Assurance Report on Security Assessment of Rocket Vault

14 May 2021

1 About the Provider

Zokyo is a cybersecurity team that renders GRC (Governance, Risks management, Compliance), IT and IT security services including comprehensive security audits and penetration testing.

Our mission is helping customers ensure information security requirements: confidentiality, integrity, availability, etc. Our holistic approach covers all lifecycle phases of IT systems and ensures that our service deliverables include not only list of vulnerabilities and ways of their exploitation, but also recommendations on organizational and technical improvements, which can be done to reduce both present security risks and the ones, which can emerge in the future.

Zokyo dedicated security team members have personal international security certifications (CISSP, OSCP, CEH, CISM, CISA, CLPTP, etc.) and strictly adhere to laws, regulations, and Code of Ethics.

Zokyo uses a variety of security standards and frameworks (ISO, NIST, ISF, PCI DSS), as well as specific penetration testing methodologies. Our corporate security assessment methodology is based on the world's best security standards, frameworks and methodologies including, but not limited to OWASP, PCI DSS Penetration Testing Guidance, ISO 27000, ISF SoGP, NIST 800-115, EC-Council.

We have highly qualified pentesters in the area of web systems, client-server systems, wired and wireless networks, embedded systems, and social engineering. Our specialists were among the winners of the CTF (Capture The Flag) hacker competitions, where we showed effective solutions, therefore took 2nd place from 500 participants. We also take part in bug bounty programs. Our qualification allows us to perform the most complicated cyber security tasks like manual security review of source code, reverse engineering, 0-day vulnerability researches or Red Team exercises.

Business values of the security services by Zokyo are ensuring that not only world's best security practices are applied during all stages of software building, implementation and maintenance, but also realistic attack simulations are modeled, performed, analyzed and mitigated, therefore, probability of fraud, data leakage and other security incidents is minimized.

2 Introduction

On the request from Rocket Vault (Customer, Company) received on 19 April 2021 and according to the Statements of Work, Zokyo (pentesters, pentest team, testers, auditors) have delivered

the professional information security service including security assessment, namely, penetration test and risk assessment of the Customer's web solution Rocket Vault also referred below as the target object, solution, product.

The penetration test (pentest) is an acknowledged effective method to check and assess quality and security of information systems. During the pentest, security experts imitate actions of cyber criminals to check the possibility of intercepting the confidential data, misuse systems, interrupting normal operations and other security threats. Penetration testing is mainly manual work and is deeper analysis than just an automated vulnerability scanning.

Security risk assessment was conducted using analysis of the documentation and information obtained from the penetration test. To improve analysis of the threats and risks related to the found security issues, to optimize risk evaluation and risk treatment decisions, an integrated approach based on ISO 27005, CRAMM, British Standards Institution (BSI), and IT-Grundschutz recommendations was employed.

3 Short Description of the Project

Project goal was to find ways of unauthorized access to the target object, its data, ways of destruction or disruption the target object, other security violations, or to make the conclusion that no such ways can be found within the project scope and with the project parameters.

Project scope. During the pre-engagement process, Zokyo and the Customer have agreed the Rules of Engagement for the project. The Rules of Engagement included the detailed project specification, which defines parameters of the active pentest phase. In short, these parameters were the following.

The pentest target object was the test system running at one external host ***rocket-vaults-finance-old.netlify.app***.

The pentest was performed in black box mode – the pentest team had no internal knowledge of the target system. Brute force techniques were allowed. Social engineering methods were not allowed.

Project duration: from 26 April to 12 May, 2021. Retest was done on 13 May, 2021.

Project resources included the dedicated security team and software tools.

4 Rules of Engagement

Prior to the engagement, the pentesters and the Customers agreed the Rules of the Engagement for the assessment. These rules were included to the Statement of Works that outlined the following pentest parameters, as well as procedures for notification of vulnerability scanning, notification of vulnerabilities and vulnerability exploitation.

- SSL, DNSSEC, Cookie Security, Security Headers, WAF, SPF, Open Ports, VDP.

- Key storage, Key Generation, Wallet limits, Logging, ACL management (Hashicorp Consul), End-to-end encryption.
- Business Logic via API.
- Business Logic via API, 2FA, Strong password policy, CAPTCHA, Anti-phishing identifier.
- IP address whitelisting option, Withdrawal access whitelisting option, Email confirmation on Withdrawal.
- Requirements: Confidentiality, integrity, and availability of the target object.
- Relevant threats: Confidential information leakage, information corruption, business disruption, etc.
- OWASP top 10 (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project) software development and configuration vulnerabilities.
- Other possible vulnerabilities that can be found using automated tools and manually.
- Pentesting mode: Black box. Pentesters have limited information about the target object before the project start.
- Access to the target object: project works should be performed remotely using the Internet.
- Attacker profile (model of an attacker):
  - promiscuous cybercriminal (cyber hooligan);
  - purposeful cybercriminal targeting any victim;
  - purposeful cybercriminal targeting the Customer.
- Pentest vectors (attack scenarios): no limitations.
- Allowed time for active pentesting phase: round-clock.
- Methodologies and standards: NIST SP800-115, PTES, OWASP, ISACA Penetration testing procedure (P8).
- Tools include but not limited to: Kali Linux, Nessus, OpenVAS, Acunetix, Qualys, WireShark, nmap, hping3, socat, scapy, Firefox, ike-scan, whois, BeEF framework, Metasploit, PortSwinger Burpsuite PRO, Google, Cain & Abel, Maltego, Paterva, Colasoft Packet Builder, Fiddler, Mantra Security Framework, SAINT, Vega, WebScarab, Xenotix, John the Ripper, Colasoft Capsa Network Analyzer, OWASP Zed Attack Proxy (ZAP), Nikto Web Scanner, THC-Hydra, w3af, SQLmap, Karma, Kismet, NetStumbler, VisualCodeGrepper (VCG), onlinehashcrack.com, sslsplit, Pineapple, Reaver, reaver-wps-fork-t6x, Flawfinder, RATS, FindBugs, CodePro Analytix, PMD, Graudit, Wpscan.
- Productive and test systems and data – present. No dedicated test environment will be provided.
- Brute force techniques productive systems – allowed.
- Changes to the target during the pentest – not allowed.

- Changes to the pentesting parameters – allowed (if this can optimize reaching the project goals and if the Customer agrees).
- Pentest visibility – overt. The Customer will not test the ability of their personnel to respond to cybersecurity attacks within this project.
- Social engineering tests – not allowed.
- Known problems (optional parameter) – not to test what is anyway known, etc. No information.

5 Penetration Testing Methodology

The best practice OSSTMM (Open Source Security Testing Methodology Manual), OWASP (Open Web Application Security Project), NIST and ISACA penetration testing and auditing standards and guidelines were used. The testing was conducted against the supporting environment such as operating system.

The test was done using a combination of manual and automated tools and techniques to identify vulnerabilities within the target environment and exploit them. Social Engineering attacks were deemed out of scope during this test. Denial of service attacks were part of the test.

6 Penetration Testing Workflow

The pentest workflow has included:

1) Scope clarification
2) Vulnerability testing
3) Manual verification

Following relevant OWASP top 10 vulnerabilities were checked during the project:

A1 **Injection**

A2 **Broken Authentication**

A3 **Sensitive Data Exposure**

A5 **Broken Access Control**

A6 **Security Misconfiguration**

A7 **Cross-Site Scripting (XSS)**

A8 **Insecure Deserialization**

A9 **Using Components with Known Vulnerabilities**

Other types of vulnerabilities were also tested.

7 Conclusion

The target object was studied and analyzed according to the project plan. During the penetration test and attack simulations, it was found that an unauthorized person (attacker, intruder) **cannot penetrate** the target object or cause any serious security violations.

The assessment was conducted in a manner that simulated a malicious individual who has access to the Customer's external network over the Internet. Automated and manual techniques were used to assess the security of the target systems.

Pentesters have identified some vulnerabilities, made the recommendations for mitigation, continuous improvement and future security assessments. The Customer has followed the recommendations of the pentesters and mitigated the identified vulnerabilities. Then the retest was performed to ensure that no critical vulnerabilities were remained. The results of the follow-up consultations and the retest testify the **industry acceptable security level** of the product as of the date of the pentest project completion.