**LỜI MỞ ĐẦU**

Công nghệ thông tin là một trong những ngành mũi nhọn trong chiến lược phát triển kinh tế, xây dựng đất nước của hầu hết các quốc gia. Sự phát triển của Công nghệ thông tin trong những thập niên gần đây đã làm thay đổi sâu sắc bộ mặt của thế giới. Vào thế kỷ XVIII, một nước muốn công nghiệp hóa thường mất 100 năm. Đầu thế kỷ XX, còn khoảng 30 năm. Vào thập niên 70 - 80 rút xuống 20 năm. Thập niên 90 chỉ còn trên dưới 10 năm (1).

Cùng với các ngành nghề công nghệ khác như Công nghệ sinh học, Công nghệ năng lượng, các sản phẩm Công nghệ thông tin đã và đang được ứng dụng rộng rãi trong mọi lĩnh vực của đời sống kinh tế, xã hội và hầu hết đều đem đến những giá trị thiết thực. Ví dụ như đối với nền kinh tế thì các quy trình sản xuất đều được tự động hóa, máy móc không chỉ thay thế con người trong những công việc nặng nhọc mà còn thay thế con người cả ở những khâu phức tạp của việc sản xuất và quản lý, không chỉ thay thế các thao tác lao động mà còn cả các thao tác tư duy. Trong nền kinh tế toàn cầu, với sự phát triển của internet, thương mại điện tử đang trở thành một lĩnh vực phát triển rất mạnh mẽ, nó thúc đẩy các ngành sản xuất dịch vụ trên phạm vi toàn thế giới. Còn đối với y tế thì hiện nay đã sử dụng công nghệ siêu âm 3D, hoặc sử dụng CNTT để hỗ trợ về mặt kỹ thuật và phương pháp điều trị cho những vùng xa trung tâm y tế đã mang lại giá trị to lớn về mặt tinh thần cũng như vật chất cho nhân dân…

Bên cạnh những ưu điểm nêu trên CNTT không phải không có những khuyết điểm. Ngày nay với công nghệ tiên tiến, bất kì cái gì có thể được tự động hoá sẽ được tự động hoá, điều đó nghĩa là nhiều việc làm sẽ tiếp tục biến mất. Nhiều người không tin điều đó, cũng như họ đã không thấy robots có thể làm việc làm tốt hơn con người trong chế tạo, xây dựng và văn phòng. Chẳng hạn, hệ thống trả lời điện thoại đã thay thế cho nhiều nhân viên điện thoại và người tiếp tân. Hệ thống tổ chức hồ sơ đã thay thế cho nhiều thư kí hồ sơ và phần mềm xử lí văn bản đã thay thế nhiều thư kí đánh máy. Vài năm trước, không ai nghĩ robots có thể thay thế các phóng viên, người viết bài cho báo chí nhưng ngày nay 35% tin tức được robot viết. Nhiều tờ báo đang dùng phần mềm viết tự động để lấy tin tức nhanh hơn, đặc biệt với những báo trực tuyến và giảm số người viết và phóng viên (2). Ngoài ra, với sự xuất hiện và hoạt động của mạng Internet trên phạm vi toàn cầu, nhiều quốc gia không quản lý được các hoạt động trên Internet, những văn hóa phẩm độc hại được đưa vào mạng và tác động tiêu cực đến sự phát triển đạo đức ở hàng loạt quốc gia. Nghiêm trọng hơn là các vấn đề tấn công, xâm nhập vào các hệ thống mạng nhằm phá hoại hay đánh cắp các dữ liệu. Có thể nó không ảnh hưởng đến sinh mạng của người dân, nhưng những thông tin các nhân bị đánh cắp có thể gây ra hậu quả nghiêm trọng hơn rất nhiều. Tháng 11/2015, hang sản xuất đồ chơi VTech của Trung Quốc đã để một lỗ hổng bảo mật tồn tại trong chiếc máy tính bảng dành cho trẻ em của mình. Nó khiến cho các hacker có khả năng đánh cắp thông tin cá nhân của hơn 4,9 triệu tài khoản của phụ huynh và 6,7 triệu tài khoản của trẻ em. Các thông tin bị đánh cắp gồm cả tên, địa chỉ, email, các mật khẩu đã bị mã hóa, địa chỉ IP và nhiều thông tin khác. Tuy nhiên nghiêm trọng nhất là cả những bức ảnh chụp của trẻ cũng bị đánh cắp và nó có thể dẫn đến những mối đe dọa nguy hiểm hơn, như bắt cóc tống tiền (3).

Theo sự phát triển của CNTT nói chung cũng như là Internet nói riêng thì Bảo mật luôn luôn là vấn đề được đặt lên hàng đầu, đặc biệt là đối với các ứng dụng web. Từ những ngày đầu của Internet, người ta đã quan tâm đến tính an toàn trong việc trao đổi thông tin. Tuy không có sự an toàn tuyệt đối nhưng những phát triển trong lĩnh vực này thì rất nhanh và mang lại nhiều thành quả vì đây là vấn đề cấp bách của nhiều tổ chức, doanh nghiệp,… Chính vì thế sự an toàn của web service trên mạng cũng không thể nằm ngoài vấn đề này. Có thể nói ngày nay ngoài việc nghiên cứu làm sao để tạo ra một web services tốt mang lại nhiều lợi ích thì việc nghiên cứu để làm sao mang lại sự an toàn cho web services cũng là một trong những vấn đề quan trọng nhất.

Không những vậy, các hình thức phá hoại, tấn công mạng cũng trở nên tinh vi và phức tạp hơn. Việc tấn công mạng hiện nay không chỉ là việc ăn cắp tiền từ tài khoản ngân hàng của các nạn nhân mà còn ăn cắp thông tin cá nhân của người dùng, sử dụng mã độc mã hóa dữ liệu tống tiền (ransomeware), sử dụng các phần mềm quảng cáo bất hợp pháp núp bóng dưới các phần mềm tiện ích, … (4). Do đó, đối với mỗi hệ thống, nhiệm vụ bảo mật được đặt ra cho người quản trị mạng là hết sức quan trọng và cần thiết. Xuất phát từ những thực tế đó, chúng tôi sẽ tìm hiểu về các cách tấn công phổ biến nhất hiện nay cũng như cách phòng chống các loại tấn công này. Chính vì vậy nhóm chúng tôi đã quyết định chọn đề tài “*Tìm hiểu các phương pháp tấn công và phòng chống trên Web Server*” làm đề tài nghiên cứu.

Mục tiêu nhóm chúng tôi đưa ra để nghiên cứu đề tài như sau:

* + Mục tiêu tổng quát: Như đã nói ở trên, hình thức tân công mạng hiện nay ngày càng đa dạng và phức tạp nên nhóm chúng tôi chỉtiến hành nghiên cứu về một số hình thức tấn công Website phổ biến nhất hiện nay cũng như cách phòng chống chúng. Giúp các bạn phần nào hiểu rõ hơn về các ứng dụng Website cũng như các mối đe dọa vấn đề an toàn thông tin khi chúng ta làm việc trên các ứng dụng web hàng ngày, các kỹ thuật tấn công và bảo mật web.
  + Mục tiêu cụ thể: Nhóm sẽ đưa ra lý thuyết về cách tấn công và phòng thủ của một số hình thức tấn công như: SQLi, DDOS, Local attack, Cross Site Scripting (XSS). Sau đó nhóm sẽ tiến hành làm demo trên máy ảo để các bạn có thể hiểu rõ hơn về cách tấn công và phòng chống trên thực tế.

Với những việc đã nêu ở sơ lược đề tài nhóm chia bố cục như sau:

1. Tổng quan về website.
2. Các loại tấn công và bảo mật ứng dụng web phổ biến.
   1. Local Attack.
   2. Tấn công từ chối dịch vụ.
   3. SQL Injection.
   4. Cross Site Scripting(XSS).
3. Demo Tấn công và phòng thủ trên Web Server.

**Tài liệu tham khảo:**

(1) Nhiều tác giả, “*Almanach những nền văn minh thế giới*”, NXB văn hóa thông tin, 1943, 1997.

(2) <http://kcntt.duytan.edu.vn/Home/ArticleDetail/vn/170/2663/nhung-mat-han-che-cua-cong-nghe-thong-tin>

(3), (4) <http://genk.vn/internet/10-vu-hacker-tan-cong-de-lai-hau-qua-nghiem-trong-nhat-nam-2015-20151215160108425.chn>