ICORATING

Exchange Security Report

Over the years, digital thieves have stolen millions of dollars' worth of cryptocurrency from various exchanges. The crypto market attracts a huge number of investors and everyone hopes to get the highest returns and it doesn't bother anyone that once your crypto is stolen, you won't get the refund, transactions and assets are not secured in any way, which makes investing in cryptocurrencies really hazardous. The largest crypto exchanges contain vast amounts of digital cash. These facts are really attractive for hackers.

Over the past 8 years about 31 crypto exchanges have been hacked and more than a 1 billion dollars (actually, $ 1.3 bn) stolen. Some of the crypto exchanges learned from their mistakes and managed to recover, the others went bankrupt and several the most "happy" ones, such as Mt.Gox, Bitcoinica, PicoStocks, Bitcurex, have been attacked even multiple times.

Today more than 200 crypto-exchanges offer their services and this number is constantly growing, therefore, the fall or hacking of the one exchange will not lead to a drop in the market, as it could have been before, furthermore many countries are beginning to introduce regulatory requirements for crypto-exchanges, but still nobody is fully protected from the loss of their crypto assets, therefore, invest in reliable assets, diversify your portfolio and choose good crypto exchanges.

When preparing this security rating, we have assessed security measures against the following potential vulnerabilities that could negatively impact exchanges and their users.

The report will discuss the following issues in detail:

- **Console errors**
- **User Account Security**
- **Registrar and Domain Security**
- **Web Protocols Security**

We selected exchanges whose daily trade value exceeds one million USD; the total number of exchanges on the list is 100.

Console errors

These errors in the code can result in the malfunctioning of some systems that might lead to problems for their users. This type of vulnerability is usually not critical, however it should be taken into account as in some instances these errors have resulted in data loss.

- Exchanges that have neither error nor a warning about this type of error: 49%
- Exchanges with no errors: 68%

Conclusion: 32% of exchanges have code errors, which leads to certain defects in operation.

User Account Security

A separate account has been created on each exchange. The following parameters have been assessed:

1. The possibility of creating a password with fewer than 8 symbols
2. The possibility of creating a password with either digits or letters alone
3. Email verification immediately after account creation
4. The presence or absence of 2FA

The results of this assessment are as follows:

- 41% of exchanges allow passwords with fewer than 8 symbols
- 37% of exchanges allow passwords with either digits or letters alone
- **5% of exchanges allow the creation of accounts without email verification**
- **3% of exchanges lack 2FA**
- **Only 46% of exchanges meet all four parameters**

Registrar and Domain Security

We have used the cloudflare platform (https://www.cloudflare.com/domain-security-check) to check these exchanges for vulnerabilities connected with their registrar and domain:

1. **Registry lock**; Registry lock is a special flag in the registry (not your registrar) that prevents anyone from making changes to your domain without out-of-band communication with the registry.
2. **Registrar lock;** Registrar Lock (not to be confused with Registry Lock) prevents this kind of domain hijacking by requiring more than just an auth code to change information in the global registry.
3. **Role accounts;** Security-conscious organizations avoid leaking this kind of private information by using role accounts to register their domain names. Role accounts protect individuals in your organization from being targeted by attackers.
4. **Expiration;** We recommend at least a 6-month expiration window for high profile domains. This is enough leeway to deal with unforeseen complications such as an

employee owning the domain leaving the company (again, this is a good reason to use Role Accounts).

5. **DNSSEC;** DNSSEC eliminates the threat of DNS cache poisoning by authenticating all DNS queries with cryptographic signatures. Instead of blindly caching DNS records, DNS servers will reject unauthenticated responses.

There are three possible outcomes for each item: All items above operate correctly (1), None operate properly (0), warning (0.5). The results of this assessment are as follows:

- **Only 2% of exchanges use registry lock**
- **Only 10% of exchanges use DNSSEC**
- **There were no exchanges that had problems with all five items**
- Only **4%** of exchanges using best practice in 4 out of 5 of these areas.

Web Protocols Security

We have checked whether the exchanges under scrutiny possess headers that ensure protection against various attacks. We used the following resource: https://www.htbridge.com/websec/. Depending on whether an exchange had the protocol in question, it was rated either 1 or 0. We checked whether the following headers were present:

1. Strict-Transport-Security header (an HTTP-Strict-Transport-Security (HSTS) header forces browsers to browse the website in HTTPS).
2. X-XSS-Protection header (X-XSS-Protection defines how browsers should enforce cross-site scripting protection).
3. Content Security Policy header (Content-Security-Policy (CSP) enables the definition of permitted sources for each type of content, helping to defend against XSS attacks. It also enables the ability to define several browser behaviors, such as sandbox enforcement, to the value to be sent in the HTTP Referer header.)
4. X-frame-options header (an X-frame-options header specifies whether the website should allow itself to be framed, and from which origin. Blocking framing helps defend against attacks such as clickjacking.)
5. X-content-type-options header (x-content-type-options can direct browsers to disable the ability to sniff page content type and only use content type defined in the directive itself. This provides protection against XSS or drive-by-download attacks.)

The results of this assessment are as follows:

- Only **10%** of exchanges have all five headers
- **29%** of exchanges have none of the above mentioned headers
- Only **17** exchanges have a Content Security Policy header

General Exchange Security Rating

The selected exchanges have been analyzed according to the above mentioned categories with the following scoring system:

- Console errors: Maximum 5 points per category, 2 parameters analyzed
- User Account Security: Maximum 18 points, 4 parameters analyzed
- Registrar and Domain Security: Maximum 34 points, 5 parameters analyzed
- Web Protocols Security: Maximum 43 points, 5 parameters analyzed

100 points maximum possible score when totalling the above.

	Name	Console Errors	User Security	Registrar & Domain Security	Web Security	Score
1	**Coinbase Pro**	2/2	4/4	3,5/5	5/5	**89**
2	**Kraken**	2/2	4/4	2/5	5/5	**80**
3	**BitMEX**	2/2	4/4	2/5	5/5	**78**
4	**GOPAX**	2/2	4/4	2/5	5/5	**78**
5	**CPDAX**	1/2	4/4	2/5	5/5	**74**
6	**Bitlish**	2/2	3/4	2/5	5/5	**74**
7	**BtcTurk**	2/2	3/4	2/5	5/5	**74**
8	**Cobinhood**	0/2	4/4	4/5	3/5	**71**
9	**Hotbit**	2/2	3/4	3/5	4/5	**69**
10	**Coinut**	1/2	2/4	2,5/5	5/5	**69**
11	**Luno**	1/2	4/4	1/5	5/5	**68**
12	**Ethfinex**	2/2	4/4	2/5	4/5	**67**
13	**Bittrex**	2/2	3/4	2,5/5	4/5	**66**
14	**UEX**	2/2	2/4	3/5	4/5	**65**

15	**Bancor Network**	1/2	4/4	2/5	4/5	**65**
16	**Coinhub**	1/2	4/4	3/5	3/5	**64**
17	**Binance**	1/2	4/4	2/5	4/5	**63**
18	**HitBTC**	2/2	3/4	2/5	4/5	**63**
19	**ABCC**	1/2	4/4	2,5/5	3/5	**61**
20	**DSX**	2/2	4/4	0.5/5	4/5	**61**
21	**Coinroom**	2/2	4/4	2/5	3/5	**59**
22	**Bitbank**	1/2	3/4	2/5	4/5	**59**
23	**xBTCe**	1/2	4/4	2/5	3/5	**58**
24	**Bibox**	0/2	3/4	4/5	2/5	**56**
25	**DragonEX**	2/2	4/4	1,5/5	3/5	**56**
26	**DigiFinex**	1/2	3/4	4/5	1/5	**55**
27	**YoBit**	1/2	4/4	2/5	3/5	**55**
28	**Livecoin**	2/2	4/4	2,5/5	2/5	**54**
29	**CoinEx**	1/2	2/4	3/5	3/5	**53**
30	**Rfinex**	1/2	2/4	2,5/5	3/5	**53**
31	**Coinbe**	2/2	4/4	1/5	3/5	**53**
32	**CEX.IO**	2/2	2/4	2/5	3/5	**53**
33	**Neraex**	0/2	2/4	3/5	3/5	**52**
34	**BigONE**	2/2	4/4	2/5	2/5	**51**
35	**QuadrigaCX**	2/2	2/4	2/5	3/5	**50**
36	**LBank**	2/2	2/4	3/5	2/5	**49**
37	**bitFlyer**	0/2	n/a	1/5	5/5	**49**
38	**Exrates**	1/2	4/4	1/5	3/5	**49**
39	**Iquant**	2/2	2/4	1,5/5	3/5	**48**

40	**Cryptonex**	1/2	2/4	4/5	1/5	**48**
41	**CoinsBank**	2/2	1/4	2/5	3/5	**48**
42	**OKEx**	1/2	2/4	1,5/5	3/5	**47**
43	**Simex**	1/2	2/4	2/5	3/5	**47**
44	**Poloniex**	2/2	3/4	3/5	1/5	**47**
45	**BitBay**	2/2	3/4	2/5	2/5	**47**
46	**HADAX**	2/2	3/4	1,5/5	2/5	**47**
47	**Huobi**	1/2	4/4	n/a	3/5	**46**
48	**CoinBene**	2/2	4/4	2,5/5	1/5	**46**
49	**Indodax**	2/2	2/4	1/5	3/5	**45**
50	**BiteBTC**	2/2	2/4	1/5	3/5	**45**
51	**BTCC**	1/2	4/4	2,5/5	1/5	**45**
52	**Cryptopia**	2/2	4/4	2/5	1/5	**45**
53	**Gate.io**	1/2	3/4	3/5	1/5	**44**
54	**Bitfinex**	2/2	4/4	2/5	1/5	**43**
55	**Gemini**	2/2	4/4	2/5	1/5	**43**
56	**Exmo**	2/2	2/4	2/5	2/5	**43**
57	**Coinone**	1/2	4/4	2,5/5	1/5	**42**
58	**Kucoin**	2/2	3/4	2,5/5	1/5	**42**
59	**LATOKEN**	1/2	4/4	2,5/5	1/5	**42**
60	**ZB.COM**	2/2	4/4	3/5	0/5	**41**
61	**RightBTC**	2/2	4/4	3/5	0/5	**41**
62	**OOOBTC**	2/2	4/4	3/5	0/5	**41**
63	**BitForex**	1/2	4/4	3/5	0/5	**40**
64	**IDCM**	1/2	4/4	3/5	0/5	**40**

65	**itBit**	2/2	4/4	1/5	1/5	**40**
66	**Bitsane**	1/2	4/4	2/5	1/5	**39**
67	**Sistemkoin**	2/2	2/4	2,5/5	1/5	**38**
68	**Bitstamp**	1/2	4/4	2,5/5	0/5	**37**
69	**OEX**	2/2	3/4	3/5	0/5	**37**
70	**CoinTiger**	1/2	4/4	2,5/5	0/5	**37**
71	**CoinEgg**	1/2	4/4	3/5	0/5	**37**
72	**BitMart**	2/2	3/4	3/5	0/5	**37**
73	**Liqui**	1/2	2/4	3/5	1/5	**37**
74	**Upbit**	1/2	4/4	1,5/5	1/5	**36**
75	**FCoin**	2/2	4/4	2/5	0/5	**35**
76	**Kryptono**	2/2	3/4	n/a	2/5	**35**
77	**BTC-Alpha**	1/2	3/4	2/5	1/5	**35**
78	**Bithumb**	1/2	4/4	2/5	0/5	**34**
79	**Bitinka**	1/2	4/4	2,5/5	0/5	**34**
80	**Coindeal**	1/2	4/4	2,5/5	0/5	**34**
81	**CryptoBridge**	1/2	3/4	3/5	0/5	**34**
82	**Fisco**	2/2	3/4	1/5	1/5	**33**
83	**Paribu**	0/2	2/4	2,5/5	1/5	**33**
84	**TOPBTC**	1/2	2/4	3/5	0/5	**32**
85	**CoinExchange**	0/2	2/4	1/5	2/5	**32**
86	**Coinsuper**	1/2	4/4	1,5/5	0/5	**31**
87	**Bit-Z**	2/2	3/4	2/5	0/5	**31**
88	**Fatbtc**	2/2	3/4	2/5	0/5	**31**
89	**Zaif**	1/2	3/4	1/5	1/5	**29**

90	**Trade By Trade**	2/2	4/4	1/5	0/5	**29**
91	**Instant Bitex**	1/2	1/4	3/5	0/5	**26**
92	**IDAX**	2/2	3/4	1/5	0/5	**25**
93	**Mercatox**	1/2	2/4	1/5	1/5	**25**
94	**EXX**	0/2	2/4	2,5/5	0/5	**24**
95	**BCEX**	2/2	2/4	1,5/5	0/5	**24**
96	**DOBI trade**	0/2	3/4	1,5/5	0/5	**23**
97	**BTCBOX**	1/2	2/4	1/5	0/5	**20**
98	**Tidex**	1/2	2/4	1,5/5	0/5	**20**
99	**Allcoin**	2/2	1/4	1,5/5	0/5	**19**
100	**OKCoin.cn**	1/2	1/4	1/5	0/5	**15**