1) SQl Injection là gì:

- Sql Inject là một trong những kiểu hack web đang dần trở nên phổ biến hiện nay. Bằng cách inject các mã SQL query/command vào input trước khi chuyển cho ứng dụng web xử lý, bạn có thể login mà không cần username và password, remote execution, dump data và lấy root của sql server. Công cụ dùng để tấn công trình duyệt webbất kì, chẳng hạn như internet explorer, nertscape,lynx,...

- Ngăn chặn SQL Inject:

+ Loại bỏ các ký tự meta như ' " / \ ; và các ký tự extend như null,cr,lf,... trong các string nhận được từ:

. input do người dùng đệ trình

. các tham số từ url

. các giá trị từ cookie

+ đối với các giá trị numeric, hẫy chuyển nó sang integer trước khi query SQL, hoặc dùng ISNUMERIC để chắc chắn nó là một số integer.

+ thay đổi "Startup and run SQL Server" dùng mức low privilege user trong tab SQL Server Security.

+ Xóa các stored procedure trong database master mà không dùng.

2) DoS và DDoS.

- DoS là gì: là cuộc tấn công nhằm làm sập một máy chủ hoặc mạng, khiến người dùng khai thác không thể truy cập vào máy chủ, mạng đó.

- DDoS là gì: là nỗ lực làm sập một dịch vụ trực tuyến bằng cách làm tràn ngập nó với traffic từ nhiều nguồn.

có 3 loại tấn công cơ bản:

+ Volume-based: Sử dụng lưu lượng truy cập cao để làm tràn ngập băng thông mạng

+ Protocol: Tập trung vào việc khai thác các tài nguyên máy chủ.

+ Application: Tập trung vào các ứng dụng web và được xem là loại tấn công tinh vi và nghiêm trọng nhất.

- Cách phòng chống:

+ cài đặt và duy trì phần mềm chống virus.

+ Cài đặt tường lửa và cấu hình nó để giới hạn lưu lượng đến và đi từ máy tính của bạn.

+ Làm theo hướng dẫn thực hành an toàn về phân phối địa chỉ email của bạn.

+ dùng các bộ lọc email để giúp bạn quản lý lưu lượng không mong muốn.

3) Brute Force.

- Brute Force là một loại tấn công mạng, trong đó bạn có một phần mềm, xoay vòng các ký tự khác nhau, kết hợp để tạo ra một mật khẩu đúng. Phầm mềm Brute Force Attack password cracker đơn giản sẽ sử dụng tất cả các kết hợp có thể để tìm ra mật khẩu cho máy tính hoặc máy chủ mạng. Nó rất đơn giản và không sử dụng bất kỳ kỹ thuật thông minh nào.

- Cách phòng chống:

+ Mật khẩu có ít nhất một chữ hoa

+ Có ít nhất một chữ số

+ Có ít nhất một ký tự đặc biệt

+ Mật khẩu phải có tối thiểu 8-10 ký tự.

+ Bao gồm ký tự ASCII, nếu bạn muốn.

4) Cross-site (XSS)

- XSS là một kiểu tấn công bảo mật trong đó kẻ tấn công đưa các tập lệnh độc hại và phần nội dung của các trang web đáng tin cậy khác. Tấn công Cross-site scripting xảy ra kho một nguồn không đán tin cậy được phép đưa code của chính nó vào một ứng dụng web và mã độc đó được bao gồm trong nội dung gửi đến trình duyệt của nạn nhân.

- Có 3 loại lỗ hổng Cross-site scripting: Stored XSS, Reflected XSS và DOM-based XSS.

+ Stored XSS là loại tấ công cross-site scripting gây thiệt hại nhiều nhất.Kẻ tấn công truyền một tập lệnh còn được gọi là payload - được lưu trữ vĩnh viễn trên ứng dụng đích, chẳng hạn như csdl.

+ Reflected XSS là loại lỗ hổng cross-site scripting phổ biến nhất. Trong kiểu tấn công này, kẻ tấn công phải chuyền payload cho nạn nhân. Do đó, tập lệnh payload của kẻ tấn công phải là một phần của yêu cầu được gửi đến máy chủ web và được phản chiếu lại để phản hồi HTTP, bao gồm payload từ yêu cầu HTTP.

+ DOM-based cross-site scripting là loại tấn công XSS nâng cao, có thể thực hiện được khi tập lệnh phía máy khách của ứng dụng web ghi dữ liệu do nguồi dùng cung cấp vào Document Object Model (DOM).

- Phương pháp ngăn chặn:

+ Escape đầu vào của người dùng là một cách để ngăn các lỗi hổng XSS xuất hiện trong các ứng dụng.(Escape là chuyển đổi các kí tự đơn thành chuỗi.)

+ Sàng lọc đầu vào của người dùng là một cách khác để ngăn chặn các cuộc tấn công Cross-site scripting, đặc biệt hữu ích trên trang web cho phép HTML markup.

+ Xác thực đầu vào đảm bảo việc ứng dụng hiển thị dữ liệu chính xác và ngăn dữ liệu độc hại cho trang web, cơ sở dữ và người dùng.

5)CSRF (Cross Site Request Forgery)

-CSRF là gì: 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 và đó hacker có thể thực thi những thao tác phải yêu cầu sự chứng thực. Hiểu một cách nôm na, đây là kỹ thuật tấn công dựa vào mượn quền trái phép. (CSRF còn được gọi là "session riding","XSRF"

-Cách phòng chống:

+ Dựa trên nguyên tắc của CSRF "lừa trình duyệt của người dùng (hoặc người dùng) gửi các câu lệnh HTTP", các kĩ thuật phòng tránh sẽ tập trung và việc tìm cách phân việt và hạn chế câu lệnh giả mạo.

+ Phía user:. nên thoát khỏi các website quan trọng: Tài khoản ngân hàng, thanh toán trực tuyến, các mạng xã hội,gmail,yahoo... khi đã thực hiện xong giao dịch hay các công việc cần làm. không nên click vào các đường dẫn, phía dưới bên trái của trình duyệt thường có địa chỉ website đích, bạn nên lưu ý đẻ đến đúng trang mình muốn.

. Không lưu các thông tin về mật khẩu tại trình duyệt của mình(không nên chọn các phương thức "đăng nhập lần sau", "lưu mật khẩu"...).

. Trong quá trình thực hiện giao dịch hay vào các website quan trọng không nên vào các website khác, có thể chứa các mã khai thác của kẻ tấn công.

+ Phía server: Có lời khuyến các được đưa ra, tuy nhiên cho đến nay vẫn chưa có biện pháp nào có thể phòng chống triệt để CSRF.

. Lựa chọn việc sử dụng GET và POST theo chuẩn RESTful.

. sử dụng captcha, các thông báo xác nhận

. sử dụng token

. sử dụng cookie riêng biệt cho trang quản trị

. kiểm tra REFERRER

. kiểm tra IP