mehedishakeel
Oct 23, 2022 · 3 min read · Listen

Broken Link Hijacking — My Second Finding on Hackerone!

Broken Link Hijacking (BLH) or **Link Takeover**, whatever you called it, the concept is very simple. If you get any broken links of any website and it's easy to be taken by someone , then it's a broken link hijacking or takeover bug. It's a similar kind of bug like **Subdomain Takeover**. Just the difference is in subdomain takeover you have to takeover the subdomain and in broken link hijacking you have to take over the link.

BLH can be done for various broken social media links (also known as social media takeover), broken link of file or scripts , and as well as short links like tinyurl, bitly, tinycc. To get this easy bugs you just have to keep your eyes open and luck while bug hunting.

Now let's discuss how i get my second bug and what are the tools and technique i use,

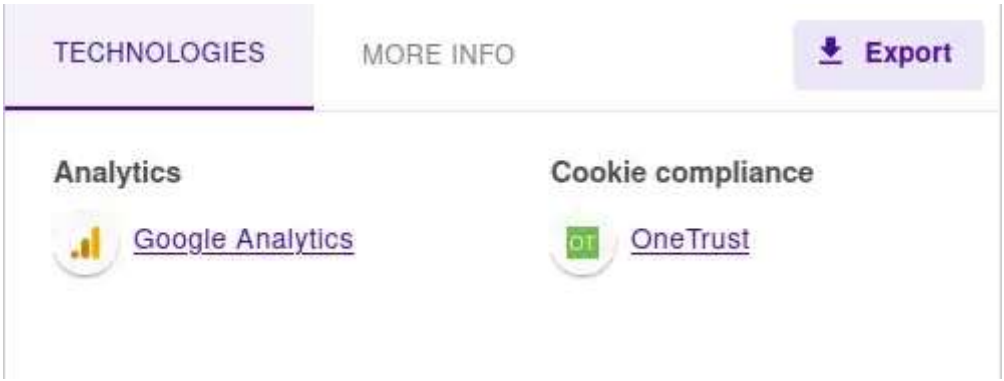
It's was a private program, So i will not be able to share the company name, domain or screen shot or any other info into this write up. Even when they resolved the report, they mark it as confidential. I want to mention that the target scope was huge so lets take the example scope domains as

```
*.mehedishakeel.com
```

So, I did the same what every bug bounty hunter do in these type of case with huge in-scope items "**Subdomain Enumeration**" . So i used two very well known tools **subfinder** & **httpx** . In bug bounty hunting for collecting subdomains and basic info those tools are very useful and fast enough. I got the following interesting subdomains

```
https://sr5-demo05.mehedishakeel.com/
https://sr6-demo06.mehedishakeel.com/
https://sr7-demo09.mehedishakeel.com/
https://sr8-demo08.mehedishakeel.com/
https://sr9-demo10.mehedishakeel.com/
```

When, I open the url in browser, i saw nothing, complete blank page. I open **Wappalyzer** add-on and get the following result,



Wappalyzer

Suddenly, electricity is gone, load shedding for almost 8 hours.

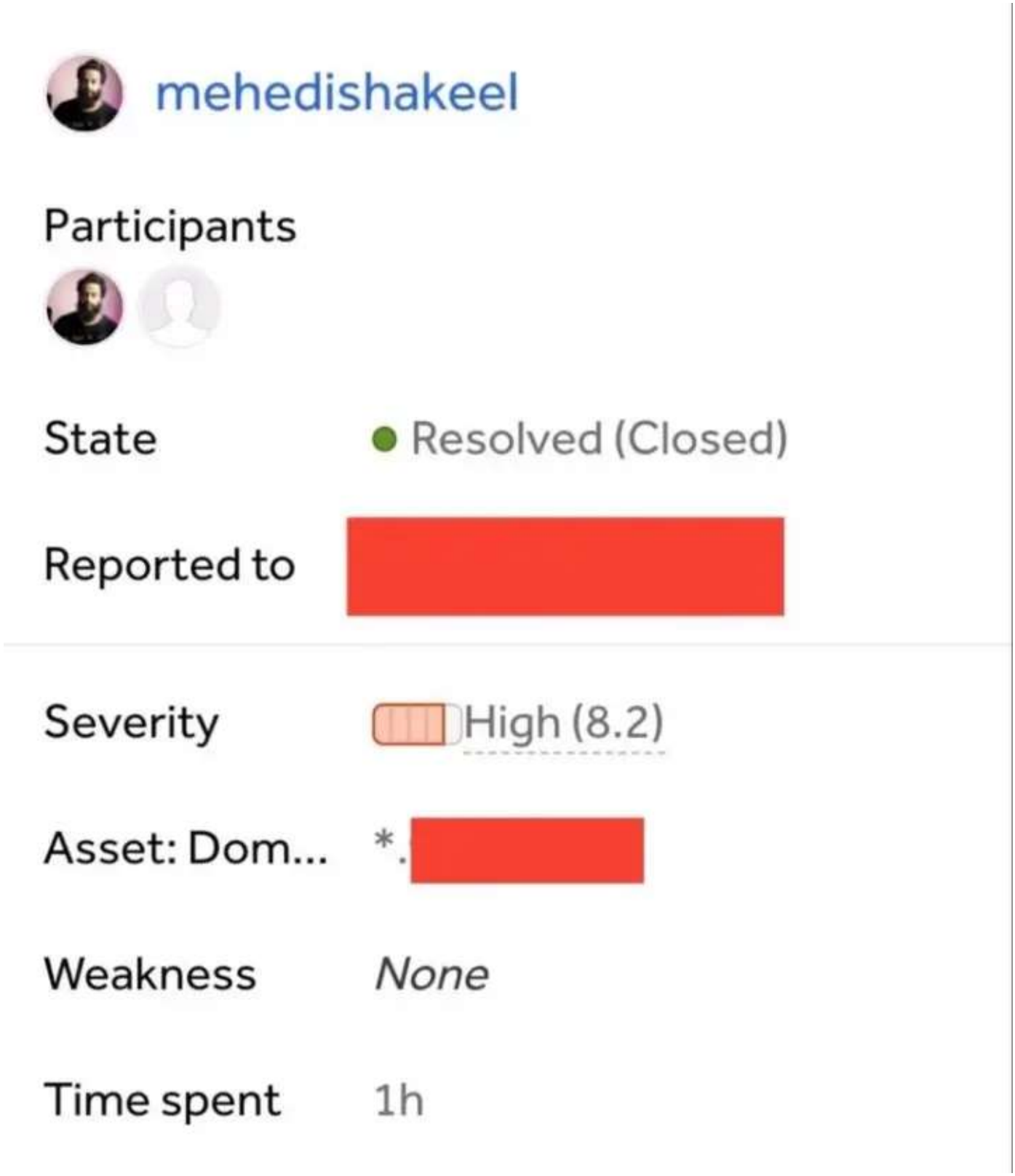
Next day, I start again where i left, Open all the url, and now i'm seeing a same message in all of those subdomains. Something like,

```
These test environment is only up during business hours..... and more
support visit http://tiny.cc/this_is_not_the_exact_link
```

I understand that when first time i visit those url, that is there business time and on that time these website are available for some kind of testing and now it's not available. So , open the mentioned link and it redirect me to tiny.cc website, and the link was broken. **FOUND A BROKEN LINK!**

Now, it's time to takeover the link, so tried to create my short link for on of my github page, with the custom name **tiny.cc/this_is_not_the_exact_link,** But failed to create, i get an error "Domain is not trusted". So,not every domain is accepted to tinycc.

Then i tried to create the short link with my hackerone profile url, and finally, the tinycc accepted that, This is how i hijacked the broken link and submit the report in hackerone.



In just 30 minutes my report got resolved. That's how i got my second resolved bug on Hackerone. Thank you for reading!

Mehedishakeel Bug Bounty Tips Bug Bounty Hackerone