XSS

XSS là gì?

- Cross Site Scripting (XSS) là một trong những tấn công phổ biến và dễ bị tấn công nhất mà tất cả các Tester có kinh nghiệm đều biết đến. Nó được coi là một trong những tấn công nguy hiểm nhất đối với các ứng dụng web và có thể mang lại những hậu quả nghiêm trọng. Giới thiệu về tấn công XSS Tấn công XSS là một đoạn mã độc, để khái thác một lỗ hổng XSS, hacker sẽ chèn mã độc thông qua các đoạn script để thực thi chúng ở phía Client. Thông thường, các cuộc tấn công XSS được sử dụng để vượt qua truy cập và mạo danh người dùng.
- Mục đích chính của cuộc tấn công này là ăn cắp dữ liệu nhận dạng của người dùng như: cookies, session tokens và các thông tin khác. Trong hầu hết các trường hợp, cuộc tấn công này đang được sử dụng để ăn cắp cookie của người khác. Như chúng ta biết, cookie giúp chúng tôi đăng nhập tự động. Do đó với cookie bị đánh cắp, chúng tôi có thể đăng nhập bằng các thông tin nhận dạng khác. Và đây là một trong những lý do, tại sao cuộc tấn công này được coi là một trong những cuộc tấn công nguy hiểm nhất.
- Tấn công XSS đang được thực hiện ở phía client. Nó có thể được thực hiện với các ngôn ngữ lập trình phía client khác nhau. Tuy nhiên, thường xuyên nhất cuộc tấn công này được thực hiện với Javascript và HTML.

Tấn công XSS thực hiện như thế nào?

Tấn công Cross Site Scripting nghĩa là gửi và chèn lệnh và script độc hại, những mã độc này thường được viết với ngôn ngữ lập trình phía client như Javascript, HTML, VBScript, Flash… Tuy nhiên, cách tấn công này thông thường sử dụng Javascript và HTML. Cách tấn công này có thể được thực hiện theo nhiều cách khác nhau, phụ thuộc vào loại tấn công XSS, những mã độc có thể được phản chiếu trên trình duyệt của nạn nhân hoặc được lưu trữ trong cơ sở dữ liệu và được chạy mỗi khi người dùng gọi chức năng thích hợp. Nguyên nhân chính của loại tấn công này là xác thực đầu vào dữ liệu người dùng không phù hợp, dữ liệu độc hại từ đầu vào có thể xâm nhập vào dữ liệu đầu ra. Mã độc có thể nhập một script và được chèn vào mã nguồn của website. Khi đó trình duyệt không thể biết mã thực thi có phải độc hại hay không. Do đó mã độc hại có thể đang được thực thi trên trình duyệt của nạn nhân hoặc bất kỳ hình thức giả nào đang được hiển thị cho người sử dụng. Có một số hình thức tấn công XSS có thể xảy ra. Bên dưới là những hình thức tấn công chính của Cross Site Scripting:

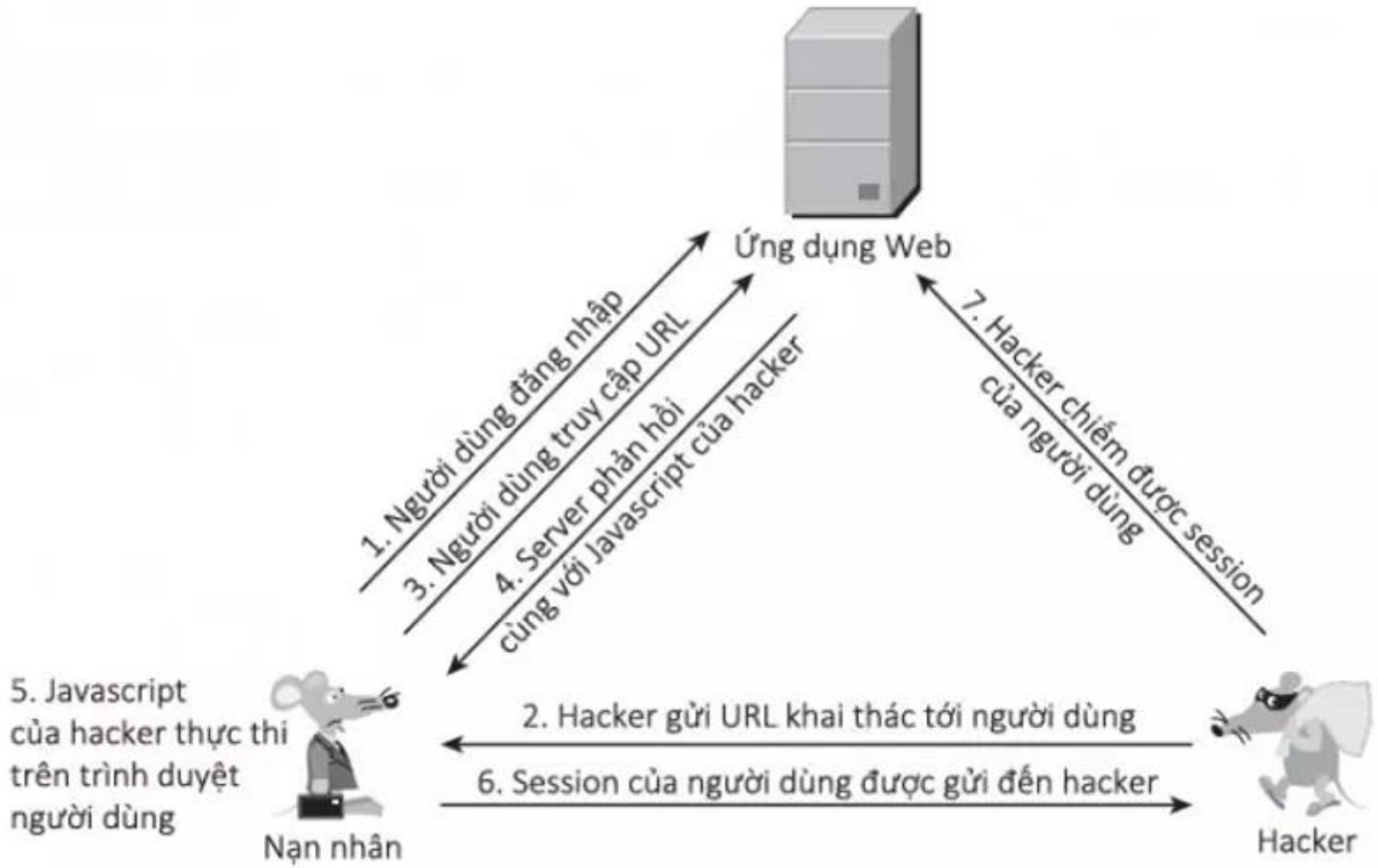
- Cross Site Scripting có thể xảy ra trên tập lệnh độc hại được thực hiện ở phía client.
- Trang web hoặc form giả mạo được hiển thị cho người dùng (nơi nạn nhân nhập thông tin đăng nhập hoặc nhấp vào liên kết độc hại).
- Trên các trang web có quảng cáo được hiển thị.
- Email độc hại được gửi đến nạn nhân. Tấn công xảy ra khi tin tặc tìm kiếm những lỗ hổng trên website và gửi nó làm đầu vào độc hại. Tập lệnh độc hại được tiêm vào mã lệnh và sau đó được gửi dưới dạng đầu ra cho người dùng cuối cùng.

Các loại tấn công XSS

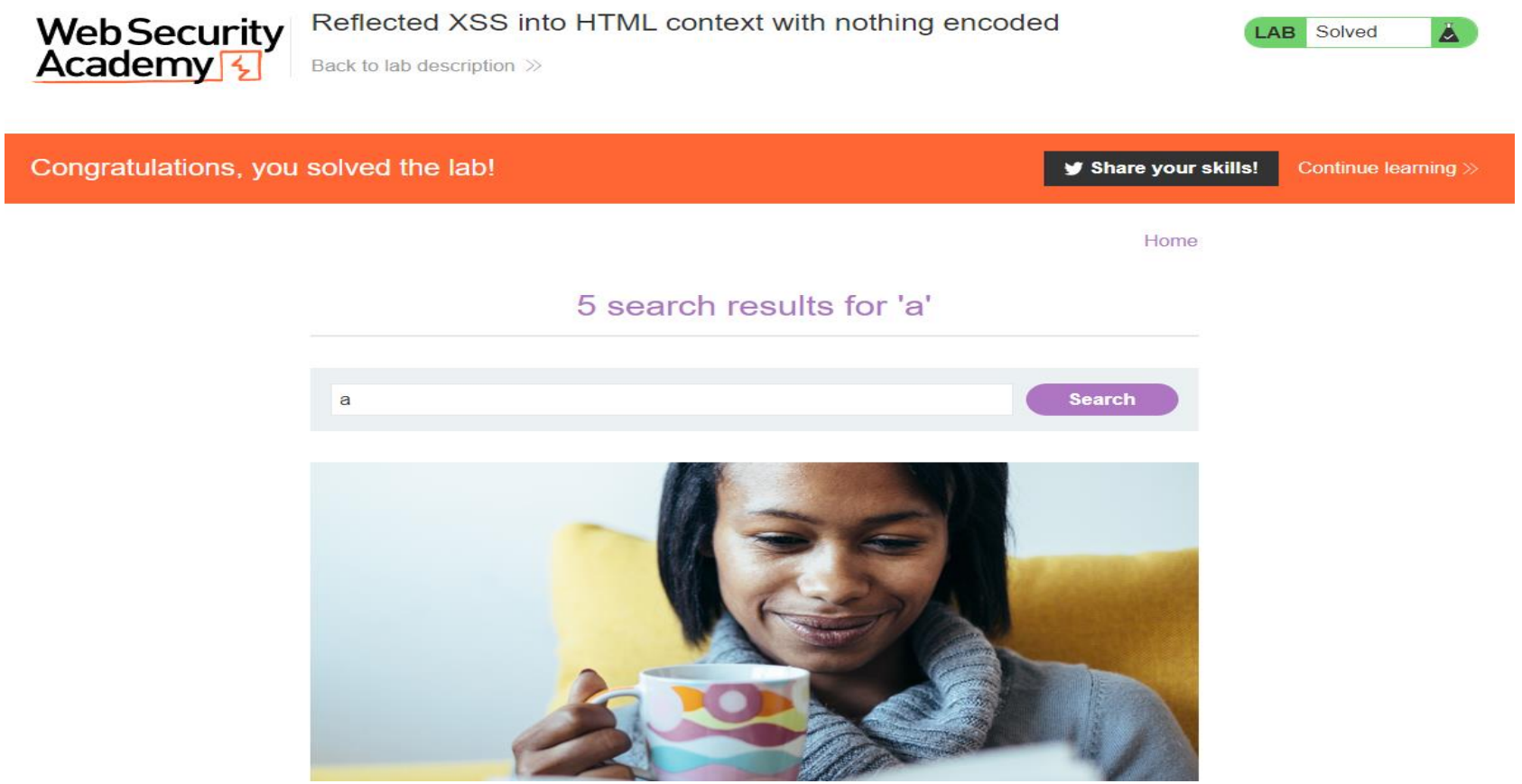
- Có 3 loại tấn công XSS chính như sau:

1. Reflected 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. Chi tiết được mô tả qua những bước sau:


Ứng dụng Web
1. Người dùng đăng nhập
3. Người dùng truy cập URL
4. Server phản hồi cùng với Javascript của hacker
7. Hacker chiếm được session của người dùng
5. Javascript của hacker thực thi trên trình duyệt người dùng
2. Hacker gửi URL khai thác tới người dùng
6. Session của người dùng được gửi đến hacker
Nạn nhân
Hacker

EX: Ta có thể thấy lỗi Reflected XSS trong chức năng tìm kiếm của website này. Khi tìm kiếm dữ liệu, website trả về dữ liệu mà mình nhập vào. Từ đó ta có thể sử dụng lỗi reflected xss để tấn công trang web này bằng lệnh: <script>alert(1)</script>



Web Security Academy

Reflected XSS into HTML context with nothing encoded

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home

5 search results for 'a'

<script>alert(1)</script> Search

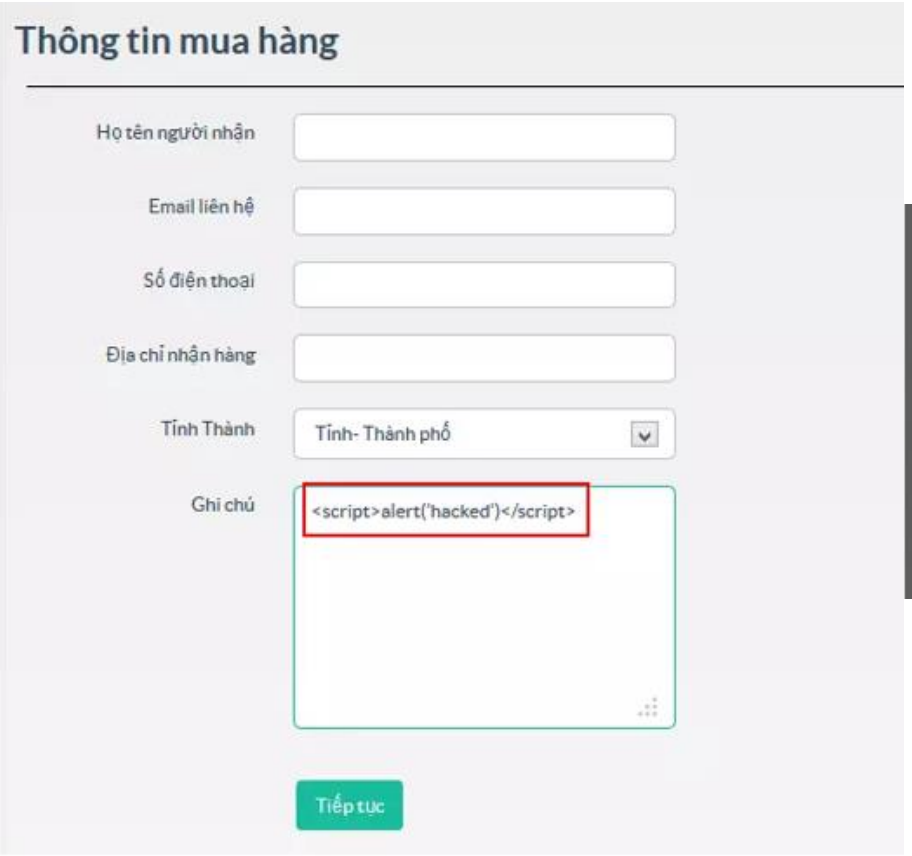
...91888079503002800b8.web-security-academy.net cho biết

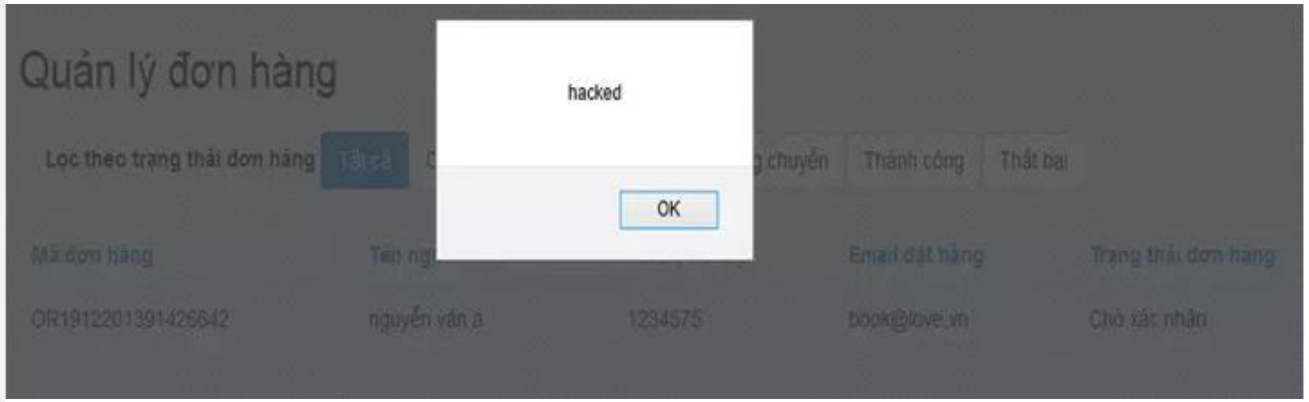
1

OK

2. Stored XSS:

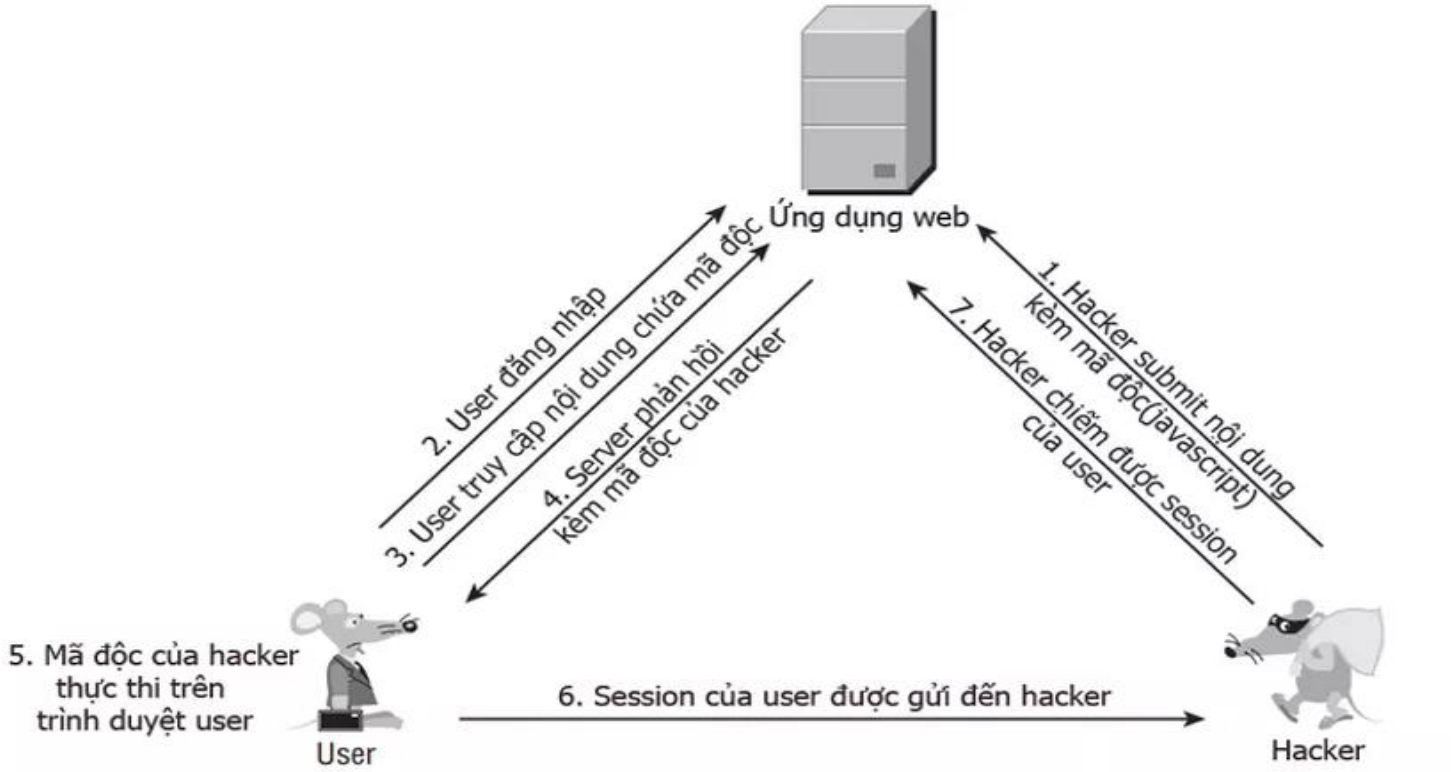
- Khác với Reflected tấn công trực tiếp vào một số nạn nhân mà hacker nhắm đến, Stored XSS hướng đến nhiều nạn nhân hơn. Lỗi này xảy ra khi ứng dụng web không kiểm tra kỹ các dữ liệu đầu vào trước khi lưu vào cơ sở dữ liệu (ở đây tôi dùng khái niệm này để chỉ database, file hay những khu vực khác nhằm 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.

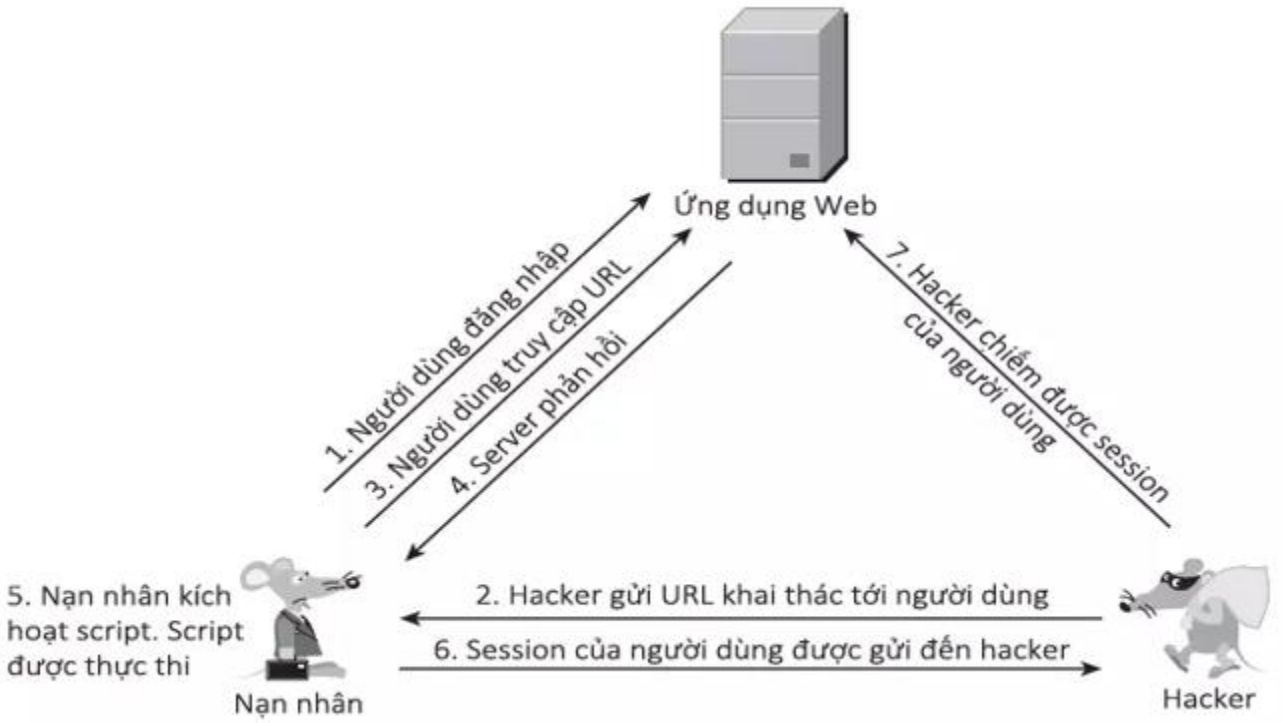
Kịch bản khai thác:



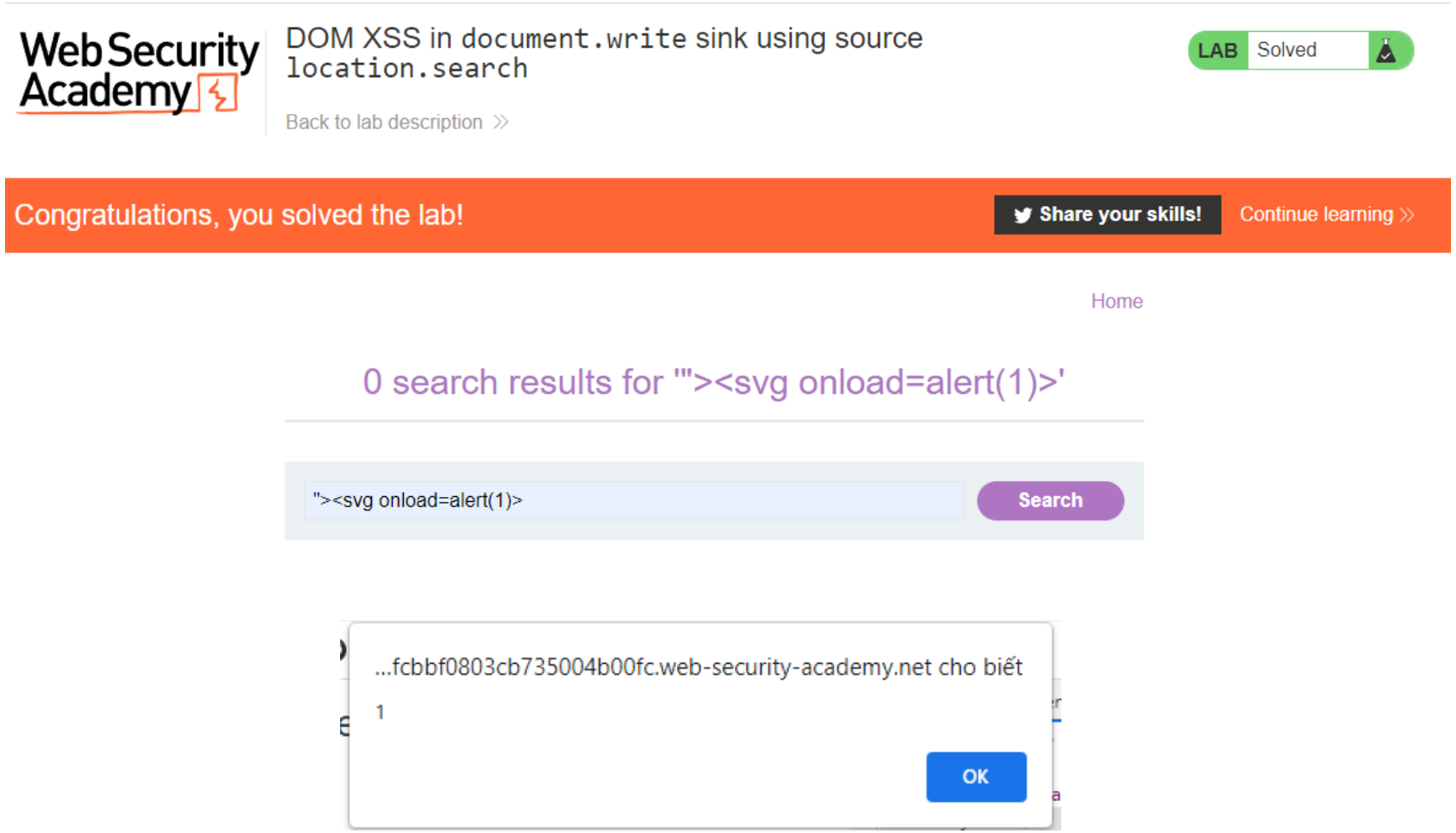
- Reflected XSS và Stored XSS có 2 sự khác biệt lớn trong quá trình tấn công.
- Thứ nhất, để khai thác Reflected XSS, hacker phải lừa được nạn nhân truy cập vào URL của mình. Còn Stored XSS không cần phải thực hiện việc này, sau khi chèn được mã nguy hiểm vào CSDL của ứng dụng, hacker chỉ việc ngồi chờ nạn nhân tự động truy cập vào. Với nạn nhân, việc này là hoàn toàn bình thường vì họ không hề hay biết dữ liệu mình truy cập đã bị nhiễm độc.
- Thứ hai, mục tiêu của hacker sẽ dễ dàng đạt được hơn nếu tại thời điểm tấn công nạn nhân vẫn trong phiên làm việc(session) của ứng dụng web. Với Reflected XSS, hacker có thể thuyết phục hay lừa nạn nhân đăng nhập rồi truy cập đến URL mà hắn ta cung cấp để thực thi mã độc. Nhưng Stored XSS thì khác, vì mã độc đã được lưu trong CSDL Web nên bất cứ khi nào người dùng truy cập các chức năng liên quan thì mã độc sẽ được thực thi, và nhiều khả năng là những chức năng này yêu cầu phải xác thực(đăng nhập) trước nên hiển nhiên trong thời gian này người dùng vẫn đang trong phiên làm việc.
- Từ những điều này có thể thấy Stored XSS nguy hiểm hơn Reflected XSS rất nhiều, đối tượng bị ảnh hưởng có thể là tất cả nhưng người sử dụng ứng dụng web đó. Và nếu nạn nhân có vai trò quản trị thì còn có nguy cơ bị chiếm quyền điều khiển web.

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.



- Trong ví dụ dưới đây ta có thể sử dụng DOM Based XSS để thay đổi cấu trúc của câu lệnh tìm kiếm: "><svg onload=alert(1)>



Cách ngăn chặn tấn công XSS

Kiểu tấn công này là một trong những kiểu tấn công có nhiều nguy hiểm và rủi ro nhất. Tuy nhiên, vẫn có rất nhiều cách để ngăn chặn tấn công này. Phương pháp ngăn chặn tấn công XSS bao gồm:

- Data validation.
- Filtering.
- Escaping.

- Bước đầu tiên trong việc ngăn chặn cuộc tấn công này là **Input validation** (Xác thực đầu vào). Mọi thứ do người dùng nhập phải được xác thực chính xác vì thông tin input của người dùng có thể tìm đường đến output. Data validation (Xác thực dữ liệu) có thể được đặt tên là cơ sở để đảm bảo tính bảo mật của hệ thống.

- Một phương pháp ngăn chặn tốt hơn là lọc input filtering (thông tin đầu vào) của người dùng. Ý tưởng của bộ lọc là tìm kiếm các từ khóa gây rủi ro trong thông tin input của người dùng và xóa chúng hoặc thay thế chúng bằng các chuỗi trống. Những từ khóa đó có thể là:

- <script></script> tags.
- Javascript commands.
- HTML markup.

- Còn một phương pháp ngăn chặn có thể thực hiện là phương pháp **characters escaping**. Trong phương pháp này, các ký tự thích hợp đang được thay đổi bằng các code đặc biệt. Ví dụ: Ký tự escaping có thể trông giống như &#60.