

Forum: [Hack Forums](#)

Thread: [\[XSS\] NASA.gov \(Oday 17/09/2019\)](#)

Choups - September 17, 2019, 1:57 pm

Vulnerable domain: www.mdscn.nasa.gov

All info in: <http://paulochoupina.com/notes/nasa.html>

Proof-of-concept video included.

~[DogiD]~ - September 17, 2019, 11:11 pm

Nice found.

If they are running bug bounty program, you could easily earn \$10-100 with that.

But usually hackers just got thank you message, sometimes not even that.

~ DogiD

Choups - September 18, 2019, 3:33 am

(Sep 17, 2019 11:11 PM)~[DogiD]~ Wrote: [\[CITE\]](#) Nice found.

If they are running bug bounty program, you could easily earn \$10-100 with that.

But usually hackers just got thank you message, sometimes not even that.

~ DogiD

I tried to report it like 5 times and no response..

~[DogiD]~ - September 18, 2019, 3:48 am

(Sep 18, 2019 03:33 AM)Choups Wrote: [\[CITE\]](#) I tried to report it like 5 times and no response..

Typical. Dont waste you time with goverments, they arent interested of security.

<https://hackerone.com/> if you havent yet joined here. HackerOne is #1 bug bounty program site.

~ DogiD

Choups - September 18, 2019, 12:58 pm

(Sep 18, 2019 03:48 AM)~[DogiD]~ Wrote: [\[CITE\]](#) Typical. Dont waste you time with goverments, they arent interested of security.

<https://hackerone.com/> if you havent yet joined here. HackerOne is #1 bug bounty program site.

~ DogiD

[HackerOne](#)

01001 - September 19, 2019, 8:27 am

It's pretty nice. I once found an SQLi vulnerability on Harvard's website. All I got was a 'Thank you' in the form of a ticket, in which they stated that your issue has been resolved!

Goku - September 19, 2019, 8:32 am

Although this is sad they aren't obligated to give you some kind of reward.
I would only bug hunt for a company that would.

And if you really want a "reward" for a vuln than you can always go blackhat and blackmail them...
Doesn't always turn out great but hey at least you get some "reward" worth your time.

Choups - September 19, 2019, 11:05 am

(Sep 19, 2019 08:27 AM)01001 Wrote: [\[CITE\]](#) It's pretty nice. I once found an SQLi vulnerability on Harvard's website. All I got was a 'Thank you' in the form of a ticket, in which they stated that your issue has been resolved!

I found a sqli in yahoo but the mothef_kers dont let me disclose it.

I talk about it in my website tho xD shh ^^

(Sep 19, 2019 08:32 AM)Goku Wrote: [\[CITE\]](#) Although this is sad they aren't obligated to give you some kind of reward.

I would only bug hunt for a company that would.

And if you really want a "reward" for a vuln than you can always go blackhat and blackmail them...
Doesn't always turn out great but hey at least you get some "reward" worth your time.

never done blackmail, is not my mo.

you can try to shell and root, then sell the access for good money, depending on the host.

But I quit blackhat many years ago

Sitrep - September 20, 2019, 7:34 pm

Nice find, to bad government sites just patch the bug and move on like nothing happened after your report tho...

FUC K YOU FBI - September 21, 2019, 3:41 am

(Sep 20, 2019 07:34 PM)Sitrep Wrote: [\[CITE\]](#) Nice find, to bad government sites just patch the bug and move on like nothing happened after your report tho...

Because with this security breach you are not able to do anything bad for them.

Its not stored XSS, you can do this basically to 20% websites who have search function.

Sitrep - September 21, 2019, 3:42 am

(Sep 21, 2019 03:41 AM)FUC K YOU FBI Wrote: [\[CITE\]](#) Because with this security breach you are not able to do anything bad for them.

Its not stored XSS, you can do this basically to 20% websites who have search function.

Yeah I know, probably a lot more than 20% tho ?

FUC K YOU FBI - September 21, 2019, 6:25 am

(Sep 21, 2019 03:42 AM)Sitrep Wrote: [\[CITE\]](#) Yeah I know, probably a lot more than 20% tho ?

And he calls it Oday wtf ? ?

SwitchOff - September 4, 2020, 10:02 pm

(Sep 21, 2019 03:42 AM)Sitrep Wrote: [\[CITE\]](#) Yeah I know, probably a lot more than 20% tho ?

-Oday long before dinosaurs ?

Sitrep - September 11, 2020, 12:58 pm

(Sep 4, 2020 10:02 PM)SwitchOff Wrote: [\[CITE\]](#) -Oday long before dinosaurs ?

IKR ?