Armors Labs

Fairdesk

2022/5/16

Document information

Project Name:	Fairdesk Exchange
Start and end time:	2022/04/26-2022/05/16

Copyright description

Catalogue

I.Test process

The penetration was carried out in accordance with the authorization of the Fairdesk exchange, and the penetration test was carried out on the related businesses of the Fairdesk exchange from a remote location. How to accurately and effectively discover the real risks and security vulnerabilities existing in the system, and how to avoid and protect them effectively is the main goal of our penetration test.

Since this system is the actual operating system of the Fairdesk exchange, we try to avoid using denial of service attacks during the testing process, so as to avoid affecting the related business operations of the Fairdesk exchange during the testing process.

Information collection and analysis in the early stage is very important for the later penetration testing. Vulnerability discovery is mainly carried out through manual analysis and tool scanning. Security analysis will be evaluated from three aspects: technical dimension, business dimension, and management dimension. The vulnerability disposal process will complete the overall process disposal process from five aspects: vulnerability discovery, vulnerability verification, vulnerability rating, vulnerability retest, and vulnerability closure. The development of remote penetration testing is more conducive to the development of the project, and external network penetration testing can better illustrate the seriousness of security than internal network penetration testing.

a Client entrustment

Client entrustment is a necessary condition for the implementing company to conduct penetration testing. The implementing company will do its best to ensure that Party A is aware of all details and risks of the penetration test, and all processes are carried out under the control of Party A, which is also the implementing company. The professional services of a hacker are different in nature.

The penetration testing power of attorney (authorization letter) should contain the following:

(a). Scope of penetration test (including IP address or domain name);

(b). Penetration test time (including start time and end time);

(c). The power of attorney (authorization) for penetration test shall be submitted in writing and stamped with the official seal of Party A.

b Information collecting

Information collection and analysis is the premise / prelude / basic of almost all intrusion attacks. Through information collection and analysis, attackers (testers) can make corresponding and targeted plans for intrusion attacks, improve the success rate of intrusion and reduce the probability of exposure or discovery.

The methods of information collection include application fingerprint information detection, system service information detection, search engine collection, third-party service information collection, etc. The basis of the analysis after information collection is the key knowledge base of security weaknesses.

c Vulnerability analysis

Vulnerability analysis is a necessary work for vulnerability discovery. Through a comprehensive assessment of the security weaknesses found in the actual business test of the enterprise, and through evaluation and analysis from the aspects of vulnerability utilization conditions, technical implementation difficulty, data sensitivity, business importance, etc., we can ensure the preciseness of the vulnerability discovery process and analysis.

d Risk rating

Risk rating is based on vulnerability analysis. The vulnerability risk rating will be assessed from three dimensions: technical risk, business impact risk, and management risk, which will serve as data support for the implementation of security management work to ensure that relevant risks can be properly handled.

e Report

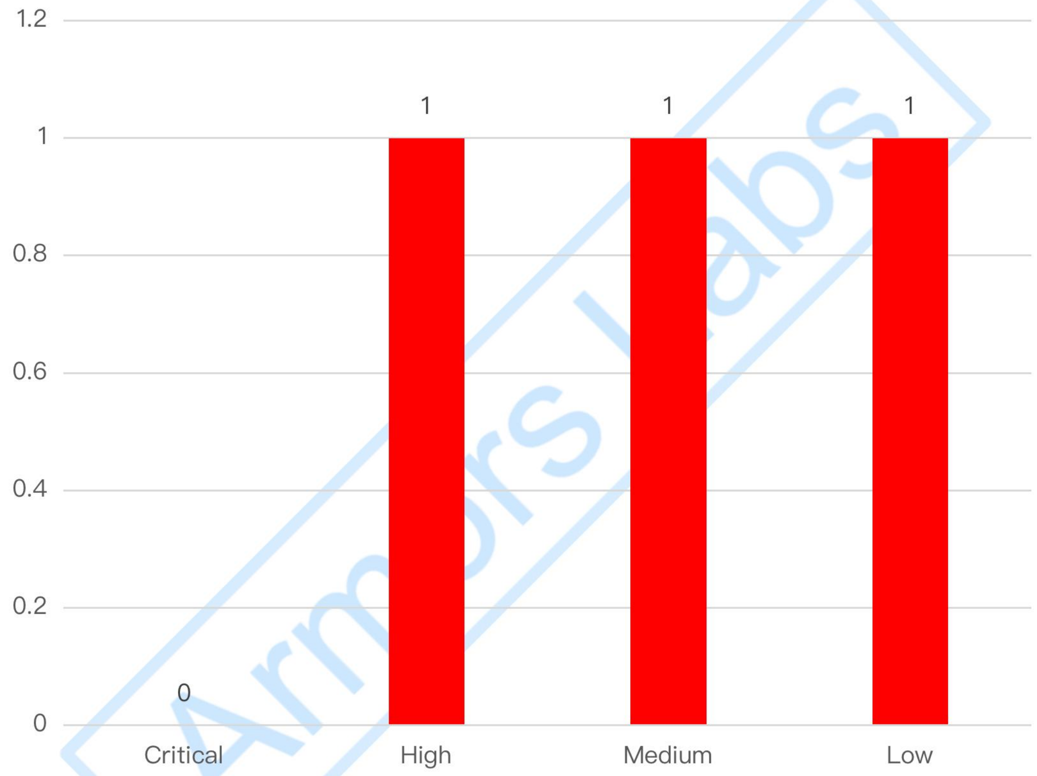
In order to enable customers to better understand and supervise the whole process of penetration test, the penetration test will be recorded in various ways such as written text and key screenshots. The key screenshots can reflect the whole process of penetration test more intuitively and truly than written text.

After the penetration test is completed, the safety experts of Armors (Beijing) Technology Co., Ltd. will write the penetration test report according to the process documents of the penetration test to describe the process and results of the penetration test in detail, and propose solutions to the problems found.

II.Test result

a Vulnerability statistics

Vulnerabilities Number	Critical risk	High risk	Medium risk	Low risk
3	0	1	1	1



b Vulnerability distribution statistics table

ID	Type	Severity	Status
ZA-2022-0426-T9A18p	Parallel ultra vires	Low	Closed
ZA-2022-0501-QihoVv	Remote command / Code execute	High	Closed
ZA-2022-0429-mOq6rH	Remote command / Code execute	Medium	Closed

III.Project summary and suggestions

a Project summary

For this comprehensive security analysis of the business system provided by Fairdesk Technology PTE. LTD, we have basically understood the security of Fairdesk Technology PTE. LTD business. This project includes vulnerability mining, risk analysis, and vulnerability verification. The level of security system construction needs to be improved. There are remote command / code execute and parallel ultra vires vulnerabilities in the security vulnerabilities found in the analysis. These vulnerabilities confirm that the development structure is weak and the website identity authentication is not perfect. In the future, it is recommended to strengthen the security awareness of developers and Improve the overall software development architecture system.

through the analysis of the business scope and the security assessment of the open services and data exposure surfaces of the target system, we found that Fairdesk Technology PTE. LTD imposes strict restrictions on access control. Only a few security holes were found. After a comprehensive review of its core payment business, some data security loopholes were found. Overall security is mature. Regarding safe construction is acceptable.

We have conducted a comprehensive analysis on the exposure of IT assets of Fairdesk Technology PTE. LTD’ s business, and found that related business of Fairdesk Technology PTE. LTD all deployed in cloud. Considering its businesses highly dependent on cloud service providers, infrastructure security more dependent on cloud service providers and the security characteristics of Internet business, we suggest that the security team and the operation and maintenance support team pay timely attention to the security of cloud server, system, middleware and related components.

b Suggestions for future safety planning

Based on some problems found during this penetration test, we suggest Fairdesk Technology PTE. LTD Company focus on the following aspects:

i.Gradually improving security development specifications and system developmen

Strictly abide by the safety development specifications, and prohibit substandard launching. For the design of new products and functions, product security design and realization of security mechanisms are required. Combined with the existing security development specifications (security coding, authority control, special character filtering, file uploading whitelist, etc.), the new security risk scenarios are gradually improved. Detailed security inspection before the launching of the product should be carried out. According to types of different vulnerabilities, different functions, and different business scenarios, multi-dimensional and all-around security inspections should be carried out to ensure stable operation of the platform after the launching of the product. Update and improve the existing security development specifications and system construction in time according to the safety risks of new business scenarios.

ii.Improving construction of security protection system and security monitoring and response system

Considering the business and security characteristics of Fairdesk Technology PTE. LTD, we suggest Fairdesk Technology PTE. LTD security team pay attention to Internet vulnerability information promptly, focusing on cloud service providers' security and related vulnerability information of third-party components and services, and monitor Internet assets regularly at the same time, pay close attention to the security status of assets on the cloud in time, and improve the business security utilizing the security protection system on the cloud, focus on upgrading security protection equipment and policy rules on the cloud, and build a sound security monitoring response system, to make an early warning for the latest security vulnerability monitoring and perform iteration for the early warning, thus to timely respond and update and maintain the system.

iii.Regularly educating all employees and key positions on cybersecurity awareness and strengthen the management of third-party safety responsibility

Strengthen the cybersecurity awareness of all employees and regularly organize education and training on network security awareness for business operation teams, key technical staff, functional personnel, and management teams to improve security awareness of all employees. Meanwhile, the third-party partners of Fairdesk Technology PTE. LTD are required to be responsible for the security as well, to reduce the risk of third-party outsourcing.

iv.Further strengthening mobile application security and user privacy protection

While implementing globalization strategy, the business development of Fairdesk Technology PTE. LTD should comply with the requirements of local cybersecurity management specifications. From the security analysis of the business of Fairdesk Technology PTE. LTD, we suggest Fairdesk Technology PTE. LTD gradually increase its investment in the security of mobile applications and third-party SDK. A comprehensive evaluation of the security of its SDK and third-party SDK should be conducted to manage the data security responsibility boundary, emphasizing user privacy protection. In the meantime, it is strongly recommended that Fairdesk Technology PTE. LTD should establish and maintain good cooperation with relevant government safety regulatory agencies, and pay close attention to the policy trends of relevant regulatory authorities promptly.

v.Regularly carry out penetration testing and fix system vulnerabilities on time

Penetration testing is not done once and for all. With the continuous changes in network technology, new security vulnerabilities are continuously disclosed, new attack methods are constantly produced, and at the same time, the continuous development of payment technology, the continuous launch of new services, the continuous update of codes and third-party libraries. It will bring potential new system security risks at any time. Therefore, cybersecurity is dynamically changing. In order to quantify the network security indicators of the system and realize the maximum visualization of the security posture of the system, Fairdesk Technology PTE. LTD an Internet company that is highly sensitive to network security, is established regularly (3 months, 6 months) to conduct penetration tests and security remediation plans. Critical. This is an important measure to maintain the security and healthy development of the system. It is strongly recommended that Fairdesk Technology PTE. LTD establish a long-term mechanism for similar system security

IV.About Armors

Armors is the first group of institutions engaged in blockchain security services in the world, mainly engaged in blockchain code audit and smart contracts development. Since its establishment five years ago, it has served more than 1000 customers and the audit partner of OK, Huobi, binance, bitthumb, bitfinex and other exchanges. Protect blockchain assets worth more than $15 billion. In 2021, Armors officially realized full profitability. Compared with competitors, Armors has zero audit accident rate and is better at smart contracts development. At the same time, Armors team has comprehensive ability. In addition to ETH related ecology, it has the ability of safety audit and ecological development for new active public chains such as Solana, ADA, Polygon and Metis, which has been officially recognized.