### Bảo mật website

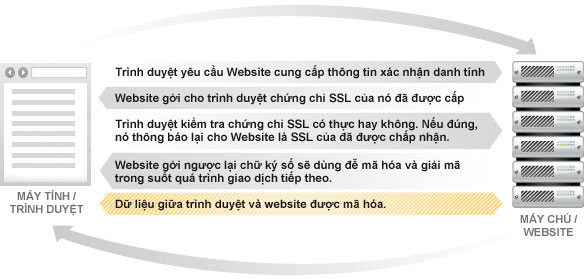
Bảo mật là tiêu chí hàng đầu để thiết kế một website hiện nay. Chúng ta không thể ngăn chặn được tất cả mối đe dọa từ bên ngoài nhưng có thể hạn chế được rất nhiều rủi do bảo mật bằng cách lập trình.

#### Triển khai SSL

SSL là viết tắt của từ Secure Sockets Layer. Đây là một tiêu chuẩn an ninh công nghệ toàn cầu tạo ra một liên kết được mã hóa giữa máy chủ web và trình duyệt. Liên kết này đảm bảo tất cả các dữ liệu trao đổi giữa máy chủ web và trình duyệt luôn được bảo mật và an toàn. [10]

SSL đảm bảo rằng tất cả các dữ liệu được truyền giữa các máy chủ web và các trình duyệt được mang tính riêng tư, tách rời. SSL là một chuẩn công nghiệp được sử dụng bởi hàng triệu trang web trong việc bảo vệ các giao dịch trực tuyến.[10]

Mục đích chính của một chứng chỉ SSL là để mã hóa thông tin sao cho chỉ có thể được đọc và hiểu bởi các bên giao dịch. Thông tin được đệ trình trên các mẫu Internet thường đi qua nhiều máy tính trước khi đến đích cuối cùng, và càng có nhiều “điểm dừng” thì càng có nhiều cơ hội để bên thứ ba có thể truy cập. SSL chèn các ký tự ngẫu nhiên vào các thông tin ban đầu, làm cho không ai có thể hiểu được mà không có mã hóa chính xác. Nếu không có mã hóa, thông tin là vô dụng. [11]



Quy trình máy tính kết nối với một Website đã được chứng thực SSL

Triển khai SSL giúp Website phòng chống được nhiều loại tấn công liên quan đến chặn bắt gói tin, trong đó điển hình là kiểu tấn công Man-in-the-Middle (MITM) và Section Hijacking.

#### Che giấu thông tin Webserver

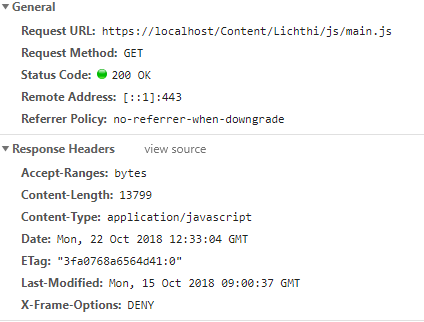
Các thông tin liên quan đến Webserver cũng sẽ được khai thác bởi một kẻ tấn công để tấn công vào hệ thống.

Website sử dụng công nghệ ASP.NET sử dụng Webserver IIS trên Window, khi trình duyệt gửi một request lên server, các thông tin version sẽ đi theo header của response trả về cho trình duyệt như:

X-AspNet-Version hiển thị phiên bản ASP.NET được sử dụng.

X-AspNetMvc-Version hiển thị phiên bản của ASP.NET MVC.

X-Powered-By hiển thị phiên bản framework mà website đang chạy.



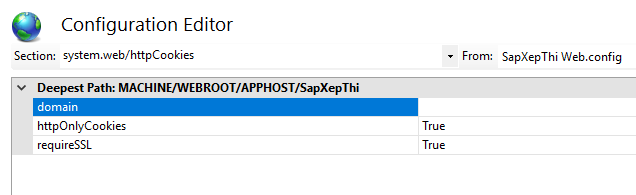
Header gói tin trả về sau khi che thông tin về Webserver

#### Cookie Stealing

Website sử dụng cookies để lưu thông tin user giữa các request (user’s session). Cookies có thể chứa những thông tin không quan trọng như preferences hay history hoặc có thể lưu những thông tin rất quan trọng ví dụ như authentication ticket.

Cùng với sự tiện lợi thì cookies cũng là cơ hội để hacker sử dụng XSS để ăn cắp cookies của user và sau đó sử dụng nó để giả danh user thực hiện các thao tác khác. Bởi vì XSS phụ thuộc vào script để có thể ăn cắp cookies nên một cách hiệu quả để chống mất cắp cookies là không cho phép script access cookies bằng cách sử dụng cờ HttpOnly.

Để ngăn cản script access lên tất cả cookies của site, set config sau trong Web.config.



Cấu hình HTTP Only và requireSSL trên IIS 10

#### ASP.NET Core Identity

ASP.NET Core Identity là một thành phần (built-in) của ASP.NET Core, nó cung cấp các tính năng đầy đủ và đa dạng về xác thực tài khoản.

##### Phòng chống tấn công Bruteforce

Bruteforce hay còn gọi là tấn công vén cạn là cách thức thử tất cả các khả năng có thể có để đoán các thông tin cá nhân đăng nhập: tài khoản, mật khẩu, số thẻ tín dụng… Nhiều hệ thống cho phép sử dụng mật khẩu hoặc thuật toán mã hóa yếu sẽ tạo điều kiện cho tin tặc sử dụng phương pháp tấn công này để đoán tài khoản và mật khẩu đăng nhập. Sau đó sử dụng các thông tin này để đăng nhập truy cập vào tài nguyên hệ thống. [12]

Sử dụng cơ chế Identity của ASP.NET Core và giới hạn số lần đăng nhập không hợp lệ giúp phòng chống cách thức tấn công vén cạn, tài khoản sẽ bị khóa trong một khoảng thời gian nhất định khi đã đạt giới hạn đăng nhập sai.

.

##### Phòng chống SQL Injection

SQL Injection 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 lí, hacker có thể login mà không cần username và password, remote execution, dump data và lấy root của SQL server. [13]

Thông thường để phòng tránh tấn công SQL Injection lập trình viên sẽ phải làm rất nhiều bước như lọc các ký tự có thể làm sai câu truy vấn SQL từ đầu vào input, mã hóa chuối kết nối cơ sở dữ liệu,.. Để phòng tránh tấn công SQL Injection, Website Lichthit36 được lập trình với cơ chế xác thực tài khoản bằng ASP.NET Core Identity kết hợp với các câu truy vấn bằng LINQ thì việc bị tấn công SQL Injection đã được khắc phục hoàn toàn.

##### Phòng chống XSS

Tấn công Cross-site Scripting (XSS) là cách tấn công bằng việc đẩy các đoạn mã javascript vào hệ thống thông qua các trường nhập liệu, kiểu tấn công này là phổ biến nhất và cho phép các hacker có thể lấy cắp thông tin đăng nhập và các dữ liệu có giá trị nhằm khai thác hệ thống. [14]

Mặc định ASP.NET đã ngăn chặn tấn công XSS, dưới đây là lỗi xẩy ra bởi vì MVC đã kiểm tra dữ liệu được nhập vào từ người dùng và nếu người dùng cố gắng thực thi đoạn script sẽ không được phép.

### Kiểm thử bảo mật website

Kiểm thử bảo mật (Security Testing) là một trong những phần quan trọng trong phát triển phần mềm, nhằm đảm bảo các hệ thống và ứng dụng trong một tổ chức không có bất kỳ sơ hở nào có thể gây ra các tổn thất về an toàn bảo mật. [15]

Hiện nay, trên thế giới có những công cụ quét lỗi bảo mật khá nổi tiếng như là: Shadow Security Scanner, Retina Network Security Scanner, Metasploit cao cấp hơn và phải có độ hiểu biết nhất định là Nmap, Netcat ... Trong đó phải kể đến phần mềm Acunetix dùng để quét các lỗi bảo mật hệ thống website. [16]

Acunetix là một công cụ quét lỗi cho ứng dụng Web dựa trên một cơ sở dữ liệu rộng lớn được cập nhật thường xuyên, với các thuật toán heuristic đáp ứng được các cơ chế họat động phức tạp của môi trường Web. Acunetix có thể tự động kiểm tra các lổ hỗng thông dụng như XSS, SQL Injection và các mối nhạy cảm khác của những website có thể truy cập bằng trình duyệt. [16]

Website Lichthit36 lựa chọn phần mềm Acunetix để kiểm tra các lỗ hổng bảo mật hệ thống.

A screenshot of a social media post

Description generated with very high confidence

Quét lỗ hổng bảo mật web trên Acunetix

Kết quả cho thấy phần mềm Acunetix đánh giá mức độ đảm bảo của website là “Safe” nghĩa là ở mức độ an toàn cao. Điều đó cho thấy các lỗ hổng cơ bản mà hacker có thể khai thác điều đã được khắc phục. Qua đó tính tin cậy và an toàn của website được đảm bảo.