danh sách 10 lỗi trong ứng dụng mà các hacker có thể sử dụng để tấn công các hệ thống máy chủ

1. Kiểm soát truy nhập bị phá: Những hạn chế xác thực cho các user được phép truy nhập vào trang web không có hiệu lực. Do đó, những kẻ tấn công có thể khai thác những kẽ hở này để truy nhập vào tài khoản của một user khác, xem các file nhạy cảm hay sử dụng các những chức nang không được phép.

2. Quản lý tài khoản bị bẻ: Các mã thông báo và chứng từ về tài khoản không được bảo vệ thoả đáng. Những kẻ tấn công có thể an cắp mật khẩu, khoá các cookies hay những mã thông báo khác để "bẻ gẫy" các yêu cầu xác thực truy nhập vào ứng dụng web và lấy những nhận dạng của người sử dụng khác.

3. Các thông số không được xác nhận: Thông tin từ các yêu cầu của trang web không được xác nhận trước khi được sử dụng bởi một ứng dụng web. Những kẻ tấn công có thể sử dụng những kẻ hở này để tấn công thông qua một ứng dụng web.

4. Các kẽ hở CSS (Cross-Site Scripting): ứng dụng web có thể bị sử dụng như là cơ chế để chuyển một cuộc tấn công đến trình duyệt của một người sử dụng đầu cuối nào đó. Cuộc tấn công đó sẽ làm lộ ra các mã thông báo của người sử dụng đầu cuối đó và lấy đi những thông tin nhạy cảm trong máy.

5. Các lỗi phát lệnh: Những ứng dụng web phải vượt qua các thông số khi chúng tiếp cận với các hệ thống bên ngoài hay một hệ điều hành cục bộ. Nếu cuộc tấn công có thể đưa các lệnh "ác tâm" vào các thông số này, thì hệ thống bên ngoài có thể điều hành những lệnh này thay ứng dụng web đó.

6. Các vấn đề xử lý lỗi: Các lỗi xảy ra trong khi hoạt động bình thường không được xử lý tốt. Nếu một cuộc tấn công có thể gây ra những lỗi, điều này xảy ra tình trạng ứng dụng web không xử lý được, những kẻ tấn công có thể lấy được các thông tin hệ thống chi tiết, từ chối dịch vụ, khiến cho cơ chế bảo mật thất bại hoặc là phá hoại máy chủ.

7. Sử dụng mật mã không an toàn: Các ứng dụng web thường sử dụng các chức nang mật mã để bảo vệ thông tin (ví dụ như các chứng từ uỷ nhiệm). Tuy nhiên, các chức nang và mã này để tích hợp rất khó mã hoá, dẫn đến tình trạng chức nang bảo vệ bị kém đi.

8. Những kẽ hở quản lý từ xa: Nhiều ứng dụng web cho phép những người quản trị hệ thống có thể truy nhập vào web site và sử dụng một giao diện web từ xa. Nếu những chức nang quản trị này không được bảo vệ cẩn thận, một cuộc tấn công có thể truy nhập đến tất cả các CSDL có liên quan của một trang web.

9. Cấu hình máy chủ ứng dụng và web bị lỗi: có một chuẩn cấu hình máy chủ mạnh là thiết yếu đối với một ứng dụng web an toàn. Những máy chủ này có nhiều lựa chọn cấu hình, mà có thể ảnh hưởng đến sự an toàn đối với hệ thống và người truy cập.

10. Tràn bộ nhớ đệm: Các thiết bị ứng dụng web trong một số ngôn ngữ không có hiệu lực đầu vào có thể bị phá huỷ, hay trong một số trường hợp được sử dụng để điều khiển một tiến trình. Những thiết bị này có thể gồm CGI, các driver, thư viện và các thiết bị máy chủ của ứng dụng web.

xem , rút kinh nghiệm , patch và ..biết