Các cách hack website phổ biến

1. SQL Injection: SQL injection là một kỹ thuật cho phép những kẻ tấn công lợi dụng lỗ hổng của việc kiểm tra dữ liệu đầu vào trong các ứng dụng web và các thông báo lỗi của hệ quản trị cơ sở dữ liệu trả về để inject (tiêm vào) và thi hành các câu lệnh SQL bất hợp pháp, Sql injection có thể cho phép những kẻ tấn công thực hiện các thao tác, delete, insert, update,… trên cơ sỡ dữ liệu của ứng dụng, thậm chí là server mà ứng dụng đó đang chạy, lỗi này thường xãy ra trên các ứng dụng web có dữ liệu được quản lý bằng các hệ quản trị cơ sở dữ liệu như SQL Server, MySQL, Oracle, DB2, Sysbase. Cách này được xem là phổ biến nhất vì hầu hết website trên internet đều sử dụng cơ sở dữ liệu động. Ngay cả Facebook cũng từng vài lần bị tấn công bởi lỗi này.

2. Cross-site scripting (XSS): Là một kỹ thuật cho phép kẻ tấn công nhúng mã khai thác vào website. Không thể phủ nhận phương pháp này không gây ra hậu quả nghiêm trọng. Với những website mang tính cộng tính cộng đồng thì ảnh hưởng của nó là không hề nhỏ. Lỗi này đặc biệt phổ biến.

3. Ddos hay còn gọi là Tấn công từ chối dịch vụ: là một nỗ lực làm cho những người dùng không thể sử dụng tài nguyên của một máy tính. Mặc dù phương tiện để tiến hành, động cơ, mục tiêu của tấn công từ chối dịch vụ có thể khác nhau, nhưng nói chung nó gồm có sự phối hợp, sự cố gắng ác ý của một người hay nhiều người để một trang, hay hệ thống mạng không thể sử dụng, làm gián đoạn, hoặc làm cho hệ thống đó chậm đi một cách đáng kể với người dùng bình thường, bằng cách làm quá tải tài nguyên của hệ thống.

4. Cross-site Request Forgery (CSRF): là kỹ thuật tấn công bằng cách sử dụng quyền chứng thực của người dùng đối với một website. CSRF là kỹ thuật tấn công vào người dùng, dựa vào đó hacker có thể thực thi những thao tác phải yêu cầu sự chứng thực.

5. Server-Side Includes (SSI) Injection: Là kỹ thuật khai thác dựa trên lỗ hổng cho phép truyền lệnh thực thi từ phía client đến Webserver. Lỗi này không quá phổ biến nhưng cũng mang tầm quan trọng không kém.

6. Remote File Inclusion (RFI): Kỹ thuật khai thác khá phổ biến. Nó cho phép kẻ tấn công đính một tập tin từ xa. Thông thường là những tập tin thực thi, hoặc webcode. Tùy vào việc xử lý của người lập trình website mà lỗi này mang mức độ nguy hiểm khá cao.

7. Local File Inclusion (LFI): Cũng giống như RFI, chỉ khác ở điểm là LFI chỉ có thể đính file có trong nội tại máy chủ chứa website.

8. Remote Command Execution: Cho phép thực thi một lệnh được truyền từ tham vấn bên ngoài. Lỗi này thường gây ra lỗ hổng lớn trong các hệ thống website.

\* Đây chỉ là những khái niệm mà mình tìm kiếm trên mang và dựa vào kinh nghiệm cá nhân. Nó không phải là tài liệu đúng nhất hay chung nhất. Ngoài ra cách hack website còn rất nhiều. Bạn có thể tham khảo tại website<https://www.owasp.org/index.php/Category:Attack> đễ tìm hiểu thêm.