Hardening ColdFusion

Pete Freitag, Foundeo Inc.
Who is Pete Freitag?

- Owner of Foundeo, Inc.
- Blog: petefreitag.com
- 10+ Years working with ColdFusion
Agenda

• Installation Tips
• ColdFusion Administrator Settings
• Sandbox Security
• Hiding Version Information
• Overview of Web App Firewalls
Out of Scope

- Network, Operating System, or Web Server Security
- Writing Secure CFML
However...

• Before Installing ColdFusion...
  • Make sure your OS and Web Server have been patched and updated with the latest security fixes.
  • Make sure your server is behind a network firewall.
Installation Tips

• Choose a non-default installation path.
• Create a dedicated user account for ColdFusion to use.
• Don’t Install Components You Aren’t Using
• Choose a Strong Administrator Password
Installation Tips

• Make sure ColdFusion Administrator is only accessible via a restricted IP, such as 127.0.0.1

• Require SSL to connect to Administrator.

• Add Web Server Password (useful for auditing who changed what)
ColdFusion
Administrator Settings
Server Settings

Default: 60 seconds
Recommendation: 5-10 seconds

Why: DOS Mitigation

Timeout Requests after (seconds) [10]
When checked, requests that take longer than the specified time are terminated. This prevents unusually long requests from occupying server resources and impairing the performance of other requests.
Server Settings

Default: Unchecked
Recommendation: Checked

Why: Session Hijacking, increases entropy of session id
Server Settings

Default: Unchecked
Recommendation: Checked

Why: Developers can monkey with server. May be used by frameworks or apis.
Server Settings

Default: Unchecked with "//"
Recommendation: Checked with "//"

Why: JSON Hijacking
Server Settings

Default: Checked every 60 seconds
Recommendation: Unchecked

Why: If attacker modifies config it won’t take effect until restart, otherwise you need to respond to attacks in less than 60 seconds.
Server Settings

Default: Unchecked
Recommendation: Understand it

Why: This feature has a VERY LIMITED ability to protect you from Cross Site Scripting. Don’t let this setting give you a false sense of security. See my blog for explanation.
Server Settings

Default: /CFIDE/scripts/
Recommendation: Something else

Server Settings

**Default:** Empty

**Recommendation:** Create custom handlers

**Why:** Information Disclosure. The default handlers disclose CF, and possibly other information. The missing template handler should match your server 404 handler.
Request Size Limits

Default: 100mb
Recommendation: 1-10mb

Why: DOS Mitigation. Most applications only need to upload small files, 100mb is generally too big. This limit can and should be setup on your web server as well.
Request Size Limits

Default: 4mb
Recommendation: 1mb

Why: DOS Mitigation. For most applications a majority of requests will be under 1mb.
Request Size Limits

Default: 200mb
Recommendation: 1-50mb

Why: DOS Mitigation. Limits the total number of queued requests. 200mb of Heap is almost half the default max heap size.
Client Variables

Default: Registry
Recommended: None

Why: DOS Mitigation.
Memory Variables

Default: Unchecked
Recommended: Checked

Why: Session Hijacking. J2EE Sessions use a cookie that expires when the browser closes by default. The generated session id is also typically generated using a highly random algorithm.
Memory Variables

Default: 2 days
Recommended: As low as possible

Why: Session Hijacking. The lower the session timeout, the smaller the window of opportunity for session hijacking is.
Datasources

Default: SELECT, INSERT, UPDATE, DELETE, Create, DROP, ALTER, GRANT, REVOKE, Stored Procedures

Recommendation: SELECT, INSERT, UPDATE, DELETE
Or less
Datasources

Default: 30 seconds
Recommendation: 5 seconds

Why: Ties up threads if database is down.
Datasources

- Each datasource should have its own username
- DB User should have limited permissions.
Datasources

- Remove Example Datasources
Web Services

If you are using Web Services you can hide the end point, username, and password from the code.
Flex Integration

Default: Checked
Recommendation: Unchecked if not needed

Why: Anything you can turn off that is not in use should be turned off.
Debug Output Settings

Default: Checked
Recommendation: Unchecked

Why: Information Disclosure. You should NOT disclose paths, SQL, source code, etc.
Debug Output Settings

Enable Request Debugging Output
Enables the page-level debugging output on CFML pages. Uncheck this box to override all of the settings below. Debugging information is appended to the end of each request.

Default: Unchecked
Recommendation: Unchecked

Why: Information Disclosure
Logging Settings

Default: `{cfroot}/logs`
Recommendation: Somewhere else

Why: Harder for an attacker to cover their tracks
Logging Settings

Default: 5000KB, 10
Recommendation: Higher Values

Why: Should be high enough to make sure an attacker can’t cover their tracks. PCI or other standards may require you to keep logs for at least a year.
Logging Settings

Default: Unchecked
Recommendation: Checked

Why: Lots of tools available to work with syslog
Security: Administrator

Default: Single Username & Password
Recommendation: Separate user name and password

Why: Principal of least privilege.
User Manager

- Restrict Access to Parts Of Administrator
- Restrict Access to Admin API
- Restrict Access to sandbox settings
- Unfortunately the super user is always has the username “admin”, can’t change this.
Sandbox Security

- Restrict Access to:
  - Tags
  - Functions
  - Datasources
  - Network IP’s and Ports
  - Filesystem Access
Sandbox Security

• Requested Template’s Security Policy Overrides any Included Templates

• Remove Execute Permission on directories that shouldn’t contain cfm’s (such as images, js, or css folders)
  • /images/- (Recursive)
  • /images/* (Folder Only)
Sandbox Security

- May need to edit jvm.config on enterprise / multiserver to enable it.
- You can also setup a sandbox on Standard Edition, however you can only have one sandbox for the entire server.
Hiding ColdFusion

- Why Hide It?
  - To mitigate effectiveness of attacks that might target ColdFusion, or a specific version of ColdFusion.
Hiding ColdFusion

- Disable “Server” HTTP Header
- Discloses Version Numbers
- A Web Server Setting
Content Generating Tags

- Content Generating Tags May Disclose the ColdFusion Version
- Examples: cfform, cfchart, ajax tags, etc.
Disable Direct CFC Access

- Can be 404’d with a URL rewriting filter on the web server such as mod_rewrite, or ISAPI Rewrite.
- Or by removing CFCServlet from web.xml
  - Also disables SOAP Web Services
Hiding ColdFusion

- CFM File Extensions
  - Choose a file extension other than .cfm (configured in web.xml)
  - Use mod_rewrite (Apache), or ISAPI Rewrite (IIS).
CFIDE

- Make Sure `/CFIDE/*` does not resolve.
- `/CFIDE/administrator/` better not resolve publicly.
Web Application Firewalls

- Application Layer Firewall for HTTP
- Log, block, filter malicious requests
- Software or Hardware Based
- PCI DSS 6.6
- Commonly called a “WAF”
Founddeo Web App
Firewall for ColdFusion

- Commercial Product
- Software Based - written in CFML
- Works on most Shared Hosts
- Works on CF6+, Railo 3+, OpenBD 1+
- CFC API for custom filters and loggers
- http://founddeo.com/security/
Summary

• Eliminate Defaults
• Remove / Disable things that are not used.
• Use the minimum amount of privilege possible.
• Tradeoffs
  • Security vs. Performance
  • Security vs. Usability
Thank You

Questions?

foundeo.com  |  pete@foundeo.com  |  petefreitag.com