

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

KHATTHANAM PHOUCHANTHONG

NGHIÊN CỨU MỘT SỐ GIẢI PHÁP
PHÒNG CHỐNG TẤN CÔNG DỮ LIỆU
ĐỐI VỚI WEBSITE THƯƠNG MẠI ĐIỆN TỬ

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Thái Nguyên – 2020

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

KHATTHANAM PHOUCHANTHAVONG

**NGHIÊN CỨU MỘT SỐ GIẢI PHÁP
PHÒNG CHỐNG TẤN CÔNG DỮ LIỆU
ĐỐI VỚI WEBSITE THƯƠNG MẠI ĐIỆN TỬ**

Chuyên ngành: Khoa học máy tính

Mã số chuyên ngành: 8480101

LUẬN VĂN THẠC SĨ KHOA HỌC MÁY TÍNH

Hướng dẫn khoa học: *TS. Nguyễn Đức Bình*

Thái Nguyên – 2020

LỜI CẢM ƠN

Trước hết tôi xin gửi lời cảm ơn sâu sắc đến thầy hướng dẫn khoa học **TS. Nguyễn Đức Bình** về những chỉ dẫn khoa học, định hướng nghiên cứu và tận tình hướng dẫn tôi trong suốt quá trình làm luận văn.

Tôi xin cảm ơn các thầy trong khoa Công nghệ thông tin, các thầy cô giáo trong trường Đại học Công nghệ thông tin và Truyền thông – Đại học Thái Nguyên đã cung cấp cho tôi những kiến thức vô cùng quý báu và cần thiết trong suốt thời gian học tập tại trường để tôi có thể thực hiện và hoàn thành tốt luận văn này.

Tôi xin bày tỏ lòng biết ơn sâu sắc nhất tới Chính phủ Lào và Chính phủ Việt Nam, Bộ Giáo dục và Thể thao Lào, Bộ Giáo dục và Đào tạo Việt Nam đã tạo điều kiện cấp suất học bổng cao học này cho tôi. Xin trân trọng cảm ơn sâu sắc nhất tới Ban Lãnh đạo Bộ giáo dục và thể thao Lào đã tạo điều kiện và luôn ủng hộ tôi.

Với thời gian nghiên cứu còn hạn chế, ngôn ngữ còn khiêm tốn, luận văn không tránh khỏi những thiếu sót, tôi rất mong nhận được các ý kiến đóng góp chân thành từ các thầy cô giáo, đồng nghiệp và bạn bè.

Cuối cùng, tôi xin cảm ơn gia đình và bạn bè, những người đã luôn ủng hộ và động viên tôi, giúp tôi yên tâm và có tâm lý thuận lợi nhất để tôi nghiên cứu luận văn này. Tuy nhiên do giới hạn về mặt thời gian và kiến thức nên luận văn chắc chắn sẽ không tránh khỏi những sai sót ngoài ý muốn. Tôi rất mong nhận được sự thông cảm và đóng góp ý kiến của các thầy cô giáo, đồng nghiệp và bạn bè.

Thái Nguyên, tháng 11 năm 2020

HỌC VIÊN

Khatthnam PHOUCANTHAVONG

LỜI CAM ĐOAN

Tôi xin cam đoan toàn bộ nội dung văn bản này là do tôi tự sưu tầm, tra cứu và sắp xếp cho phù hợp với nội dung yêu cầu của đề tài.

Nội dung luận văn này chưa từng được công bố hay xuất bản dưới bất kỳ hình thức nào và cũng không sao chép từ bất kỳ một công trình nghiên cứu nào.

Tất cả phần mã nguồn của chương trình đều do tôi tự thiết kế và xây dựng, trong đó có sử dụng một số thư viện chuẩn và các thuật toán được các tác giả xuất bản công khai và miễn phí trên mạng Internet.

Thái Nguyên, tháng 11 năm 2020

Tác giả luận văn

Khatthanam PHOUCANTHAVONG

MỤC LỤC

| | |
|---|-----|
| LỜI CẢM ƠN | I |
| LỜI CAM ĐOAN | II |
| MỤC LỤC..... | III |
| DANH SÁNH HÌNH VẼ..... | VI |
| DANH SÁCH TỪ VIẾT TẮT | VII |
| MỞ ĐẦU..... | 1 |
| CHƯƠNG 1 TỔNG QUAN VỀ AN TOÀN DỊCH VỤ VÀ DỮ LIỆU WEB VÀ LỖI BẢO MẬT THÔNG DỤNG..... | 3 |
| 1.1 Khái niệm chung về thương mại điện tử | 3 |
| 1.1.1 Sự ra đời và phát triển của Internet..... | 3 |
| 1.1.2 Khái niệm thương mại điện tử..... | 4 |
| 1.1.3 Hệ thống các hoạt động cơ bản trong thương mại điện tử | 5 |
| 1.2 Tổng quan về ứng dụng Website | 6 |
| 1.2.1 Khái niệm ứng dụng Website | 6 |
| 1.2.2 Cách thức hoạt động | 7 |
| 1.2.3 Các dịch vụ và ứng dụng trên nền Website | 8 |
| 1.3 Tổng quan về an ninh mạng..... | 9 |
| 1.3.1 Khái niệm về an toàn và an ninh mạng | 9 |
| 1.3.2 Sự cần thiết phải bảo vệ thông tin | 9 |
| 1.4 Các thuật ngữ liên quan..... | 10 |
| 1.4.1 Hacker..... | 10 |
| 1.4.2 HTTP Header | 10 |
| 1.4.3 Session | 12 |
| 1.4.4 Cookie..... | 13 |
| 1.4.5 Proxy..... | 15 |

| | |
|--|----|
| CHƯƠNG 2 CÁC LOẠI TẤN CÔNG WEB PHỔ BIẾN..... | 16 |
| 2.1 Đặc trưng của các Website thương mại điện tử | 16 |
| 2.2 Tổng quan về Local Attack..... | 17 |
| 2.2.1 Giới thiệu về Local Attack..... | 17 |
| 2.2.2 Phương thức tấn công Local Attack | 17 |
| 2.3 Tấn công từ chối dịch vụ (denial of service) | 19 |
| 2.3.1 DOS (Denial of Service)..... | 19 |
| 2.3.2 DDoS (Distributed Denial of Service)..... | 20 |
| 2.4 Tấn công SQL Injection | 24 |
| 2.4.1 SQL Injection là gì?..... | 24 |
| 2.4.2 SQL Injection và vấn đề an ninh cơ sở dữ liệu..... | 24 |
| 2.5 Các phương pháp tấn công SQL Injection phổ biến | 27 |
| 2.5.1 Tấn công khai thác dữ liệu thông qua toán tử UNION..... | 28 |
| 2.5.2 Tìm số cột và kiểu dữ liệu của cột..... | 28 |
| 2.5.3 Tìm cột có khả năng “chứa” thông tin khai thác được | 28 |
| 2.5.4 Khai thác thông qua các câu lệnh điều kiện | 30 |
| 2.5.5 Blind SQL Injection – phương thức tấn công nâng cao | 31 |
| 2.5.6 Vấn đề qua mặt các bộ lọc tham số đầu vào..... | 31 |
| 2.5.7 Sử dụng các byte NULL | 32 |
| 2.6 Tấn công Cross Site Scripting (XSS)..... | 32 |
| 2.6.1 Hoạt động của XSS..... | 33 |
| 2.6.2 Phương pháp tấn công | 34 |
| CHƯƠNG 3 MỘT SỐ GIẢI PHÁP PHÒNG CHỐNG TẤN CÔNG DỮ LIỆU WEBSITE THƯƠNG MẠI ĐIỆN TỬ | 35 |
| 3.1 Mô hình đề xuất | 35 |
| 3.2 Các giải pháp đề xuất cụ thể | 36 |
| 3.2.1 Giải pháp phòng chống Local Attack | 36 |

| | |
|--|----|
| 3.2.2 Giải pháp phòng chống tấn công SQL Injection | 38 |
| 3.2.3 Xây dựng truy vấn theo mô hình tham số hóa..... | 40 |
| 3.2.4 Chuẩn hóa dữ liệu | 44 |
| 3.2.5 Giải pháp về bảo mật dữ liệu với mã hóa AES. | 44 |
| 3.3 Demo ứng dụng Website thương mại điện tử ứng dụng các giải pháp phòng chống tấn công dữ liệu | 48 |
| 3.3.1 Xây dựng website thương mại điện tử khóa học | 48 |
| 3.3.2 Mã hoá dữ liệu bên trong hệ quản trị cơ sở dữ liệu | 50 |
| 3.3.3 Một số giao diện chức năng Admin | 52 |
| 3.4 Đánh giá kết quả..... | 55 |
| KẾT LUẬN VÀ ĐỀ NGHỊ..... | 56 |
| TÀI LIỆU THAM KHẢO..... | 57 |

DANH SÁNH HÌNH VẼ

| | |
|--|----|
| Hình 1. 1: Mô hình ứng dụng thương mại điện tử trong các giai đoạn của chuỗi giá trị ... | 5 |
| Hình 1. 2: Kiến trúc một ứng dụng Website | 6 |
| Hình 1. 3: Mô hình hoạt động của ứng dụng Website. | 7 |
| Hình 2. 1: Sơ đồ chính phân loại mô hình tấn công DDoS..... | 21 |
| Hình 2. 2: Kiến trúc attack-network kiểu Agent – Handler | 22 |
| Hình 2. 3: Kiến trúc attack-network của kiểu IRC-Base | 23 |
| Hình 2. 4: Thống kê 10 điểm yếu phổ biến nhất (2008) | 25 |
| Hình 2. 5: Thống kê 10 điểm yếu phổ biến nhất (2009) | 25 |
| Hình 2. 6: Thống kê thời gian trung bình khắc phục điểm yếu (2008)..... | 26 |
| Hình 2. 7: Thống kê thời gian trung bình khắc phục điểm yếu (2009)..... | 26 |
| Hình 2. 8: Thống kê các điểm yếu thường được khai thác nhất 2019 | 27 |
| Hình 2. 9: Tìm cột mang dữ liệu | 29 |
| Hình 2. 10: Khai thác thông tin username | 29 |
| Hình 3. 1: Mô hình đề xuất | 35 |
| Hình 3. 2: Hàm prepare trong MySQL | 41 |
| Hình 3. 3: Trang chủ website thương mại điện tử khóa học..... | 48 |
| Hình 3. 4: Một số sản phẩm của website thương mại điện tử khóa học | 49 |
| Hình 3. 5: Một số sản phẩm của website thương mại điện tử khóa học | 50 |
| Hình 3. 6: Bảng điểm (point) sau khi mã hóa dữ liệu với AES | 50 |
| Hình 3. 7: Giao diện sau khi đăng nhập..... | 53 |
| Hình 3. 8: Giao diện thêm mới khóa học | 53 |
| Hình 3. 9: Giao diện Danh sách các khóa học | 54 |
| Hình 3. 10: Giao diện Danh sách các lớp học..... | 54 |

DANH SÁCH TỪ VIẾT TẮT

| TT | Chữ viết tắt | Ý nghĩa |
|-----------|---------------------|-------------------------------|
| 1 | TMĐT | Thương mại điện tử |
| 2 | HTML | Hyper text markup language |
| 3 | JSP | JavaServer Pages |
| 4 | ASP | Active Server Pages |
| 5 | DBMS | Database Management System |
| 6 | ODBC | Database Connectivity |
| 7 | DOS | Denial of Service |
| 8 | DDoS | Distributed Denial of Service |
| 9 | IRC | Internet Relay Chat |
| 10 | IPS | Intrusion Prevention System |
| 11 | XSS | Cross-Site Scripting |

MỞ ĐẦU

Thương mại điện tử (TMĐT) là việc tiến hành một phần hay toàn bộ hoạt động thương mại bằng những phương tiện điện tử qua môi trường Internet giúp các hoạt động thương mại được thực hiện nhanh hơn, hiệu quả hơn, giúp tiết kiệm chi phí và mở rộng không gian kinh doanh. Với vai trò và ảnh hưởng rộng lớn, đặc biệt liên quan đến tài chính trong nhiều lĩnh vực hoạt động kinh tế, các website TMĐT với đặc điểm chứa nhiều thông tin giá trị, đặc biệt là về mặt tài chính. Điều này dẫn tới các website TMĐT là mục tiêu tấn công bất hợp pháp nhằm khai thác dữ liệu có giá trị.

Công nghệ thông tin và Thương mại điện tử đã xâm nhập vào mọi góc cạnh của đời sống xã hội nói chung và của doanh nghiệp nói riêng. Đối với doanh nghiệp, Thương mại điện tử góp phần hình thành những mô hình kinh doanh mới, giảm chi phí, nâng cao hiệu quả kinh doanh. Đối với người tiêu dùng, Thương mại điện tử giúp mua sắm thuận tiện hàng hóa và dịch vụ trên các thị trường ở mọi nơi trên thế giới. Để doanh nghiệp luôn phát triển trong môi trường công nghệ có tốc độ phát triển như hiện nay thì doanh nghiệp phải nắm rõ được các thông tin cơ bản để có thể vận hành thương mại điện tử vào trong tổ chức của mình.

Thế giới ngày nay đã có nhiều tiến bộ mạnh mẽ về công nghệ thông tin (CNTT) từ một tiềm năng thông tin đã trở thành một tài nguyên thực sự, trở thành sản phẩm hàng hoá trong xã hội tạo ra một sự thay đổi to lớn trong lực lượng sản xuất, cơ sở hạ tầng, cấu trúc kinh tế, tính chất lao động và cả cách thức quản lý trong các lĩnh vực của xã hội.

Trong những năm gần đây, các ứng dụng của công nghệ thông tin ngày càng phát triển. Đặc biệt là ứng dụng Website, hầu như mọi người ai cũng từng nghe và làm việc trên ứng dụng Website. Website trở nên phổ biến và trở thành một phần quan trọng của mọi người và nhất là các doanh nghiệp, công ty. Bên cạnh đó lý do an toàn bảo mật cho ứng dụng Website luôn là vấn đề nan giải của mọi người.

Với các lý do trên, em đã lựa chọn đề tài “**Nghiên cứu một số giải pháp phòng chống tấn công dữ liệu đối với website thương mại điện tử**” để làm đề tài luận văn cho mình. Em thấy đây là đề tài mang tính thực tế cao, giúp cho các nhà quản trị Website