

Forum: [Hack Forums](#)

Thread: [\[MsSQLi\]*.nasa.gov](#)

RTSecurity - May 8, 2013, 8:44 am

[img]http://s23.postimg.org/6j6axt8wr/secimg.png[/img]

hmm..HELLO HACKFORUMS

My First Post !

h4{k5 - May 8, 2013, 10:54 am

Not a good idea to do that..thats all?

The Fail Collective - May 8, 2013, 10:55 am

as I said in my other post:

Skid... proof:

nasa: <https://rstforums.com/forum/67818-mssqli-nasa-gov.rst>

yahoo: <https://rstforums.com/forum/67687-sqli-yahoo-com.rst>

Savages - May 8, 2013, 10:56 am

Not smart to exploit this.

You would have federal agents at your door within 24 hours.

Upgraded - May 8, 2013, 12:39 pm

You could report it, but your name might get put into a lookout list.

As a user already said, do not exploit this.

They will track you, and arrest you.

Pendragon - May 8, 2013, 1:37 pm

If this is actually yours, I would advise covering up the screen shot a bit better next time. From the PoC you provided I was able to figure out the following:

1. Server is running ColdFusion MX 6 or 7
2. The sub domain is around 15 characters long.
3. Site is using https
4. The vuln is exploitable through a GET param

From this information, I can craft a google dork that fits this criteria:

Code site:nasa.gov inurl:https:// inurl:.cfm?*=

There's a good chance that the vulnerable site is among the results. GLWS OP.

Cathal - May 8, 2013, 1:39 pm

(May 8, 2013 01:37 PM)Pendragon Wrote: [\[CITE\]](#) If this is actually yours, I would advise covering up the screen shot a bit better next time. From the PoC you provided I was able to figure out the following:

1. Server is running ColdFusion MX 6 or 7
2. The sub domain is around 15 characters long.
3. Site is using https
4. The vuln is exploitable through a GET param

From this information, I can craft a google dork that fits this criteria:

Code site:nasa.gov inurl:https:// inurl:.cfm?*=

There's a good chance that the vulnerable site is among the results. GLWS OP.

He copied the image from a year old post on another forum.

Pendragon - May 8, 2013, 1:42 pm

(May 8, 2013 01:39 PM)MrCathal09 Wrote: [\[CITE\]](#) He copied the image from a year old post on another forum.

Nvm then. I enjoyed testing my deduction skills though.

amus3d - May 8, 2013, 1:57 pm

(May 8, 2013 01:42 PM)Pendragon Wrote: [\[CITE\]](#) Nvm then. I enjoyed testing my deduction skills though.

I agree, it is like propper CSI shit.

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

Good work, FBI agent David Matthews.

Underestimated - May 8, 2013, 2:13 pm

LOL amus3d, that pic, just wow.
muthafuckingfacism

~!White!~ - May 8, 2013, 2:58 pm

Dam you so cool bro.

Pic might be large

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

But i'm cooler