Contents

[1. Trickster 2](#_Toc198818849)

[2. NoSQL injection 2](#_Toc198818850)

[3. Apriti Sesamo 2](#_Toc198818851)

[4. SOAP 2](#_Toc198818852)

[5. More sqli 2](#_Toc198818853)

[6. Roboto Sans 3](#_Toc198818854)

[7. sqliLite 3](#_Toc198818855)

[8. MatchTheRegex 4](#_Toc198818856)

[9. Power cookies 4](#_Toc198818857)

# Trickster

Find whether this website is php or not. Use index.php or index.phps to try. If yes, use robots.txt and read the disallow file. Then it gives the hint.

You need to find a simple php webshell . Put it as webshell.png.php to trick the website. After upload, you can search content in /var/www/html. Open the suspicious file.

# NoSQL injection

You need to get the post packet which can be catch in network tab in inspect. Then, edit and resend with this payload:

{"email":"{\"$ne\":null}","password":"{\"$ne\":null}"}

You will log in complete and get a packet which contains the suspicious token with base 64 encryption

# Apriti Sesamo

You need to view page source. Put ~ at the back of the url to force website to get newest version of file. Then decrypt with our best friend deepseek. We know that there’s a condition that if sha hash for username is same as sha hash for password, it will show out the flag. So, I use two pdf with same hash and put it in post request to the website by python. In webshell, type “python3 sha1.py” and wait

# SOAP

When you inspect the post package , you will see there is xml version. You can use xml exploitation for this.

<!--?xml version="1.0" ?-->

<!DOCTYPE foo [<!ENTITY example SYSTEM "/etc/passwd"> ]>

<data>&example;</data>

Send it again with burpsuite, website inspect will block.

# More sqli

You need to bypass the sql by putting ‘ or 1=1-- into the password section. This is because it will make password== ‘’ or 1=1-- . It will direct us to the table page. Now there is 2 ways:

1. First is use burpsuite catch the package. The flag is in the package once you logged in but not appear in website
2. Use sql system table to find it. You will find what table is in the sql by Algies' union select sql,1,1 from sqlite\_master;-- Algies is the component on the current table. Then find the table which has the flag in it . By opening it, use Algiers' union select flag,id,1 from more\_table;-- flag is the component in the more\_table.

# Roboto Sans

You already get hint by the names. Try robots.txt at the end of url. After that , you decrypt the 2 lines of base64 ciphertext. 2 line decrypt is half useless and get flag1.txt. You try search flag1.txt and get nothing. Then, remove the first line and decrypt second line. You will get js/myfile.txt, put it on end of url.

# sqliLite

try bypass with these in password

SQLi lite injection

' or 1=1; '

Admin’ –

‘ /\*

‘;

ad'||'min';

username='sobatista'//UNION//SELECT////FROM//users//LIMIT/\*/1;

a’ is not ‘b This is for password

Authentication bypass

Then you inspect the page after you log in successfully

# MatchTheRegex

View page source, you will see something suspicious on script. Then, you can see it accept any variables that starts from p and ends with F!?. Type picoCTF!? And you get the flag.

# Power cookies

You can inspect and see the cookie or use burpsuite to change the cookie. You also can do with kali command

# SQL Direct

Type \l to list out all the databases

Type \c to connect the database

\d list out all the tables

Type select tablename; (must be all lowercase)

Type select \* from tablename (must be all lowercase)