AN NINH ỨNG DỤNG

1. Danh sách thành viên

|  |  |  |
| --- | --- | --- |
| Họ và tên | MSV | Công việc |
| Nguyễn Văn Sơn |  |  |
| Phùng Văn Thành |  |  |
| Phạm Thu Trang | 14000859 |  |
| Hoàng Thế Thượng |  |  |

1. Tổng quan về An ninh ứng dụng
2. Xác thực (Authentication)

Xác thực là một quá trình xác định duy nhất một người dùng bằng cách xác minh các chứng chỉ của họ. Xác thực người dùng có thể được yêu cầu khi người dùng cố gắng chạy hoặc cài đặt ứng dụng, hay khi ứng dụng tạo một kết nối với một dịch vụ từ xa hoặc truy cập dữ liệu được tổ chức trên máy local.

* 1. Các kịch bản xác thực Smart Client

Tùy thuộc vào phong cách và tính năng của ứng dụng Smart-Client của bạn, bạn có thể cần xác thực người dùng ở một hoặc nhiều thời điểm trong suốt quá trình tương tác của người dùng với ứng dụng. Có bốn thời điểm mà bạn có thể chọn để xác thực người dùng:

* Khi ứng dụng được cài đặt
* Khi ứng dụng được chạy
* Khi người dùng truy cập vào Dữ liệu nhạy cảm được tổ chức trên máy Local
* Khi người dùng truy cập các dịch vụ mở rộng qua mạng

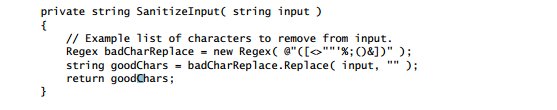
1. Cài đặt

* Nếu ứng dụng của bạn được triển khai ở trung tâm (ví dụ như sử dụng triển khai không cảm ứng), bạn có thể cần phải bảo mật ứng dụng trên máy chủ Web để nó chỉ có thể được cài đặt bởi người dùng có thẩm quyền. Những người dùng này trước tiên phải được chứng thực bởi máy chủ Web, nó sẽ kiểm tra xem họ có quyền truy cập vào ứng dụng và tải nó xuống máy tính của họ.
* Bảo đảm quyền truy cập vào ứng dụng Smart-Client triển khai không cảm ứng tương tự như việc bảo đảm bất kỳ máy chủ Web nào nằm ở vị trí hiện tại, chẳng hạn như một trang Web. Microsoft Internet Information Services (IIS) cung cấp một số cơ chế xác thực, chẳng hạn như Integrated Windows, digest, hoặc basic authentication.

1. Phân quyền (Autorization)
2. Tra soát Dữ liệu (Data Validation)

Các ứng dụng có xác nhận đầu vào kém có thể bị xâm nhập đầu vào nguy hiểm bởi một kẻ tấn công. Xác nhận đầu vào của người dùng là một trong những bước đầu tiên để bảo vệ cho ứng dụng của bạn. Xem xét các nguyên tắc xác thực đầu vào sau đây cho ứng dụng client thông minh của bạn

* 1. Hãy chắc chắn rằng ứng dụng client thông minh của bạn xác thực tất cả đầu vào trước khi xử lý hoặc chuyển nó đến các nguồn tài nguyên
  2. Thực hiện kiểm tra kỹ lưỡng dữ liệu đầu vào của người dùng nếu bạn chuyển nó đến một API không được quản lý. Làm như vậy giúp ngăn chặn tràn bộ đệm. Bạn nên giới hạn dữ liệu nhập vào của người dùng trước khi được chuyển đến các API không được quản lý.
  3. Luôn kiểm tra dữ liệu thu được từ tất cả các nguồn bên ngoài, chẳng hạn như các trang Web và dịch vụ Web.
  4. Không bao giờ dựa vào xác thực phía máy khách của dữ liệu được chuyển đến dịch vụ Web của bạn hoặc ứng dụng Web. Xác thực dữ liệu trên máy khách và sau đó kiểm tra lại nó trên máy chủ để ngăn chặn đầu vào nguy hiểm mà bỏ qua sự xác nhận phía máy khách.
  5. Không bao giờ cho phép người dùng nhập các truy vấn SQL trực tiếp. Luôn cung cấp gói sẵn hoặc truy vấn tham số được xem xét kỹ lưỡng cho các vấn đề về bảo mật. Cho phép người dùng nhập các truy vấn SQL trực tiếp sẽ khiến cho việc câu lệnh truy vấn của SQL sẽ bị tiêm vào dẫn đến nguy cơ sẽ bị đánh cắp dữ liệu.
  6. Ràng buộc và xác thực đầu vào của người dùng cho các giá trị hoặc mẫu được xác định đúng còn tốt hơn là cho các đầu vào không chính xác. Dễ dàng hơn để kiểm tra danh sách hữu hạn các giá trị đã biết để kiểm tra một danh sách với vô số các loại đầu vào độc hại không rõ. Bạn có thể từ chối các đầu vào không hợp lệ hoặc các kí tự tiềm ẩn không an toàn trước khi thao tác trên nó.
  7. Ràng buộc đầu vào bằng cách xác nhận cho nó loại, chiều dài, định dạng và phạm vi. Một cách thông thường để xử lý vấn đề này đó là sử dụng biểu thức chính quy.
  8. Loại bỏ dữ liệu không rõ và sau đó làm sạch đầu vào. Nếu ứng dụng của bạn cần chấp nhận một số đầu vào người dùng ở dạng tự do (ví dụ như nhận xét trong một hộp văn bản), bạn có thể làm sạch đầu vào như thể hiện trong ví dụ sau đây:



* Cuối cùng ta có nhận xét sau: Bạn nên tập trung thường xuyên vào việc xác nhận đầu vào để giảm thiểu việc cố gắng phát triển và hỗ trợ bảo trì trong tương lai.

1. Bảo vệ Dữ liệu nhạy cảm
2. Kiểm soát và ghi nhật ký
3. Xử lý các sự kiện ngoại lệ
4. Quản lý cấu hình và thay đổi
5. Đánh giá
6. Minh họa