# ColdFusion: Security
## SOTR 2009

create
manage
deliver

Tag:

# About This Presentation

- What is security
  - How to deal with XSS, CSRF and SQL Injection
  - Why do I need a cross domain file
- How does ColdFusion help us with security
  - What extras should we bring to the party
- How to code for security
  - How do I test for security
- The bigger picture
  - ISO27000, PCI, Data Protection Act

create
manage
deliver

# ColdFusion Security

## What is ‘Security’
## Why is it important

create
manage
deliver

Tag:

# Why Security Matters

## Drunken BOFH wreaks $1.2m in Oz damage

**Will retrain as chef**

When a former IT consultant knocked out a government system in Australia's Northern Territories, costing taxpayers $1.2m (Australian), he was drunk and upset that his fiancee had broken off their engagement.

## UK transport minister's website pwned

**Wrong kind of hats on the line**

The website of junior transport minister Paul Clarke was hacked over the weekend

## UltraDNS back online after DDoS assault

**Back off the canvas**

## XSS flaws poke ridicule at entertainment industry

**MPAA spanked by Pirate Bay backlash**

# Why Security Matters

- External threats
  - Viruses, worms, Trojans
  - 100,000+ ‘in the wild’
  - Spam
  - 80%+ of all e-mail
  - Now big business (botnets, blended attacks)
  - Hackers
  - Automated attacks
  - Now big business (botnets, zero-day attacks)
  - Cyber-crime
  - Phishing, identify theft, grand larceny
  - Fraud, cyber terrorism
  - Competitors
  - Malcontents, activists
- Internal threats
  - Fraud, error, unauthorized or illegal system use, data theft

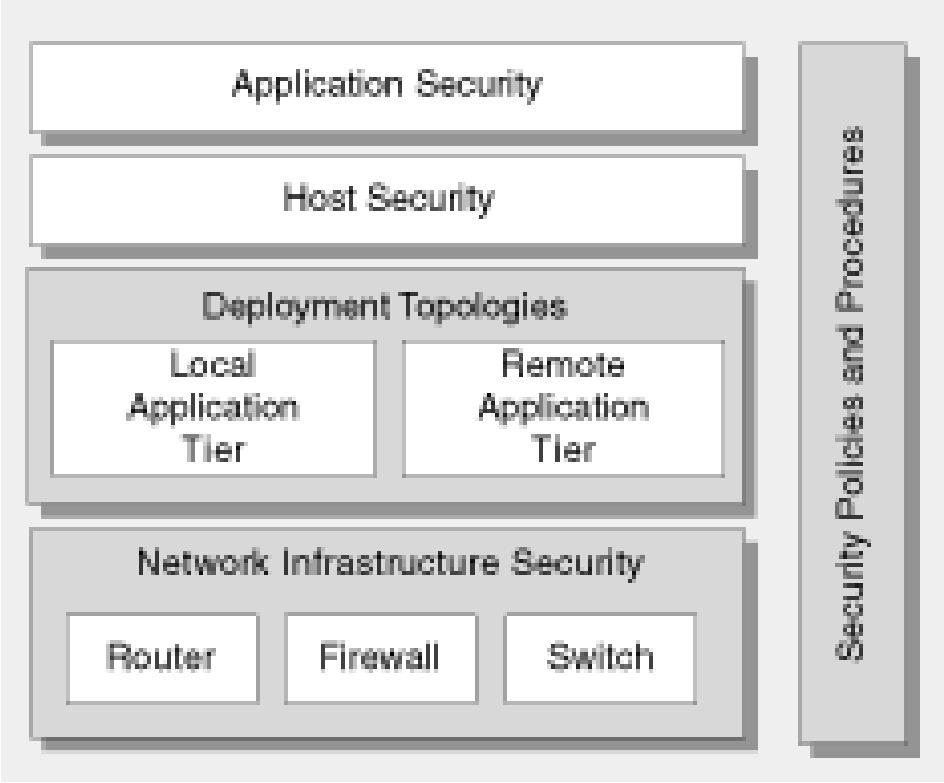
# Why Security Matters to You

- Negative Reasons
  - Don’t want Bad Press
  - Use of Credit Cards (PCI)
  - Penetration Testing
  - Compliance
    Sox, ISO27000, Data Protection Act etc
- Positive Reasons
  - We want to write good code
  - To get new business: RFIs RFQ etc

create
manage
deliver

# What is Security?

- **C**onfidentiality
- **I**ntegrity
- **A**vailability



# Security and the Data Protection Act

- Personal Data must be
  - Fairly and lawfully processed;
  - Processed for limited purposes;
  - Adequate, relevant and not excessive;
  - Accurate and up to date;
  - Not kept for longer than is necessary;
  - Processed in line with your rights;
  - **Secure**;
  - Not transferred to other countries without adequate protection.
- To comply, you will need to follow BS10012
- There are  28 breaches/month reported to the ICO
- The fines are about to become a lot more stringent

create
manage
deliver

# Security for PCI

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

create
manage
deliver

# Security for BSI and ISO

We need to address

- Security policy
- Organization of information security
- Resource management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition
- Information systems development and maintenance
- Information security incident management
- Business continuity management
- Compliance

create
manage
deliver

# Security and ISO27000

- ISO27000 defines a system of IS Management
  - 10 Categories to manage information security
  - 36 generic security goals
  - 127 concrete security requirements

- High level of Abstraction, Technology Agnostic
  - E.g. It specifies that input controls are needed
    it doesn't specify the controls need to protect against XSS
  - For specialised requirements it needs to be supplemented by industry standards E.g.
    PCI, COBIT. ITIL, CLASP, OWASP

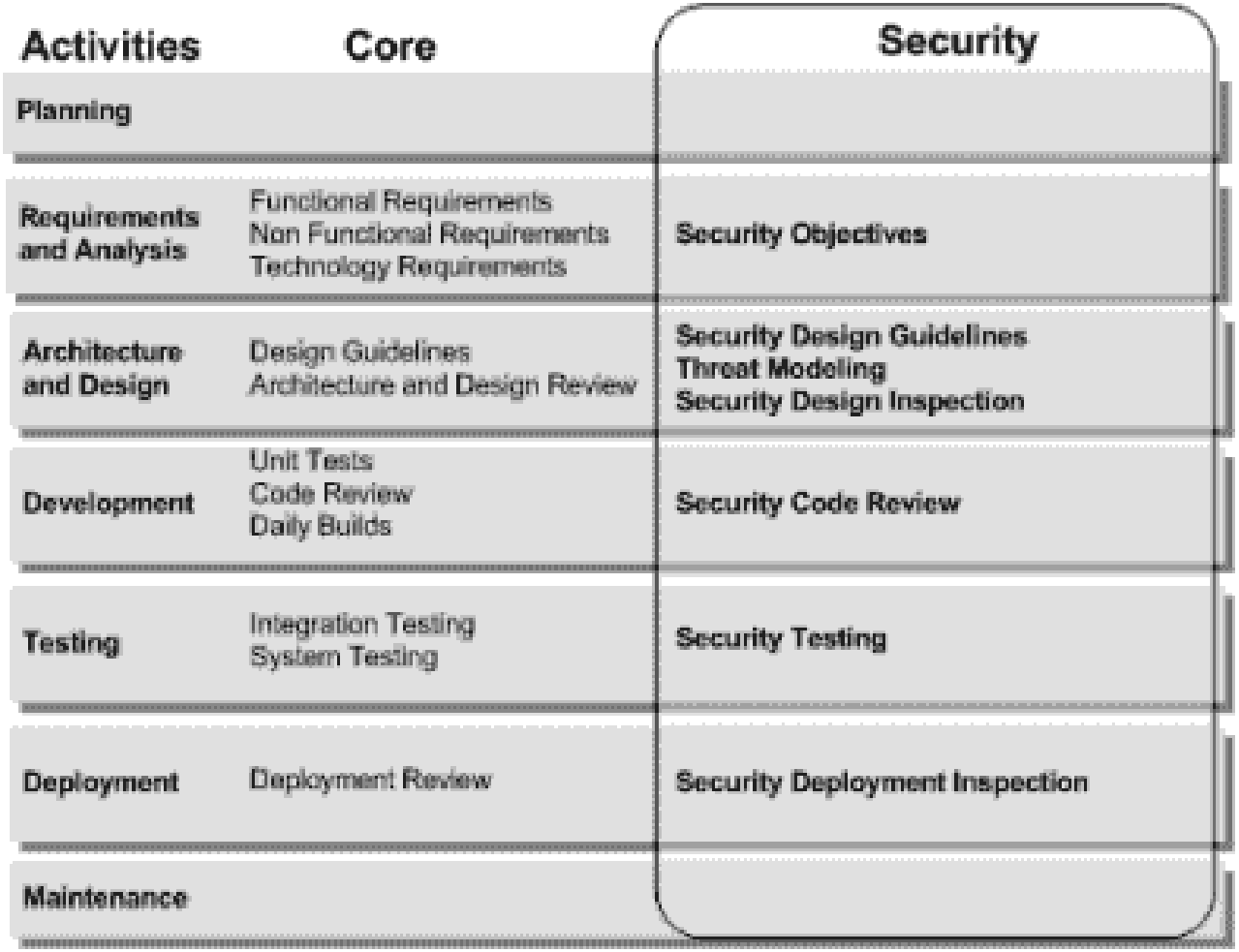
# ColdFusion Security

## So how ho we develop secure apps?

create
manage
deliver

Tag:

# Security Life Cycle



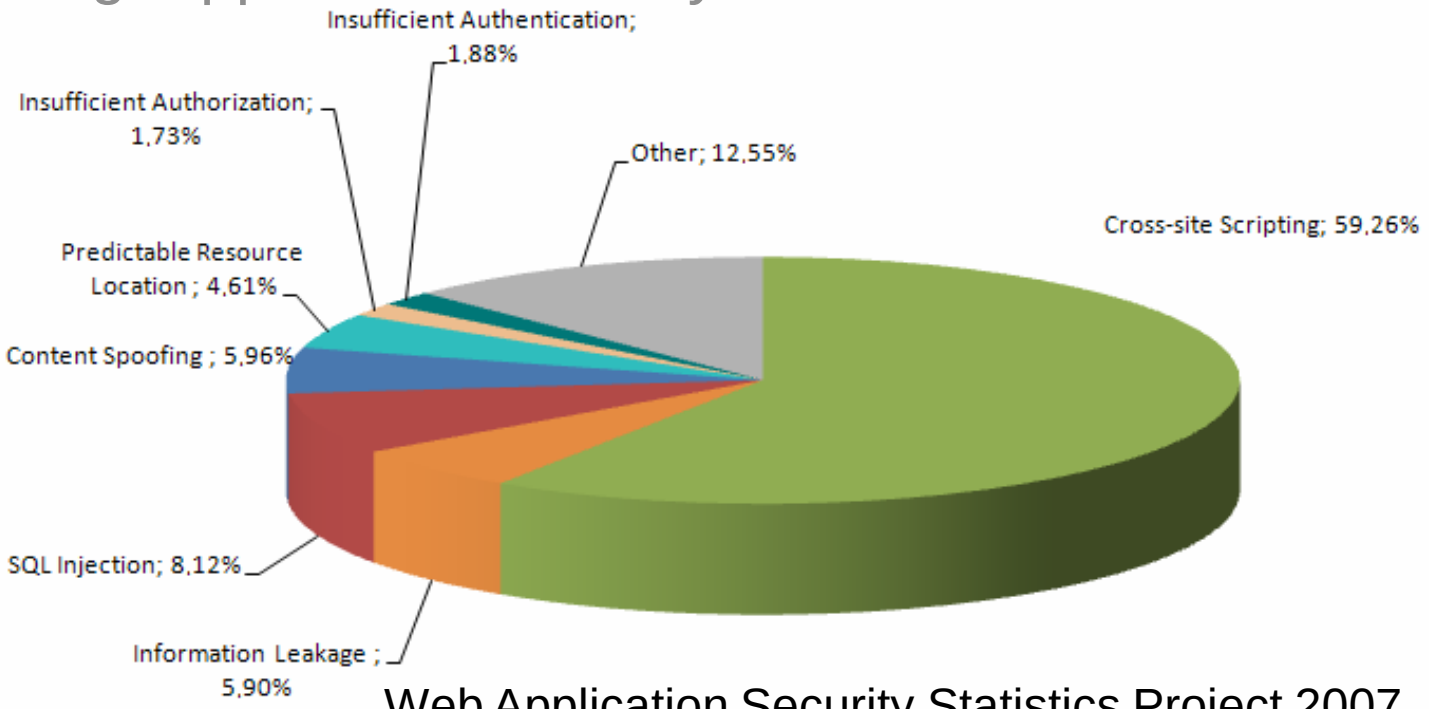

create
manage
deliver

# Threat Modelling

- Analyze the Application
  - Identify trust boundaries.
  - Identify data flow.
  - Identify entry points.
  - Identify privileged code.
  - Document the security profile.
- Identify the Threats: STRIDE
  - Spoofing of user identity
  - Tampering
  - Repudiation
  - Information disclosure (privacy breach)
  - Denial of Service (D.o.S.)
  - Elevation of privilege
- Rate the threats: DREAD
  - DAMAGE
  - REPRODUCABILITY
  - EXPLOITABILITY
  - AFFECTED USERS
  - DISCOVERABILITY
- Implement Controls, Countermeasures

# OWASP

- OWASP: international security organisation
- Provides statistics on common vulnerabilities
- Provides guidelines and coding standards
  e.g. Application Security Verification Standard




Web Application Security Statistics Project 2007

create
anage
deliver

# OWASP: 10 Vulnerability Categories

- Input validation
- Authentication
- Authorization
- Configuration management
- Sensitive data
- Session management
- Cryptography
- Parameter manipulation
- Exception management
- Auditing and logging

create
manage
deliver

# Auditing and Logging

- Anatomy of an Attack
  - Survey and assess
  - Exploit and penetrate
  - Escalate privileges
  - Maintain access
  - Deny service
- Issues
  - User denies performing an operation
  - Attacker exploits an application without trace;
  - Attacker covers his or her tracks
- Mitigation
  - Logging: Use  CFLog
  - Automate the logging: SQL Triggers
  - Centralized logging and log correlation
  - Intrusion Detection/Prevention
  - Evidence!

create
manage
deliver

# Authentication

- Issues:
  - Network eavesdropping
  - brute force attacks
  - dictionary attacks
  - cookie replay
  - credential theft
- Mitigation
  - Use SSL for credentials
  - Password policy
    - Complexity control
    - Password change frequency
    - Limited retries
  - Disclosure: don’t disclose why login failed
  - Short Cookie timeouts
  - Store passwords securely

# Authorization

- Issues
  - Elevation of privilege
  - Disclosure of confidential data
  - Data tampering
  - Luring attacks
- Mitigation is very application specific
- ColdFusion Security framework
  - Support for LDAP, NTLM, database
  - CFLOGINUSER
  - isUserLoggedIn
  - getUserRoles
  - isUserInRole/isUserInAnyRole
- Framework is very basic
  - Larger apps need security groups, roles, functions per role etc

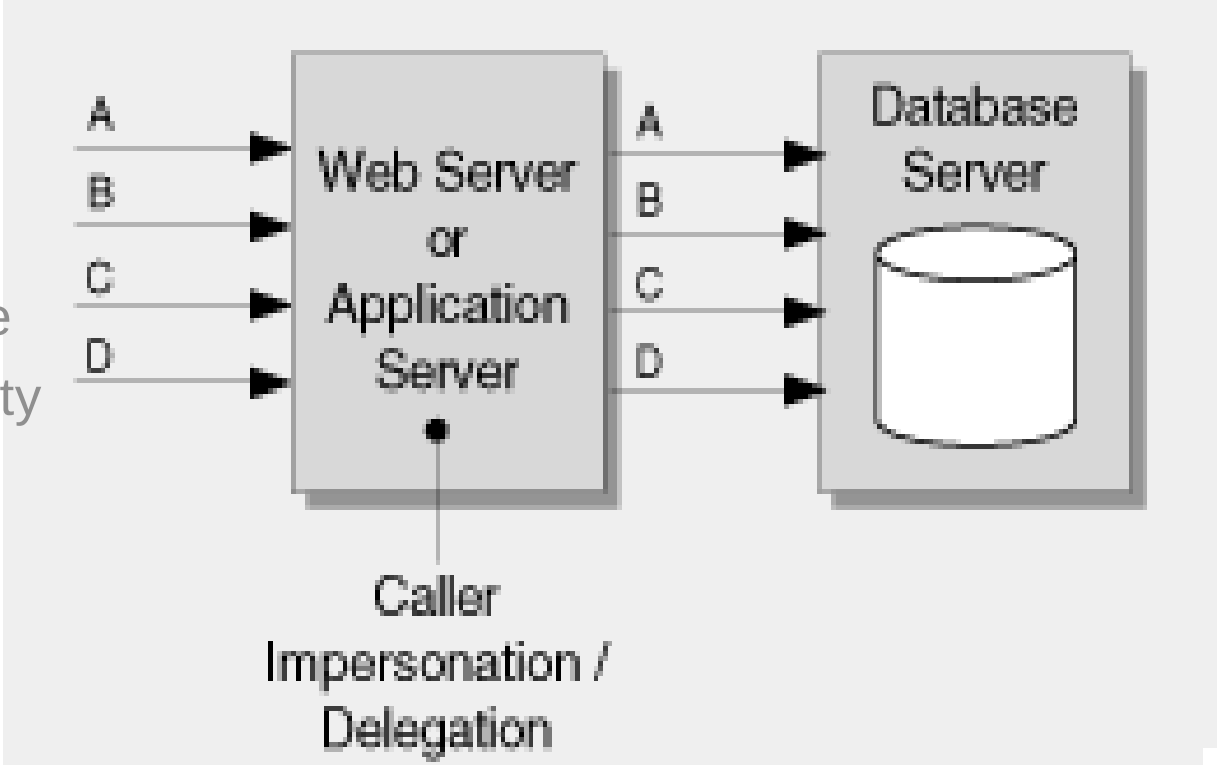
# Configuration Management

- Issues
  - Unauthorized access to administration interfaces
  - Unauthorized access to configuration stores
  - Retrieval of clear text configuration data
  - Lack of individual accountability
  - Over-privileged process and service accounts
- Mitigation
  - Remove CFIDE from port 80
  - Disable default accounts, etc
  - Auditing, Logging <CFLog>
  - Principle of Least Privilege

create
manage
deliver

# Least Privilege and Database Authentication

- Single account
- Account per role
- Account per user
- Tradeoffs
  - Performance
  - Maintainability
  - Security
- How do you audit if not per user?




create
manage
deliver

# Exception Management

- Issues:
  - Information disclosure
- Mitigation
  - Use customized error handling
  - User sees friendly error message
  - You see stack trace

```
<cferror
type="EXCEPTION"
template="/ValidationError.cfm“
mailto=“a@b.com"
exception="any">
```

create
manage
deliver

# Cryptography and Sensitive Data

- Issues:
  - Poor key generation or key management
  - weak or custom encryption
    - Access sensitive data in storage
    - Network eavesdropping
    - Data tampering
- Mitigation
  - ColdFusion 8 Enterprise is FIPS-140 compliant
  - Use AES or higher for symmetric encryption
  - Use SHA-256 or higher for the hash function
  - Use SSL and encrypted file systems

# Parameter Manipulation and Input Validation

- Issues
  - Query string manipulation and Canonicalization
  - Form field manipulation
  - Cross-site scripting
  - SQL injection

# ColdFusion and ScriptProtect

- Filters all requests using these rules – very limited

```
<var name=
  "&lt;\s*(object|embed|script|applet|meta)">
  <string>&lt;InvalidTag</string>
</var>
```

- Easy to supplement with additional rules in neo-security.xml
  - 
```
<var name="&lt;\s*(object|embed|script|applet|meta
        |iframe|link|body|style|input)">
        <string>&lt;InvalidTag</string>
</var>
<var name=";\s*(select\s|insert\s|update
        \s|delete\s|drop\s|alter\s|create\s)">
<string>SQL_INJECTION_HACK_ATTEMPT</string>
</var>
<var name="javascript:">
        <string>java-script:</string>
</var>
<var name="ContentType:">
        <string>MAIL_INJECTION_ATTEMPT</string>
</var>
```

- This is pretty good on IE7 and FF3 and above,
  It is not comprehensive
  And what do you do if your site has HTML editor?

# Parameter Validation

- Validate and type check all request parameters
  - Use <CFPARAM or isValid
  - `<cfparam name="form.emailAddr" type="email">`
  - If its a string, if possible use regex
  - `<cfparam name="username" type="regex" pattern="\w">`
- Type check all CFC input parameters
  - `<cfargument name="userName" type="string" />`
- SQL Param all SQL parameters
  - `<cfqueryparam value="#userName#" cfsqltype="CF_SQL_VARCHAR" maxlength="25" />`
- Sanitize all output
  - HTMLEditFormat
  - Jsstringformat
- Review ALL code

# Parameter Manipulation - Mitigation

- Firewall
  - ScriptProtect
  - Apache and Mod_security
  - Application Firewall
- Parameter validation
  - cfparam, isValid, cfargument
  - cfqueryparam
- Sanitize Output / Output encoding
  - HTMLEditFormat
  - Jsstringformat
- Third party libraries
  - OWASP AntiSamy (HMTL/Email)

# Session Management

- Issues
  - Session replay
  - Man in the middle
  - Session hijacking
  - Cookie Manipulation
- Typical Mitigation
  - Use J2EE Sessions
  - Use UUID for <CFTOKEN>
  - Keep Session timeout small
  - CFCOOKIE – use HttpOnly and secure attributes
- Extra Measures
  - Use SSL
  - Additional hashed cookie
    message authenticity check (MAC) code
    (users name, ip, browser type, sessionid)
  - Hidden form fields with changing hash (CSRF)

# Session Management – Session Surfing – CSRF

- Site A sends malicious content to user to access site B
  - Open an mail whilst on your banking site
  - Samy closed down MySpace for ‘maintenance’
- Typically JavaScript, but could be any html tag
  - `<IMG SRC=http://webbank/transfer_funds.cgi?from=314159265&to=`
- Traditionally, mitigated by checking HTTP_REFERER
- HTTP requests can also be made by
  - Flash
  - Flex
  - Java
  - Silverlight

create
manage
deliver

# CSRF, Flash and HTTP_REFERER

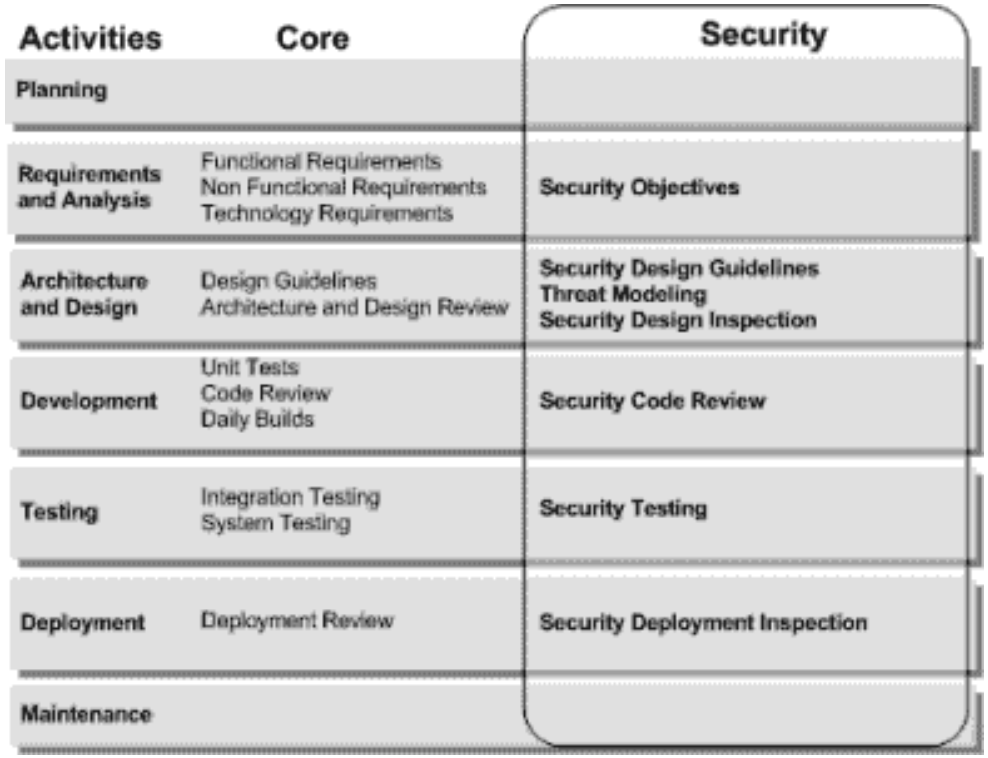
- Browser based CSRF
  - the HTTP_REFERER  is of the malicious site
  - So we can block browser CSRF
- Flash doesn't let you change HTTP_REFERER directly
  - Good
- Some earlier versions of Flash allow referer injection
  - `XML.contentType = "text/plain\r\nReferer: anything";`
- And even multiple http requests
  - 
```
req.addRequestHeader("Content-Length:0\r\n\r\n"
+ "POST\t/anotherpath\tHTTP/1.1\r\n"
+ "Host:host\r\n" + "Referer:faked\r\n"
+ "User-Agent:faked\r\n"
+ "Content-Type:faked\r\n"
+ "Content-Length:3\r\n"
+ "\r\n" + "foo\n", "bar");
```

# Session Management – CSRF

- Mitigation
  - Set trusted sites in your CrossDomain file
    AND
    Enforce HTTP_REFERER
  - OR Use a hidden form variable
    - Random one-time key for every form you serve
  - OR Use VerifyClient (CF8 with Ajax)
- Client side
  - Use Firefox with 'NOSCRIPT' plugin
- Issues
  - VerifyClient is AJAX only
  - The HTTP_REFERER is OK with Browsers
  - HTTP_REFERER can be hacked

# QA

- Security Lifecycle
  - Design Reviews
  - Code Reviews
  - Etc
- Testing
  - Easy to use
    - FF+Tamper
    - Charles Proxy
  - What the hackers use
    - OWASP Live CD VM



| Activities | Core | Security |
|---|---|---|
| Planning | | |
| Requirements and Analysis | Functional Requirements<br>Non Functional Requirements<br>Technology Requirements | Security Objectives |
| Architecture and Design | Design Guidelines<br>Architecture and Design Review | Security Design Guidelines<br>Threat Modeling<br>Security Design Inspection |
| Development | Unit Tests<br>Code Review<br>Daily Builds | Security Code Review |
| Testing | Integration Testing<br>System Testing | Security Testing |
| Deployment | Deployment Review | Security Deployment Inspection |
| Maintenance | | |

- WebScarab, WebGoat, CAL9000, JBroFuzz, Paros Proxy, nmap & Zenmap, Wireshark, tcpdump, Firefox 3, Burp Suite, Grenedel-Scan, DirBuster, SQLiX, WSFuzzer, Metasploit 3, w3af & GTK GUI for w3af, Netcats collection, Wapiti, Nikto, Fierce Domain Scaner, Maltego CE, Httprint, SQLBrute, Spike Proxy, Rat Proxy

# Deployment

- Server and Firewall Topology
- Business Continuity
- Patch policy
  - E.g

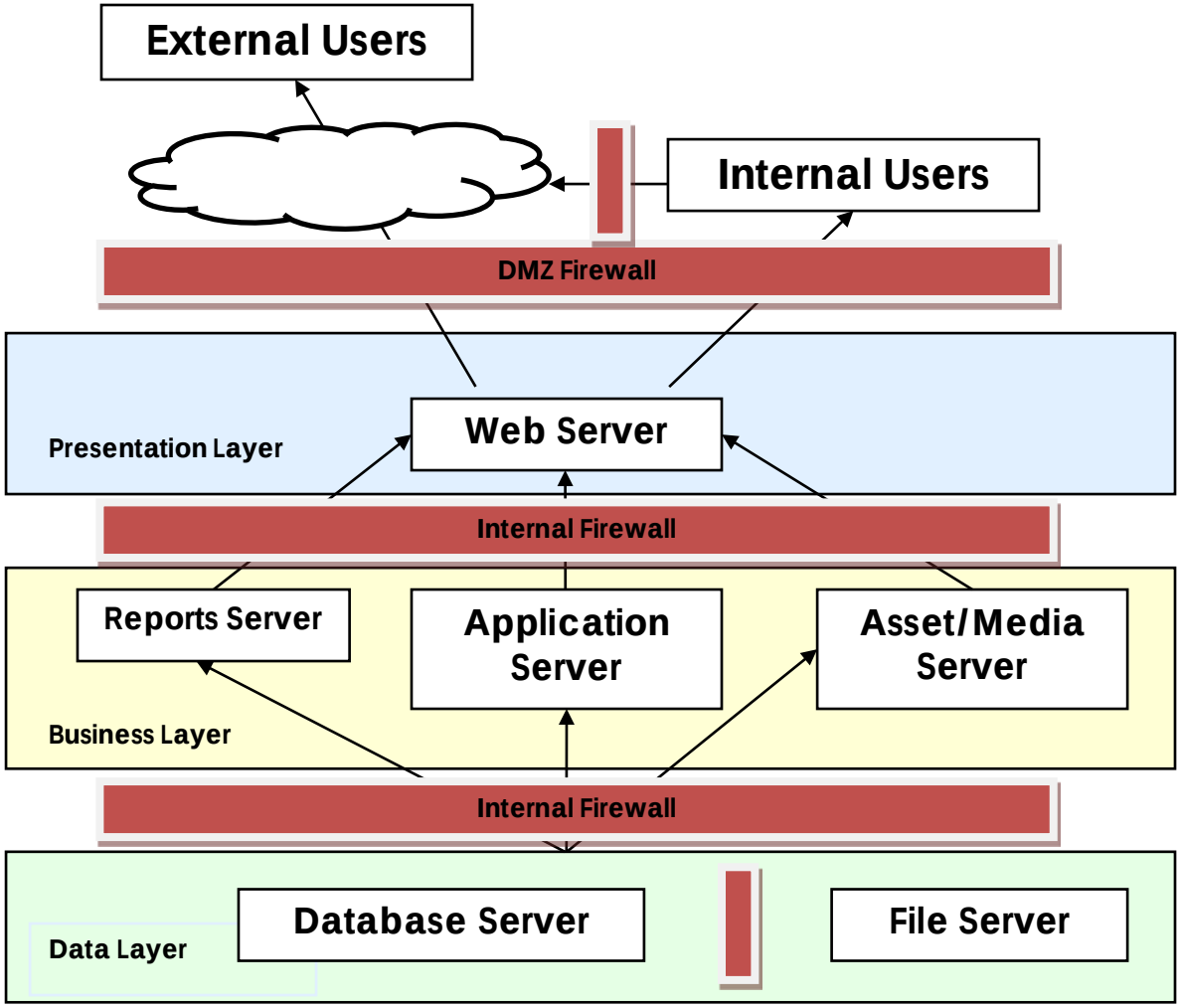
**Microsoft Security Bulletin MS09-004 - Important**

Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution (959420)

Published: February 10, 2009 | Updated: March 18, 2009

create
manage
deliver

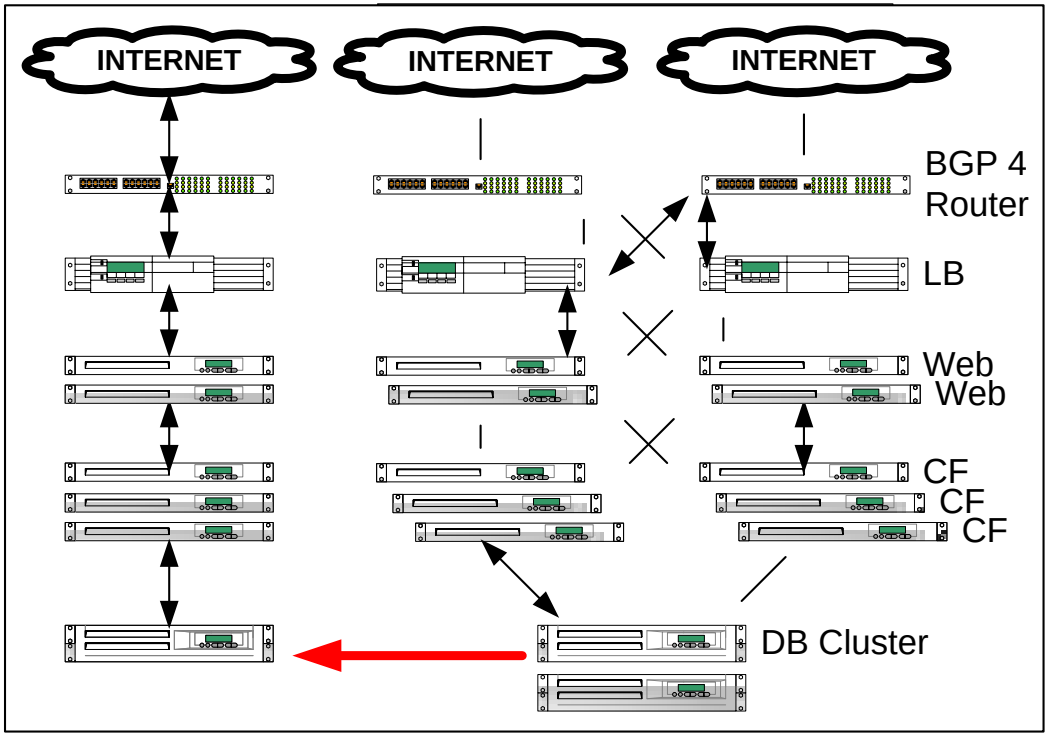
# Server and Firewall Topology




create
manage
deliver

# Business Continuity

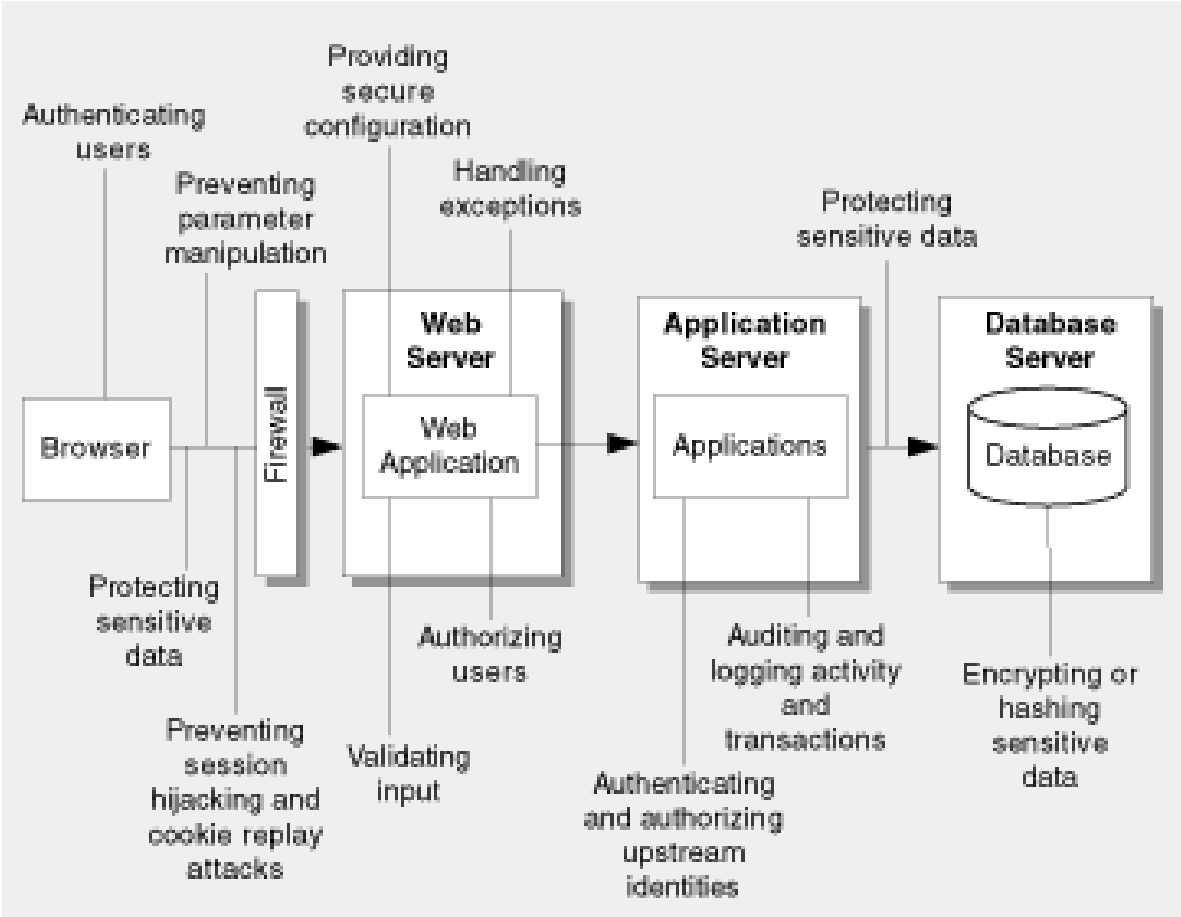
- Duplicate
  - Multiple ISPs
  - Load Balancing
  - Multiple servers
  - Clustered DB
- Replicate
  - Disaster Recovery




create
manage
deliver

# What is Security?

- **C**onfidentiality
- **I**ntegrity
- **A**vailability




create
manage
deliver

# ColdFusion: Security
## SOTR 2009

create
manage
deliver

Tag: