

# Securing Web Applications

## Art, Passion and Character

Rajkumar Pandian Sakthivel  
Lakshmi Narayanan Narasimhan  
HCL Technologies Ltd

## Users' (your) Perspective\*

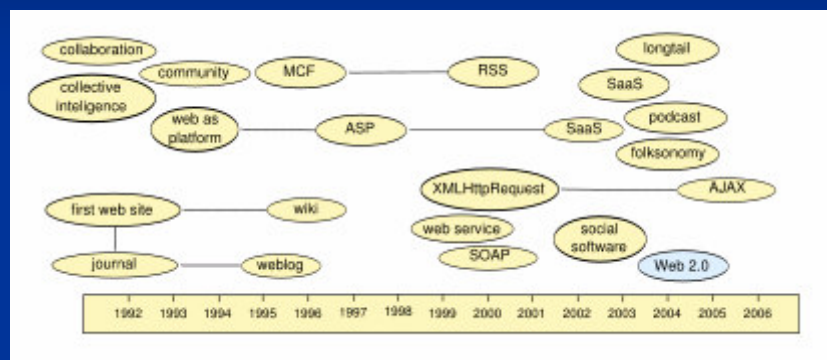
- You have just logged to your “Internet Banking” web site.
- Few minutes later, you get an email on a web attack against all banking web sites.
- ***You get email from your bank that their web site is immune to the recent attack.***
- ***What if the web site is fragile to the attack?***
- As an user, what's your thoughts on both the scenario?

\* Imaginary case study but quite possible

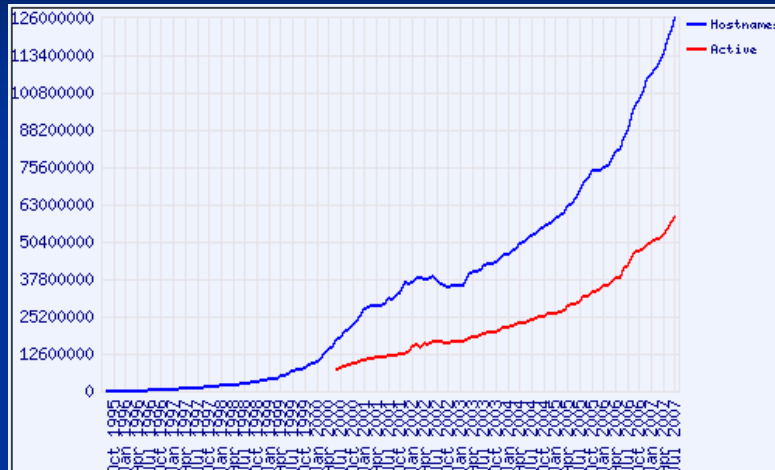
## Agenda

- Web Applications & Trends
- Threat Classification
- “panic & patch” approach
- SDLC Practices
- Penetration Testing
- Security Standards
- Looking ahead

## Web Technologies



## Growth of Web Applications



## Webapps and Security

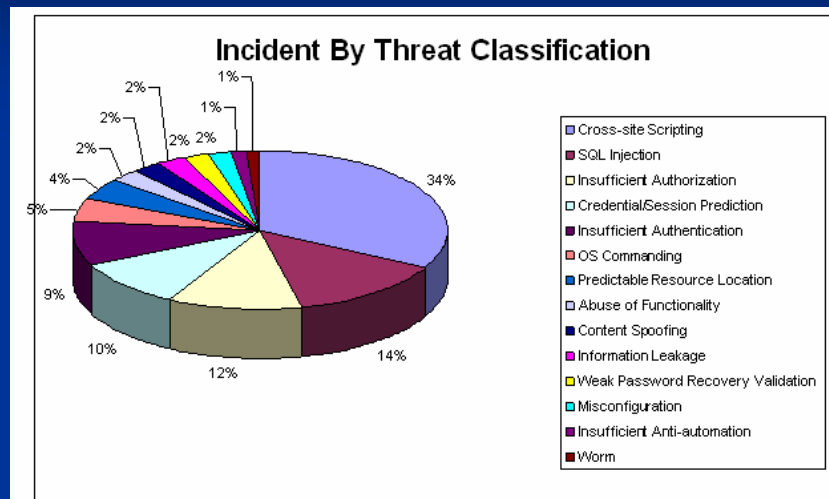
- The majority of web applications is built for layman
- Web applications once deployed in the Internet will be universally accessible
- Securing Web application with Firewall/IPS is very hard/impossible
- Attacking web applications is much simpler than attacking standalone application

## Attacking Web Apps – How Simple?

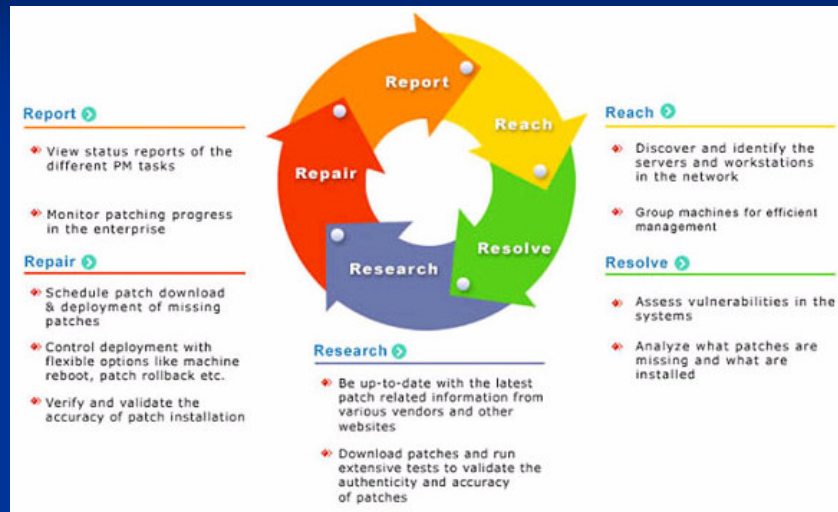
Delete	Books in your Shopping Cart	Qty.	Rate (Rs.)	Amount
Ⓢ	<b>HACKING EXPOSED</b> By KURTZ	<input type="text" value="-10"/>	355.50	<b>-3,555.00</b>
Ⓢ	<b>HACKING EXPOSED 3/ED W/CD</b> By MCCLURE	<input type="text" value="-20"/>	355.50	<b>-7,110.00</b>
<input type="button" value="Update Quantity"/>			Sub-Total: <b>Rs. -10,665.00</b>	
<small>If you have changed any quantity, click above link to update the cart.</small>				
<input type="button" value="Check Out"/>				

Most of the websites don't  
 validation or do at wrong place ☹

## Web Attacks

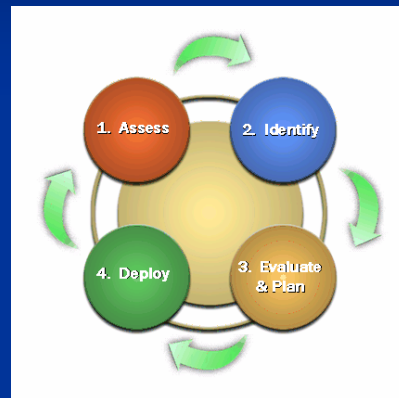


## “panic & patch”



## Patch Management

- Patch has to be supplied at correct time
- Any delays will lead to heavy financial losses
- Increased operational costs even if it is delivered on time.
- Loss of reputation
- Affect businesses (downtime)



## Security in SDLC

- Your product has security by design.
- You don't choose security by pressure but by choice
- Increased profitability
- It is easier to fit security in SDLC
- Security is a component not a plug-in
- Thinking ahead of attackers

## Requirements

- What is the expected behavior of the system?
- Non-Repudiation
- Cryptographic support
- User Data Protection
- Identification and Authentication
- Privacy
- Resource Utilization
- Trusted Path/Channel

## Design

- Specify assumptions
- Identify possible attacks
- Architectural Risk Analysis
- It is good to know and grade architectural flaws
- Not knowing them is flaw
- Example
  - HTTPS traffic is secured in transit
  - HTTP is unsecured and clear text protocol

## Implementation

- Following secure coding practices
- Automatic source code inspection
  - Discover low hanging fruits
  - Reiterate
- Manual code review to identify vulnerabilities
  - Domain specific
  - Application specific
  - Language specific
  - Platform/Environment specific

## Testing

- Approaching testing as functional testing
  - Input and Output Validation
  - Authentication
  - Session Management
- Doing risk based security testing
  - Fuzzing
  - Abuse Testing
  - Attack Patterns

## Penetration Testing

- Tested by experts in Live Environment
- System will be studied carefully and then attacked
- Simulates the scenario of a cracker attacking the system
- A final report on vulnerabilities, assessment of the impact and technical solution will be reported

## What it takes to follow?

- Initiative and Interest
- Ability to think and act like the attackers
- Endurance to detect vulnerabilities
- Technically savvy
- Researching vulnerability pattern
- Collaborating with others
- Openness to accept deficiencies

## Security Vs Functionality

*"So now, when we face a choice between adding features and resolving security issues, we need to choose security." -Bill Gates*

*If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.*

*-Bruce Schneier*

## Useful Resources

- Forums
  - Web Application Security Consortium
  - Open Web Application Security Project
- Books
  - Hacking Web Applications Exposed
  - How to Break Web Software
  - Software Security: Building Security In

## Q & A

Thanks a lot