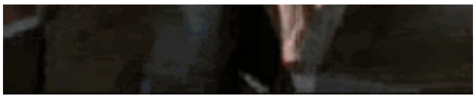
how i earned 56000 as my first bounty from hackerone

Kirsu bal Follow
Sep 17, 2019 · 4 min read

Hi folks, i am kishor balan from kerala,india.This is my first write-up and maybe you could identify my grammatical/spelling mistakes but i am not gonna give you any bounties for that, because those are the known vulnerabilities 😁.

okay i coming to the story, its been 8months that i am researching web security on hackerone platform. And there were no bounties, only some duplicate and invalid bug reports from my side 😢.

i was so disappointed and frustrated like



Then one day, i was just walking through some subdomains of one of the monstor company and i found a Host injection vulnerability there but the host was out of scope(it was an another website).. oohh damn wtf…i m keep falling down again and again 😫.

i just closed my laptop, cuz there were i had some ugly stuffs(college assignments)to do..😏

The next day, i was just thinking about the bug and suddenly one thing came in my mind, that is what if i report the bug in that website instead of that monstor website🧐. Here i am not gonna disclose the website becasue it is a private program.🙃

bug: https://dzone.com/articles/what-is-a-host-header-attack

okay let’s say the website name as “redacted.com”

but its was a subdomain of it let’s call it as “redacted.aa.bb.com”

okay i am coming to the method i tested the bug.

we all know that a host injection vulnerability allows us to customize the host address in the HTTP request and what will happen if we changed the host address of the password reset request when we requesting it from the forgot password page??

yea.. the new customized host address will defenitly appear on the password reset link….

got it?, got confused?? 😂 okay i will make it more easy to catch.

Normally, when we requesting the password reset link, we will receive the mail and how will be the password reset link look like?

it will be like this…

https://redacted.aa.bb.com/passwordreset/token=gdhdggshdggshhdggsggdggsgdgg

Right??

when we click on the link, we will navigate to the specified host address in the link and there we can reset our password.

okay, now what if we just changed the Host address in the password request of a website having Host injection vulnerability??

defenitly the received link will be also changed it's host address to the new address we customized.😉

so i just tried to change it's Host address from redacted.aa.bb.com to evil.aa.bb.com..

But i just shocked, because the result was "500"… yeass "the internal server error"…. oohhhh god ..what the hell is this??!!

👏 80

wasn't there any bugs? were everything just my foolishnesses??!!😒😒

wait… what if i could change the two parts after the first part in the Host address?? i mean instead of changing the part "redacted", change the parts "aa.bb"after the "redacted" ??

just for a curiosity, i took an effort for that too 😉😉

i just changed those parts and now the address is redacted.hacker.here.com.

Then i just forward the request….ohhh yeaahhhh thank god, the status was “200"(ok).

woww…. i was just like ..

next is i wanted to check the reset mail also, i checked it and i found the reset link was look like

https://reacted.evil.here.com/passwordreset/token=ggsfsddaffhhdhhsffdg

now what?? yeahhhhh the bug is verified and i successfully exploited…

😍😍😍

Do you know that how it allows hackers to hack your account completely?

We all know that the password reset token is a sensitive object cuz it allows us to change our password, so what will happen if we click the link of passwrd reset mail which was send by the hacker, by changing the real host address to his domain? yes , we will navigate to his domain with our password reset token and that’s all the hacker need. He can easily steal our password reset token from his domain and he will use that token to change our password ,it will possible because our token is a valid one, so the hacker will change our password and he will takeover our account from us.🙃

Time to report

i just reported the bug to that website and then they invited me to their hackerone private program, i just re-submitted the report through hackerone and there were no duplicates of it.

and after two days, they just triaged the report and gave me a reward of $800 (56000 indian rupees).

Thank you…

NOTE:- don’t try to report the spelling/grammatical mistakes, i will consider them as known vulnerabilites..😁😁😁😁😁

Security Bug Hunting Xss Vulnerability Hackerone