthenticated Access to Staff Directory / Employee Contact Information	Resolved

TEST-26	Improper Error Handling Leads to Internal Implementation Disclosure	Resolved
TEST-23	Logging Sensitive Financial Data (Trading Parameters and Asset Balances)	Resolved
TEST-18	Vulnerable SSL/TLS Implementation	Resolved
TEST-17	Insufficient Authentication for API Key Deletion	Resolved
TEST-15	Lack of Rate Limit on Listing Application	Resolved
TEST-10	Weak Cryptographic Algorithm (RSA/ECB/PKCS1Padding)	Resolved
TEST-9	Weak Hash Algorithm (MD5)	Resolved
TEST-8	Use of Random Instead of SecureRandom	Resolved
TEST-3	Development/Staging Server URLs Retained in Production Code	Resolved

ABOUT PROJECT

Test company Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco.

ASSESSMENT METHODOLOGY

This penetration test was performed in accordance with the Penetration Testing Execution Standard (PTES) as the primary testing methodology. The assessment followed the PTES phases, including:

- Pre-engagement interactions (scope definition and rules of engagement)
- Intelligence gathering and reconnaissance
- Threat modeling and attack surface analysis
- Vulnerability analysis
- Exploitation
- Post-exploitation and impact validation
- Reporting and remediation guidance

Application security testing was additionally aligned with:

- OWASP Web Security Testing Guide (WSTG) for web application testing;
- OWASP Top 10 (2021) for common web application risks;
- OWASP API Security Top 10 (2023) for API-specific security testing.

Testing was performed using a combination of manual security assessment and industry-standard security tools. Identified findings were manually validated to eliminate false positives and assess real-world exploitability.

DISCLAIMER

HackenProof Disclaimer

The application provided for assessment has been analyzed in accordance with generally accepted industry practices applicable at the time this report was prepared. The assessment focused on identifying cybersecurity vulnerabilities and security issues in the application's source code, deployment, configuration, and functionality, based solely on the materials, access, and scope made available for the engagement.

This report does not provide any representation or warranty that all vulnerabilities, weaknesses, or misconfigurations have been identified, nor does it guarantee the absolute security, reliability, or bug-free status of the application. The conclusions herein apply only to the specific version and scope reviewed and may no longer remain valid after any modification,

update, or environmental change. This report should not be regarded as a definitive or exhaustive statement of the application's security posture.

Technical Disclaimer

Applications, whether decentralized applications (DApps) or other software systems, are deployed and operated within technical environments that may include blockchains, cloud services, operating systems, programming languages, frameworks, libraries, APIs, third-party services, and infrastructure components. Any of these elements may contain inherent weaknesses, undisclosed vulnerabilities, or configuration issues that can result in security incidents, operational failures, or unauthorized access.

The assessment reflects the condition of the application only at the time of testing and within the agreed scope, and the absence of findings in this report must not be interpreted as evidence that no vulnerabilities exist. Continuous security practices, including secure development, independent reviews, monitoring, patch management, and periodic reassessments, remain necessary to maintain an appropriate level of security.

HackenProof

Expert crowdsourced security provider

PENETRATION TESTING

Contact us:

Linkedin | X | Website | Mail

2026