mehedishakeel

Oct 21, 2022 · 3 min read · Listen

Information Disclosure — My First Finding on Hackerone!

Information Disclosure is a kind of bug that is not so hard to find but could make huge impact on target. Some time you can get very sensitive information with less effort. That's how i got my first report resolved on **hackerone**.

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

On that target program scope i it was a private program. So i am not authorized to include the real domain and company name into this write up. so

lets take the example domain as

```
https://mehedishakeel.com
```

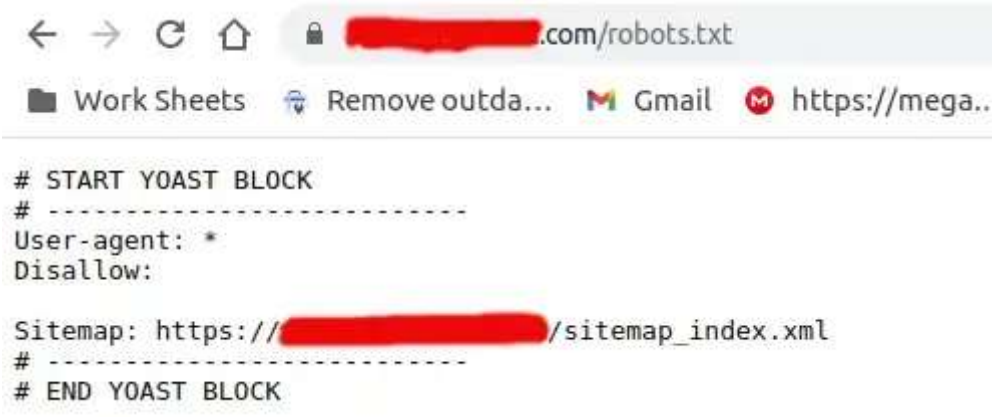
I start visiting the website in my Firefox browser. There is a famous add-on name **Wappalyzer**. So after visiting couple of pages, i clicked on wappalyzer and it shows me that target website using WordPress & Wp-Engine.

Wappalyzer Info

After getting that, before running **wpscan**, i think of visiting a common juicy file name "**robots.txt**". Unfortunately, i didn't get anything special on that file.

> *Remember, always visit all the URL which is disallowed on* ***/robots.txt*** *file.*

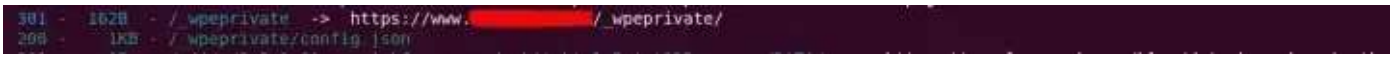
```
https://mehedishakeel.com/robots.txt
```



After, not getting any valuable directory and files listing on "**robots.txt**" file. I thought to look for sensitive directory and file, so i fire up a tool name **dirsearch** which is a very useful tool to find directory and sensitive files faster then **dirb**.

```
dirsearch -u https://mehedishakeel.com
```

and there i find a file directory name "**_wpeprivate/config.json".** This is one of the goldmine of those WordPress website which are using **wpengine.**



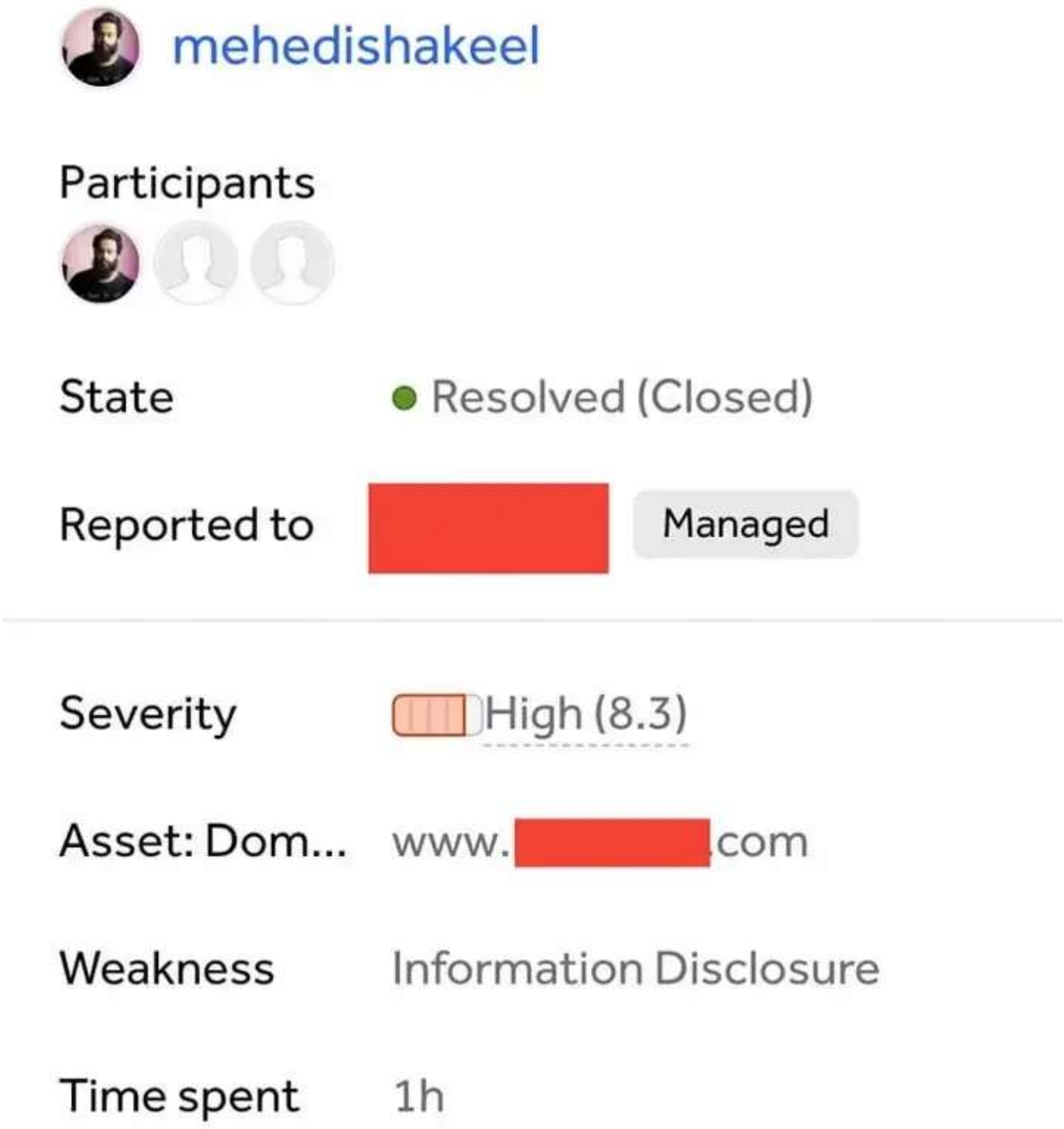
dirsearch output

I open this url with the target domain , and i just got entire database username, password.

```
https://mehedishakeel.com/_wpeprivate/config.json
```

"**_wpeprivate/config.json**" revealed API key of WPEngine, DB username, DB password and so on in plain text. That's how i got my first resolved bug on hackerone.

> *So whenever you got a target with WordPress and WPengine, always look for "**_wpeprivate/config.json**" file.*



Thank you for reading!

Hackerone Bug Bounty Bug Bounty Tips Mehedishakeel Ethical Hacking