

Forum:[Hack Forums](#)

Thread: [Vulnerability in Nasa](#)

myt9h - April 2, 2014, 2:24 pm

<http://vmo.nasa.gov/vxo/metadata.php?id=wtf+is+this+?>

??

SohnGottes - April 2, 2014, 2:26 pm

looks to me like it just outputs whatever you put for id. how is this a vulnerability? the output goes through htmlentities()... ?

?ain - April 2, 2014, 2:32 pm

Idk about this but I do know NASA has a ton of XSS vulns

myt9h - April 2, 2014, 2:34 pm

aww it should not output though in manner like that , reported already to nasa ,but still not fixed

Cubs - April 2, 2014, 2:34 pm

I am such a l33t haxor

<http://vmo.nasa.gov/vxo/metadata.php?id=cubs+was%20+here+?>

lillix - April 2, 2014, 2:35 pm

This isn't an XSS vuln, any HTML script is filtered, you'd at least have to bypass the filter before this is a working vuln.

(Apr 2, 2014 02:34 PM)myt9h Wrote: [\[CITE\]](#) aww it should not output though in manner like that , reported already to nasa ,but still not fixedlolwat

myt9h - April 2, 2014, 2:35 pm

(Apr 2, 2014 02:32 PM)G0dOf4ll Wrote: [\[CITE\]](#) Idk about this but I do know NASA has a ton of XSS vulns

yeah buddy agree it has lots of xss.....

Effexion - April 2, 2014, 2:36 pm

Lol, I thought you had hacked NASA whe9n I read the title. Ohhhhhh O..P.

myt9h - April 2, 2014, 2:38 pm

(Apr 2, 2014 02:36 PM)Effexion Wrote: [\[CITE\]](#) Lol, I thought you had hacked NASA whe9n I read the title. Ohhhhhh O..P.

buddy i just found this worthy ,i share it therefore

SHADOW REALM - April 2, 2014, 2:40 pm

(Apr 2, 2014 02:38 PM)myt9h Wrote: [\[CITE\]](#) buddy i just found this worthy ,i share it therefore it is almost as worthless as an xss

poxoq - April 3, 2014, 9:55 am

all those "vuln" are honeypots.....

WACKO - April 3, 2014, 6:18 pm

(Apr 2, 2014 02:40 PM)SHADOW REALM Wrote: [\[CITE\]](#) it is almost as worthless as an xss
I think it's worth less than an XSS. Nothing can even be executed here.

(Apr 3, 2014 09:55 AM)poxoq Wrote: [\[CITE\]](#) all those "vuln" are honeypots.....

Why the fuck would they have XSS honeypots? Nobody's going to track somebody down for a reflective XSS unless they do something stupid like email Nasa with the link to a cookie stealer or some shit.

Th3PonyWizard - April 4, 2014, 2:51 am

Nasa has more holes than swiss cheese. This one isn't an actual vulnerability although that's arguable. Outputting user input through GET is still a minor risk considering people are retarded enough to fall for Phishing and various SE attempts of which this can be used with.