Chac cu qua mon - ATTT

An toàn thông tin (Trường Đại học Sư phạm Kỹ Thuật Thành phố Hồ Chí Minh)

KIỂM TRA LÝ THUYẾT PHẦN TỰ LUẬN (70%)

Môn: An toàn thông tin

1. *(3 điểm)* **Trình bày giải pháp để đảm bảo an toàn cho ứng dụng Web?**

Lỗ hổng (vulnerability) được hiểu là những điểm yếu có thể bị khai thác bởi các tác nhân xấu để thực hiện các hành động không cho phép (unauthorized actions) trong: Police, Design, Implementation, Operation.

Các lỗ hổng có thể cho phép kẻ tấn công chạy mã, truy cập bộ nhớ của hệ thống, cài đặt phần mềm độc hại và đánh cắp, phá hủy hoặc sửa đổi những dữ liệu nhạy cảm.

Ứng dụng web nào cũng có điểm yếu, nên ứng dụng web nào cũng có thể bị tấn công. Trước hết, các lỗ hổng phần mềm được xác định bởi 3 yếu tố:

+ Existence: tồn tại lỗ hổng.
+ Access: khả năng kết nối của kẻ tấn công đến lỗ hổng.
+ Exploit: khả năng khai thác lỗ hổng thông qua các công cụ hoặc kỹ thuật nhất định nào đó.

Để có thể tìm được giải pháp phù hợp đảm bảo an toàn cho ứng dụng Web, đầu tiên, ta cần tiến hành phân tích các nguyên nhân gây ra lỗ hổng:

+ Độ phức tạp: Các hệ thống phức tạp làm tăng xác suất của lỗ hổng, sai sót trong cấu hình hoặc truy cập ngoài ý muốn. Nó đồng nghĩa với việc hệ thống càng phức tạp thì lỗ hổng càng nhiều.
+ Tính phổ biến: Các loại mã, phần mềm, hệ điều hành và phần cứng có tính phổ biến (Microsoft, Windows,…) sẽ làm tăng khả năng kẻ tấn công có thể khai thác và tìm thấy hoặc có thông tin về các lỗ hổng đã biết.
+ Mức độ kết nối: Thiết bị càng được kết nối nhiều thì khả năng xuất hiện lỗ hổng càng cao vì hầu hêý những lỗ hổng này xuất hiện trong quá trình kết nổi.
+ Quản lý bảo mật kém: Những mật khẩu yếu có thể bị phá bằng tấn công brute-force và việc sử dụng lại mật khẩu có thể biến một vi phạm dữ liệu trở thành nhiều vụ vi phạm xảy ra.
+ Lỗi hệ điều hành: Giống như bất kỳ phần mềm nào khác, hệ điều hành cũng có thể có lỗ hổng. Các hệ điều hành không an toàn – chạy mặc định và để tất cả mọi người dùng có quyền truy cập đầy đủ sẽ có thể cho phép virus và phần mềm độc hại thực thi các lệnh.
+ Sử dụng Internet: Internet có rất nhiều loại phần mềm gián điệp và phần mềm quảng cáo có thể được cài đặt tự động trên máy tính. Những loại phần mềm này có thể tồn tại mã độc hoặc virus,… tấn công độc hại đến người dùng.

+ Lỗi phần mềm: Lập trình viên có thể vô tình hoặc cố ý để lại một lỗi có thể khai thác trong phần mềm. Do đó lỗi phần mềm sẽ luôn có và có thể khai thác.

+ Đầu vào của người dùng không được kiểm tra: Nếu trang web hoặc phần mềm cho rằng tất cả đầu vào đều an toàn, chúng có thể thực thi các lệnh SQL ngoài ý muốn.

+ Con người: Lỗ hổng lớn nhất trong bất kỳ tổ chức nào là con người đằng sau hệ thống đó (do con người giám sát, thiết kế, thực thi và vận hành). Tấn công phi kỹ thuật (social engineering) là mối đe dọa lớn nhất đối với đa số các tổ chức.

Với những nguy cơ đó, hệ thống không thể đảm bảo an toàn tuyệt đối, do đó ta cần cố gắng đảm bảo mỗi khâu an toàn nhất có thể để đảm bảo liên hệ giữa các lớp.

Dựa vào nguyên nhân gây ra lỗ hổng mà có các giải pháp phù hợp:

+ Hệ thống phức tạp, khó quản lí, kiểm soát: Phân chia hệ thống thành các phần chuyên biệt để dễ dàng quản lí và cài đặt.

+ Quản lý các thiết bị kết nối, tránh trường hợp nhiều thiết bị kết nối, dễ gây ra lỗ hổng bằng cách đặt giới hạn số thiết bị.

+ Dựa trên các nguyên tắc về quyền tối thiểu: Mỗi chương trình hoặc user chỉ nên được cấp quyền đủ để truy cấp, tránh việc cấp dư quyền.

+ Tăng cường quản lí mật khẩu, sử dụng strong password - mật khẩu có tính bảo mật cao, hạn chế sử dụng một loại mật khẩu cho nhiều tài khoản các nhau. Đồng thời, sử dụng PAM (Privileged Account/Access Management) để quản lý hệ thống server của các admin, tránh trường hợp xảy ra sự cố với admin.

+ Trên ứng dụng, đánh giá sự tồn tại của các lỗ hổng trên hệ thống, qua đó xem xét khả năng hình thành lỗ hổng. Thông qua các điểm yếu nhận định nó có thể được khai thác cho mục đích tấn công hay không.

+ Kiểm soát các lỗ hổng thông qua:
    - Các công cụ quét lỗ hổng bảo mật như Acunetix, Nexpose, Retina,….
    - Đối với Buffer Overflow:
        - Stack Guard: kiểm tra khi có thay đổi giá trị so với ban đầu dẫn đến xảy ra Buffer Overflow thì thông báo đến người dùng.
        - Stack Shield: sao lưu giá trị return address, sau khi thực thi, nếu giá trị Stack Shiled không thay đổi thì không sao, ngược lại thì xảy ra buffer overflow.
        - Random Space: Random địa chỉ lưu.
        - Ngăn không cho thực hiện lệnh trên vùng Memory.

2. *(4 điểm)* **Trình bày các nguyên tắc để đảm bảo an toàn cho dữ liệu?**

Các nguyên tắc để đảm bảo an toàn cho dữ liệu:

+ Một hệ thống phải đảm bảo 3 tính chất (CIA) mới được gọi là bảo mật:
    - Bí mật (Confidentiality): chỉ các thực thể được ủy quyền mới có quyền truy cập vào dữ liệu.
    - Toàn vẹn (Integrity): dữ liệu sẽ không được sửa đổi khi không được cho phép.
    - Sẵn sàng (Availability): các tài nguyên và dữ liệu luôn sẵn sàng để truy cập khi thực tể được cấp quyền.
+ Một hệ thống thường được bảo vệ theo Defense in Depth (bảo vệ theo chiều sâu, bảo vệ theo từng layer). Các cơ chế bảo vệ được phân lớp để đảm bảo dữ liệu và thông tin có giá trị an toàn, và tùy theo quy mô hoạt động, mối quan tâm và nguồn lực mà hệ thống sẽ được bảo vệ như thế nào:
+ Data > Application > Host > LAN > Border Gateway > Physical Security > Human.
+ Khi xây dựng một hệ thống CNTT, thì bảo mật hệ thống phải đạt được mục tiêu: Ngăn chặn (prevention) – Phát hiện (detection) – Phục hồi (recovery).
+ Nguyên tắc đóng gói trong đảm bảo an toàn thông tin: Thường xuyên backup dữ liệu hoặc update phiên bản cho phần mềm.
+ Nguyên tắc cách ly trong đảm bảo an toàn thông tin: Giảm các tấn công bề mặt, tiêu biểu như các cổng kết nối,…
+ Ngăn chặn các mối đe dọa đã biết đến. Ngăn chặn các mối đe dọa chưa được biết đến, có thể kể đến zero-day,... và có thể kiểm tra thông qua sandbox.
+ Ngoài ra, dựa trên nguyên tắc quyền tối thiểu: Mỗi chương trình hoặc user chỉ nên được cấp quyền đủ để truy cập, tránh việc cấp dư quyền.
+ Đồng thời, sử dụng PAM (Privileged Account/Access Management) để quản lý hệ thống server của các admin, tránh trường hợp xảy ra sự cố với admin.
+ Sử dụng các chuẩn an toàn ISO 27001/27002, COBIT, ITIL, RMF, CSA STAR,... để tuân thủ khi xây dựng hệ thống.
+ Đặc biệt, an ninh mạng còn có thể tuân theo các mô hình:
    - CIA (Confidentiality – Integrity – Availability): Bí mật – Toàn vẹn – Sẵn sàng.
    - PPT (People – Process – Technology): Con người – Tiến trình – Công nghệ.
    - AAA (Authentication - Authorization - Accounting): Xác thực - Phân quyền - Ghi nhận.