Secure your apps using ColdFusion 10

Hemant Khandelwal

Who am I

- Sr Engineering Manager – ColdFusion server & Builder
- 8+ years with CF team
- Shipped CF 8, 9, 10, CFB 1 & 2
- Was expert group member on EJB & JEE specification
- Twitter - @khandelwalh

How do we go about it?

Starting Point

- Threat Landscape Analysis
- Application Security
- Deployment & Updates
- Customer Communications

We set following Goals

- Improve patch adoption
- Improve the default configuration
- Make it easier for developers to create secure ColdFusion application.

Three-Prong Strategy

- Process improvements
- Product enhancements
- Delivery & communication

Process Improvements

Process Improvements

Team Setup

- Dedicated security czar
- Dedicated security QE
- Process for reviewing security issues

Training

- 100% of team to have level-1 security belt (including mgrs)
- Architects to have level-2 belt
- At least one level-3 & 4 belt within the team

Testing process

- Security scan – Veracode, AppScan, Fuzzing etc
- Dedicated security QE

Development process

- Review all reported security issues, backlog to zero
- Review 3rd party libraries
- Regular bug fix schedule
- Security bug markers, higher priority
- Security is part of feature sign-off checklist

Product Enhancements

ColdFusion 10 Enhancements – At a glance

- Session/Cookie protection
- XSS
- CSRF
- Session fixation
- Clickjacking
- Secure profile
- CF Administrator
- Others

Session/Cookie Protection

- Make cookies more secure

- HTTP-only
  - Browser restricts access to it from "non-http API's" (JavaScript)
- Secure
  - Send cookie only on secure connection (SSL/https)

- More configuration option
  - Support both Application.cfc & Application.cfm
  - Server level via Administrator or Admin APIs

- Demo

XSS – Cross Site Scripting

- What does this do & problem it creates?
  - Enables attackers to inject client-side script into web pages
  - Session Hijacking
- Demo
- Persistent & Non Persistent

XSS Mitigation in ColdFusion 10

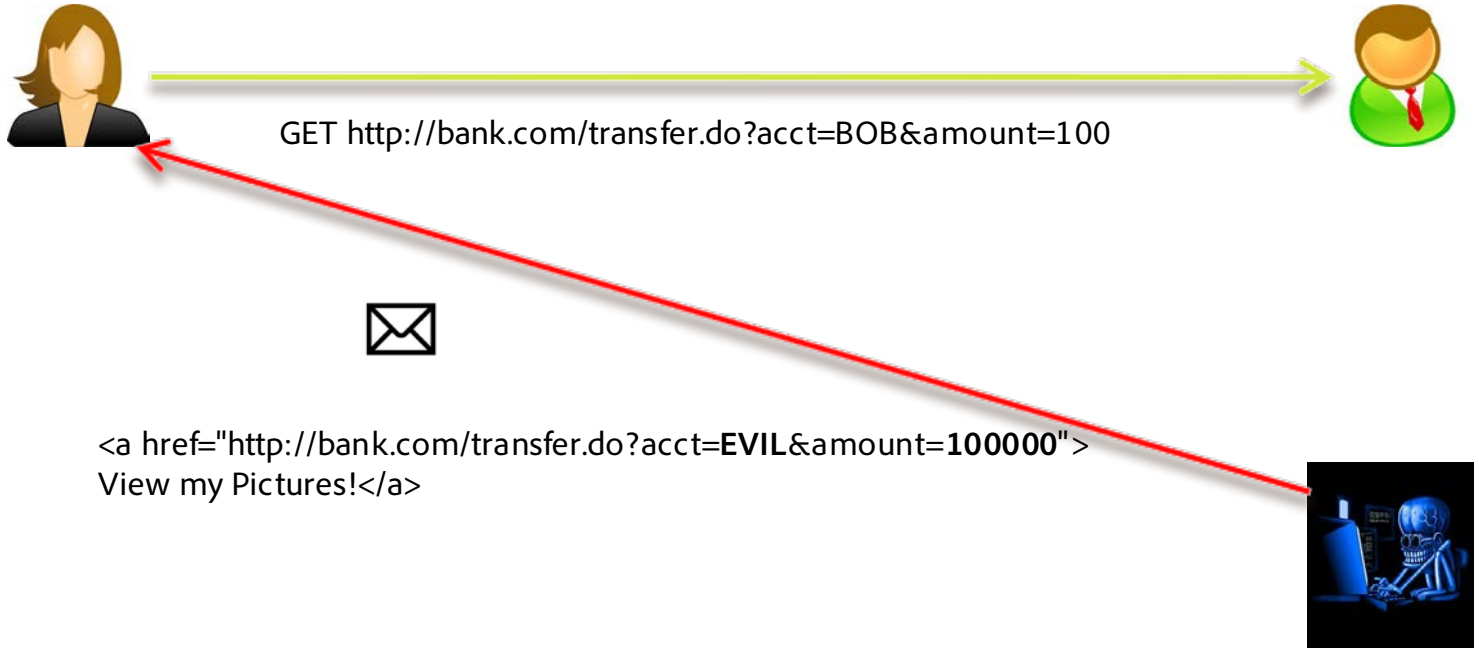
- ESAPI from OWASP is available from within CF

Context	Example	CF10 API to use
HTML	* Hi #url.name# *	*encodeForHTML*
HTML Attribute	* *	*encodeForHTMLAttribute*
JavaScript	*<script>x='#url.name#'</script>* *<a onmouseover="foo(#url.name#)"/>*	*encodeForJavaScript*
CSS	* *	*encodeForCSS*
URL	*<a href="index.cfm?name=#url.name#" />*	*encodeForURL*

- Decoding
  - *decodeForHTML, decodeFromURL*
  - *Canonicalize*
- Demo
- CF Administrator is using these APIs

CSRF – Cross Site Request Forgery

- What does this do & problem it creates?
  - Uses victims browser to send legitimate request to target server where the victim has authenticated



- Possible with GET or POST
- Demo

CSRF Mitigation in ColdFusion 10

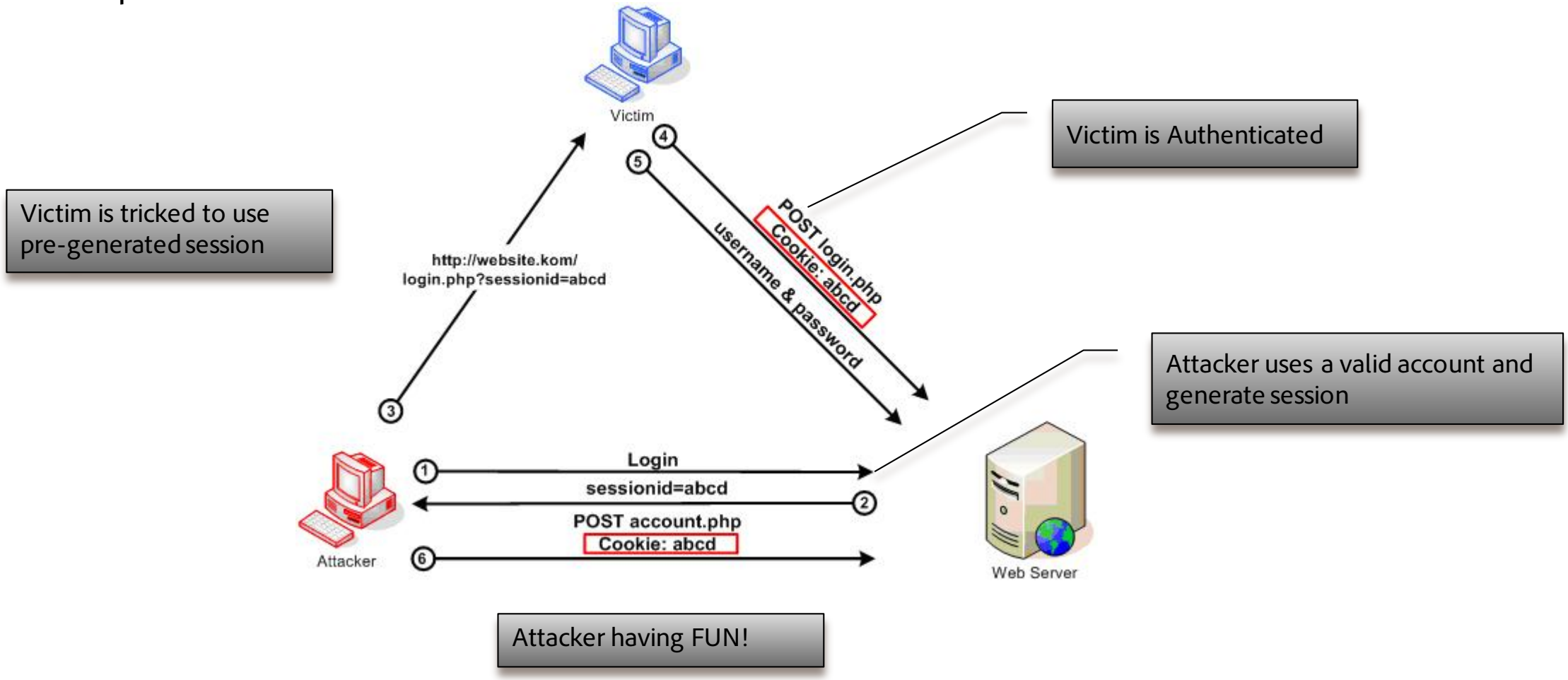
- Synchronizer Token Pattern Approach
  - Use a random token as a hidden field
  - Store the token in session
  - Verify the token

- New CF APIs
  - Submit form using token
    - ***CSRFGenerateToken([key],[forcenew])***
  - Validate submitted form using
    - ***CSRFVerifyToken(token,[key])***

- Demo

Session Fixation

- What does this do & problem it creates?
  - Reuse a prior session

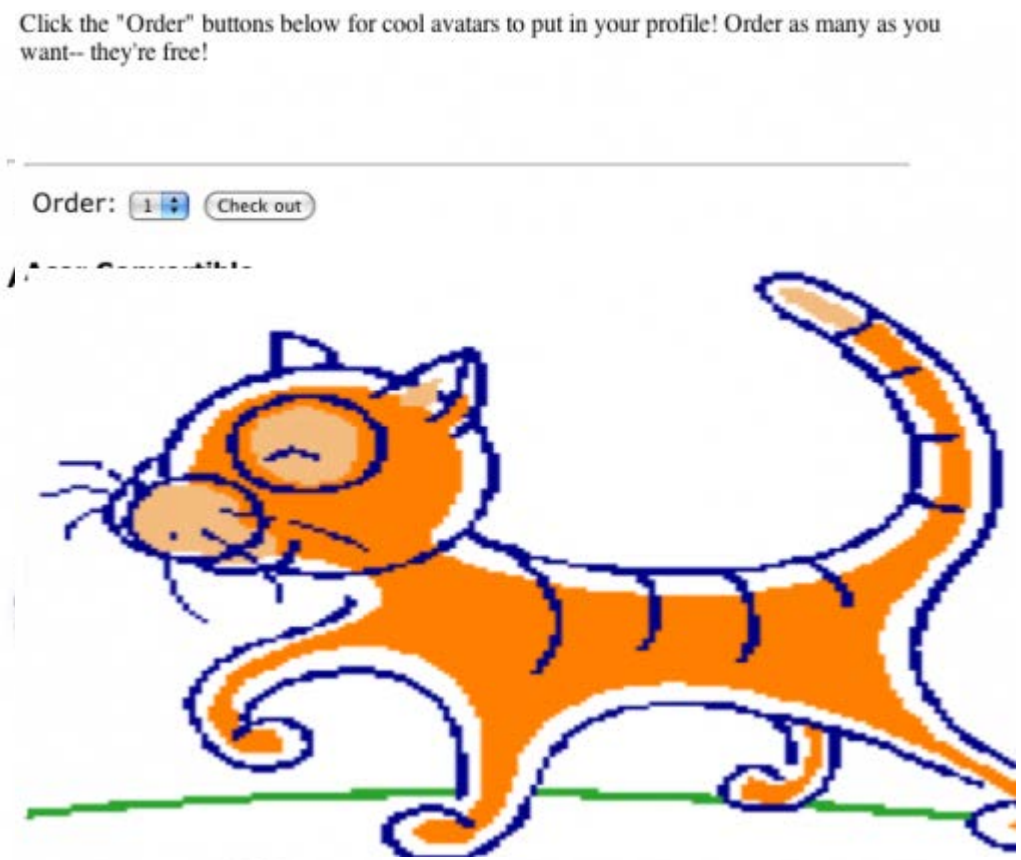


Session Fixation Mitigation in ColdFusion 10

- CF creates new session if a live valid session is not found
  - Avoids using pre-generated session
  - Disable using -Dcoldfusion.session.protectfixation=false
- SessionRotate()
  - Can be used to prevent fixation attack
  - Use after authentication to create new session
  - CF Administrator uses this
- SessionInvalidate()
  - Use it to invalidate session during logout
- Demo

Clickjacking

- What does this do & problem it creates?
  - A hacker tricks a user into clicking something different to what user sees
- Protection by adding X-FRAME-OPTIONS in the response header
  - DENY
    - Page will not render in a subframe
  - SAMEORIGIN
    - Page may be framed by any page from the same origin



*Source: IE Blog

Clickjacking Mitigation in ColdFusion 10

- To protect your applications
  - Open the Web.xml file located at ***<server-doc-root>/WEB-INF***
  - Add URL filter mapping for your application
    - ***CFClickJackFilterSameOrigin***
    - ***CFClickJackFilterDeny***.

```
<filter-mapping>
    <filter-name>CFClickJackFilterDeny</filter-name>
    <url-pattern>/testClick/*</url-pattern>
</filter-mapping>
```

- ColdFusion administrator protect against clickjacking

Secure Profile

- Disables RDS, Flash Remoting, Web Sockets, directory browsing
- Allowed SQL changes, IP address
- Full List - http://www.adobe.com/go/cf_secureprofile

	Administrator Settings	Path	Default Admin Profile	Secure Profile	Changes to the setting post migration to ColdFusion 10
1	Use UUID for cftoken	**Server Settings** > **Settings**	Enabled	Enabled	Overwritten
2	Disable access to internal ColdFusion Java components	**Server Settings** > **Settings**	Disabled	Enabled	Overwritten
3	Enable Global Script Protection	**Server Settings** > **Settings**	Enabled	Enabled	Overwritten
4	Maximum size of post data	**Server Settings** > **Settings**	20MB	20MB	Overwritten
5	Missing Template Handler	**Server Settings** > **Settings**	No Value	Custom missing error template	Retained if specified
6	Site-wide Error Handler	**Server Settings** > **Settings**	No Value	Custom site-wide error template	Retained if specified
7	Request Queue Timeout Page	**Server Settings** > **Request Tuning**	No value	Custom error template	Retained if specified
8	Cookie Timeout	**Server Settings** > **Memory Variables**	15767000 minute	1440 minute	N/A
9	Disabling updating of ColdFusion internal cookies using ColdFusion tags/functions	**Server Settings** > **Memory Variables**	Disabled	Enabled	N/A
10	Enable WebSocket Server	**Server Settings** > **WebSocket**	Enabled	Disabled	N/A
11	Start Flash Policy Server	**Server Settings** > **WebSocket**	Enabled	Disabled	N/A
12	Allowed SQL (all settings)	**Data & Services** > **Data Sources** > *[database]* > **Advanced Settings**	Enabled.	Create, Drop, Alter, Grant, Revoke, Stored Procedures are disabled	Retained if specified
13	Enable Robust Exception Information	**Debugging & Logging** > **Debug Output Settings**	Disabled	Disabled	Overwritten
14	Enable CFSTAT	**Debugging & Logging** > **Debug Output Settings**	Enabled.	Disabled	Overwritten
15	Select the type of Administrator authentication	**Security** > **Administrator**	Use a single password only	Separate user name and password authentication (allows multiple users)	N/A
16	Enable RDS Service	**Security** > **RDS**	Configurable at install time	Disabled	N/A
17	Select the type of RDS authentication	**Security** > **RDS**	Use a single password only	Separate user name and password authentication (allows multiple users)	N/A
18	Enable ColdFusion Sandbox Security	**Security** > **Sandbox Security**	Disabled	Disabled	Overwritten
19	Allowed IP addresses for ColdFusion Administrator access	**Security** > **Allowed IP Addresses**	Not available at install time	Available at install time	N/A

Administrator

- Password changes
  - Increased Password complexity
  - To change password, old Password is needed
- Improved XSS protection
- RDS enabled/disable control from Administrator
- Audit logs for Administrator
- IP restrictions on Admin access
- Default settings for a new sandbox are changed
  - Runtime permissions are not given by default
- Updated secure defaults
  - UUID for cftoken
  - ScriptProtect on but is not enough

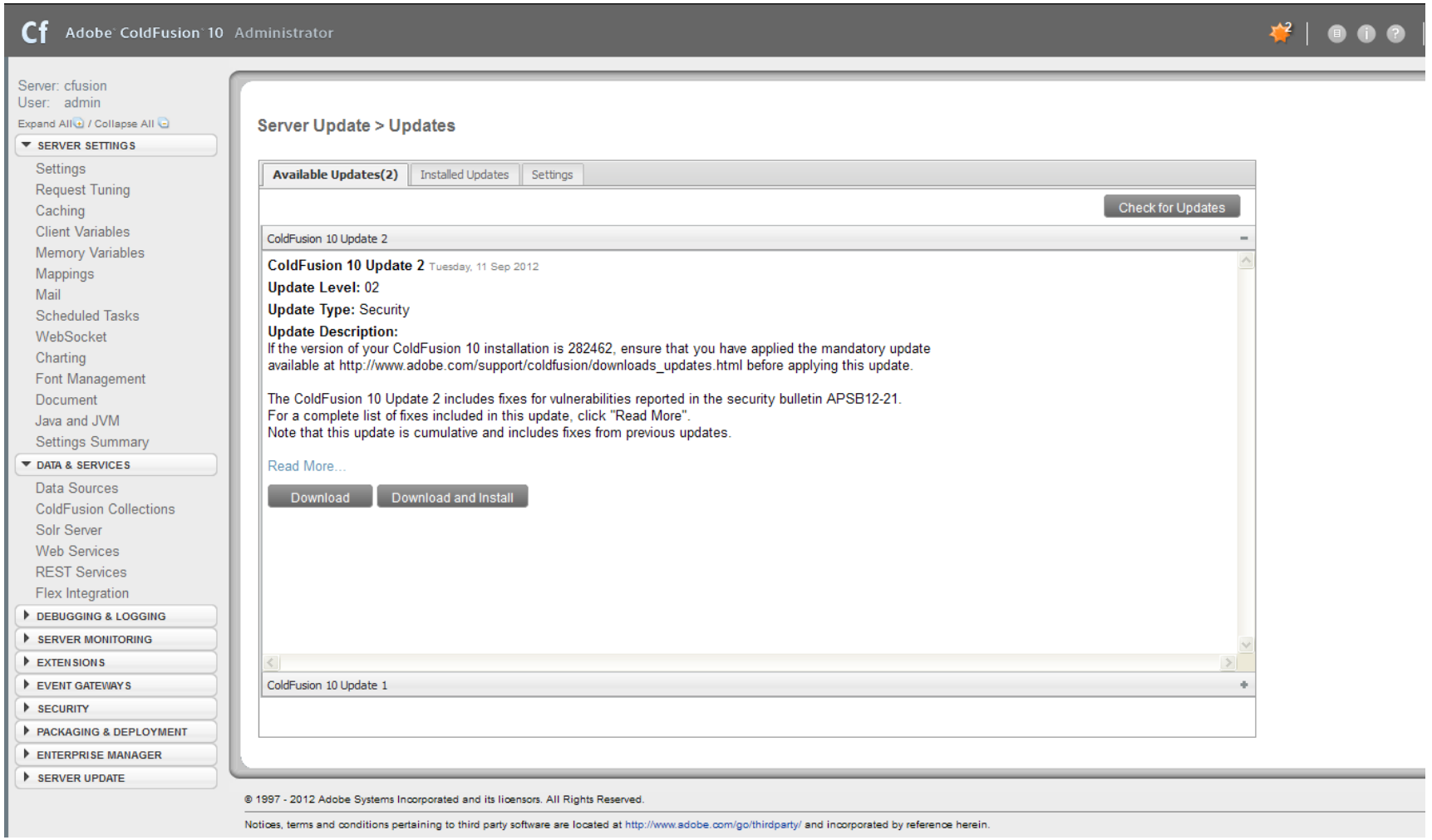
Others

- CRLF protection
  - cfheader, cfcontent, cfmail, cfmailpart, and cfmailparam
- Limit Number of POST Variables
- Tomcat – Active development & security fixes
- Mime-type determination after inspecting file
- CFForm name attribute character restriction
- RSA Crypto-J library upgraded to version 6
- CFLogin improvement
  - Authorization cookie is better secure
  - Only one active session is allowed per user per application
- Cryptography
  - Hash iterations
  - HMAC Function
- Ram disk application isolation
- All service passwords are encrypted
  - Configurable seed in admin

Delivery & Communication

At a glance

- Hotfix installer
- Demo



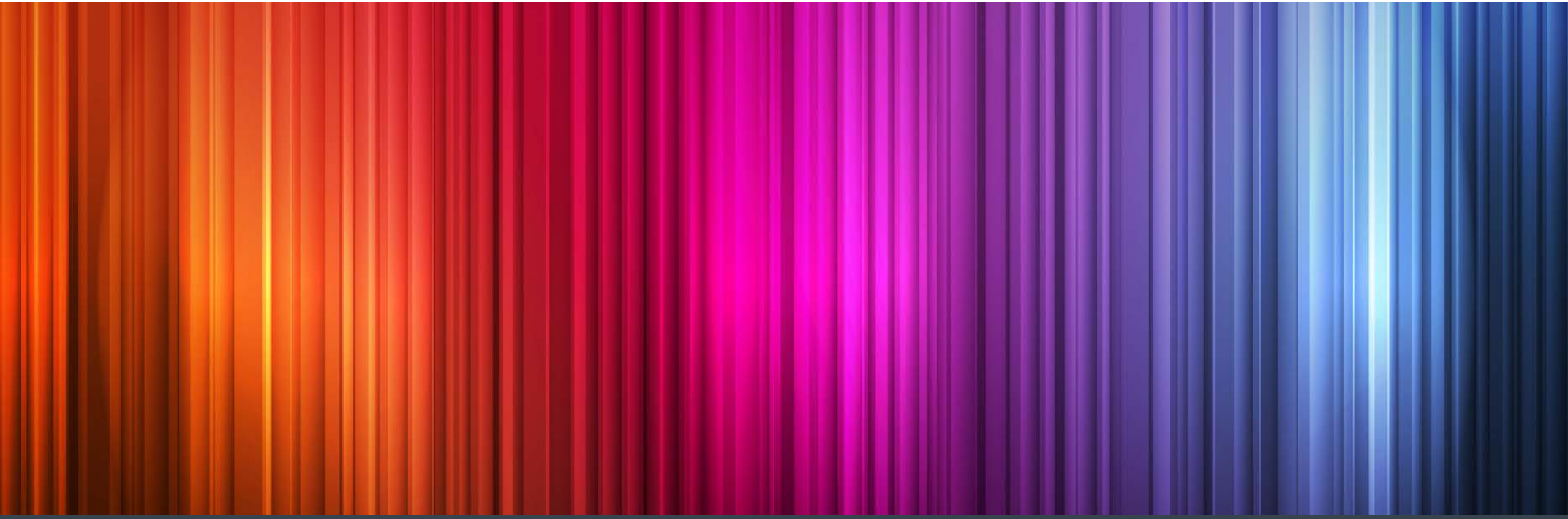
Resources

- http://www.adobe.com/devnet/coldfusion/articles/security-improvements.html
- http://www.adobe.com/devnet/coldfusion/security.html
- http://www.adobe.com/products/coldfusion/whitepapers/pdf/91025512_cf9_lockdownguide_wp_ue.pdf

- http://blogs.coldfusion.com/
- http://blogs.adobe.com/psirt/
- http://www.shilpikhariwal.com/

- @khandelwalh

Final Takeaway



Summary

- ColdFusion 10 is leaps & bounds ahead of earlier versions
- Improved patch adoption
- Improved default configuration
- Easier to create secure CF applications


Adobe