BỘ GIÁO DỤC VÀ ĐÀO TẠO

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP.HCM**



**BÁO CÁO**

**HACKING WEB APPLICATION**

Ngành: **CÔNG NGHỆ THÔNG TIN**

Môn: **BẢO MẬT THÔNG TIN**

Giảng viên hướng dẫn: Hoàng Văn Thiện

**Các thành viên trong nhóm thực hiện:**

Họ và tên: Nguyễn Minh Thông

MSSV: 1811160288 Lớp: 18DTHE3

Họ và tên: Phạm Duy Hoàng

MSSV: 234343434 Lớp: 18DTHE3

Họ và tên: Nguyễn Hoàng Long

MSSV: 1811160288 Lớp: 18DTHE3

TP. Hồ chí minh, 2021

**MỤC LỤC**

[LỜI NÓI ĐẦU 4](#_Toc77624241)

[CHƯƠNG I: NHỮNG KHÁI NIỆM CƠ BẢN 5](#_Toc77624242)

[**1/Web Application** 5](#_Toc77624243)

[**1.1/Khái niệm:** 5](#_Toc77624244)

[**1.2/Cách thức hoạt động của ứng dụng Web.** 6](#_Toc77624245)

[**1.3/Web 2.0 và các thế hệ Web 3.0 trở đi** 6](#_Toc77624246)

[**2/Các tầng gây thương tích** 10](#_Toc77624247)

# **LỜI NÓI ĐẦU**

Kính chào thầy, cô và các bạn, nhóm chúng em xin gửi lời chào tới tất cả người đọc thân mật nhất. Ở bài báo cáo này nhóm chúng em sẽ nghiên cứu về cách tấn công lên phần mềm trên trang web. Nhưng nhóm chúng em làm vậy chỉ để cho những người đọc báo cáo này có thể nhận biết được những thủ đoạn tinh vi của những hacker và đồng thời cho người đọc thấy được rằng trình duyệt web không phải là nơi an toàn nhất để có thể lưu trữ thông tin. Việc người dùng càng tin tưởng sử dụng những trình duyệt như Google Chrome và Firefox mà những kẻ xấu đã lợi dụng điều này và phát tán những trang web giả mạo để nhắm tới người bình thường lướt web. Thậm chí không riêng người dùng mà những đối tượng như những người làm ăn kinh doanh cũng là miếng mồi ngon béo bở để cho các hacker có thể lợi dụng và xâm nhập, đánh cắp dữ liệu và đánh cắp tiền thông qua các phần mềm trên trình duyệt web. Nhưng những kẻ xấu sẽ không dùng những phần mềm đã có sẵn trên hệ điều hành Windows để có thể xâm nhập vào hệ thống của người dùng. Vì vậy việc biết trước được những thủ đoạn tinh vi hacker mà những người dùng máy vi tính đều có thể lường trước được và có thể tìm cách bảo vệ bản thân người dùng trước mạng toàn cầu Internet. Đặc biệt là thời điểm mà thế giới đang đi theo xu hướng công nghệ hóa như hiện nay thì việc bảo vệ bản thân người dùng máy vi tính là mục tiêu quan trọng nhất của mỗi doanh nghiệp. Thậm chí kể cả doanh nghiệp cũng phải biết bảo vệ mình trước nguy cơ bị lấy mất thông tin dữ liệu của công ty. Mục tiêu của nhóm em ở trong cuốn báo cáo này là để cho người dùng thấy đây không những cách tấn công của các hacker mà còn cung cấp kiến thức cơ bản nhất và chung nhất về cách sử dụng trình duyệt Web đúng đắn nhất để phòng ngừa khỏi bị những hacker có mưu đồ để tấn công. Đặc biệt ở thời đại công nghệ số 4.0 như hiện nay, việc bảo vệ thông tin người dùng không chỉ vậy mà còn bảo vệ được dữ liệu của mình trên mạng Internet là một việc cần thiết để làm đối với các doanh nghiệp lẫn người dùng máy vi tính. Ngày càng Internet càng phát triển mạnh thì những kẻ xấu luôn luôn có những phương pháp tiếp cận ngày càng tinh vi hơn và khó phát hiện hơn.

# **CHƯƠNG I: NHỮNG KHÁI NIỆM CƠ BẢN**

## **1/Web Application**

## **1.1/Khái niệm:**

Web Application là ứng dụng web mà có hình ảnh hay còn gọi là giao diện để cho người dùng có thể tương tác với các Web Server hay những cơ sở dữ liệu trên mạng. Ví dụ như là người dùng thực hiện thao tác chuyển tiền qua ví điện tử e-wallet MOMO nổi tiếng.

Icon

Description automatically generated

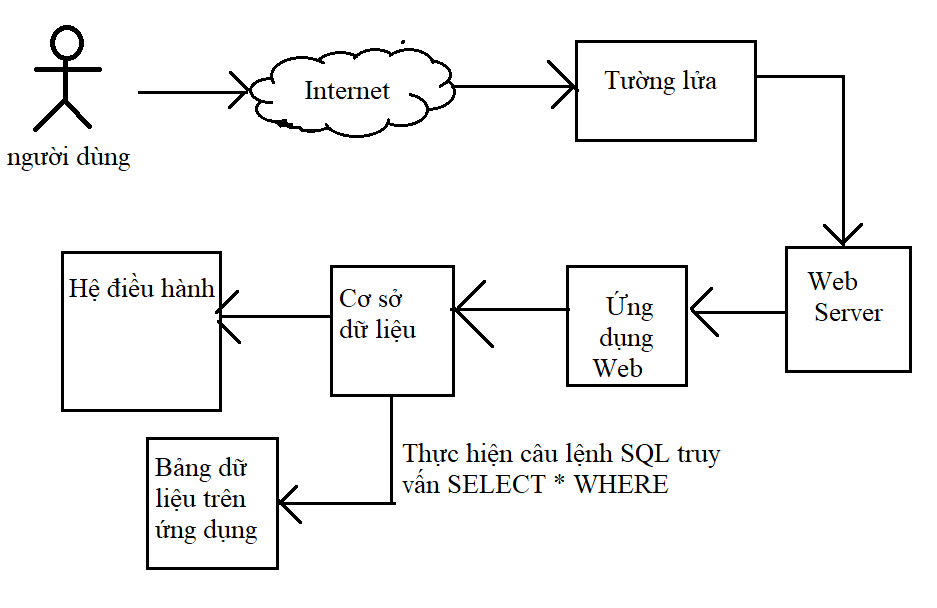
**Hình 1.1.1: Logo ví điện tử MOMO.**

A picture containing text, clipart

Description automatically generatedHay mọi người hay chia sẻ hình ảnh hoặc tập tin qua mạng Facebook. Facebook cũng được coi là phần mềm Web tại vì người dùng có thể tương tác được với Facebook thông qua mạng Internet bằng cách chia sẻ hình ảnh và chia sẻ nhạc.

**Hình 1.1.2: Logo Facebook.**

## **1.2/Cách thức hoạt động của ứng dụng Web.**



**Hình 1.2.1: Hình minh họa cơ chế hoạt động chung của bất kỳ ứng dụng Web**

### **1.3/Web 2.0 và các thế hệ Web 3.0 trở đi**

Thế hệ Web thời nay từ năm 2000 cho đến nay đã rất là khác nhau. Từ cấu trúc cho đến cơ sở hạ tầng của Web thay đổi liên tục. Ngay cả ứng dụng Web cũng cung cấp cho người dùng một giao diện linh động hơn và tinh tế hơn và chứa được nhiều người truy cập website một lúc hơn. Trong tương lai dự kiến sẽ có Web phiên bản 3.0 sẽ mới hơn và giao diện thông minh hơn và cải tiến hơn và không bị đứng máy khi số lượng người truy cập vào trang web lớn hơn 1000000000, sức chứa hơn hẳn Web 2.0.

Diagram

Description automatically generated

**Hình 1.3.1: Hình minh họa sức chứa lượng người truy cập trang web mỗi ngày của các thế hệ Web trong tương lai.**

**1.4/ Kiến trúc nền tảng của mỗi ứng dụng Web**

**A picture containing diagram

Description automatically generated**

**Hình 1.4.1: Kiến trúc chung của ứng dụng Web.**

Trong tập tin Clients bao gồm nhiều thành phần gộp chung lại với nhau và liên kết qua lại với nhau qua Internet và dịch vụ cung cấp Web:

+ Các trình duyệt Web.

+ Lớp trình chiếu bao gồm nhiều lớp con như:

* Các lớp con Flash.
* Các lớp con Silverlight.
* Các lớp con Java Script.

+Các thiết bị như: điện thoại di động, Tivi, máy vi tính.

Tập tin Clients liên kết với tập tin Web Server và ngược lại tập tin Web Server liên kết với tập tin Clients. Hai tập tin liên kết qua lại với nhau và cấu trúc bên trong của tập tin Web Server bao gồm nhiều thành phần con cấu thành:

+Lớp trình chiếu bao gồm các lớp con:

* Tường lửa bất kỳ.
* HTTP Request Parser.

+Lớp Proxy Server.

+Lớp Cache.

+Lớp Servlet Container.

+Lớp Resource Handler.

+Lớp Authentication.

+Lớp Login.

Tập tin tầng công việc hành chính(Business Layer) liên kết qua lại với nhau bằng tập tin Web Server và tập tin tầng Cơ sở dữ liệu (Database Layer), cấu trúc bên trong của tập tin gồm nhiều lớp con và lớp cha hợp lại với nhau:

+Lớp Application Server.

+Lớp J2EE.

+Lớp .NET.

+Lớp COM.

+Lớp XCode.

+Lớp C++.

+Lớp COM+.

+Lớp Business Logic.

+Lớp Legacy Application.

+Lớp Data Access.

Tập tin tầng Cơ sở dữ liệu bao gồm:

+Lớp Cloud Services.

+Lớp B2B.

+Lớp Data Server.

## **2/Các tầng gây thương tích**

Tầng 1: Về Bảo mật thì có IPS và IDS.

Tầng 2: Về Mạng thì có Router và Switch.

Tầng 3: Về Hệ điều hành thì có Windows, Linux, Hệ điều hành X.

Tầng 4: Về Web Server thì có Apache hay Microsoft IIS.

Tầng 5: Về Cơ sở dữ liệu (Database) thì có Oracle hay MSSQL.

Tầng 6: Về thành phần bên thứ ba thì có Mã nguồn mở, thương mai.

Tầng 7: Về Ứng dụng Web thì có Lỗi doanh nghiệp và Lỗi kỹ thuật.

Sắp xếp theo thứ từ lớn đến bé thì tầng 7 là tầng có sự nguy hiểm nhẹ nhất trong tất cả các tầng và tầng 1 là tầng nếu như bị lỗi thì sẽ nặng hơn.

## **3/Các lỗi phổ biến dễ gặp trên ứng dụng Web**

### **3.1/Nhập thông tin không hợp lệ**

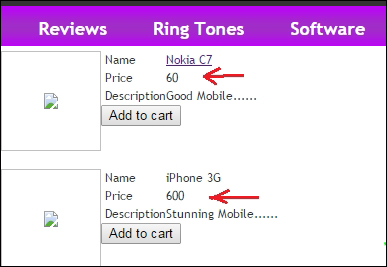
Lỗi nhập thông tin không hợp lệ nếu người dùng nhập đúng mật khẩu và tên tài khoản của mình mà vẫn xuất hiện lỗi thì liên qua tới lỗi của của chính ứng dụng Web khi thông tin người dùng không hợp lệ trước khi được xử lý bởi các Web Server và các ứng dụng Web.

Hacker có thể lợi dụng lỗi nhập thông tin không hợp lệ của các ứng dụng Web để thực hiện các thủ thuật tấn công website như kỹ thuật cross-site-scripting, buffer overflow, kỹ thuật tiêm,… Ứng dụng Web sẽ bị lỗi về giao diện màn hình và bị chập chờn.

### **3.2/Thao túng Form của Web và Url của Web:**

Ngay cả lỗi này kể cả các ứng dụng Web và các trang Web đều dễ bị dính. Đối với người dùng thì lỗi này sẽ được coi là do mạng wifi nhà của người dùng yếu cho nên mới xảy ra lỗi về Form của Web hay Url của trang Web đột nhiên thay đổi.

Nhưng đối với môn bảo mật thông tin và những kẻ tấn công thì lỗi này chắc chắn do bàn tay của một kẻ xấu nhúng vào chứ không hề là lỗi bình thường tự nhiên như người dùng nghĩ.

Từ đó, Hacker mũ đen có thể lợi dụng ý nghĩ này của người dùng để thực hiện các kỹ thuật tấn công mạng như Cross-Site-Scripting, tiêm mã SQL,…

**Hình 3.1: Đây là kết quả của lỗi hình ảnh một trang web bất kỳ không hiển thị được liên quan đến lỗi thao túng Form và Url của Web**

**3.3/Liên kết tới các thư mục để thao túng dữ liệu(Directory Traversal)**

Kẻ tấn công có thể truy cập vào các dữ liệu bị khóa bao gồm các source code và các tập tin hệ thống ngoài lề của các thư mục trong Web Server.

Hacker mũ đen đã lợi dụng những tập tin bên ngoài để thao túng và truy cập vào rồi để tấn công trực tiếp các Web Server và các tập tin hệ thống khác.

Kẻ tấn công có thể thao túng những tham số có liên quan tới các tập tin với chuỗi “../” và sự đa dạng của nó.

### **3.3/Lỗi không cài đặt được bảo mật cho các ứng dụng Web và hệ điều hành và tập tin.**

Các hacker mũ đen lợi dụng các ứng dụng cài đặt bảo mật cho hệ thống để gián tiếp thông qua các ứng dụng cài đặt bảo mật và các ứng dụng diệt virus để bắt đầu thực hiện những kỹ thuật hack như tiêm mã độc,… và những lỗi như lỗi thao túng Form của các ứng dụng lẫn trên hệ điều hành và cả các ứng dụng Web.