Ng Wee Kai
Senior Security Consultant
PulseSecure Pte Ltd

About PulseSecure

- IT Security Consulting Company
- Part of Consortium in IDA (T)-606 Term Tender
- Cover most of the IT Security services:
  - Audit & Review
  - Assessment & Penetration Testing
  - Policies & Standards Development
  - Training
- Particularly strong in **Web Application, Ethical Hacking** and **Secure Code Review**

Our Accomplishments

- In 2008
  - Performed penetration test on over 60 applications
  - Conducted security training to over 1,500 customer users
  - Audited huge government infrastructure, over 26 government agencies with 40,000 stations
  - Awarded global assessment term contract from world leading top 5 Insurance Group
- Developed and published exploits codes such as *MITM* for bank's *2 factor authentication*
- Active participation in *Hack in the Box &* contribution to security articles

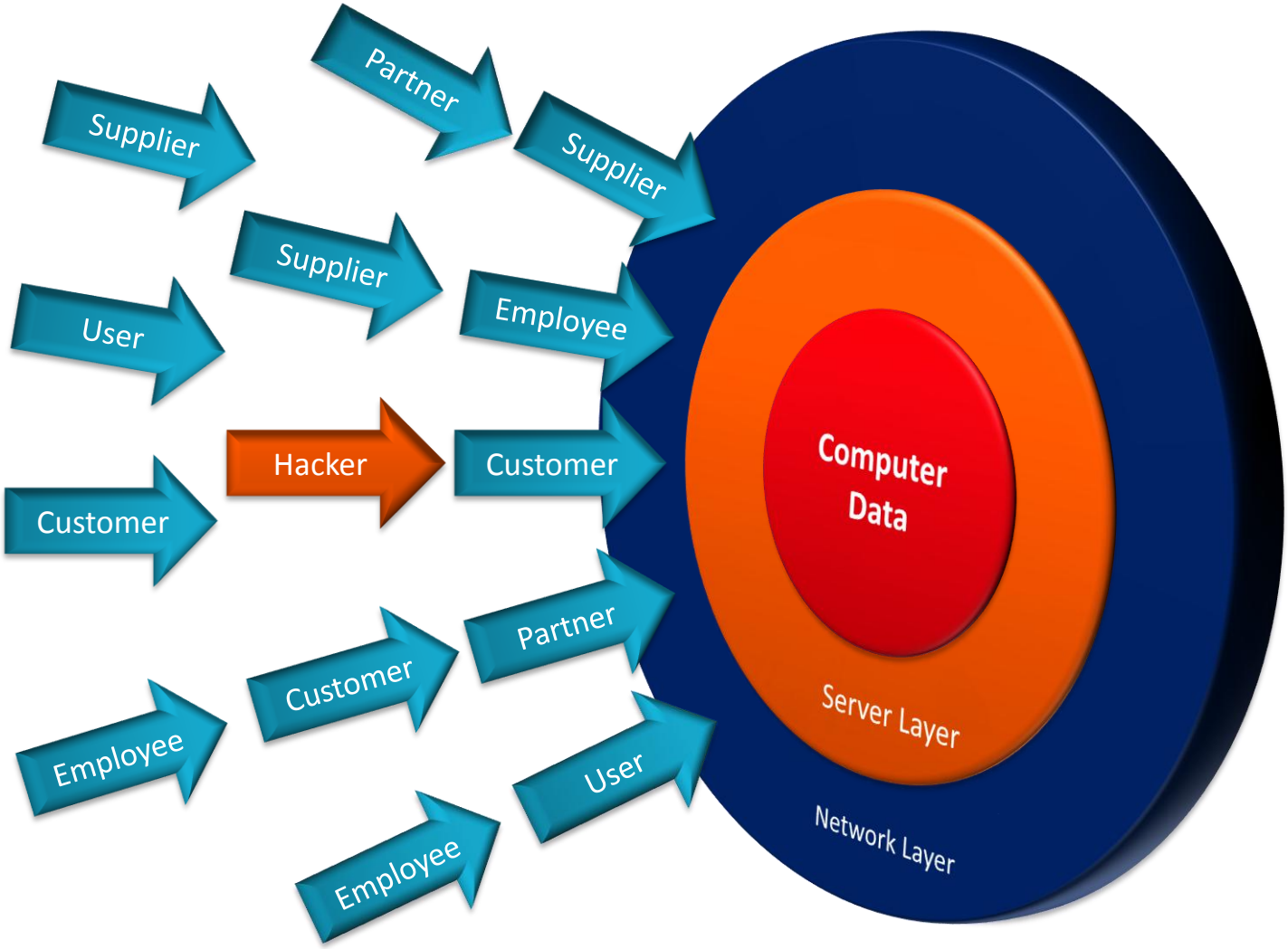
Agenda

- Hackers' New Target
- Why Are Web Application Attacks Getting Popular?
- What Is Needed To Exploit A Web Application?
- Increasing Institutional Pressure
- Demo of Attacks
- What Can You Do About This?
- Summary

What Are Web Applications

- Web applications have many non-traditional characteristics:
  - Uses HTTP protocol
  - Reliance on web browser
  - No intrinsic notion of a “session”
  - Standardized but optional security via HTTPS/SSL

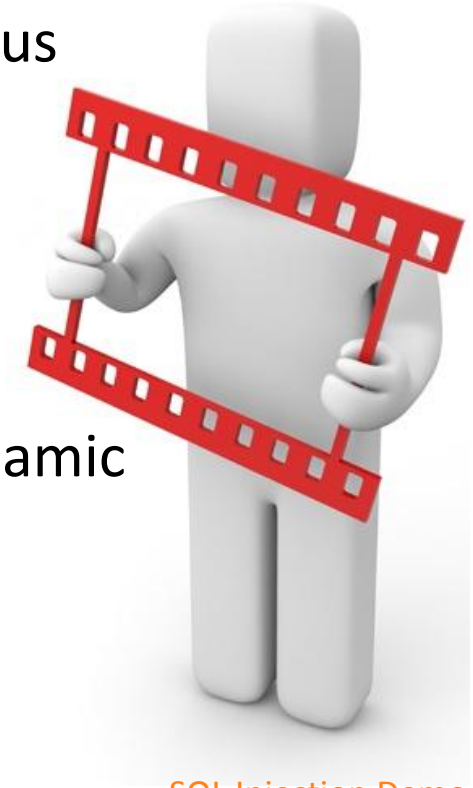
Web Applications Invite Public Access To Your Most Sensitive Data



SQL Injection Demo

- SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution.

- Occurs when external input is used in dynamic construction of database commands.



SQL Injection Demo

“For Profit” Hacking

What does the hacker desire?

- ~~Gaining Access to the network or executing arbitrary commands on servers.~~
- Perform some **application-level action** such as stealing personal information, transferring funds, or making cheap purchases.

New Wave of IT Security Threat

In 2008

- Gartner Group:
  - "Today over 75% of attacks against a company's network come at the Application Layer, not at the Network or System Layer."

Why Are Web Application Attacks Getting Popular?

Hackers Knows That Most Web Application Are Vulnerable!

- **70% of websites at immediate risk of being hacked!**
  - Accunetix – Jan 2007 http://www.acunetix.com/news/security-audit-results.htm
- **"8 out of 10 websites vulnerable to attack"**
  - WhiteHat "security report – Nov 2006" https://whitehatsec.market2lead.com/go/whitehatsec/webappstats1106
- **"Since 2008, more than 70% of all the vulnerabilities reported worldwide are web Application related and are mostly classified as trivially exploitable percent of hacks happen at the application."**
  - InforWorld
- **"64 percent of developers are not confident in their ability to write secure applications."**
  - Microsoft Developer Research
- **The battle between hackers and security professionals has moved from the network layer to the Web applications themselves.**
  - Network World

Web Attack “How-To” Is Easily Available

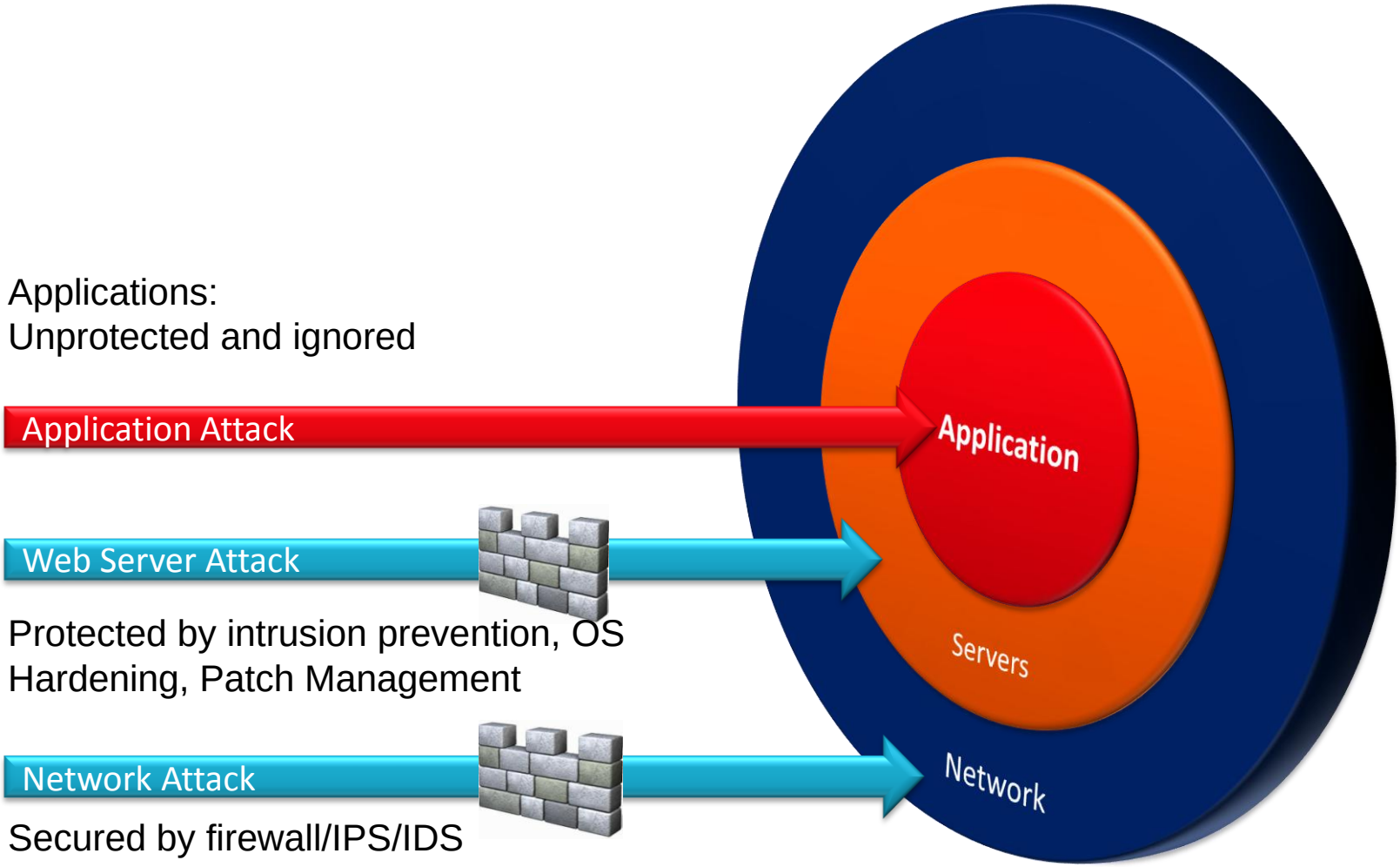
- A simple Google search results
  - “SQL Injection Techniques” – 2,260,000 web pages
  - “SQL Attack” – 30,141 Blogs
  - “SQL Attack Tools” – 322,000
  - “XSS Techniques” – 752,000 web pages
  - “XSS Attack” – 9,769 Blogs
  - “XSS Attack Tools” – 251,000 web pages

Attack Characteristics

- Web Attacks are Stealth
  - Incidents are not detected.
- Simpler Attack Vector
  - Traditional Technology that require compiler, system functions like C++, C, Java
  - Javascript, XML, CSS, HTML and forgiving browser
- Online services provide anonymous hosting
  - Less traceable
- Indirectly
  - Place traps so that victims are ensnared

Traditional Methods Do Not Protect You from Web Attack

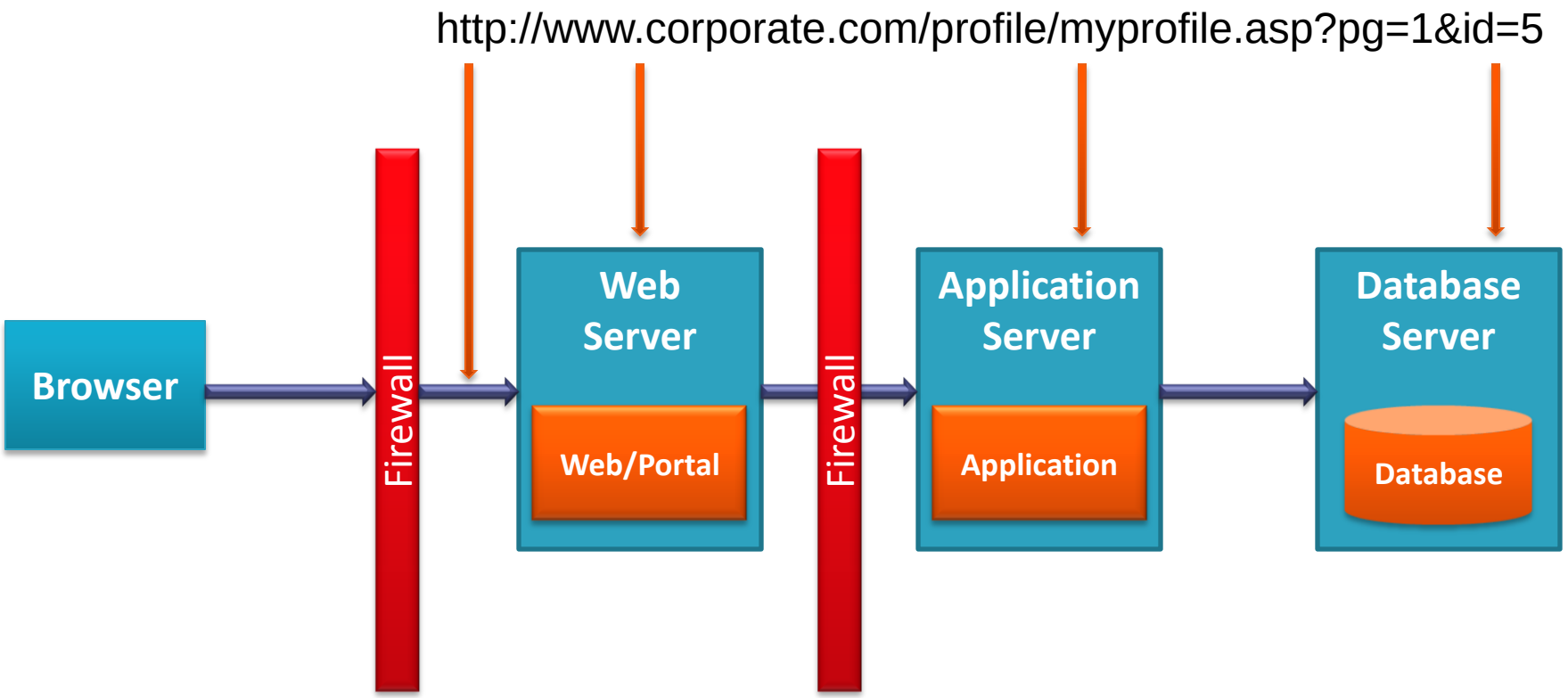
Applications:
Unprotected and ignored



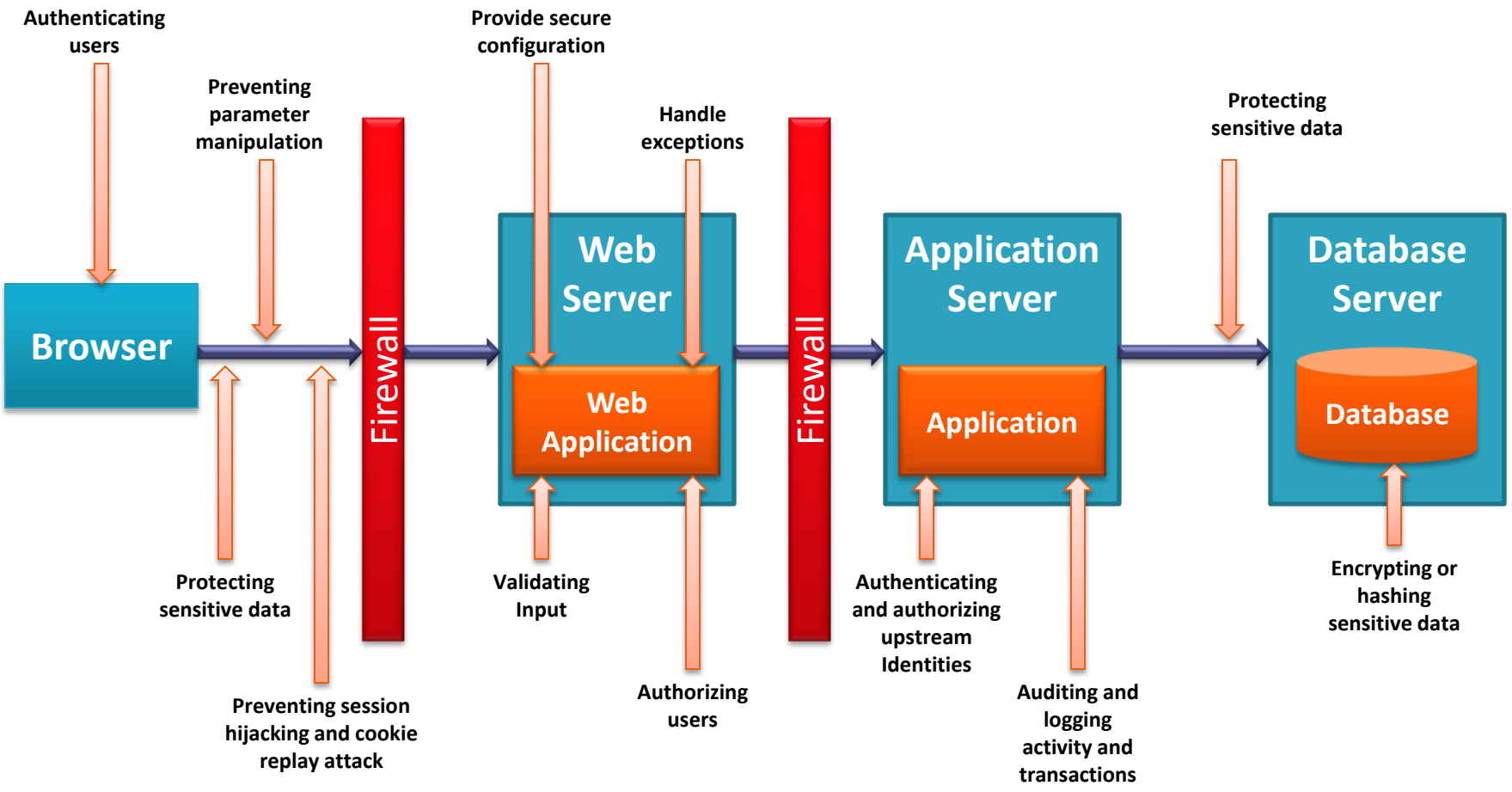
Protected by intrusion prevention, OS Hardening, Patch Management

Secured by firewall/IPS/IDS

Typical Web Application

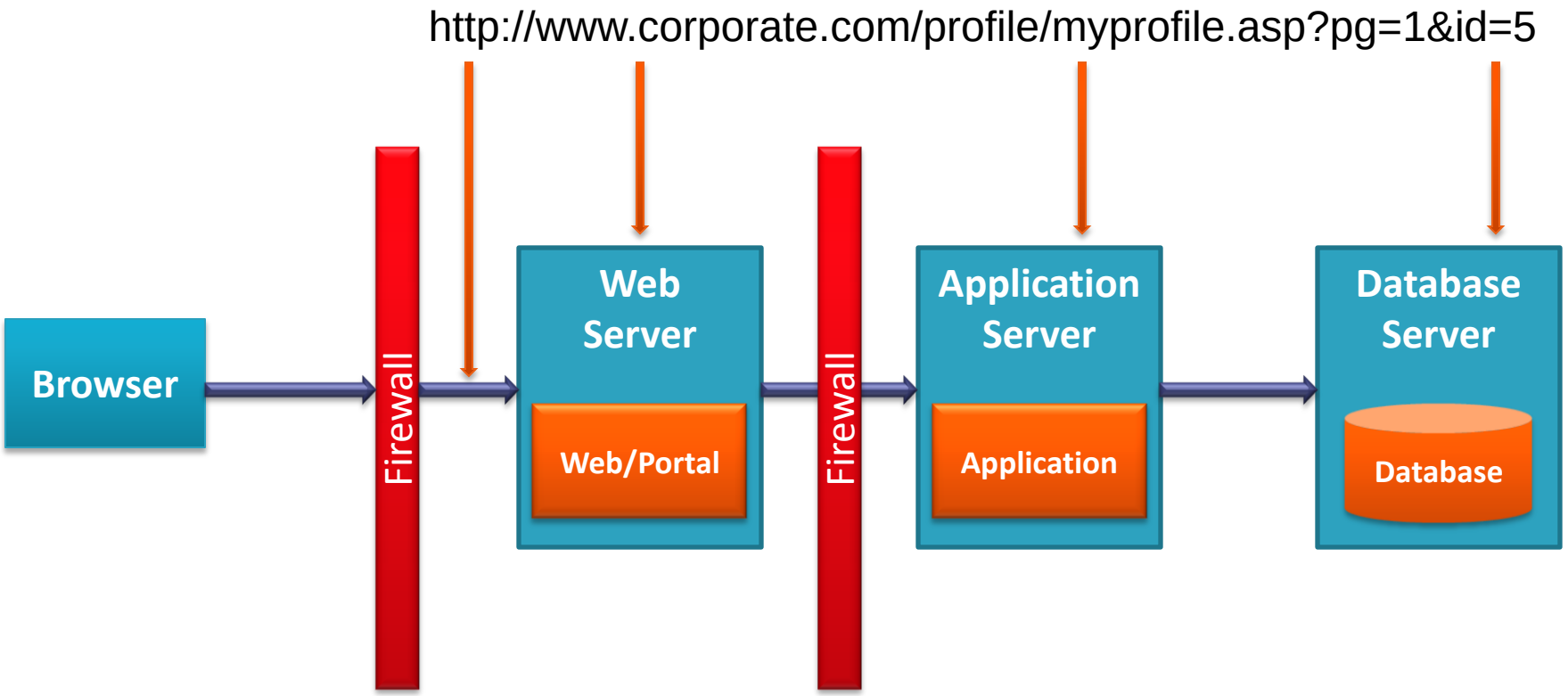


Typical Point of Attacks



What Is Needed To Exploit A Web Application?

URL is a Cruise Missile



New Form of Backdoor

Increasing Institutional Pressure

- There is an increasing institutional awareness of the fact that standards, which organizations must comply with, need to be determined.

- These institutional standards are appearing in both the public and private sectors and include:

PCI Security Standards

ISO27001

Sarbanes-Oxley Act

CMMI

Google Flagging

Etc…

Data security and your brand

- How much would your brand be worth if you lose your customers trust?
- Would your customers' stay with you?

Customer confidence seriously impacted by a data breach

In the case of a breach….

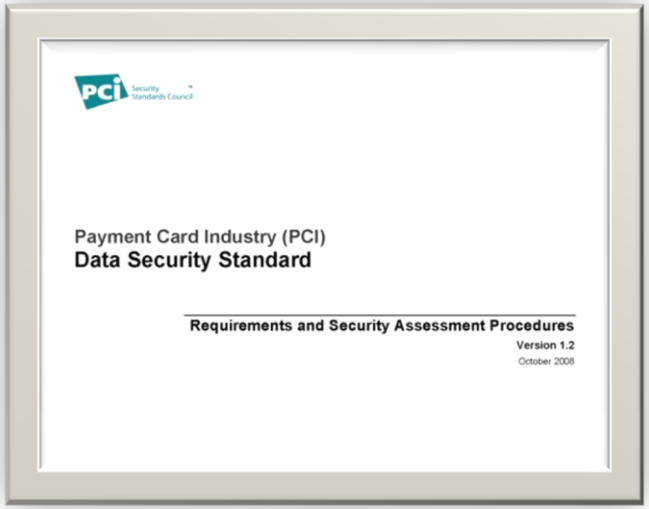
- 49% of customers believe merchants to be the most likely source of the data breach
- 3 out of 4 customers won't shop again at a compromised merchant
- 84% of customers want to shop at merchants who are security market leaders

Investing in PCI DSS should be part of your customer retention plans

The PCI Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a set of comprehensive requirements for enhancing payment account data security

- The PCI DSS is a multifaceted security standard that includes requirements for:
  - Security management
  - Policies and procedures
  - Network architecture
  - Software design
  - Other critical protective measures



- This comprehensive standard is intended to help organizations proactively protect customer payment data

6 Control Objectives and 12 Requirements

Build and Maintain a Secure Network	Install and maintain a firewall configuration to protect cardholder data
	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	Protect stored cardholder data
	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	Use and regularly update anti-virus software
	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Restrict access to cardholder data by business need-to-know
	Assign a unique ID to each person with computer access
	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	Track and monitor all access to network resources and cardholder data
	Regularly test security systems and processes
Maintain an Information Security Policy	Maintain a policy that addresses information security

6 Contr

Section 6.5: Develop secure web apps, cover prevention of OWASP vulnerabilities

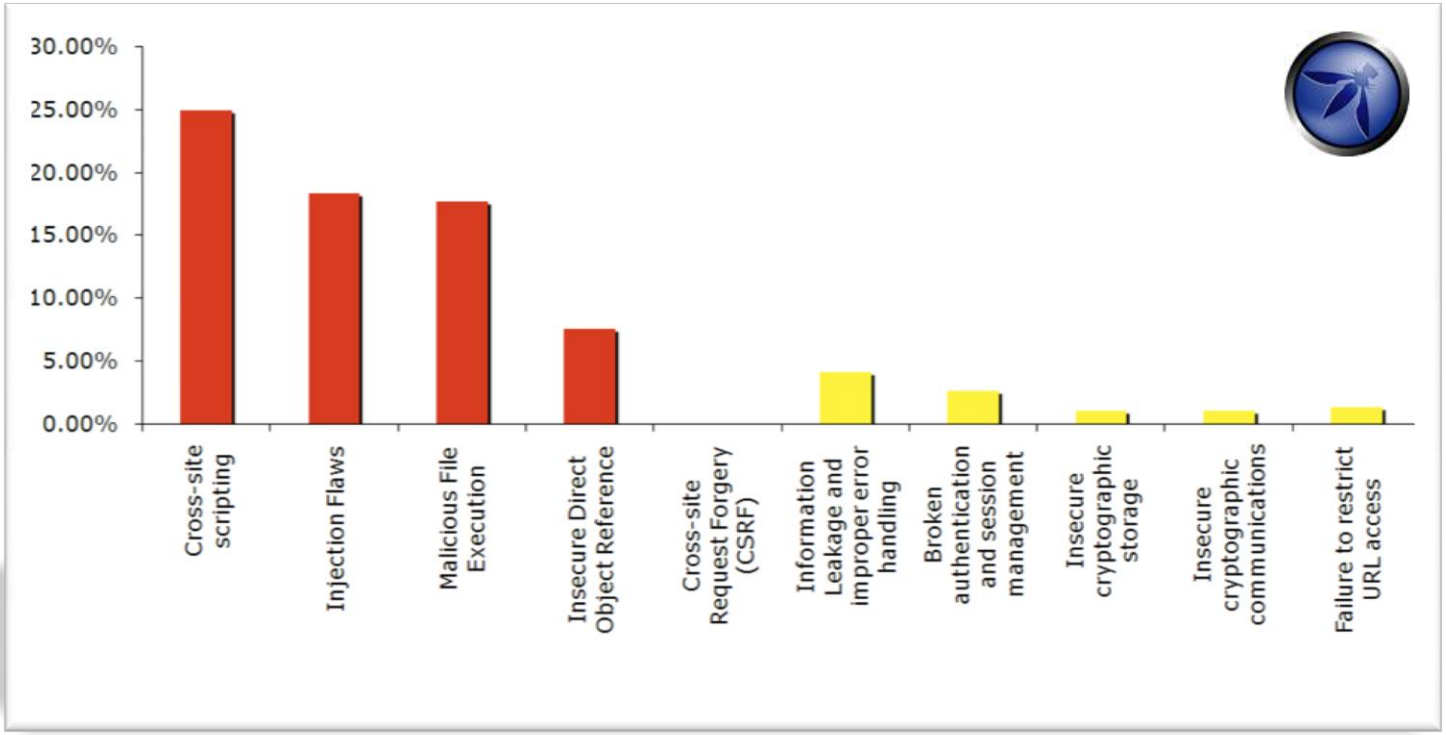
Section 6.6: Ensure all web-facing apps are protected against known attacks using either of the following methods

- web applications are reviewed at least annually and after any changes
- installing a Web App FW* to detect and prevent web-based attacks

Build and Maintain a Secure Network	
Protect Cardholder Data	
Maintain a Vulnerability Management Program	Use and re… anti-virus software
	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Restrict access to cardholder data by business need-to-know
	Assign a unique ID to each person with computer access
	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	Track and monitor all access to network resources and cardholder data
	Regularly test security systems and processes
Maintain an Information Security Policy	Maintain a policy that addresses information security

OWASP

- Emerging standards body
- Focus on application security
- OWASP top ten project



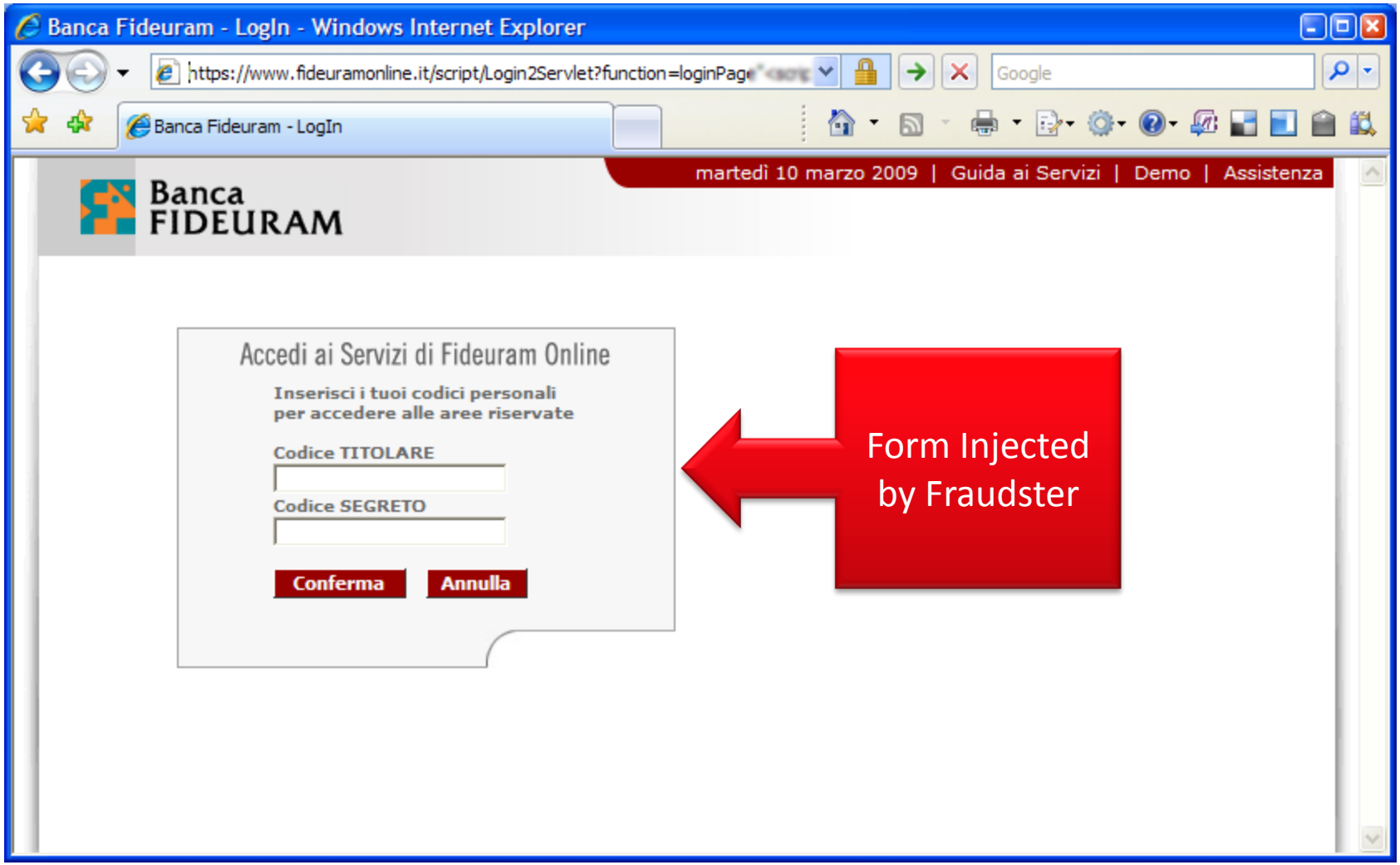
XSS Demo

- Occurs when web application uses input a user in output it generates without validating or encoding it

- Three known types of XSS
  - Reflected XSS
  - Stored XSS
  - DOM-Based XSS

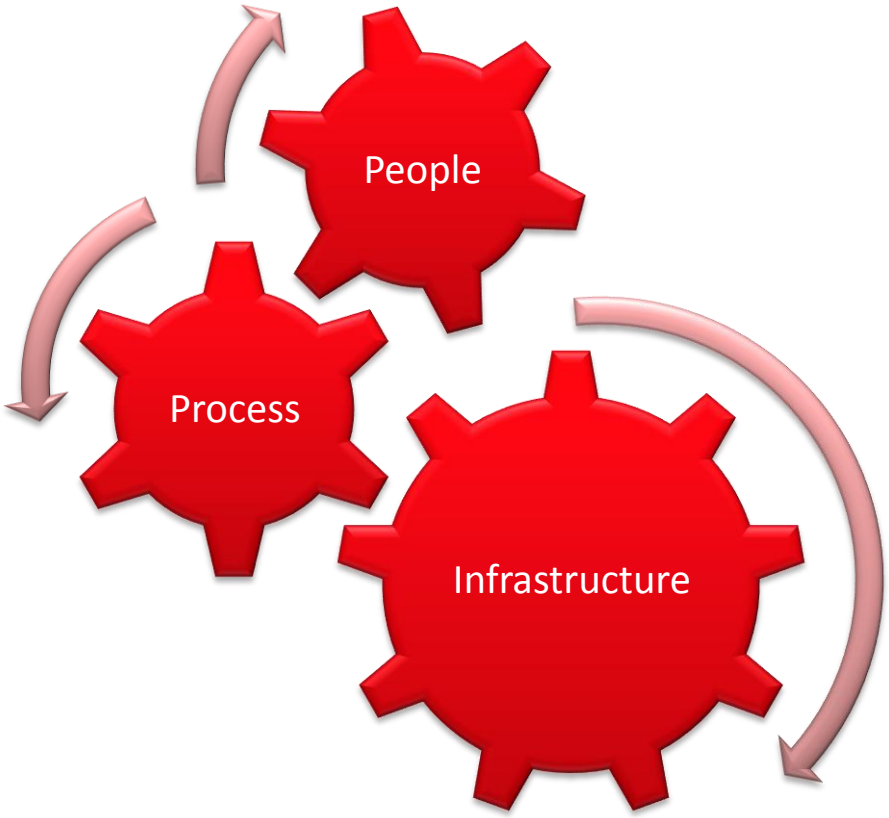
Reflect XSS Demo

Italian Bank XSS



Site Keeping Track of XSS

What Can You Do About This?



6 Control Objectives and 12

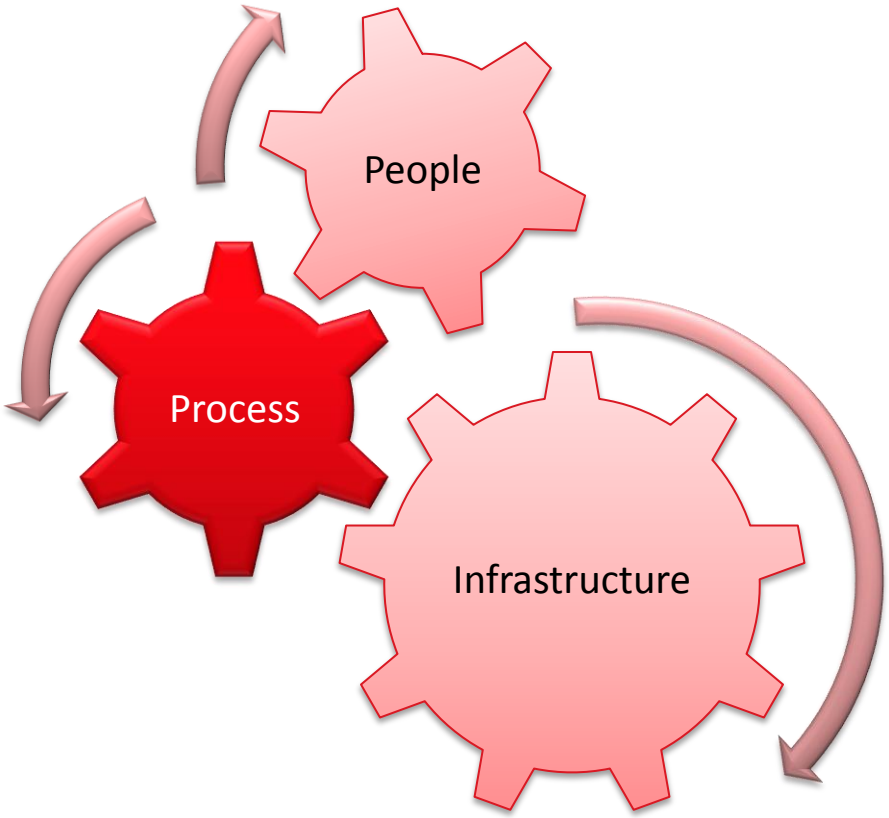
Section 6.5: Develop secure web apps, cover prevention of OWASP vulnerabilities

Section 6.6: Ensure all web-facing apps are protected against known attacks using either of the following methods

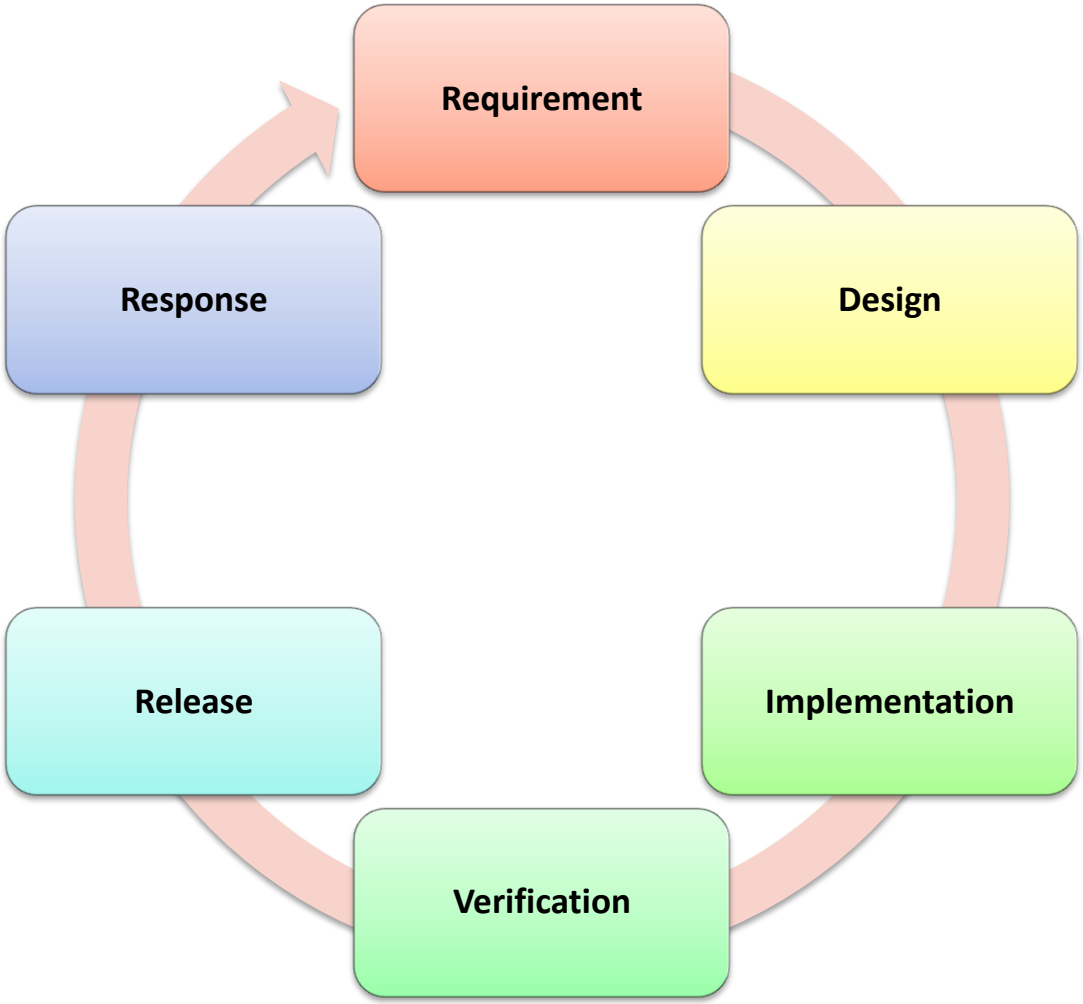
- secure coding practices
- installing a Web App FW*

Build and Maintain a Secure Network	
Protect Cardholder Data	
Maintain a Vulnerability Management Program	Use and update anti-virus software
	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Restrict access to cardholder data by business need-to-know
	Assign a unique ID to each person with computer access
	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	Track and monitor all access to network resources and cardholder data
	Regularly test security systems and processes
Maintain an Information Security Policy	Maintain a policy that addresses information security

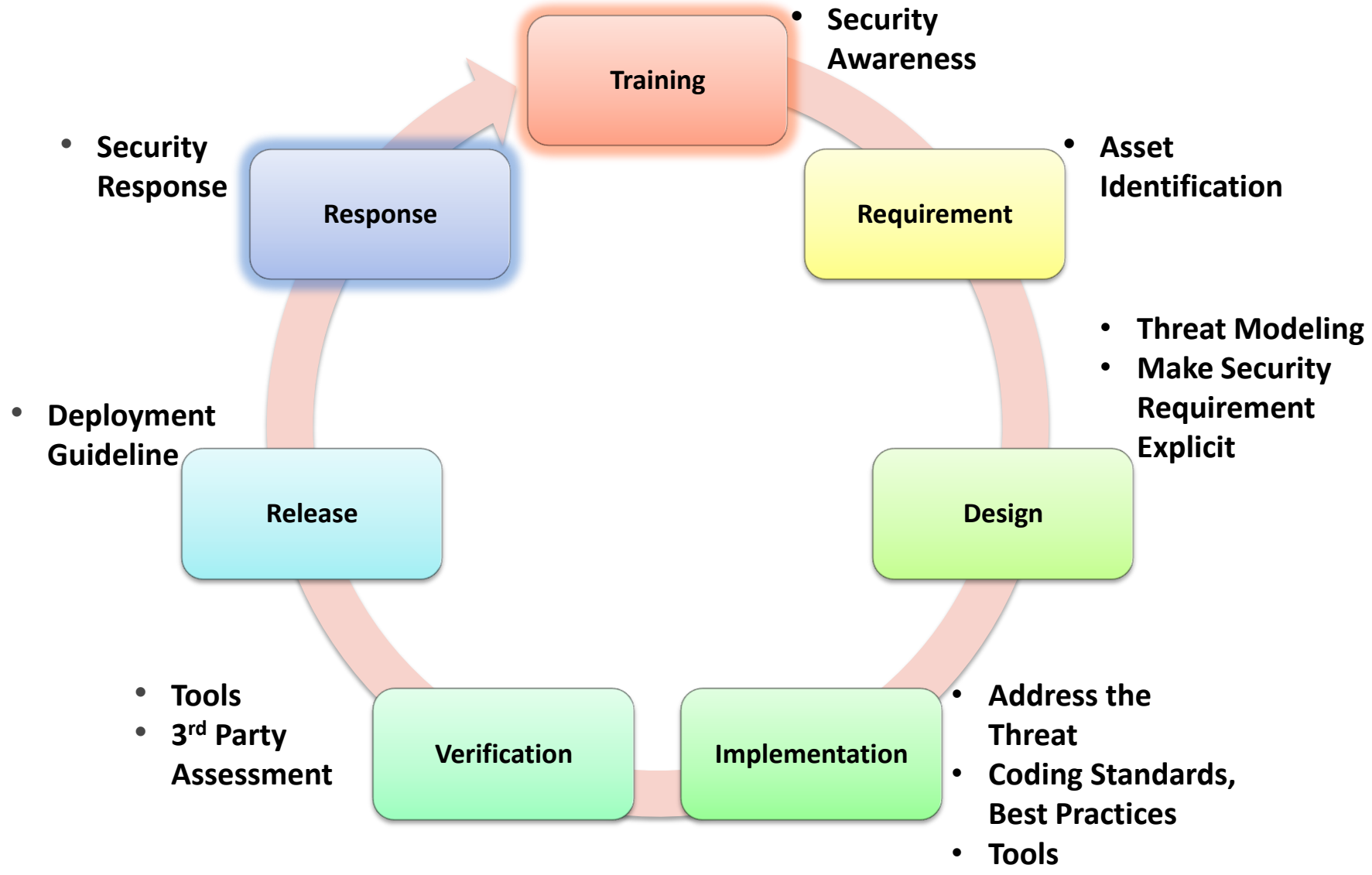
What Can You Do About This?



Traditional SDLC Focus on Features



Sec-SDLC



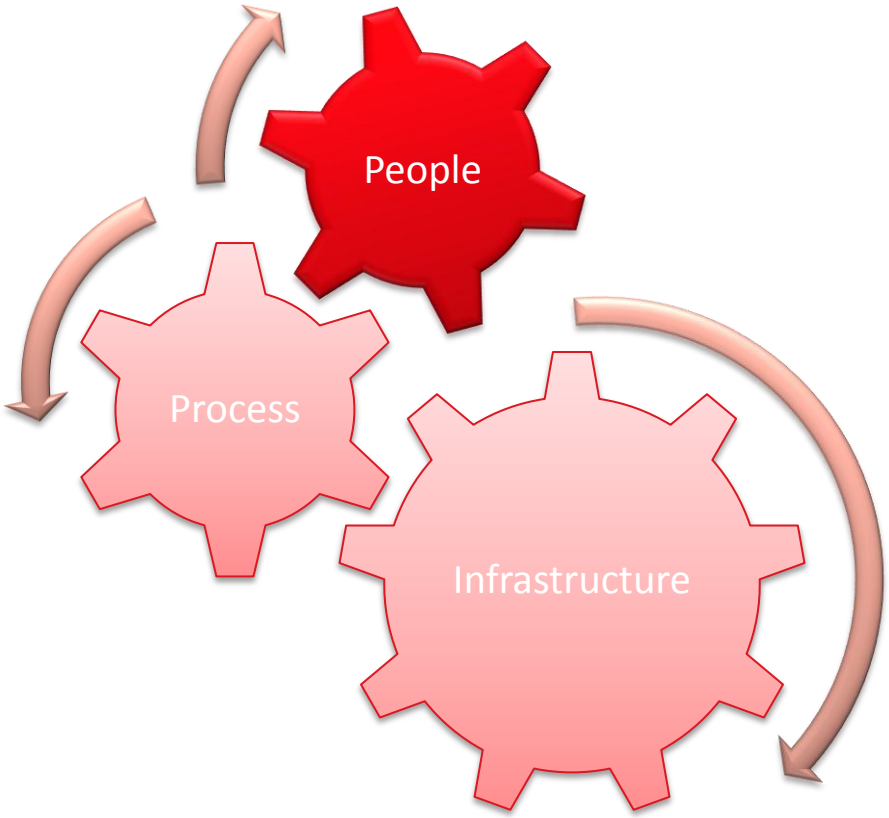
Assessment Tools

- White box assessment
  - Audit the code for insecure practice --- CodeSecure, Fortify
- Black box assessment
  - Test the application with know attacks --- Webinspect, Watchfire

Penetration Testing and Auditing

- Penetration Testing
  - Black Box/White Box approach
  - Insider/Outsider
- Auditing
  - Analyzing
    - Configuration Files
    - Architecture
    - Source Code
  - Policy Conformance
    - Operational Plans and Procedures

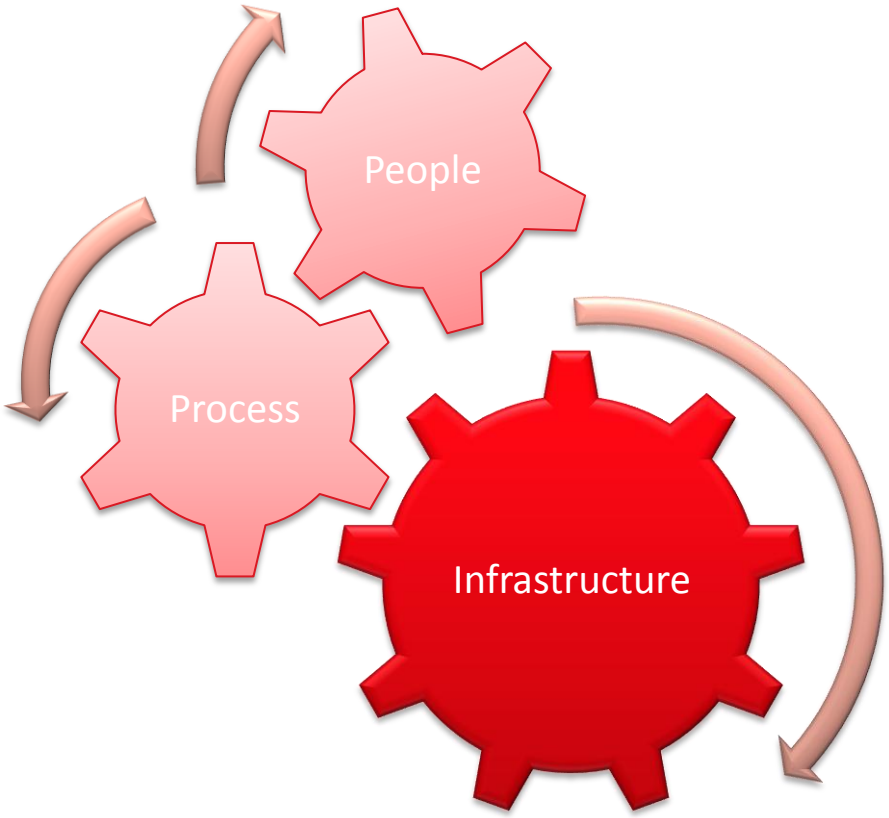
What Can You Do About This?



Developer-oriented Prevention

- Developers are increasingly seen as responsible for web application security
- The application must protect itself
- The developer must know how to include such protection in codes
- The developer must know the attacks
  - General principles
  - Variances

What Can You Do About This?



What are WAF

- New Type of Firewall to address this new threat
- Preventing attacks that network firewalls and intrusion detection systems can't, and they do not require modification of application source code

Advantage of WAF

- Protects in-house applications
- Protects third party applications
- Continuous security assessment
- Virtual Patching, giving you a window for change management
- Allows for separate roles for security officers

Summary

Moving Towards Securing Web Application

- Immediate
  - Assessment on critical applications
  - Consider protection while finding cost effective fixes to insecure code: WAF
- Mid term
  - Fills the gap with coding standards and guidelines
  - Refine SDLC process to include security
- Long Term
  - Build capability for continuous defense
  - Ensuring adoption of secure coding techniques

Contact

Email: weekai@pulsesecure.com

WebSite:www.pulsesecure.com

The End