



# EXPERT REPORT

---

on the results of the security audit  
of the [bcwallet.io](https://bcwallet.io) website owned  
by [Blockchain.ru](https://Blockchain.ru)

# Table of Contents

<b>1</b>	<b>Introduction</b>	3
	General provisions	3
	Generally accepted abbreviations	3
	Abstract	3
	Scope of works	3
<b>2</b>	<b>Security audit principles</b>	4
	IS threats	4
	Attacker model	4
	External attacker	4
<b>3</b>	<b>Attack scenarios</b>	5
	MiTM attack on a user	5
	Recovery of another user's account	5
<b>4</b>	<b>External audit the System</b>	6
	List of discovered vulnerabilities	6
	Insufficient entropy bits in a token	6
	Incorrect session management	7
	Security weaknesses	7
	No HSTS mechanism	7
	No protection from clickjacking attacks	8
	Unsafe CORS configuration	8
	OTP re-use	10
<b>5</b>	<b>Conclusion</b>	11
<b>6</b>	<b>License</b>	12
	<b>Appendix 1. Security assessment</b>	13
	Security level analysis	13
	Vulnerability severity	13
	Ease of vulnerability exploitation	14
	Vulnerability accessibility	14
	Likelihood of exploitation	15
	Vulnerability impact	15
	<b>Appendix 2. Security level analysis.</b>	16
	List of the discovered vulnerabilities and security weaknesses	16

# Introduction

This expert report contains the results of security assessment of the bcwallet.io website (hereinafter referred to as “the System”) owned by Blockchain.ru (hereinafter referred to as “the Company”) with recommendations on fixing the discovered vulnerabilities and improving the current security level of the System.

Abbreviation	Meaning
IS	Information security
DS	Data system
CIN	Corporate information network
FW	Firewall

Table 1. Generally accepted abbreviations

Cyber3’s experts conducted the security audit of the System. In the scope of work, they used and examined the external attacker model. The current security level of the System was rated “Above average”. The key recommendation suggested by the auditors is as follows:

1. Fix the discovered vulnerabilities and security weaknesses of the System.

Below, you can find a description and specification of the discovered security issues, information security risks posed by them, and a detailed list of recommendations on fixing the vulnerabilities.

The scope of the performed works included the Company’s LAN resources and the main business systems listed in Table 1.4.

No	Hostname/IP address
1	Bcwallet.io

Table 2. Generally accepted abbreviations

## Security audit principles

There are 3 types of IS threats that can affect the Company's information resources: violations of confidentiality, integrity or availability of information.

Confidentiality violations are usually aimed at information disclosure. If a violation is successful, the information becomes known to people, who should not have access to it: unauthorized personnel of the Company, clients, partners, competitors, and third parties.

Integrity violations are aimed at modification or corruption of the information, which can lead to modification of its structure or content, and to complete or partial destruction of the data.

An availability violation (denial-of-service threat) involves data system users' inability to access the information.

The core principle of this IS audit is an estimation of exploitation likelihood of the aforementioned threats affecting the Company's information resources, within the framework of a pre-defined attacker model.

A potential attacker is an individual or a group of individuals, acting either in a collusion or independently, whose intended or unintended actions can carry the aforementioned threats to the IS, infringe information resources of the System or negatively affect the Company's interests.

IS threats are basic threats to confidentiality and integrity of information and the threat of the System denial-of-service.

Attackers can pursue the following goals (and their possible combinations):

- Cause Denial of Service
- Escalate their privileges in the System
- Get unauthorized access to business-critical data

In the scope of work, the experts used an external attacker model.

The following submodel of an external attacker model was used to conduct the security assessment:

- An external attacker who has neither knowledge about the tested System nor privileges in it.

## MiTM attack on a user

## Recovery of another user's account

# Attack scenarios

The security weakness described [below](#) enables an attacker to launch an MiTM attack (man-in-the-middle).

An attacker can make a browser to pass data via a not secured network (downgrade attack).

It should be kept in mind, that an attacker and a victim must be in the same network (for example public Wi-Fi). In server responses, attackers can change the address of an actual wallet to that of the wallet they control. As a result, a victim will send cryptocurrency to an attacker's address.

By exploiting the "[Insufficient entropy bits in a token](#)" vulnerability, an attacker can generate many recovery codes and launch a brute-force attack. If it is successful, an attacker will get control over another user's account.

# 4

## List of discovered vulnerabilities

Insufficient entropy bits in a token

## External audit the System



Severity:  
high



Likelihood  
of exploitation:  
low



Overall  
impact level:  
average

### Description:

An application generates a unique token for a user to confirm critical actions. However, a generated token has insufficient entropy bits.

### Impact:

In particular cases, an attacker can successfully guess a token and perform critical actions in the System.

### Vulnerable resource:

- bcwallet.io

### Technical details:

During a password recovery, there is a letter with a link that contains a unique token sent to the specified e-mail. The number of unique bytes in a token may be  $\leq 6$ . Considering that, the number of requests from a token to a victim's email is limited, an attacker can minimize the amount of time required to guess the token.

### Recommendations:

- Increase the number of entropy bits in a token

```
https://api.bcwallet.io/activate/fdcf2e0e0c0011e834670242ac130009
https://api.bcwallet.io/activate/74115c5e0c0111e89bb20242ac130009
https://api.bcwallet.io/activate/aff85f70c0011e8b5780242ac130009
https://api.bcwallet.io/activate/7f28c144c0211e891b30242ac130009
https://api.bcwallet.io/activate/3d9abab0c0411e8be5d0242ac130009
https://api.bcwallet.io/activate/46a37970c0411e8b4cd0242ac130009
https://api.bcwallet.io/activate/49d3cee0c0411e8a3290242ac130009
https://api.bcwallet.io/activate/5016d8ee0c0411e8b2930242ac130009
https://api.bcwallet.io/activate/511a51e0c0411e8bd690242ac130009
https://api.bcwallet.io/activate/52e94730c0411e8a46a0242ac130009
https://api.bcwallet.io/activate/51df5e30c0411e890c10242ac130009
https://api.bcwallet.io/activate/526470ca0c0411e896e70242ac130009
https://api.bcwallet.io/activate/56040fd0c0511e8839d0242ac130009
https://api.bcwallet.io/activate/56f6c916c0511e89eb50242ac130009
https://api.bcwallet.io/activate/5796e5fe0c0511e8b2bd0242ac130009
https://api.bcwallet.io/activate/56645fe0c0511e8bce50242ac130009
https://api.bcwallet.io/activate/57f0844c0c0511e883450242ac130009
https://api.bcwallet.io/activate/5743d4fe0c0511e885e90242ac130009
https://api.bcwallet.io/activate/56ba7b64c0c0511e8857c0242ac130009
https://api.bcwallet.io/activate/58efc4b0c0511e8ac910242ac130009
https://api.bcwallet.io/activate/589a2ee80c0511e8a54b0242ac130009
https://api.bcwallet.io/activate/5841797e0c0511e8a0ac0242ac130009
https://api.bcwallet.io/activate/59472aee0c0511e8985d0242ac130009
https://api.bcwallet.io/activate/5a3c3d0e0c0511e8abe70242ac130009
https://api.bcwallet.io/activate/5a8d4d520c0511e8aee40242ac130009
```

Fig. 1. Links for password recovery



## Incorrect session management



Severity:  
average



Likelihood  
of exploitation:  
low



Overall  
impact level:  
low

### Description:

In case a session identifier is compromised, an attacker can get unrestricted access to a user's account.

### Impact:

With a session identifier given to a user during the authentication, an attacker can access private data after a user logs out.

### Vulnerable resource:

- bcwallet.io

### Technical details:

Refresh\_token and access\_token are valid after logout.

### Recommendations:

- Clear user session both when the set time expires and after logout.

## Security weaknesses

### No HSTS mechanism

### Description:

An attacker can launch a downgrade attack, thus forcing a user to use an unsafe connection with a web application. As a result, an attacker will be able to intercept data sent to the application by a user (e.g., passwords or cookies).

### Impact:

The web application uses no HSTS mechanism, which enables protection from traffic interception attacks.

### Vulnerable resource:

- bcwallet.io

### Technical details:

The HSTS (HTTP Strict Transport Security) mechanism forces a browser to use the safe TLS connection with the web application by default. This makes it difficult for an attacker to conduct MiTM attacks.

## No protection from clickjacking attacks

## Unsafe CORS configuration

### *Recommendations:*

- Implement the HSTS mechanism. It is necessary to add the following header to a server response: Strict-Transport-Security: max-age=%action duration%.

### *Description:*

The web server does not use X-Frame-Options parameters in the headers of web server responses.

### *Impact:*

The System's website loaded in the frame of an attacker's resource can be used to perform phishing and clickjacking attacks on users and to manipulate the Systems without them knowing about it.

For example, a user visits an attacker's website and performs some actions there (clicks, text typing). These actions will be sent to the System and processed there (not on an attacker's website) due to the website and the System being displayed on different levels.

### *Vulnerable resource:*

- bcwallet.io

### *Technical details:*

Frame-Options enables an attacker to recognize the policy of loading the site to frames on third-party resources. There is no X-Frame-Options header among the web server headers. The likelihood of an attack being launched depends on the functionality. The protection mechanisms should be implemented at least for subdomains/web site sections.

It should be noted that in the given version of the System, there is no functionality that should be protected in the described way. However, if further development of the website with the implementation of registration and user profiles is planned, the header will help protect from clickjacking by securiing new and potentially exploitable features.

### *Recommendations:*

- Add the X-Frame-Options header with the "DENY" or "SAMEORIGIN" values in all response headers.

### *Description:*

An attacker can get access to a user's sensitive data.



### Impact:

Web server misconfiguration with enabled CORS (Cross-Origin Resource Sharing) mechanism allows an attacker to get sensitive data of a website user.

### Vulnerable resource:

- \*.bcwallet.io

### Technical details:

The Origin server returns null in its response header to any domain different from https://bcwallet.io. In combination with the access-control-allow-credentials: true header, it provides an attacker with an opportunity for the cross-domain reading of a user's sensitive data.

**Request**

Raw	Params	Headers	Hex
GET /v1/api/transactions/history/?offset=0&limit=5 HTTP/1.1			
Host: api.bcwallet.io			
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0			
Accept: application/json			
Accept-Language: en-US,en;q=0.5			
Accept-Encoding: gzip, deflate			
Referer: https://bcwallet.io/history			
content-type: application/json			
authorization: Bearer e7800999-93a4-4da1-b72d-e3576adc6a34			
origin: null			
Connection: close			

**Response**

Raw	Headers	Hex
HTTP/1.1 200 OK		
Server: nginx		
Date: Tue, 13 Feb 2018 13:24:12 GMT		
Content-Type: application/json; charset=utf-8		
Content-Length: 804		
Connection: close		
cache-control: max-age=0, private, must-revalidate		
x-request-id: o8ologfdo2cvjcdfiv507on811769bsn		
vary: Origin		
access-control-allow-origin: null		
access-control-expose-headers:		
access-control-allow-credentials: true		
Application-Name: secrets		
{ "transactions": [{"date": "2018.02.13", "type": "output", "state": "done", "receiver_address": "muXSpwRJ392vC3z5zri46VdCjKTR1hGBJa", "currency": "tBTC", "comment": "{\\\"asd\\\"": true}", "amount": 0.01}, {"date": "2018.02.12", "type": "output", "state": "done", "receiver_address": "muXSpwRJ392vC3z5zri46VdCjKTR1hGBJa", "currency": "tBTC", "comment": "", "amount": 0.1}, {"date": "2018.02.12", "type": "output", "state": "done", "receiver_address": "muXSpwRJ392vC3z5zri46VdCjKTR1hGBJa", "currency": "tBTC", "comment": "", "amount": 0.2}, {"date": "2018.02.09", "type": "output", "state": "done", "receiver_address": "muXSpwRJ392vC3z5zri46VdCjKTR1hGBJa", "currency": "tBTC", "comment": "123", "amount": 1.0e-8}, {"date": "2018.02.08", "type": "input", "state": "done", "receiver_address": "mweiNpJsQ4dKUnwEfqTN4stAf6cr7he2d", "currency": "tBTC", "comment": "", "amount": 1.0}]} }		

Fig 2. Getting user data with Origin equal to null

In this case, such behavior is not considered a vulnerability since Authorization is used to authorize a user (not Cookie).

## OTP re-use

### *Recommendations:*

- Configure a whitelist of domains that are allowed to communicate with the target domain and to check entries of the values of the Origin headers into the list.
- Remove the following headers from the response: access-control-allow-credentials and access-control-expose-headers.

### *Description:*

By getting the OTP, an attacker can use it again and perform critical actions on behalf of a victim.

### *Impact:*

The application allows using the OTP (one-time password) repeatedly for different or same actions.

### *Vulnerable resource:*

- bcwallet.io

### *Technical details:*

With any type of the 2FA (via telegram or google authentication) the being used, code is valid for numerous actions.

### *Recommendations:*

- The OTP should be assigned for a particular action and valid for this action only.

## Conclusion

---

As the result of the security audit, the experts discovered a vulnerability that might enable an attacker to compromise a user's account. In addition, there were other security weaknesses detected. It is recommended to fix these security issues to enhance the current security level of the System.

The current security level of the System was rated "High".

## License

---

This document is the subject to Copyright 2018 Cyber3 under the Creative Commons Attribution NonCommercial NoDerivs (CC-NC-ND) license. You may share and repost the PDF without modification on other sites as long as you put a clear reference link to [github.com](https://github.com)

# Appendix 1. Security assessment

## Security level analysis

To analyze the security level of the System, it is necessary to measure the severity and likelihood of exploitation of the detected vulnerabilities. The likelihood of exploitation is measured, according to the ease of vulnerability exploitation and the accessibility of a vulnerability.

## Vulnerability severity

The “Severity” property of a vulnerability describes possible results of this vulnerability exploitation, regarding confidentiality, integrity, and availability of information processed on a vulnerable resource. Severity levels are described in the Table A-1.

Level	Confidentiality violation	Integrity violation	Availability violation
None	Does not happen	Does not happen	Does not happen
Low	Obtaining access to noncritical information by an attacker through privilege escalation	Integrity violation of noncritical information by an attacker with basic user rights in the System	Short-time denial-of-service of a mission-critical application
Average	Confidentiality violation of sensitive data by an attacker with basic user rights in the System	Integrity violation of sensitive data by an attacker with basic user rights in the System	Denial of service of a mission-critical application or a short-time denial of service of the System
High	Confidentiality violation of critical information by an attacker with administrator rights in the System	Integrity violation of critical information by an attacker with administrator rights in the System	Denial of Service of the System

Table A-1. Vulnerability severity levels

## Ease of vulnerability exploitation

The “Ease of exploitation” property of a vulnerability defines what hardware and software, time and computing resources, and professional skills are required to exploit a vulnerability (Table A-2).

Level	Description
Low	Vulnerability exploitation requires high computing powers, significant time resources, developing new software, configuration analysis of the System, determination and testing possible ways and conditions of successful exploitation of this vulnerability.
Average	Vulnerability exploitation requires high-performance computing, extensive time resources, special hardware and software, and analysis of a violated system configuration. An attacker does not have to have deep knowledge of the system or professional skills to perform an attack.
High	Vulnerability exploitation does not require the use of any special hardware or software, high-performance computing, time resources or any professional skills to perform an attack.

Table A-2. Ease of vulnerability exploitation levels

## Vulnerability accessibility

The “Accessibility” property of a vulnerability defines what user classes have access to a vulnerable resource (Table A-3).

Level	Description
Low	Privileged users
Average	Registered users
High	All users

Table A-3. Accessibility levels



## Likelihood of exploitation

The likelihood of exploitation is calculated according to “ease of exploitation” and “accessibility” levels (Table A-4).

Likelihood of exploitation		Ease of exploitation ↓		
		Low	Average	High
Accessibility →	Low	Low	Low	Average
	Average	Low	Average	High
	High	Average	High	High

Table A-4. Likelihood of exploitation levels

## Vulnerability impact

Vulnerability impact (for one of the existing threats) is measured, according to vulnerability severity (for one of the existing threats) and the likelihood of exploitation of a vulnerability (Table A-5).

Vulnerability impact		Likelihood of exploitation ↓		
		Low	Average	High
Vulnerability severity →	Low	Low	Low	Average
	Average	Low	Average	High
	High	Average	High	High

Table A-5. Impact levels

## Appendix 2. Security level analysis.

### List of the discovered vulnerabilities and security weaknesses

The vulnerabilities and security weaknesses discovered in the System during the security audit are listed in Table B-1.

Discovered vulnerabilities		
Vulnerability	Overall impact	See
Insufficient entropy bits in a token	Average	<a href="#">p.6</a>
Incorrect session management	Low	<a href="#">p.7</a>
Discovered security weaknesses		
Security weakness	See paragraph	
No HSTS mechanism	<a href="#">p.7</a>	
No protection from clickjacking attacks	<a href="#">p.8</a>	

Table B-1. List of discovered vulnerabilities and security weaknesses



CYBER3

