TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**ĐỒ ÁN MÔN PHÂN TÍCH THIẾT KẾ YÊU CẦU**

**XÂY DỰNG HỆ THỐNG THÔNG TIN QUẢN LÝ NHÀ HÀNG**

*Người hướng dẫn*: **TS DƯƠNG THỊ THÙY VÂN**

*Người thực hiện*: **LÊ PHẠM DUY THÔNG - 51403396**

**TRƯƠNG TẤN KHÁNH – 51403277**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2017**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**

****

**ĐỒ ÁN 1**

**NGHIÊN CỨU PHƯƠNG PHÁP TẤN CÔNG CƯỚP PHIÊN (SESSION HIJACKING) VÀ CÁCH PHÒNG TRÁNH**

*Người hướng dẫn*: **TS TRƯƠNG ĐÌNH TÚ**

*Người thực hiện*: **LÊ PHẠM DUY THÔNG - 51403396**

**TRƯƠNG TẤN KHÁNH - 51403277**

Lớp **: 14050302**

Khoá  **: 18**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2017**

# LỜI CẢM ƠN

Em xin bày tỏ lòng biết ơn sâu sắc tới TS. Trương Đình Tú – người thầy đã trực tiếp hướng dẫn và chỉ bảo cho em hoàn thành bài báo cáo đồ án này. Em xin chân thành cảm ơn bạn bè, đồng nghiệp của em đang học và làm việc tại và gia đình đã động viên, khích lệ, tạo điều kiện và giúp đỡ em trong suốt quá trình thực hiện và hoàn thành báo cáo đồ án này.

Với điều kiện về thời gian cũng như kinh nghiệm còn hạn chế của bản thân, đồ án này không thể tránh được những thiếu sót hay sai sót. Chúng em rất mong nhận được sự chỉ bảo, đóng góp ý kiến của các thầy cô để chúng em có điều kiện bổ sung, sửa sai. Xin chân thành cám ơn các thầy cô.

**ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là sản phẩm đồ án của riêng chúng tôi và được sự hướng dẫn của TS Trương Đình Tú. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình.** Trường đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày 28 tháng 12 năm 2017*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Lê Phạm Duy Thông*

*Trương Tấn Khánh*

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

**Phần xác nhận của GV hướng dẫn**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

# TÓM TẮT

Đây là đồ án nghiên cứu các vấn đề về an toàn bảo mật mạng, trong đó phương pháp tấn công cướp phiên (Session Hijacking) là phương pháp cần đáng được quan tâm. Phương pháp này liên quan đến việc làm sao để chiếm dụng quyền sử dụng tài khoản của một cá nhân, tổ chức nào đó trái phép thông qua các lỗ hổng bảo mật áp dụng ở hai mức mạng và mức ứng dụng. Ở mức mạng có tấn công phổ biến thông qua sử dụng mạo danh IP (IP Spoofing) và nhiễm độc ARP (ARP Poisioning). Ở mức ứng dụng có khá nhiều kỹ thuật tấn công, tuy nhiên ta có thể thấy các hacker sử dụng các phương pháp định hình phiên (Session fixation), chặn phiên (Session side jacking), XSS (Cross-site scripting), mã độc (Malware). Ở mỗi phương pháp ta cũng có minh chứng cho thấy cách tấn công (gồm video) và đề xuất cách khắc phục.

# MỤC LỤC

[LỜI CẢM ƠN i](#_Toc502224438)

[TÓM TẮT iv](#_Toc502224439)

[MỤC LỤC 1](#_Toc502224440)

[DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT 2](#_Toc502224441)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 3](#_Toc502224442)

[CHƯƠNG 1: GIỚI THIỆU TỔNG QUAN ĐỀ TÀI 4](#_Toc502224443)

[1.1 Khái niệm về phiên (Session) 4](#_Toc502224444)

[1.1.1 Phiên bên phía máy chủ (Server-side web sessions) 4](#_Toc502224445)

[1.1.2 Phiên bên phía máy khách (Client-side web sessions) 5](#_Toc502224446)

[1.1.3 Mã thông báo phiên HTTP (HTTP session token) 5](#_Toc502224447)

[1.2 Khái niệm về cướp (Hijacking) 6](#_Toc502224448)

[1.3 Khái niệm về Session Hijacking 7](#_Toc502224449)

[CHƯƠNG 2: NỘI DUNG NGHIÊN CỨU 9](#_Toc502224450)

[2.1 Session Hijacking ở mức mạng 9](#_Toc502224451)

[2.1.1 Giới thiệu các giao thức để tấn công thường gặp 9](#_Toc502224452)

[2.1.2 Tấn công TCP/IP 12](#_Toc502224453)

[2.2 Session Hijacking ở mức ứng dụng 17](#_Toc502224454)

[2.2.1 Brute forcing 17](#_Toc502224455)

[2.2.2 Định hình phiên (Session Fixation) 17](#_Toc502224456)

[2.2.3 Chặn phiên (Session side jacking) 21](#_Toc502224457)

[2.2.4 Cross-site scripting (XSS) 25](#_Toc502224458)

[2.2.5 Mã độc (Malware) 30](#_Toc502224459)

[2.2.6 Giao thức truyền tải đã được mã hóa 33](#_Toc502224460)

[2.3 Các biện pháp bảo mật chung phòng tránh Session Hijacking 34](#_Toc502224461)

[2.3.1 Đối với nhà phát triển (Web) 34](#_Toc502224462)

[2.3.2 Đối với người dùng 35](#_Toc502224463)

[CHƯƠNG 3: KẾT LUẬN 36](#_Toc502224464)

# DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT

**CÁC CHỮ VIẾT TẮT**

ISP Nhà cung cấp dịch vụ Internet Service Provider

TCP Giao thức truyền tải Transmission Control Protocol

UDP Giao thức truyền tải User Datagram Protocol

ARP Giao thức phân giải địa chỉ Address Resolution Protocol

ICMP Giao thức gửi các thông báo, lỗi Internet Control Message Protocol

IP Giao thức hướng dữ liệu Internet Protocol (địa chỉ truy cập)

MAC Giao thức điều khiển truy nhập môi trường Medium Access Control

XSS Phương pháp tấn công Cross-Site Scripting

MITM Phương pháp tấn công Man-in-the-middle

# DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

**DANH MỤC HÌNH**

[Hình 1‑1: Mô phỏng từ lúc bắt đầu một phiên làm việc 6](#_Toc502224465)

[Hình 2‑1: Gói ping từ 192.168.1.2 -> 192.168.1.3 10](#_Toc502224466)

[Hình 2‑2: Quá trình bắt tay ba bước 11](#_Toc502224467)

[Hình 2‑3: Gửi dữ liệu qua giao thức TCP 12](#_Toc502224468)

[Hình 2‑4: Mô phỏng quá trình tấn công IP Spoofing 13](#_Toc502224469)

[Hình 2‑5: Kết quả gửi gói tin với nguồn IP giả 14](#_Toc502224470)

[Hình 2‑6: Trước lúc IP Spoofing trang web 15](#_Toc502224471)

[Hình 2‑7: Sau khi IP Spoofing trang web 15](#_Toc502224472)

[Hình 2‑8: Mô phỏng quá trình tấn công MITM trong mạng máy tính 16](#_Toc502224473)

[Hình 2‑9: Ví dụ 1 về hình thức định hình phiên đơn giản 18](#_Toc502224474)

[Hình 2‑10: Đặt-Cookie trong phản hồi tiêu đề HTTP trong ví dụ 4 20](#_Toc502224475)

[Hình 2‑11: Giao diện chính của Ettercap 22](#_Toc502224476)

[Hình 2‑12: Tiến hành khởi động Ettercap 23](#_Toc502224477)

[Hình 2‑13: Máy người dùng Android thao tác trên mạng máy tính 23](#_Toc502224478)

[Hình 2‑14: Các gói tin bắt được bằng ferret của máy điện thoại nạn nhân (ip: 192.168.1.134) 24](#_Toc502224479)

[Hình 2‑15: Lấy cắp được mã phiên qua Session sidejacking 24](#_Toc502224480)

[Hình 2‑16: Nhập đoạn mã javascript vào text form 26](#_Toc502224481)

[Hình 2‑17: Trình duyệt chạy đoạn mã XSS 27](#_Toc502224482)

[Hình 2‑18: Cánh báo yêu cầu bị hủy vì nghi vấn tấn công XSS trong Chrome 27](#_Toc502224483)

[Hình 2‑19: Bài viết giả mạo đăng bởi người dùng ẩn danh “Anonymous” 28](#_Toc502224484)

[Hình 2‑20: Nội dung chỉ hiển thị một phần 29](#_Toc502224485)

[Hình 2‑21: Kẻ tấn công bắt được mã phiên qua tấn công XSS 29](#_Toc502224486)

[Hình 2‑22: Chọn “No, I do not want to persist this sessions at this moment in time trong ZAP” 31](#_Toc502224487)

[Hình 2‑23: Thiết lập địa chỉ máy chủ proxy cho ZAP 32](#_Toc502224488)

[Hình 2‑24: Kẻ tấn công đã thể thấy được các gói tin bắt được trong ZAP 32](#_Toc502224489)

[Hình 2‑25: Chương trình phòng chống virus Bitdefender 33](#_Toc502224490)

[Hình 2‑26: Mật khẩu đã bị lấy trộm khi không sử dụng https 34](#_Toc502224491)

# KHẢO SÁT VÀ MÔ TẢ YÊU CẦU BÀI TOÁN

## Giới thiệu

Nhà hàng Hương Phố là một nhà hàng nổi tiếng đã được nhiều người biết tới từ rất lâu ở đường Phan Văn Trị thuộc thành phố Hồ Chí Minh. Nhà hàng gồm hai tòa nhà được thiết kế với hai tầng quay ra mặt đường đối diện nhau qua đường chính Phan Văn Trị, có hầm để xe cho khách đi xe máy và cả xe hơi. Điểm đặc biệt khiến nhà hàng Hương Phố khác biệt với các nhà hàng khác đó chính là cây cầu để bắc qua hai tòa nhà, giúp cho khách có thể đi qua lại giữ hai tòa nhà một cách dễ dàng, tránh phải đi qua đường nguy hiểm vào giờ cao điểm.

Nhà hàng có hai tầng, với cách bài trí với không gian rộng lớn. Mỗi tầng sẽ có hàng lang, mỗi phòng được cách nhau một khoảng nhất định, mỗi phòng bên trong sẽ có diện tích rộng lớn, với gồm những dãy bàn dọc với nhau và một sân khấu lớn ở cuối phòng. Bên trong các phòng sẽ có một quầy bar nhỏ để cho khách hàng có thể đế thưởng thức café, rượu các loại tại quầy, hoặc nếu muốn yên tĩnh khách có thể lên sân thượng phía trên để ngắm cảnh đường phố và phi trường sân bay với một quán café riêng biệt bên trên.

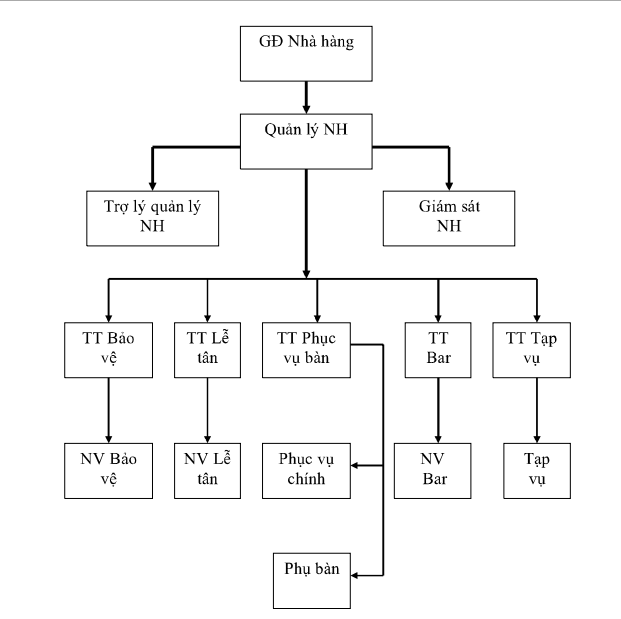
Mỗi tầng của nhà hàng bao gồm hai phòng thường và một phòng vip, hai phòng thường mỗi phòng 20-30 bàn cho việc tổ chức sinh nhật, những buổi tất niên nhỏ. Còn phòng vip từ 60-100 bàn với quy mô cho tổ chức đám cưới, tiệc họp mặt, hội thảo nghiên cứu.

Tổ chức nhà hàng có : 2 thu ngân, 2 quản lý (trưởng và phó), 4 lễ tân và hơn 50 nhân viên khác khi có tổ chức tiệc ở cả hai nhà hàng.

## Quy chế tổ chức nhà hàng

### Tổ chức bộ phận quản lý nhà hàng

#### Sơ đồ tổ chức



Hình 1‑1: Sơ đồ tổ chức của nhà hàng

#### Mô tả chi tiết công việc của các bộ phận chính

**Bộ phận quản lý nhà hàng**:

* Theo dõi nhân sự trực thuộc, đề xuất tuyển dụng, cùng với phòng nhân sự tổ chức phỏng vấn, đánh giá ứng viên.
* Tổ chức huấn luyện, kèm cặp nhân viên mới và đào tạo huấn luyện định kỳ theo quy định của nhà hàng.
* Đánh giá nhân viên thử việc, ra quyết định ký hoặc không ký hợp đồng chính thức với nhân viên đã qua thời gian thử việc.
* Tổ chức đánh giá công việc của toàn bộ nhân viên hàng tháng.
* Giải quyết các công việc phát sinh, các yêu cầu của khách mà NV không giải được trong quá trình phục vụ khách.
* Báo cáo giám đốc điều hành các ý kiến phản ánh của khách hàng.
* Đánh giá hoạt động của nhân viên, từ đó có quyết định thưởng phạt.
* Lập kế hoạch công tác tuần, tháng và chuyển kế hoạch cho giám đốc điều hành.
* Quản lý toàn bộ tài sản được giao: trang thiết bị, vật tư.
* Đề xuất các sáng kiến cải tiến, nâng cao chất lượng dịch vụ nhà hàng.

**Bộ phận lễ tân**:

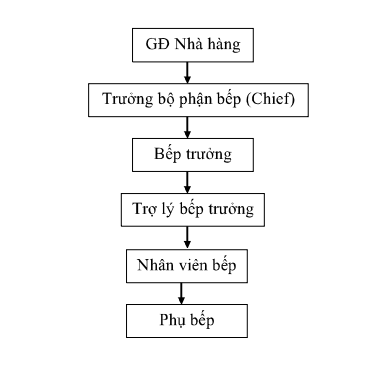
* Tiếp đón khách tại khu vực ra vào.
* Tư vấn các đặc điểm của nhà hàng cho khách.
* Dẫn khách vào bàn hoặc lên phòng.
* Tiếp nhận các thông tin đặt bàn và thực hiện theo quy định đặt bàn.
* Cuối ngày báo cáo hoạt động cho quản lý nhà hàng.

**Bộ phận phục vụ bàn**:

* Tiếp khách, tư vấn có món ăn, đồ uống, ghi order, thực hiện thanh toán.
* Phân công công việc cho nhân viên.
* Điều động nhân viên phục vụ thực hiện công việc.
* Đánh giá công việc nhân viên.
* Báo cáo các tình huống không có chuyên môn giải quyết xảy ra với quản lý nhà hàng.
* Hướng dẫn nghiệp vụ cho nhân viên thực hiện đúng theo quy định của nhà hàng.
* Báo cáo công việc hàng ngày cho quản lý nhà hàng.

### Tổ chức bộ phận bếp

#### Sơ đồ tổ chức



Hình 1‑2:

#### Mô tả chi tiết công việc của các bộ phận chính

**Bếp trưởng**:

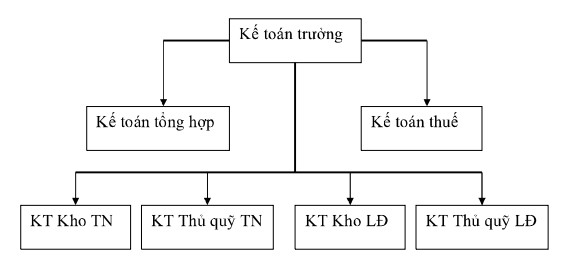
* Kiểm tra nhiên liệu, thực phẩm tồn để xác định số lượng hàng hóa, nguyên liệu cần nhập.
* Thông báo các món ăn phục vụ cho các nhân viên năm rõ
* Bố trí công việc hằng ngày trong nhà bếp, chỉ đạo, điều hàng toàn bộ nhân viên bếp.
* Tư vấn món ăn cho khách hàng nếu có yêu cầu.
* Tiếp nhận order của khách hàng
* Hỗ trợ nhân viên khi nhân viên gặp khó khăn.
* Kiểm tra, giám sát quá trình nhân viên làm và chế biến món ăn.
* Khắc phục các sai sót của nhân viên.
* Kiểm tra số lượng, chất lượng món ăn, đảm bảo món ăn đã được chuẩn bị và chế biến theo đúng quy trình, thời gian, số lượng phù hợp yêu cầu về an toàn vệ sinh thực phẩm.
* Giải quyết các trường hợp định lượng, chia, chuyển, trang trí thức ăn không đúng với yêu cầu của khách hàng, tiêu chuẩn của nhà hàng.
* Kiểm tra hệ thống trang thiết bị trong khu vực bếp.
* Tổng hợp các hóa đơn trong ngày, báo cáo chuyển cho thu ngân.
* Đào tạo kỹ năng, nghiệp vụ cho nhân viên mới.
* Đánh giá hoạt động của nhân viên, từ đó có quyết định thưởng phạt.
* Định kỳ mỗi tuần, mỗi tháng gửi báo cáo cho quản lý nhà hàng về kiểm kê công cụ, dụng cụ nhà bếp.
* Đề xuất các ý tưởng nâng cao chất lượng phục vụ.
* Nhân viên bếp.

**Nhân viên bếp**:

* Vệ sinh tủ đựng thực phẩm, sắp xếp thực phẩm, nguyên liệu trong tủ gọn gàng, ngăn nắp, đúng vị trí.
* Trực tiếp kiểm tra hệ thống bếp, đèn, thông gió … đảm bảo các hệ thống vận hành tốt trước giờ phục vụ và tắt hết sau khi không còn phục vụ.
* Kiểm tra nguyên vật liệu trước khi nhập theo phân công của bếp trưởng.
* Trực tiếp tham gia chế biến, trang trí món ăn được phân công.
* Báo cáo tình trạng thực phẩm, nguyên vật liệu, trang thiết bị cho bếp trưởng.
* Bảo quản giữ gìn máy móc, thiết bị nhà bếp định kỳ 1 tháng/lần.
* Hỗ trợ bếp trưởng kiểm kê.
* Đề xuất các biện pháp khắc phục nhằm hạn chế các sai sót xảy ra.
* Đào tạo, hướng dẫn kỹ năng nghiệp vụ cho nhân viên mới.

### Tổ chức bộ phận phòng kế toán

#### Sơ đồ tổ chức



Hình 1‑3:

#### Chức năng của phòng kế toán

* Thực hiện những công việc về nghiệp vụ tài chính kế toán đúng theo quy định của Nhà nước về chuẩn mực và nguyên tắc kế toán.
* Theo dõi, phản ánh sự vận động vốn kinh doanh của nhà hàng dưới mọi hình thái và cố vấn cho ban lãnh đạo các vấn đề liên quan.
* Thu thập và xử lý thôn tin có liên quan đến nghiệp vụ kinh tế tài chính phát sinh trong nhà hàng.
* Giữ bí mật về số liệu kế toán – tài chính và bí mật kinh doanh của nhà hàng.
* Báo cáo, tổng hợp các hoạt động về kinh tế tài chính cho ban lãnh đạo của nhà hàng.

## Quy trình nghiệp vụ, quy định chung trong quản lý của nhà hàng

### Quản lý kế hoạch của nhân viên

#### Mục đích

* Đảm bảo việc triển khau và kiểm soát công việc theo nhiệm vụ và công việc được giao.
* Đánh giá sự hiệu quả thực hiện công việc.

#### Nội dung

### Về phần đặt tiệc của khách

Khi khách đặt tiệc đến sẽ gặp lễ tân để đặt tiệc trước, lễ tân sẽ lấy ghi phiếu yêu cầu của khách hàng về số lượng bàn, yêu cầu món ăn, ước tính bao nhiêu người tham dự, ... Nhân viên lễ tân sẽ liên hệ với một quản lý trong trường hợp tiệc lớn để gặp gỡ với khách hàng, quản lý buổi tiệc sẽ bàn về những quy định thỏa thuận của nhà hàng với khách hàng.

Sau khi đã lấy yêu cầu xong, quản lý sẽ bàn giao phiếu yêu cầu 1 cái cho bên lễ tân , 1 cái cho cho bên nhà bếp, 1 cái cho bên thu ngân.

Nếu trong quá trình diễn ra tiệc, nếu khách đặt tiệc cần thêm bàn thì nhà hàng sẽ ghi một phiếu mới và đính kèm chung với phiếu cũ.

Nhân viên thu ngân sử dụng chương trình trên máy tính để tính tiền toàn bộ chi phí buổi tiệc mà khách hàng đã đặt, in hóa đơn chi tiết, trên hóa đơn có thanh toán có ghi ngày giờ thanh toán, tên quản lý lấy yêu cầu khách hàng.

Quản lý sẽ đem hóa đơn đó đưa cho khách đặt, nếu khách không có gì thắc mắc thì khách sẽ trả tiền cọc trước 50% cho nhà hàng, để nhà hàng lên kế hoạch chuẩn bị tiệc, 50% còn lại sẽ trả sau buổi tiệc kết thúc. Quản lý đặt tiệc sẽ đem tiền và hóa đơn vào cho quầy thu ngân, nhân viên thu ngân đóng dấu đã thanh toán một nửa vào hóa đơn và xác nhận với quản lý lên kế hoạch chuẩn bị.

Hầu hết các nghiệp vụ quản lý và thanh toán đều được thực hiện theo cách thủ công, gây chậm trễ, phức tạp, nhiêu khê cho khách đặt tiệc.

## Mô tả bài toán

**TÀI LIỆU THAM KHẢO**

**Tiếng Việt**

**Internet**

1. https://techtalk.vn/ki-thuat-tan-cong-cross-site-scripting.html: Kỹ thuật tấn công XSS

**Tiếng Anh**

**Internet**

1. https://www.youtube.com/watch?v=qtWy3acRw5k: Session Hijacking using XSS - David Cox
2. https://www.youtube.com/watch?v=9tsAxnSAa2U: Windows Session Hijacking | GT Hacks 2017 - Root Said
3. https://www.owasp.org/index.php/Session\_fixation: Session fixation post
4. https://www.youtube.com/watch?v=RCjHzMdOTTg: Session Fixation Attack - Andrew Sark
5. https://www.youtube.com/watch?v=1jncvd6JDoc: How ARP (Address Resolution Protocol) Works - Brian Pierce

**Sách:**

1. Certified Ethical Hacker - CEH v9 - Raymond Blockmon