Cross Site Scripting (XSS) — My Fifth Finding on HackerOne!

mehedishakeel

3 min read · Just now

Cross Site Scripting (XSS) In ChatBot — Cross site scripting is a vulnerability that allows an attacker to inject malicious code (usually in javascript form) in web applications. it will execute the script in user context allowing the attacker to access any cookies or sessions tokens retained by the browser and many more.

Now let's discuss how i get my fifth 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 50+ **domain** and one of those domain look like the following example

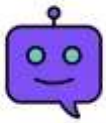
```
*.mehedishakeel.com
```

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, and the first one is about client support. So, I started with the website support subdomain. I open the following url in browser with my favorite common juicy file name “**robots.txt**”.

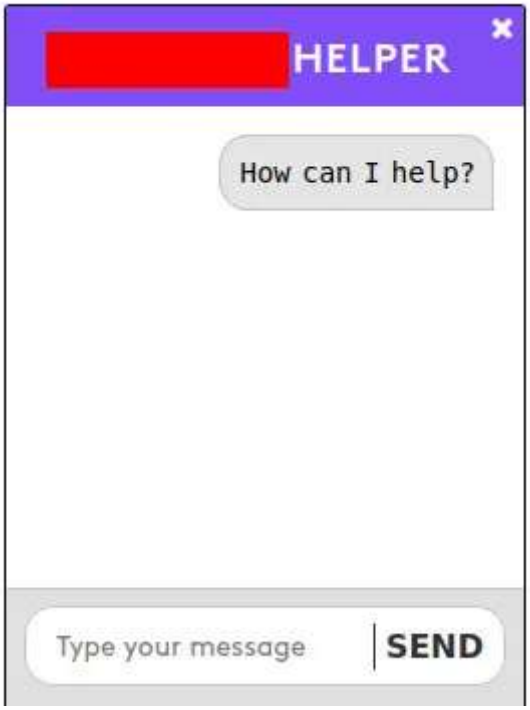
```
https://support.mehedishakeel.com/robots.txt
```

Unfortunately, i didn’t get anything special on that file. Then, i removed the /robots.txt and reload the site, I got a cute little Robot Icon,



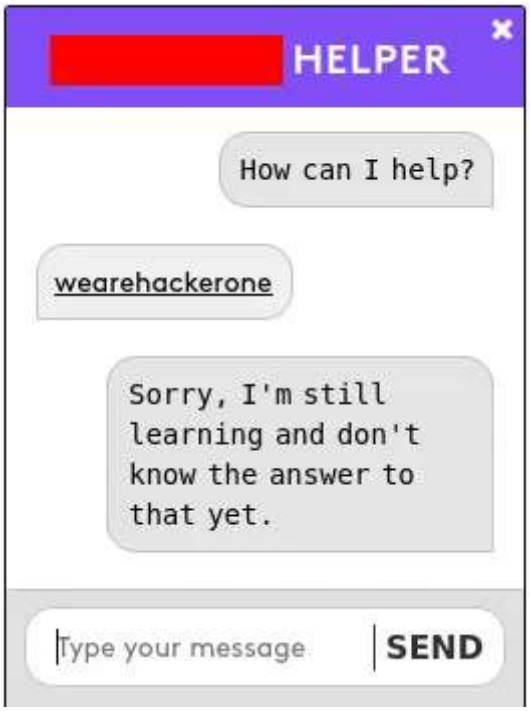
chatbot icon

I clicked on it and a chatbot box pops up on my right hand side corner name take as “**Mehedi Shakeel Helper**”



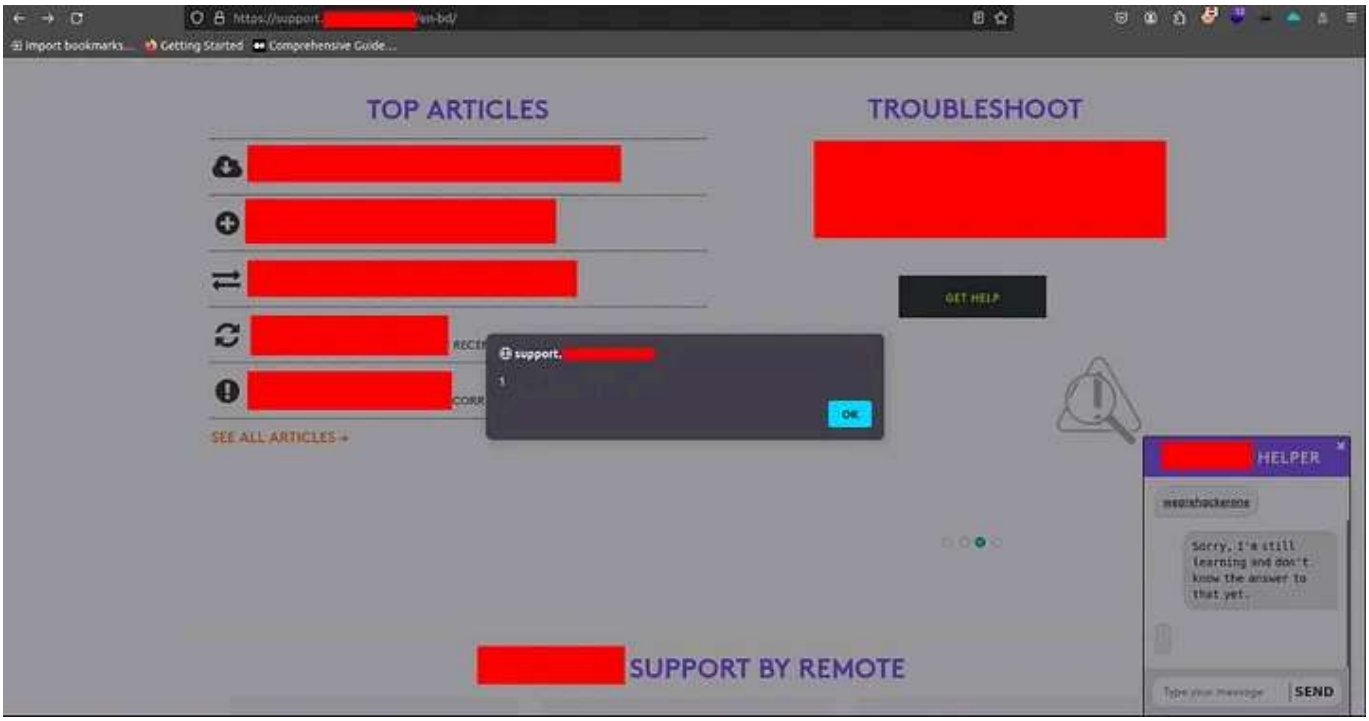
chatbot

It, ask me “**How can i help?**” I send **<u>wearehackerone</u>,** then guess what, it take the **HTML** tag and render it into the box, like the following



So, after that, I deiced to use this oportunity to escalate it into cross site scripting **XSS.** So i, send the following payload as my next message and got an alert

```
<img src=1 href=1 onerror="javascript:alert(1)">
```



XSS Alert

Now it's time submit a quick report, guiding every step to reproduce the bug and make a proper video PoC and submit the bug.

Hackerone Report

Here, my bad luck comes in, someone else submitted a report with this bug previously. My report was marked as duplicated. That's how I got my fifth bug on HackerOne. Thank you for reading!

Bugbounty Writeup | Hackerone | Ethical Hacking | Bug Bounty Tips | Hacking