# MAX 2006
# Beyond Boundaries

Dave Watts
CTO, Fig Leaf Software
Securing ColdFusion





## Overview

- Who is this presentation for?
  - ColdFusion developers
  - Application server administrators
- What will we cover?
  - Aspects of web application security
    - Network
    - Host
    - Application
    - Database
  - Maintaining a secure environment
  - Security planning




## Demonstration

- SQL injection attack demonstration




## Aspects of web application security

| Network | Host | Application | Database |
|---|---|---|---|
| Firewalls, zones, filtering | Operating system | Input validation | General configuration |
| Proxies | Web server | Error handling | Logins |
| CF Distributed Mode | CF Application server | Data storage | Database connectivity |
| | | Session tokens | |




## Network – firewalls and filtering

- Firewall configuration
  - Ingress filtering
    - Allowed inbound traffic
    - TCP/80, TCP/443 …
    - Traffic examination (HTTP-aware filtering)
    - HTTPS can't usually be examined!
  - Egress filtering
    - Outbound traffic should be extremely limited!
    - Application-specific traffic requirements needed by firewall administrators (outbound CFHTTP, SMTP, etc)




## Common network topology

- I'm still building this diagram!

## Network - proxies

- Can be used to prevent direct connections to a "public" web server
- Allow the separation of executable content from static content
- Prevent execution of unapproved or uploaded scripts
- Require some specific URL pattern for identifying executable content, such as a J2EE context root.




## Network - CF Distributed Mode

- CF can be run on a machine separate from the web server
- Web Server Configuration Utility used to connect web server to remote CF server
- Like proxies, allows separation of executable content from static content and prevents execution of unapproved/uploaded scripts




## Host – operating system

- Software filtering
  - Ingress/egress rules
  - Overlap with external firewall rules
- Determination of interaction with other network resources
  - "bastion host"
  - domain server
- Standard configuration of ACLs, user accounts, remote access, management




## Host – web server

- Web server user account rights
- Limited access to files not served by the web server
- Web server input filtering
  - IIS 6
  - URLScan in IIS 5
  - modsecurity for Apache
- Authentication
  - Basic – unencrypted
  - NTLM (IIS only)
  - Digest
  - SSL/TLS
    - Third-party certificates for encryption and verification
    - Self-signed certificates for encryption
    - Client certificates
    - Processing overhead and options
    - Negative implications of SSL/TLS - monitoring




## Host – ColdFusion server

- CF Administrator configuration options
  - Debug output and Robust Exception output
  - Site-wide error handler and missing template handler
- CF service user account
- Securing built-in CF applications
  - CF Administrator
  - Admin API
  - Disabling RDS




## Demonstration

- Configuring CF service user account
- Securing CF Administrator

## Application - input validation

- Validating input
  - Single most common application vulnerability!
- Specific issues with input validation
  - Preventing SQL injection
  - Cross-site scripting (XSS)
  - Bounds checking




## Input validation - preventing SQL injection

- CFQUERYPARAM
  - Prevents all SQL injection attacks
  - Builds a prepared statement
  - Negative implications – prevents use of query caching
- Stored procedures
  - Same effects as CFQUERYPARAM – prevents all SQL injection attacks
  - Can be cached if called using CFQUERY
  - Can be used to limit database interaction significantly, if used exclusively within an application




## Demonstration

- CFQUERYPARAM
- Stored procedures




## Input validation – cross-site scripting (XSS)

- XSS attacks don't directly target your server
- XSS payload is typically stored on your server, and delivered to a browser, where it executes
- CFMX 7's SCRIPTPROTECT attribute
  - Limited ability to block XSS
- Other strategies
  - HTMLEditFormat – remove all HTML brackets
  - Rejection of HTML tags within input
  - HTML pseudocode




## Demonstration

- Examination of XSS prevention techniques




## More input validation

- Inadequate approaches
  - Client-side validation using JavaScript
  - CFFORM "server-side" validation

## Application – error handling

- Raw error messages may contain sensitive information
- Handling errors
  - Site-wide error handler
  - Application.cfm/cfc




## Application – storing data

- Encryption within your application
  - Symmetric keys vs PKI
  - Key management
  - Encryption vs hashing
- CFMX 7 algorithm support
  - AES
  - Blowfish
  - DES
  - 3DES




## PKI application diagram

- I'm still building this diagram!




## Managing session tokens

- The problem – session hijacking
- Preventing session hijacking
  - Session duration
  - Cookies vs URL tokens
  - CFID/CFTOKEN vs J2EE session management
- Additional factors
  - Client certificates




## Database

- Host-based ingress/egress ruleset
- Secure configuration
  - Service accounts
  - Dropping unneeded packages and stored procedures
- Database logins
  - Minimal rights
  - Removal from default roles




## Demonstration

- Limiting an SQL Server login

## Maintaining security

- Monitoring
  - Intrusion Detection Systems (IDS)
  - Operating system logs
- Patching
- Avoiding "credential creep"
  - A common way to solve problems is to loosen restrictions and use elevated privileges.




## Conclusion

- Thank you for attending!
- Questions, comments?
- dwatts@figleaf.com




Better by Adobe™