WEBSITE VULNERABILITY

Mr. Sanjorn Keeratirungsan

Agenda

- Purpose
- Why Should I Care?
- Top 3 Vulnerability (For Website)
- Example Hacking & Solutions

Purpose

- Vulnerability Detection
- Website Hacking Prevention

WHITEHAT SECURITY WEBSITE SECURITY STATISTICS REPORT MAY 2013

HOW IT WAS CONDUCTED

WhiteHat's Website Security Statistics Report provides a one-of-a-kind perspective on the state of website security and the issues that organizations must address in order to conduct business online safely.

We asked WhiteHat Security customers to answer roughly a dozen survey questions abou their SDLC and application security program. W received responses to this survey from 76 organizations, and then correlated those responses with WhiteHat Sentinel website vulnerability data.

THE BIG PICTURE

86% ↑4%

of all websites had at least one serious* vulnerability during 2012.

The average number of *serious vulnerabilities per website was

56 from ↓79

*Serious vulnerabilities were resolved in an average of

193 DAYS

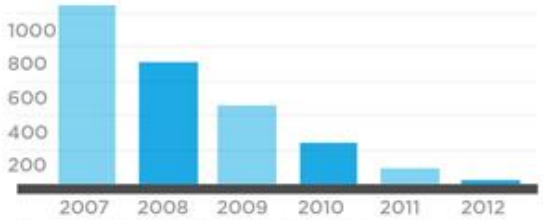
from first notification

61% ↓2%

of all *serious vulnerabilities were resolved

THE VULNERABILITIES

The number of *serious vulnerabilities discovered per site is decreasing



Vulnerability Historical Trend The annual average number of serious vulnerabilities discovered per website per year

INFORMATION LEAKAGE is the most prevalent vulnerability found with a likelihood of

55%

to have at least one *serious vulnerability appearing on a site

But CROSS-SITE SCRIPTING is the most frequently found *serious vulnerability

Overall Vulnerability Population (2012) Percentage breakdown of all the *serious vulnerabilities discovered (Sorted by vulnerability class)

THE INDUSTRIES

IT WEBSITES possess the most security issues with an average of

114

*serious vulnerabilities per site

QUICK FIX

	AVG DAYS
ENTERTAINMENT +MEDIA	33
GOVERNMENT	48
GAMING	67

fixed *serious vulnerabilities the fastest

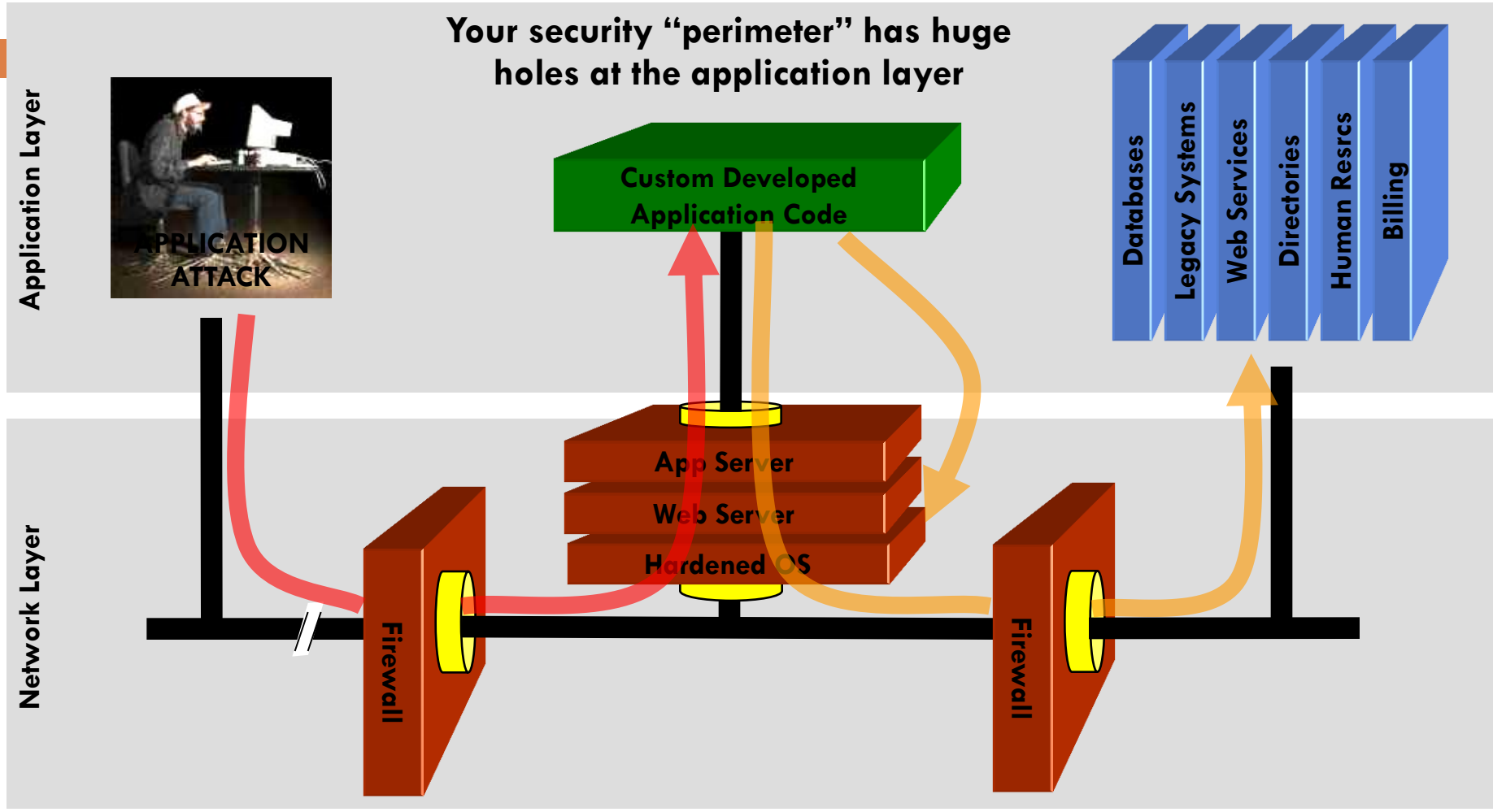
SLOW FIX

	AVG DAYS
EDUCATION	342
HEALTHCARE	276
INSURANCE	274

fixed *serious vulnerabilities the slowest

*Serious vulnerabilities are defined as those in which an attacker could take control over all, or a part, of a website, compromise user accounts, access sensitive data or violate compliance requirements.

Your Code is Part of Your Security Perimeter



You can't use network layer protection (firewall, SSL, IDS, hardening) to stop or detect application layer attacks

Consequences

- Disclosure of Database contents
- Root access to Website and Servers
- Loss of Access Control for users
- Secondary attacks from your site
- Defacement

Top 3 Vulnerability (For Website)

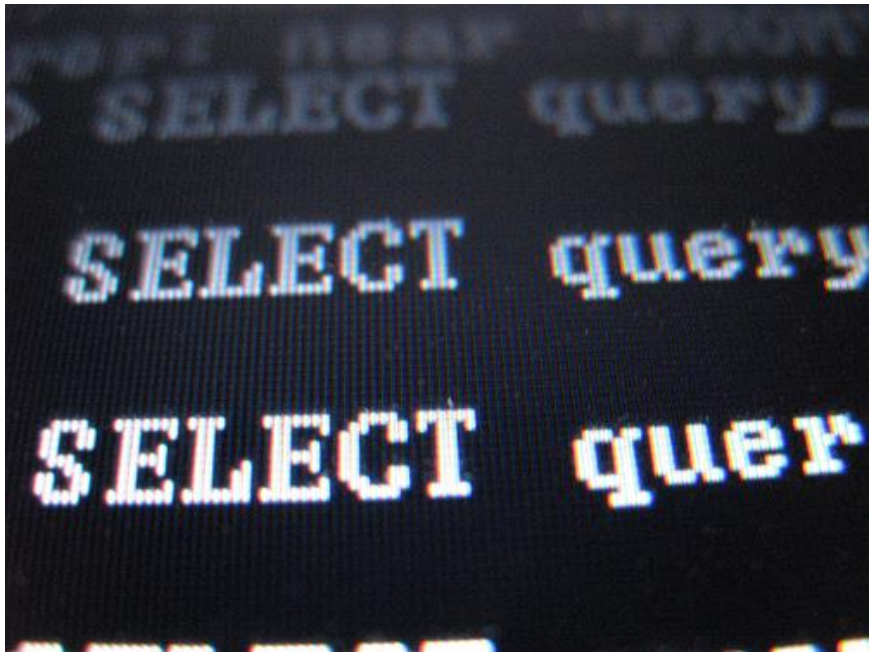
- SQL Injection
- Cross-Site Scripting (XSS)
- Unvalidated Parameters

** Base on OWASP
(Web Application Security Project)

SQL Injection

- SQL Injection : Code injection technique via SQL statements

- Very common with
  - *PHP*
  - *ASP*



SQL Injection - Example

- SELECT * FROM users WHERE id = '$id' and pass = '$pass'

Common Case

SELECT * FROM users WHERE id = 'admin' and pass = '1234'

SQL Injection

SELECT * FROM users WHERE id = 'admin';-- ' and pass = ''

SQL Injection - Solutions

- Use PHP Functions :
  - *stripslashes()*
  - *mysql_real_escape_string()*

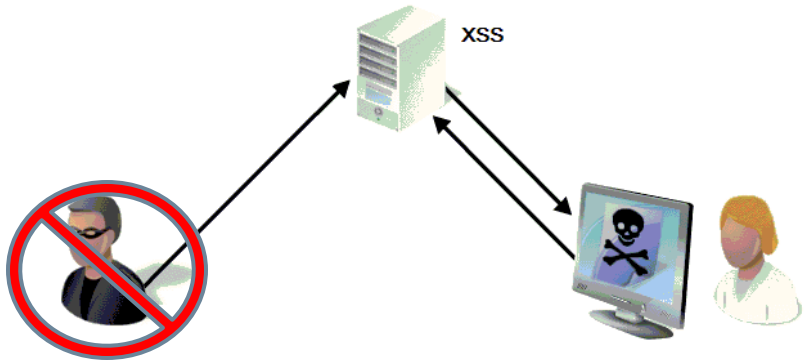
- Use Regular Expression :
  - *[^\n]+(\%3D)|(=))|(\%27)|(\')|(\-\-)|(\%23)*

XSS (Cross-Site Scripting)

- XSS : Web browsers execute code sent from websites
  - *JavaScript*
  - *Flash*
- Type of XSS
  - *Stored*
  - *Reflected*

XSS - Solutions

- Use PHP Functions :
  - *stripslashes()*
  - *mysql_real_escape_string()*
  - *htmlspecialchars()*



- Use Regular Expression :
  - */((\%3D)|(=))[^\n]*((\%3C)|<)[^\n]+((\%3E)|>)*

Unvalidated Parameters

- Attackers can tamper with any part of an HTTP request to try to bypass

- Example
  - Use data from URL (GET Function)
  - Command Execution (shell_exec Function)

Unvalidated Parameters - Solutions

- Ensure that all parameters are validated
  - Data type (string, integer, real, etc...)
  - Specific patterns (regular expressions)
  - Minimum and Maximum length
  - The parameter is required or not
  - Duplicates are allowed
  - Allowed character set
  - Null is allowed
  - Numeric range

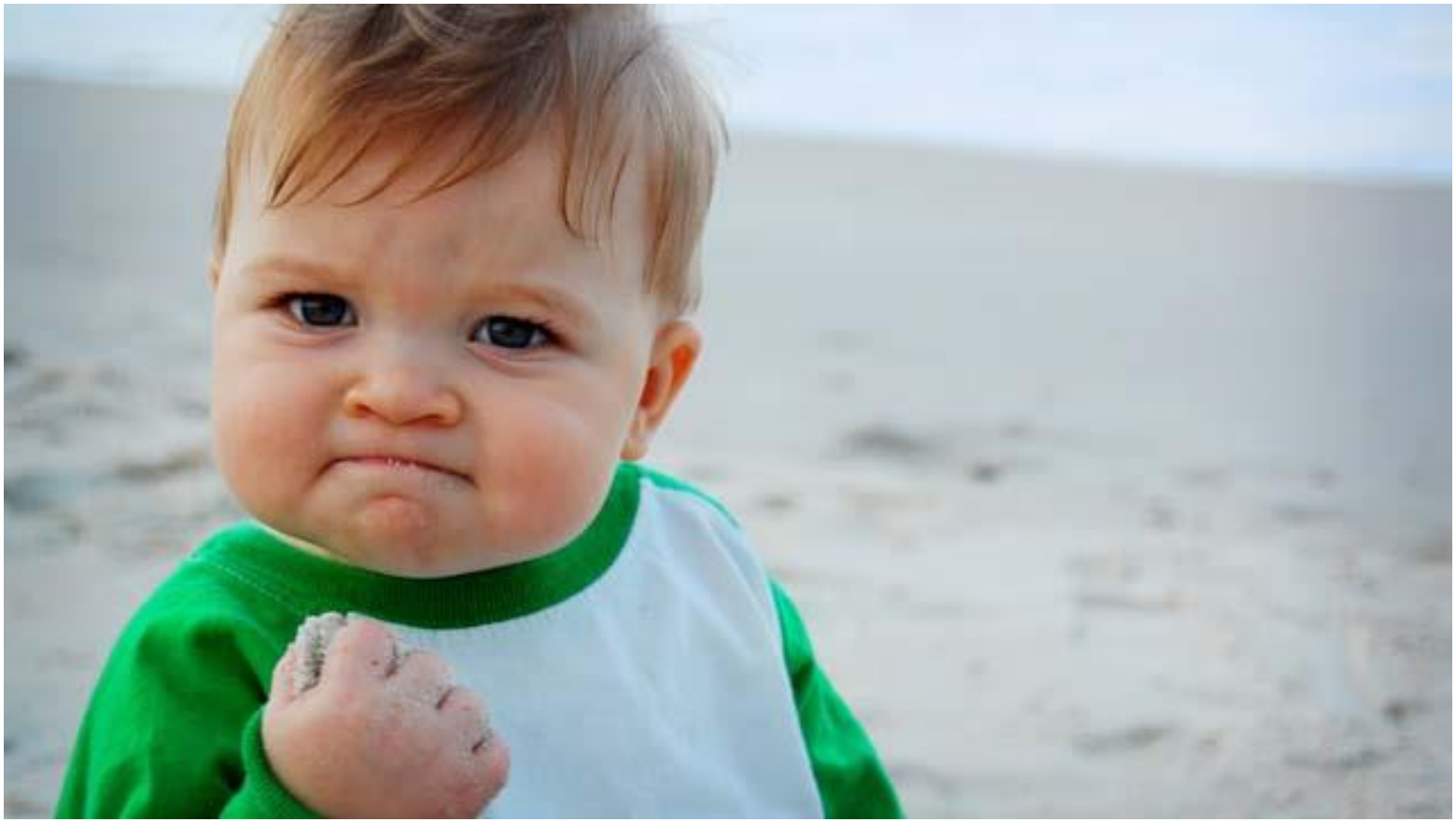
Password Management

- Password (In database)
  - Encryption + Salt

- Change Password
  - Must authenticate with Current password

Hackers Are Everywhere!!

But We Can Stop Them!



Instructor

Mr. Sanjorn Keeratirungsan (Coke)

Project Manager

AttoDreams Ltd.,Part.

sanjorn.k@attodreams.com

Q & A