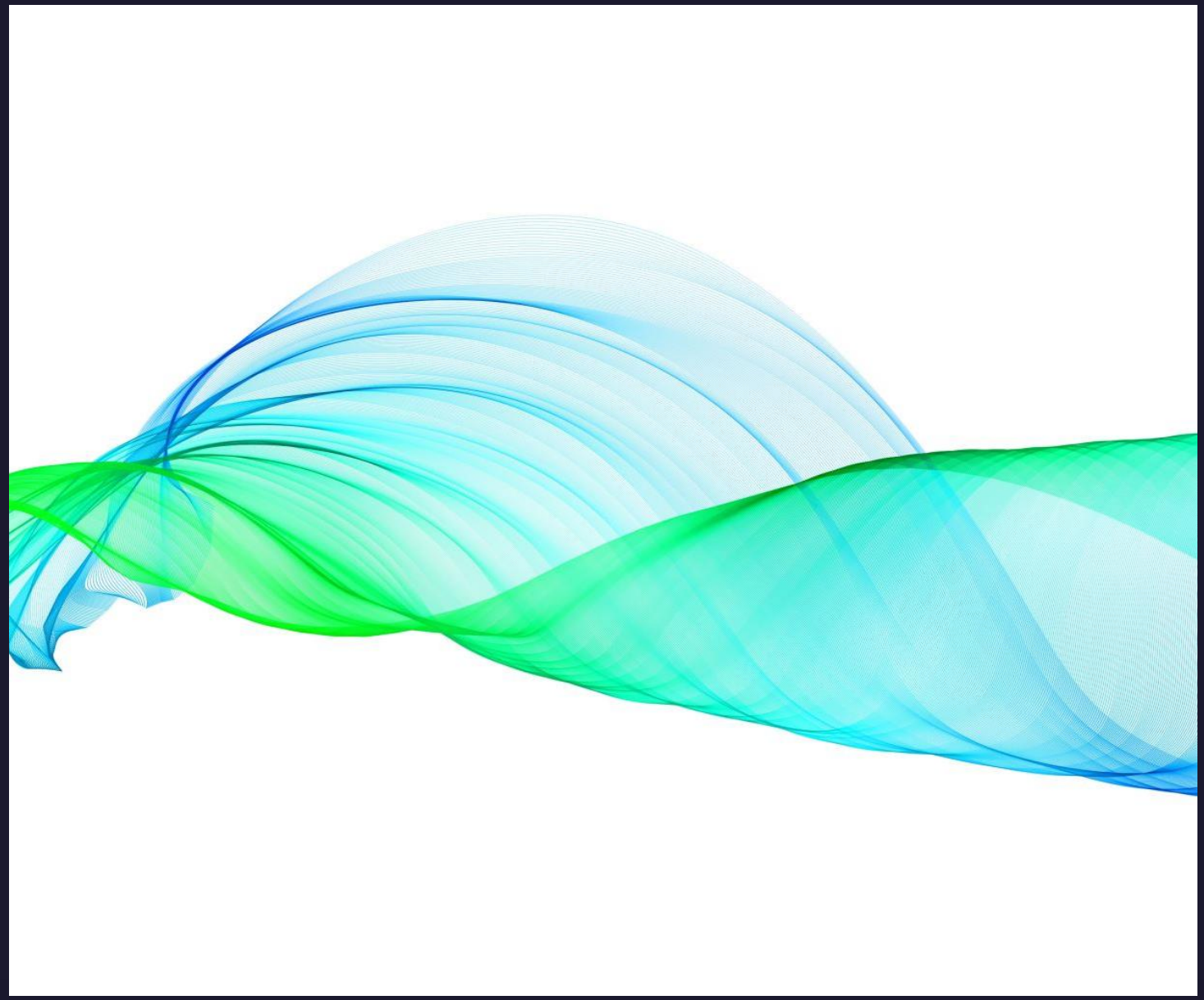
Exercice sold-out

Ismail HAOUAM



Outils utilisés

- Burpsuite:
  - Outils très utilisé en cybersécurité
  - Permets entre autres de voir toutes les requêtes faites par un navigateur
- Postman:
  - Permets de faire des requêtes HTTP précises simplement

Inscription

Request | Response

Raw | Params | Headers | Hex

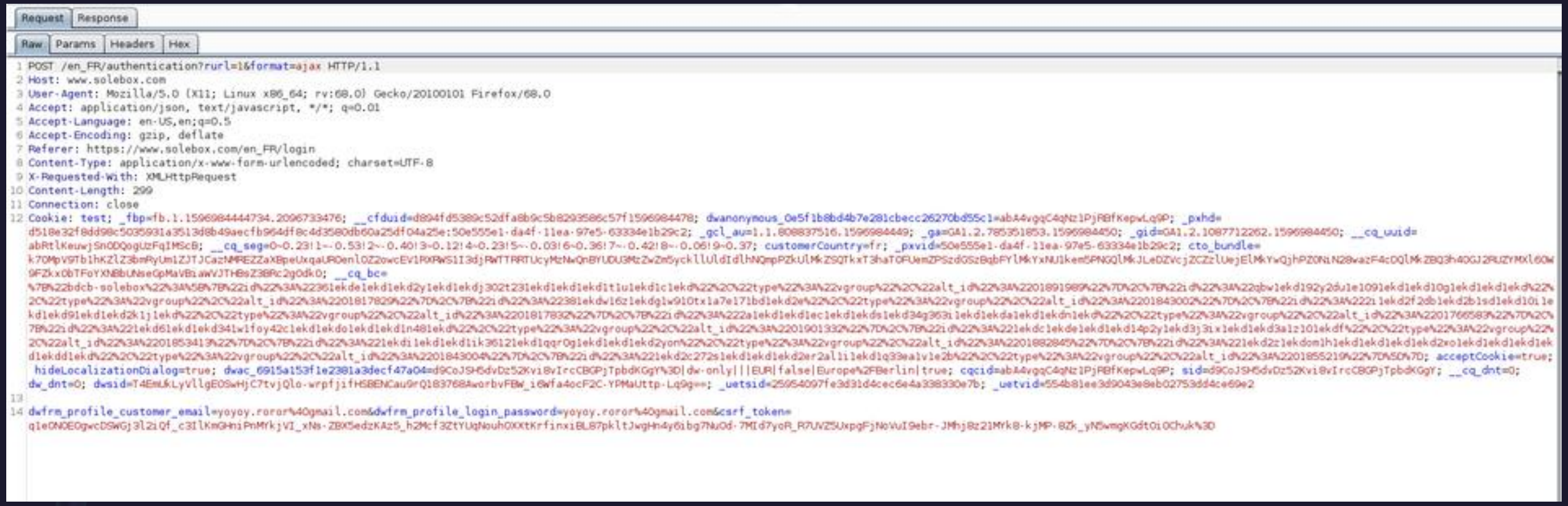
```
POST /on/demandware.store/Sites-solebox-Site/en_FR/Account-SubmitRegistration?rurl=1&format=ajax HTTP/1.1
Host: www.solebox.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.solebox.com/en_FR/registration?rurl=1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 620
Connection: close
Cookie: _fbp=fb.1.1596984444734.2096733476; __cfduid=d894fd5389c52dfa8b9c5b8293586c57f1596984478; dwanonymous_0e5f1b8bd4b7e281cbecc26270bd55c1=abA4vgqC4qNz1PjRBfKepwLq9P; _pxhd=
d518e32f8dd98c5035931a3513d8b49aecfb964df8c4d3580db60a25df04a25e:50e555e1-da4f-11ea-97e5-63334e1b29c2; _gcl_au=1.1.808837516.1596984449; _ga=GA1.2.785351853.1596984450; _gid=GA1.2.1087712262.1596984450; __cq_uuid=
abRtlKeuwjSn0DQogUzFqIMScB; __cq_seg=0~0.23!1~-0.53!2~-0.40!3~0.12!4~0.23!5~-0.03!6~0.36!7~-0.42!8~-0.06!9~0.37; customerCountry=fr; _pxvid=50e555e1-da4f-11ea-97e5-63334e1b29c2; cto_bundle=
k70MpV9Tb1hKZlZ3bmRyUm1ZJTJCazNMREZZaXBpeUxqaUR0enl0Z2owcEV1RXRWS1I3djRWTTRRTUcyMzNwQnBYUDU3MzZwZm5yckllUldIdlhNQmpPZkUlMkZSQTkxT3haT0FUemZPSzdGSzBqbFYlMkYxNU1kem5PNGQlMkJLeDZVcjZCZzlUejElMkYwQjhPZ0NiN28wazF4cDQlMkZBQ3h4OGJ2RUZYMXl6OW
9FZkxObTFoYXNBbUNseGpMaVBiaWVJTHBsZ3BRc2g0dk0; __cq_bc=
%7B%22bdcb-solebox%22%3A%5B%7B%22id%22%3A%2236lekde1ekd1ekd2y1ekd1ekdj302t231ekd1ekd1ekd1t1u1ekd1c1ekd%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201891989%22%7D%2C%7B%22id%22%3A%22qbw1ekd192y2du1e1091ekd1ekd10g1ekd1ekd1ekd%22%
2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201817829%22%7D%2C%7B%22id%22%3A%2238lekdw16z1ekdg1w910tx1a7e171bd1ekd2e%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201843002%22%7D%2C%7B%22id%22%3A%222i1ekd2f2db1ekd2b1sd1ekd10i1e
kd1ekd91ekd1ekd2k1j1ekd%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201817832%22%7D%2C%7B%22id%22%3A%222a1ekd1ekd1ec1ekd1ekds1ekd34g363i1ekd1ekda1ekd1ekdn1ekd%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201766583%22%7D%2C%
7B%22id%22%3A%221ekd61ekd1ekd341w1foy42c1ekd1ekdo1ekd1ekd1n481ekd%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201901332%22%7D%2C%7B%22id%22%3A%221ekdc1ekde1ekd1ekd14p2y1ekd3j3ix1ekd1ekd3a1z101ekdf%22%2C%22type%22%3A%22vgroup%22%
2C%22alt_id%22%3A%2201853413%22%7D%2C%7B%22id%22%3A%221ekdi1ekd1ekd1ik3612lekd1qqr0g1ekd1ekd1ekd2yon%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201882845%22%7D%2C%7B%22id%22%3A%221ekd2z1ekdom1h1ekd1ekd1ekd1ekd2xo1ekd1ekd1ekd1ek
d1ekdd1ekd%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201843004%22%7D%2C%7B%22id%22%3A%221ekd2c272s1ekd1ekd1ekd2er2all1ekd1q33ea1v1e2b%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201855219%22%7D%5D%7D; acceptCookie=true;
 hideLocalizationDialog=true; _px3=
befdeed3b34920129394f50e97bc6c9fb7c03e384c7b2ba81a2d0a19fd9d16ae:f+Rv3KKPvIuVdSBJhuXeuEf8AbbYT5eRs1uYio3au8TTt6SaHSh3elxfpqoKWeOcoM8WuWi1jba/qfeJNgr6mg==:1000:qfpDZn7oTJdorcYnn8RQPsX5wgvFb3dbykGZ4E6uOTcYWgXrCLNazQ9AURZ2OnII7MMfLUms5Py
6Ln/u/7czdhwNuSg4taHP4LcGlNZJHdZxYaruCuipBHzehDcHFPcFaHzB4xgUUB69E361iRsUSR0CGwAK5t4zc/x72cxhMro=; dwac_6915a153f1e2381a3decf47a04=xRh41jgYOW3N011xZFLzhQ4BuLl54gr-Tck%3D|dw-only|||EUR|false|Europe%2FBerlin|true; cqcid=
abA4vgqC4qNz1PjRBfKepwLq9P; sid=xRh41jgYOW3N011xZFLzhQ4BuLl54gr-Tck; __cq_dnt=0; dw_dnt=0; dwsid=6NIV_FMqbpizmgfaEG_bKSPL1ZMS0F0LM4CPUWTwRfe_QobBNLRDvOEgyO6vtOMKrB-NjTbwIYNj1LxHfPmpiA==; _uetsid=25954097fe3d31d4cec6e4a338330e7b;
_uetvid=554b81ee3d9043e8eb02753dd4ce69e2

dwfrm_profile_register_title=Herr&dwfrm_profile_register_firstName=rajeshp&dwfrm_profile_register_lastName=raj&dwfrm_profile_register_email=rajesh%40gmail.com&dwfrm_profile_register_emailConfirm=rajesh%40gmail.com&
dwfrm_profile_register_password=rajesh%40gmail.com&dwfrm_profile_register_passwordConfirm=rajesh%40gmail.com&dwfrm_profile_register_phone=&dwfrm_profile_register_birthday=&dwfrm_profile_register_acceptPolicy=true&csrf_token=
_507Tu0-V8beaVqO2aGqxXHqBmWOm5kg9v_N4cbpC47oj9mpr6FojNjP9edWoFzU2S-JJKF_XubYD6ufyAFNDP8kzf4sHDOApXmIGzs9zF_z-TvtlU7nFDVcQtbdoD4wIasnMLo7SJw5l57nLw1yTkApQi9Hpo3sKoug-uR80fxiddW-dSo%3D
```

Etapes à suivre pour s'inscrire

- Charger la page d'inscription
- Récupérer le token anti-csrf
- Simuler l'envoi de formulaire avec les données récupérées

Connection



Request | Response

Raw | Params | Headers | Hex

```
POST /en_FR/authentication?rurl=1&format=ajax HTTP/1.1
Host: www.solebox.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.solebox.com/en_FR/login
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 299
Connection: close
Cookie: test; _fbp=fb.1.1596984444734.2096733476; __cfduid=d804fd5389c52dfa8b9c5b8293586c57f1596984478; dwanonymous_0e5f1b8bd4b7e281cbecc26270bd55c1=abA4vgqC4qNz1PjRBfKepwLq9P; _pxhd=
d518e32f8dd98c5035931a3513d8b49aecfb964df8c4d3580db60a25df04a25e:50e555e1-da4f-11ea-97e5-63334e1b29c2; _gcl_au=1.1.808837516.1596984449; _ga=GA1.2.785351853.1596984450; _gid=GA1.2.1087712262.1596984450; __cq_uuid=
abRtlKeuwjSnODQogUzFqIMScB; __cq_seg=0~0.23!1~0.53!2~0.40!3~0.12!4~0.23!5~0.03!6~0.36!7~0.42!8~0.06!9~0.37; customerCountry=fr; _pxvid=50e555e1-da4f-11ea-97e5-63334e1b29c2; cto_bundle=
k7OMpV9Tb1hKZlZ3bmRyUm1ZJTJCazNMREZZaXBpeUxqaURDenlOZ2owcEV1RXRWS1I3djRWTTRRTUcyMzNwQnBYUDU3MzZwZm5yckllUldIdlhNQmpPZkUlMkZSQTkxT3haTOFUemZPSzdGSzBqbFYlMkYxNU1kem5PNGQlMkJLeDZVcjZCZzlUejElMkYwQjhPZ0N1N28wazF4cDQlMkZBQ3h4OGJ2RUZYMXl60W
9FZkxObTFoYXNBbUNseGpMaVB1aWVJTHBsZ3BRc2gOdkO; __cq_bc=
%7B%22bdcb-solebox%22%3A%5B%7B%22id%22%3A%2236lekde1ekd1ekd2y1ekd1ekdj302t231ekd1ekd1ekd1t1u1ekd1c1ekd%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201891989%22%7D%2C%7B%22id%22%3A%22qbw1ekd192y2du1e1091ekd1ekd10g1ekd1ekd1ekd%22%
2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%22018178Z9%22%7D%2C%7B%22id%22%3A%2238lekdw16z1ekdg1w910tx1a7e171bd1ekd2e%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201843002%22%7D%2C%7B%22id%22%3A%222i1ekd2f2db1ekd2b1sd1ekd10i1e
kd1ekd91ekd1ekd2k1j1ekd%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%22018178J2%22%7D%2C%7B%22id%22%3A%222a1ekd1ekd1ec1ekd1ekds1ekd34g363i1ekd1ekda1ekd1ekdn1ekd%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201766583%22%7D%2C%
7B%22id%22%3A%221ekd61ekd1ekd34lw1foy42c1ekd1ekdo1ekd1ekd1n481ekd%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201901332%22%7D%2C%7B%22id%22%3A%221ekdc1eke1ekd1ekd14p2y1ekd3j3ix1ekd1ekd3a1z101ekdf%22%2C%22type%22%3A%22vgroup%22%
2C%22alt_id%22%3A%2201853413%22%7D%2C%7B%22id%22%3A%221ekd11ekd1ekd1ik36121ekd1qqr0g1ekd1ekd1ekd2yon%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201882845%22%7D%2C%7B%22id%22%3A%221ekd2z1ekdom1h1ekd1ekd1ekd1ekd2xo1ekd1ekd1ekd1ek
d1ekdd1ekd%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201843004%22%7D%2C%7B%22id%22%3A%221ekd2c272s1ekd1ekd1ekd2er2al1i1ekd1q39ea1v1e2b%22%2C%22type%22%3A%22vgroup%22%2C%22alt_id%22%3A%2201855219%22%7D%5D%7D; acceptCookie=true;
 hideLocalizationDialog=true; dwac_6915a153f1e2381a3decf47a04=d9CoJSH5dvDz52Kvi8vIrcCBGPjTpbdKGgY%3D|dw-only|||EUR|false|Europe%2FBerlin|true; cqcid=abA4vgqC4qNz1PjRBfKepwLq9P; sid=d9CoJSH5dvDz52Kvi8vIrcCBGPjTpbdKGgY; __cq_dnt=0;
dw_dnt=0; dwsid=T4EmLkLyVllgEOSwHjC7tvjQlo-wrpfjifHSBENCau9rQ183768AworbvFBW_i6Wfa4ocF2C-YPMaUttp-Lq9g==; _uetsid=25954097fe3d31d4cec6e4a338330e7b; _uetvid=554b81ee3d9043e8eb02753dd4ce69e2

dwfrm_profile_customer_email=yoyoy.roror%40gmail.com&dwfrm_profile_login_password=yoyoy.roror%40gmail.com&csrf_token=
q1eON0EOgwcDSWGj3l2iQf_c3IlKmGHniPnMYkjVI_xNs-ZBX5edzKAz5_h2Mcf3ZtYUgNouhOXXtKrfinxiBL87pkltJwgHn4y6ibg7NuOd-7MId7ycR_R7UVZ5UxpgFjNoVuI9ebr-JMhj8z21MYk8-kjMP-8Zk_yN5wmgKGdtOiOChuk%3D
```

Etapes à suivre pour se connecter

- Charger la page de connection
- Récupérer le token anti-csrf
- Passer outre les protections anti-bot:
  - Charger "/on/demandware.static/Sites-solebox-Site/-/en_FR/v1596872710721/js/accountNamespace.js"
  - Charger "/on/demandware.store/Sites-solebox-Site/en_FR/Page-GetCustomerCountry?format=ajax"
- Simuler l'envoi de formulaire avec les données récupérées

Etapes que suis le navigateur pour ajouter une paire de chaussures au panier

- Fait une requête "GET" vers "$nom_page?chosen=size&$variable=$taille&format=ajax":
- Récupere l'identifiant de la paire de chaussures
- Fait un requête "GET" vers "/on/demandware.store/Sites-solebox-Site/en_FR/Product-Extras?format=ajax&pid=$identifiant&format=ajax "
- Fait une requête "POST" vers "/en_FR/add-product?format=ajax":
  - Mets dans le body l'identifiant du produit ainsi que les options choisies

$nom_page?chosen=size&$variable=$taille&format=ajax

- Lorsque j'essaie de faire une requête "GET" envers cette page j'obtiens (403):

{"appId":"PXuR63h57Z","jsClientSrc":"//client.perimeterx.net/PXuR63h57Z/main.min.js","firstPartyEnabled":false,"vid":"","uuid":"e17fb390-dbce-11ea-91ed-f1b7a0abf835","hostUrl":"https://collector-pxur63h57z.perimeterx.net","blockScript":"//captcha.px-cdn.net/PXuR63h57Z/captcha.js?a=c&u=e17fb390-dbce-11ea-91ed-f1b7a0abf835&v=&m=0"}
sleeping

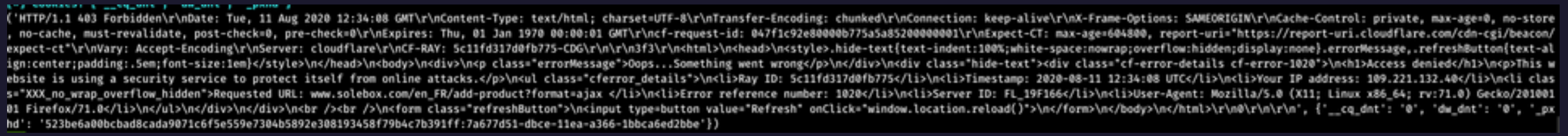
- Ma requête se fait bloquer par perimeterx
- Ce service serait vulnérable à des librairies telles que cloudscraper ou selenium

/on/demandware.store/Sites-solebox-Site/en_FR/Product-Extras?format=ajax&pid=$identifiant&format=ajax

- Il faut normalement récupérer le contenu de la variable "pid" en faisant la requête précédente
- Il est possible de forger la valeur de "pid" avec une quasi-certitude avec des informations récupérés sur la page
- J'arrive à obtenir un status 200 en faisant cette requête

/en_FR/add-product?format=ajax

- Lorsque l'on fait cette requête sans que le serveur ne nous ait donné la valeur de la variable "pid" on obtiens cela (403):



- Ma requête est bloquée par cloudflare
- Ce service aussi serait vulnérable à des librairies telles que cloudscraper ou selenium

Difficultés rencontrés

- La librairie s'arrête de lire le socket à la fin du timeout, indépendamment de la complétion de la requête j'ai donc été contraint de mettre un timeout élevé pour garantir le bon fonctionnement du Bot
- Je n'ai pas réussi à ajouter une chaussure au panier en utilisant la libraire "Requet", je pourrais cependant y arriver avec selenium en émulant un navigateur et en simulant l'utilisation d'une souris