mehedishakeel

Nov 17, 2022 · 3 min read · Listen

Information Exposure — My Fourth Finding on Hackerone!

Information Exposure Through Directory Listing — The bug title says everything about it. Find a path or URL on any website that's enable directory listing on your target website and by using that directory listing you have to access any sensitive information. It's different version of **Sensitive Information Disclosure** vulnerability.

Now let's discuss how i get my fourth bug and what are the tools and technique i use, It was a private program, So I am not authorized to include the real domain and company name into this write up. But I will try to explain everything in details so that you can imagine the scenario. On that target program scope I had **30+ domain** and one of those domain look like the following example

```
*.mehedishakeel.com
```

So, I started with subdomain enumeration and basic information collecting with **subfinder** & **httpx** . In bug bounty hunting for collecting subdomains and basic info those tools are very useful and fast enough.

Luckily i, found a huge active subdomain list. Getting the result make me change my regular approach. I decided to stick with this targets for a long time. So, I started with the main domain

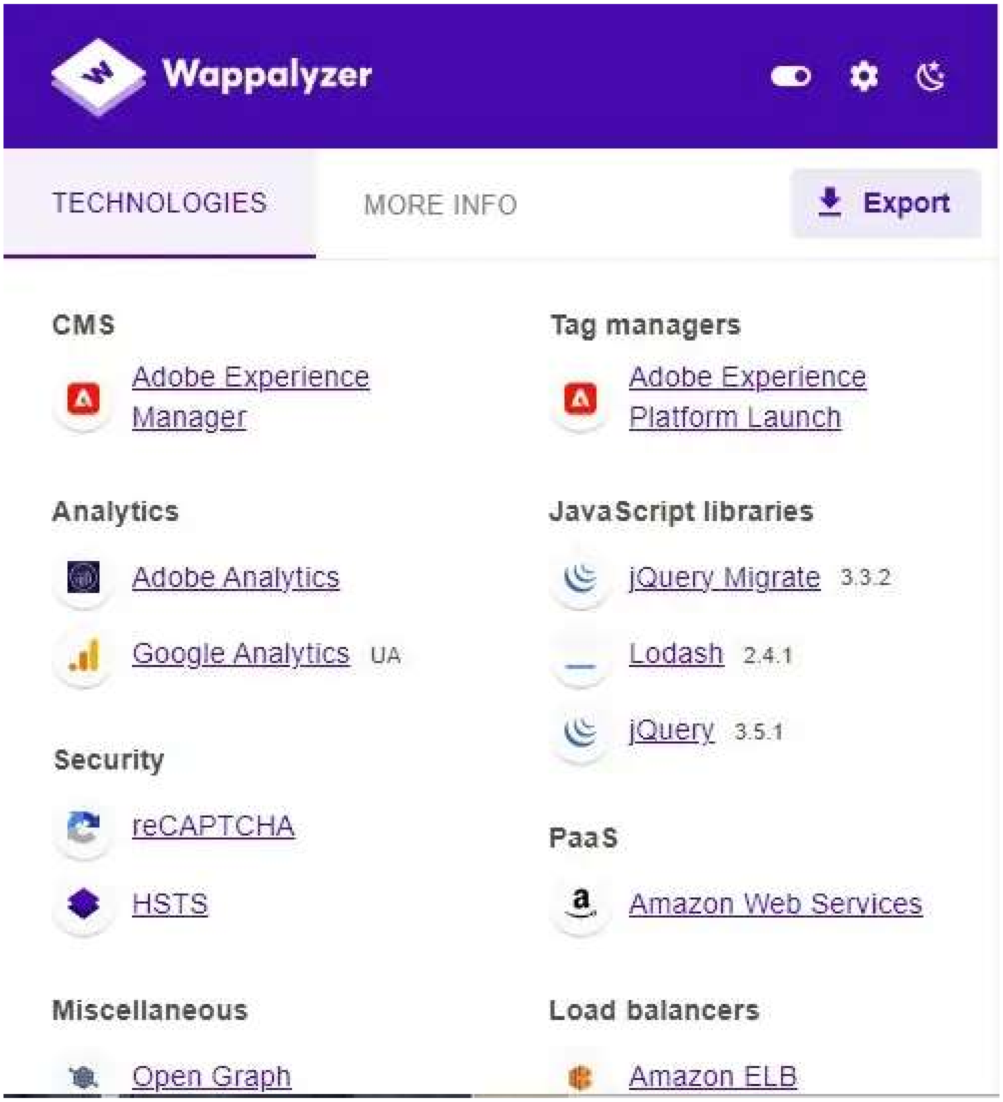
```
https://mehedishakeel.com
```

I open the URL in browser, manually visit every page but didn’t get anything interesting. 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
```

Then I open **Wappalyzer** add-on and get the following result,



CMS
Adobe Experience Manager

Tag managers
Adobe Experience Platform Launch

Analytics
Adobe Analytics
Google Analytics UA

JavaScript libraries
jQuery Migrate 3.3.2
Lodash 2.4.1
jQuery 3.5.1

Security
reCAPTCHA
HSTS

PaaS
Amazon Web Services

Miscellaneous
Open Graph

Load balancers
Amazon ELB

It, was a huge list which contains some technology i didn't know much about them. I started to learn the basic of all the technology used in this website.

But i don't want to waste my time , So here i started to find sensitive information through directory searching using **diresearch**.

If you want to know, how to use "dirsearch" tool to find sensitive information , then go through my **Information Disclosure — My First Finding on Hackerone!** write-up.

By using these automate tool i found a very interesting directory like the following,

```
https://www.mehedishakeel.com/typo3conf/ext/
```

I visit that url and it's enable directory listing, and by navigating every possible directory manually , i found an interesting directory ,

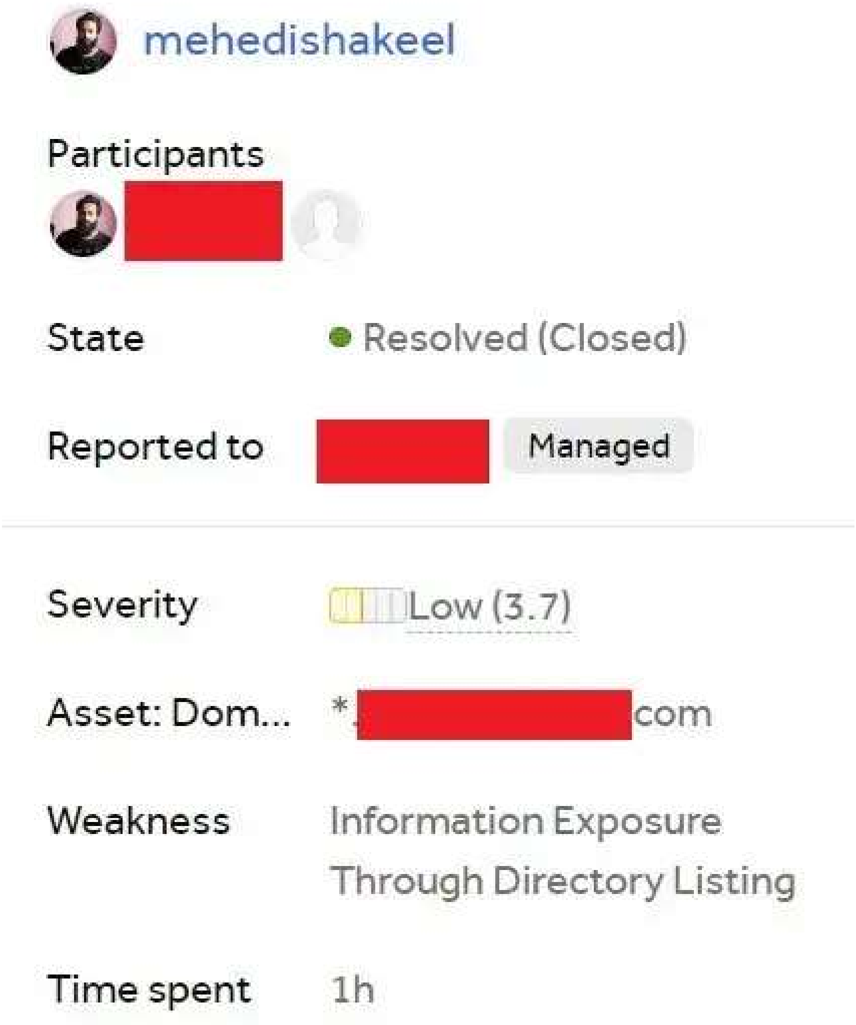
```
ext/static_info_tables
```

These directory contains two juicy file,

```
tables.sql
tables_static.sql
```

I downloaded those two file and open them into notepad, and i see some sql query and some sensitive static data into those sql files.

I quickly reported that bug ,



mehedishakeel

Participants

[redacted]

State	● Resolved (Closed)
Reported to	[redacted] Managed
Severity	Low (3.7)
Asset: Dom...	*.[redacted]com
Weakness	Information Exposure Through Directory Listing
Time spent	1h

That’s how I got my fourth resolved bug on hackerone. Thank you for reading!

Hackerone Bug Bounty Bug Bounty Tips Ethical Hacking Mehedishakeel