



# Armors Labs

## Fairdesk

2022/5/16

## Document information

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

## Copyright description

Unless otherwise specified, any text description, document format, illustrations, photos, methods, processes and other contents in this document are confidential information. Whether in electronic or non-electronic form, without the written authorization of Armors (Beijing) Technology Co.,Ltd, no individual or institution may reproduce, quote or transmit any part of this document.

## Catalogue

I. Test process	– 2 –
a Client entrustment	– 2 –
b Information collecting	– 3 –
c Vulnerability analysis	– 3 –
d Risk rating	– 3 –
e Report	– 3 –
II. Test result	– 4 –
a Vulnerability statistics	– 4 –
b Vulnerability distribution statistics table	– 4 –
III. Test summary	– 5 –
a Disclosure of sensitive information	– 7 –
b Design errors / Logic flaws	– 7 –
c SQL injection	– 7 –
d XSS attack	– 7 –
e Over Permission in parallel	– 8 –
f Unauthorized access	– 8 –
IV. Safety advice	– 8 –
a Disclosure of sensitive information	– 9 –
b Design errors / Logic flaws	– 9 –
c SQL injection	– 9 –
d XSS attack	– 10 –
e Parallel ultra vires	– 10 –
f Unauthorized access	– 10 –
V. Project summary and suggestions	– 10 –
a Project summary	– 10 –
b Suggestions for future safety planning	– 11 –
VI. About Me	– 14 –

# 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.

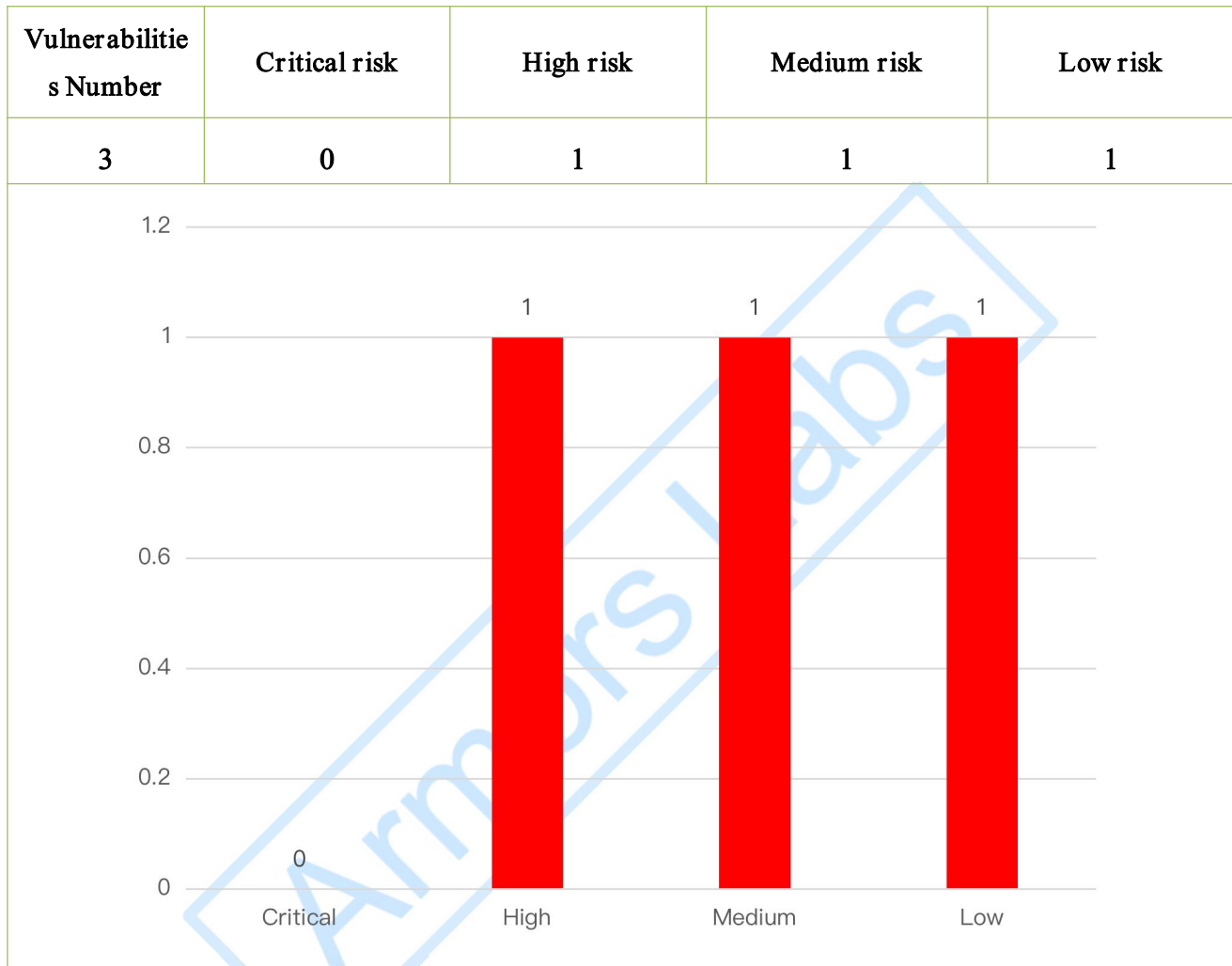
## **e Report**

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



### 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. Test summary

This time, we have conducted a comprehensive risk investigation on the Fairdesk exchange and related application businesses, and have further understood the security of Fairdesk exchange. In response to the relevant requirements and confidentiality requirements of the penetration test authorization letter, we tested this time to find problems and verify. The severity of the impact of security risks on the business is mainly, and the security risks are most likely to be discovered within the testing time range. For relevant target platforms we make a table as follows;

Test item	Vulnerability type	Function item detection description
User registration	Any user registration	Attempt to bypass validation for detection
User login	brute force	Brute force cracking by replaying packets
	Error prompt	By constantly trying to input, see the returned error information and judge
	Data not encrypted	Check if important parameter transmission is encrypted transmission by grabbing
	SQL injection	Try universal password login for SQL injection detection
Password Reset	SMS / email verification code	Try brute force cracking of verification code
		The verification code can be obtained by grabbing
		The verification process logic problem is tested by trying to bypass the verification code
		You can try to guess the link parameters, such as simply using the MD5 value of the user name
Verification Code	Timeliness	The validity period of the verification code is too long. You can try brute force cracking
	Randomness	The verification code is not random and inexhaustible. Try to guess the verification code
	Complexity	The verification code is not complex enough, the length is not enough, or the content of the graphic verification code is not mixed, which can be identified by the script program



	Security	Key parameters such as user ID are not bound when sending. Try to send beyond authority or send without restriction
Business operation	Ultra vires	The server failed to restrict or verify the account authority of the requested data, resulting in the attacker being able to manipulate the account of others
	Unauthorized access	The business function permission setting is unreasonable. Try to bypass the login and access directly
Data transmission	Parameter filtering	Through semi manual and semi automated testing of SQL injection, XSS, command execution and other vulnerabilities
	Parameter encryption	Through the form of residential data packet, detect whether plaintext is used to transmit data in HTTP protocol
Session security	Submission method	Detect whether to submit sensitive data in get mode by capturing data packets
	Parameter randomization	The parameters are controllable, can be guessed and replayed
	Disable external entities	By modifying the form of data packet, detect whether there is external entity injection vulnerability
	Authentication information	Try to log in to the system for detection through unexpired session / token and other information
	Random factor	Exploit CSRF in session, random detection without parameters
Program logic	Improper identity authentication	Use SSRF vulnerability to detect Intranet
	Improper function call	By manually trying to access system files and other means, detect whether any file reading, command execution and file inclusion exist
	Data binding	Detect vertical ultra vires and horizontal ultra vires vulnerabilities for verification
API	Customer request interface	Jsonp, request interface, return sensitive information, request controllable VPS to obtain data
Other	Middleware security	Automatic tools are used to detect the parsing vulnerabilities and command execution vulnerabilities of various middleware
	Weak password	Detect by trying common passwords
	Disclosure of sensitive	Try to find git, SVN and other sensitive



	information	information
--	-------------	-------------

Through this penetration test of the Fairdesk exchange and related business systems, I have a better understanding of the security status of the related Fairdesk exchange. From the analysis of the vulnerabilities found in the penetration test, the platform mainly has the following problems;

#### **a Disclosure of sensitive information**

Sensitive information is leaked in the page or in the returned response package, which provides a lot of useful information for attackers to penetrate.

#### **b Design errors / Logic flaws**

Because the code is not fully considered or there are problems in the verification method when the code is written and actual, the attacker can modify the return packet, bypass the front-end verification code, or the back-end verification is incomplete, so that the attacker can call out of sequence by calling The interface bypasses the normal flow.

Since the code layer and database are not locked, an attacker can send a large number of requests in a short time to cause a conditional competition vulnerability, which can break through the maximum limit set by the program.

#### **c SQL injection**

In the web program, the parameters submitted by the user are not filtered and directly spliced into the SQL statement for execution. As a result, the special characters in the parameters destroy the original logic of the SQL statement. Attackers can use this vulnerability to execute arbitrary SQL statements, such as querying data and downloading data. , write webshells, execute system commands, bypass login restrictions, etc.

#### **d XSS attack**

The parameters submitted by the user are not filtered or are not strictly filtered in the Web program code, resulting in the special characters in the parameters destroying the original logic of the HTML page. Attackers can use this vulnerability to execute malicious HTML/JS code, construct worms, and tamper with pages. Implement phishing attacks, induce users to log in again, and then obtain their login credentials.

Although XSS attack does no direct harm to the web server itself, it spreads through the website, attacks website users, steals website user account identity information, etc., which will also pose a serious threat to the website.

Storage XSS attacks can lead to the following compromises:

- (a). Identity theft: a cookie is the user's authentication mark for a specific website. XSS attack can steal the user's cookie, so as to use the cookie to steal the user's operation authority on the website.
- (b). Stealing website user information: when the user's cookie is stolen to obtain the user's identity, the attacker can steal the user's operation authority on the website and view the user's privacy information.
- (c). Spam sending: in the social networking site community, XSS vulnerabilities are used to borrow the identity of the attacker to send a large amount of spam to a specific target group.
- (d). Hijacking users' web behavior: some advanced XSS attacks can even hijack users' web behavior, so as to monitor users' browsing history, sent and received data, etc.

#### **e Over Permission in parallel**

Since there is no strict inspection and restriction on the permissions of the user's access role, the current account can perform related operations on other accounts, such as viewing and modifying. The operation of a low-privileged account with a high-privilege account is vertical override, and the operation between accounts with the same privilege becomes horizontal override, also called horizontal override.

#### **f Unauthorized access**

Due to the failure to check the login status and access rights of the sensitive pages and interfaces of the website, the attacker can access without authorization, obtain sensitive information and perform unauthorized operations.

## **IV.Safety advice**

Based on the process of penetration testing and the problems found, we propose the following security improvement suggestions for the current security construction of the Fairdesk exchange and related business systems;

## **a Disclosure of sensitive information**

- (a). If it is a useless program such as probe or test page, it is recommended to delete it or change it to a name that is difficult to guess.
- (b). Delete or prohibit access to pages that disclose sensitive information without affecting business or functions.
- (c). Fuzzify the relevant sensitive information on the server side.
- (d). Strictly check the data returned by the server to ensure that the query data is consistent with the data displayed on the page.

## **b Design errors / Logic flaws**

Modify the code logic and perform strong verification or multiple verification on the server. For conditional competition vulnerabilities, the best fix is to set locks in the code layer and database.

## **c SQL injection**

The best defense against SQL vulnerabilities in the code layer: query and bind variables with precompiled SQL statements.

- (a) When using precompiled statements and PDO, be careful not to splice variables directly into PDO statements. All query statements use the parameterized query interface provided by the database. Parameterized statements use parameters instead of embedding user input variables into SQL statements. At present, almost all database systems provide parameterized SQL statement execution interface, which can effectively prevent SQL injection attacks.
- (b) Escape the special characters ('< > & \*; etc.) entering the database or code conversion.
- (c) Confirm the type of each data. For example, digital data must be digital, and the storage field in the database must correspond to int.
- (d) The data length should be strictly regulated to prevent long SQL injection statements from being executed correctly to a certain extent.
- (e) The coding of each data layer of the website is unified. It is recommended to use UTF-8 coding. Inconsistent coding between the upper and lower layers may lead to some filtering models being bypassed.
- (f) Strictly restrict the operation authority of the website user's database, and provide this user with the authority that can only meet his work, so as to minimize the harm of injection attack to the database.

- (g) Prevent the website from displaying SQL error information, such as type error, field mismatch, etc., and prevent attackers from using these error information to make some judgments.
- (h) Filter dangerous characters. For example, regular expressions are used to match Union, sleep, and, select, and load\_ File and other keywords. If they match, the operation will be terminated.

#### **d XSS attack**

XSS vulnerability is essentially a kind of HTML injection, that is, injecting HTML code into web pages. Then the fundamental defense is to do a series of filtering and escape when displaying the code submitted by the user on the page.

- (a) Filter the input data and strictly check the dangerous characters such as: "'", '"', "<", ">", "on \*", script, iframe, etc. the input here is not only the input interface that users can interact directly, but also the variables in the cookie in the HTTP request, the variables in the HTTP request header, etc.
- (b) Verify not only the type of data, but also its format, length, scope and content.
- (c) Not only do data verification and filtering at the client, but the key filtering steps are carried out at the server.
- (d) Carry out corresponding coding conversion for the data output to the page, such as HTML entity coding, JS coding, etc. The output data should also be checked. The values in the database may be output in multiple places of a large website. Even if the input is coded, it should also be checked at the output points everywhere.

#### **e Parallel ultra vires**

- (a). Strictly check and restrict the access rights of users to roles.
- (b). In some operations, you can use session to judge and control the user's identity

#### **f Unauthorized access**

- (a). Strictly control the access rights of the page and check the access rights of the access roles.
- (b). You can use session to judge and control the user's identity.

## **V. 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.

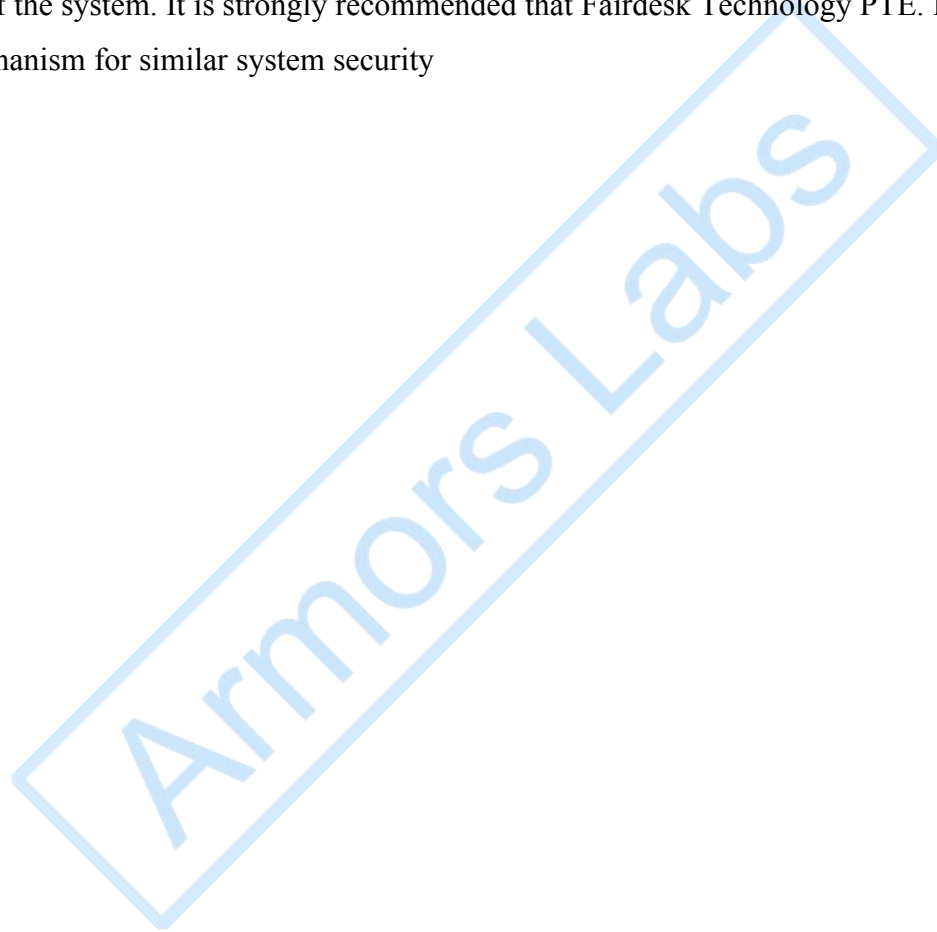
## **iv.Further strengthening mobile application security and user privacy protection**

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





## VI.About Me

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.

