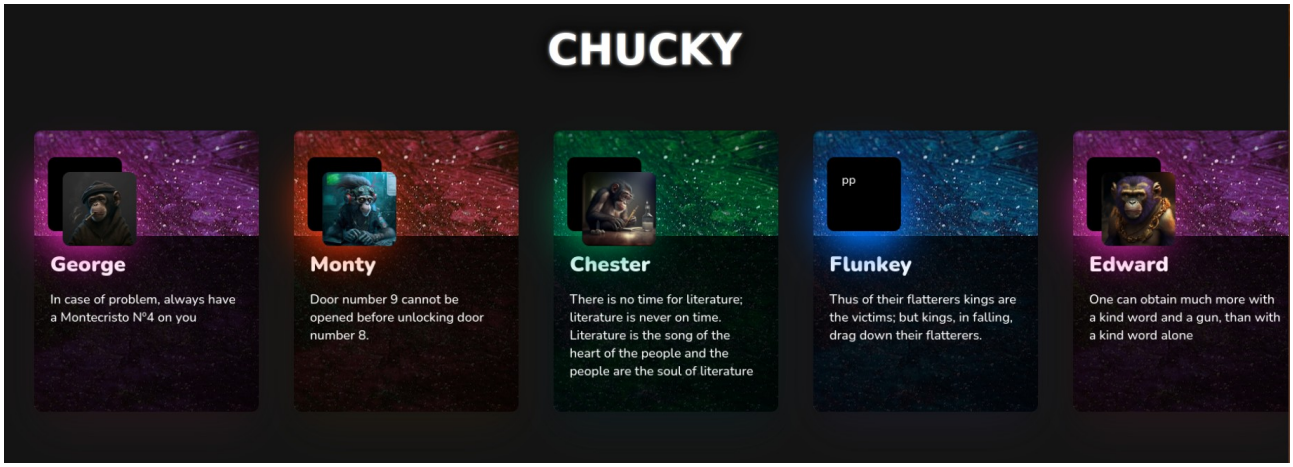
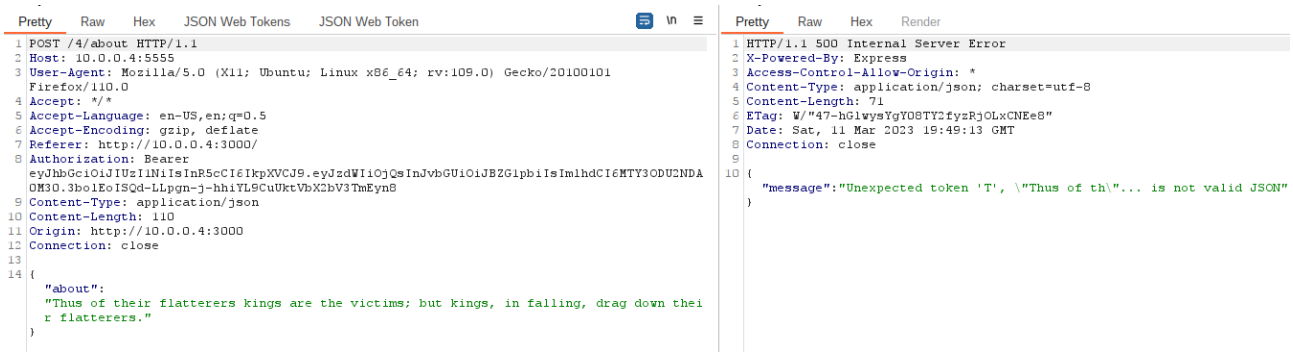
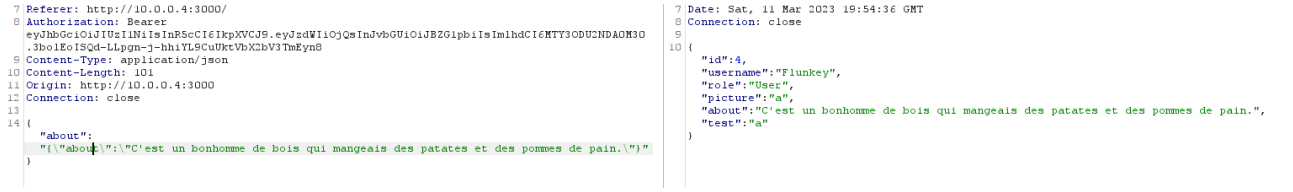
Ce challenge était donné avec des identifiants valides; délicate attention de la part de nos organisateurs. Nous entrons donc avec **Edouard:Str0ngP@ssw0rd!**.



L’application est assez banane en somme, nous pouvons cliquer sur les pseudonymes des singes, et cela nous affiche leur profil en pus grand.
Lorsque nous passons sur notre profil, un bouton *Change* apparait 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 !



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



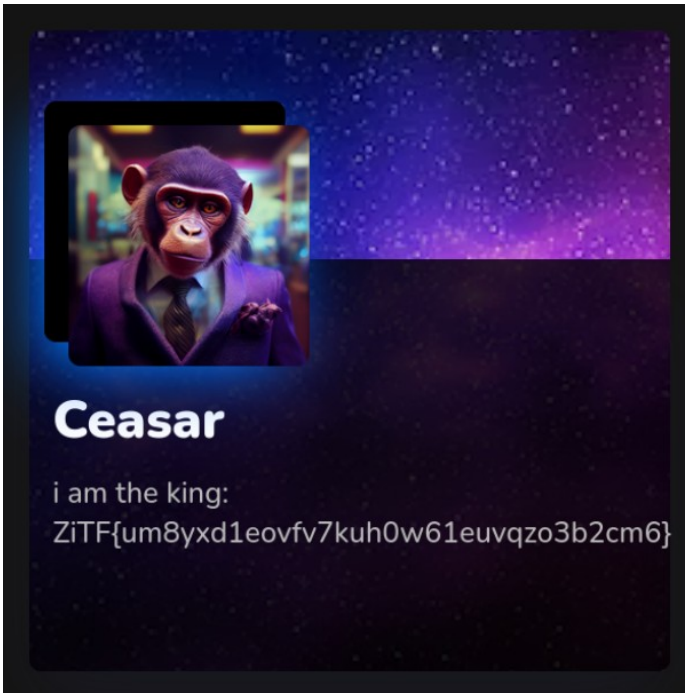
Cette modification est réfléchie sur le site web !

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}**

Écrit par Chelinka le 11 mars 2023