Security Best Practices for ColdFusion

Shilpi Khariwal | Computer Scientist | ColdFusion Security Czar

Who am I

Agenda

- Protecting server
  - Securing ColdFusion server
  - Recent security attacks
  - Locking down ColdFusion server
- Security best practices for CFM applications

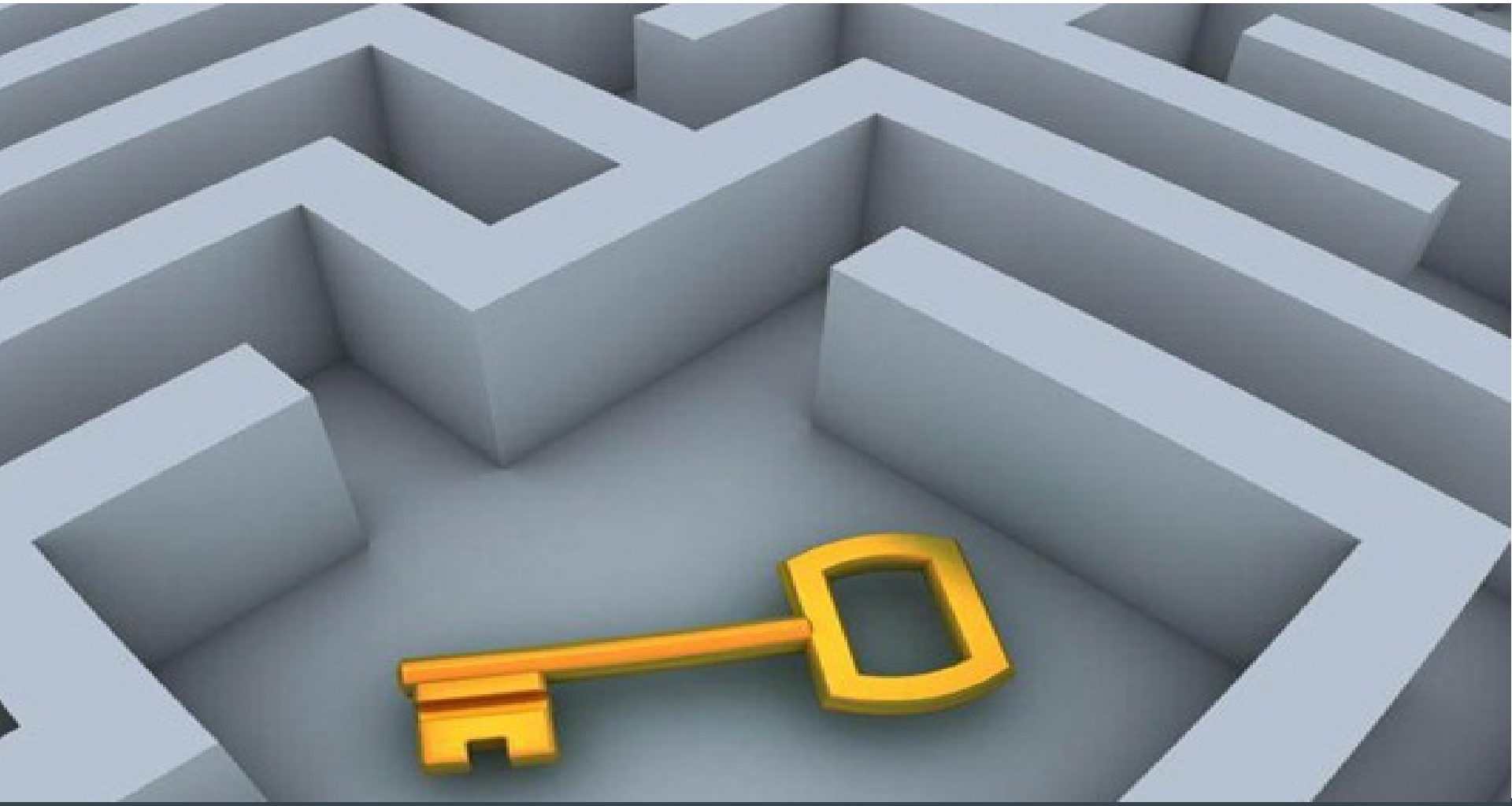
Security Attacks

Protecting server

- We will see how better configuration and locking down server can protect server against security attacks -
  - Securing ColdFusion server
  - Recent security attacks
  - Locking down ColdFusion server

Securing ColdFusion Server

- Install CF Server with Secure Profile enabled.



Securing ColdFusion Server

- Administrator -> Security
  - Enable separate user name and password for Administrator
  - Choose a strong password
  - Use a strong password for RDS
  - For production servers disable RDS by Administrator UI. As an additional protection, you should comment RDS servlet mapping from web.xml
  - Enable Sandbox Security and disable tags and functions which will not be required by application.
  - For adding additional users, provide appropriate roles and access.

Securing ColdFusion Server contd.

- Settings -> Memory variables
  - Configure application specific properties like –
    - Small timeouts for session and application, no persistent cookies
    - Cookies -
      - Cookie timeout
      - Secure
      - HttpOnly
      - Disable update
- Settings -> Enable UUID for CFToken for stronger CF session Ids

Securing ColdFusion Server contd.

- Settings –
  - Enable Global Script protection
  - Configure request limits and error handlers
  - Post parameter limit and size should be configured to prevent against HashDoS.
  - Allow only required SQL's at datasources
  - Disable event gateways if not used

Securing ColdFusion Server contd.

- Restrict access to applications shipped with CF, like Administrator, Adminapi, componentUtils, Wizards, etc.
- If on CF 9.0.2 or below, don’t leave documentation files on production server
- Disable directory browsing at server level

Recent Security Attacks

Vulnerability	Attack Vector	Prevention
CVE-2013-0625, CVE-2013-0629, CVE-2013-0631, CVE-2013-0632	RDS	Development only features, Server protection, Server lockdown
CVE-2013-1389	RDS	Development only features, Server protection, Server lockdown
CVE-2013-3336	AdminAPI	Server lockdown

These are some of the attacks which are from year 2013. In past we have seen vulnerabilities on Administrator Console and CFC Explorer. Both of which can and should be properly locked down.

Lockdown

- Configure OS specific restrictions to lockdown server
- Block URL access for internal CF applications. If required to be accessed add IP restriction. Lockdown guide is updated recently with some changes like –
  - While blocking a url, give a regular expression which protects against any smart hacks. */CFIDE/
- Disable unused services and servlets
- Configured server properly to strict values as discussed before and in lockdown guide.
- We will see how to apply these restrictions following lockdown guide.

Writing Secure CFML

- Use SSL whenever possible
- Use strong and unique passwords and encourage users on your application to do the same
- On a failed login, never tell if which of the credential details were faulty. Give a generic message.
- Don’t store user credentials in plain text. While saving critical information, use hash with salt
- Use strong Cryptographic functions. E.g. SHA-2 (SHA-256, SHA-512) or higher for Hash, and AES or higher for symmetric encryption.
- Avoid passing session ids in URL
- Rotate session after login
- Clear session and user login by called cflogout and sessioninvalidate

Writing Secure CFML contd.

- If using client variables with storage as cookie, don’t store sensitive information about client in cookie
- Use variables with scope name.
- Use error pages with least information
- Never enable debugging and detailed error pages (Robust Exception Information) in a production server.
- Use try/catch/cferror or onerror event to handle errors in applications

Writing Secure CFML contd.

- Use parameterized queries
- Sanitize/Validated user input before using them in application
- Validate data types. Like IsImage, ISXML, IsPDF etc.
- Encode whenever showing user input back to user
- Use latest features to make use of secure APIs. Ex. Encode*** for XSS, CSRF protection methods etc.
- Details about these features can be found at Security Article and a video about the same with Demos can be found here.

References

- http://www.shilpikhariwal.com
- http://www.adobe.com/content/dam/Adobe/en/products/coldfusion/pdfs/cf10/cf10-lockdown-guide.pdf
- http://www.adobe.com/devnet/coldfusion/security.html
- http://www.adobe.com/devnet/coldfusion/articles/security-improvements.html
- http://www.adobe.com/support/security/#coldfusion
- http://wwwimages.adobe.com/www.adobe.com/content/dam/Adobe/en/devnet/coldfusion/pdfs/coldfusion_security_cf8.pdf

Reach us @

- Blogs:
  - http://blogs.coldfusion.com
  - http://blogs.adobe.com/psirt
  - http://blogs.adobe.com/asset
- YouTube
  - http://www.youtube.com/user/adobecoldfusion
- Twitter:
  - @coldfusion
- Facebook:
  - http://www.facebook.com/AdobeColdFusion

Thank you!

Questions ?

shilpik@adobe.com

http://shilpikhariwal.com

@shilpikm