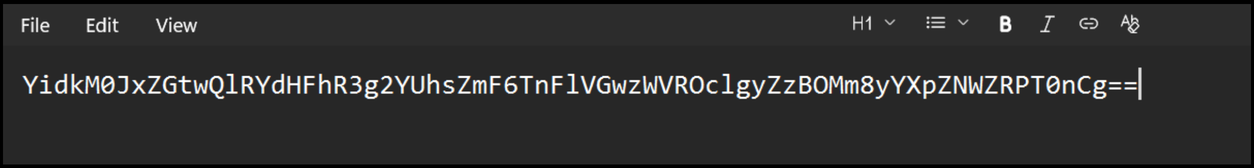
PicoCTF Challenges

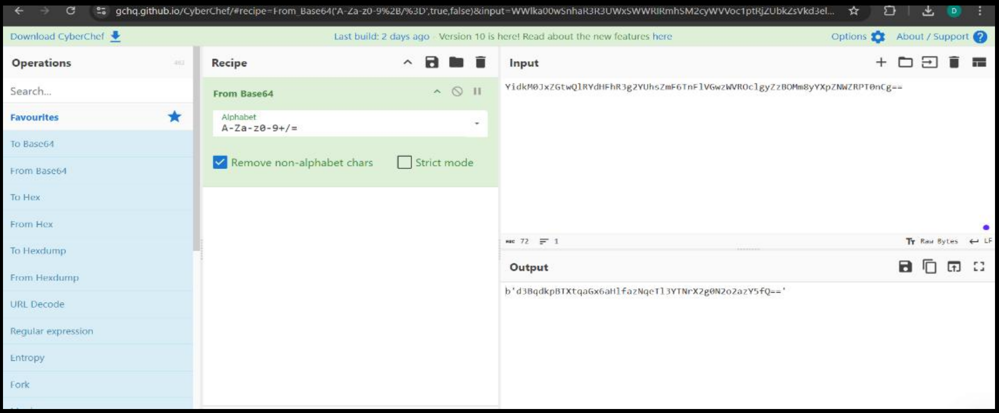
1) Steps for 1st CTF

1) first download the file and the content that are present in some random strings.



```
YidkM0JxZGtwQlRYdHFhR3g2YUhsZmF6TnFlVGwzWVROclgyZzBOMm8yYXpZNWZRPT0nCg==
```

2) than use cyber chef to decrypt the text in file.


gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=WWlka00wSnhaR3R3UWxSWWRIRmhSM2cyWVVoc1ptRjZUbkZsVkd3el...
Download CyberChef
Last build: 2 days ago · Version 10 is here! Read about the new features here
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Recipe
Input
Output
72
1
Raw Bytes
LF

From Base64

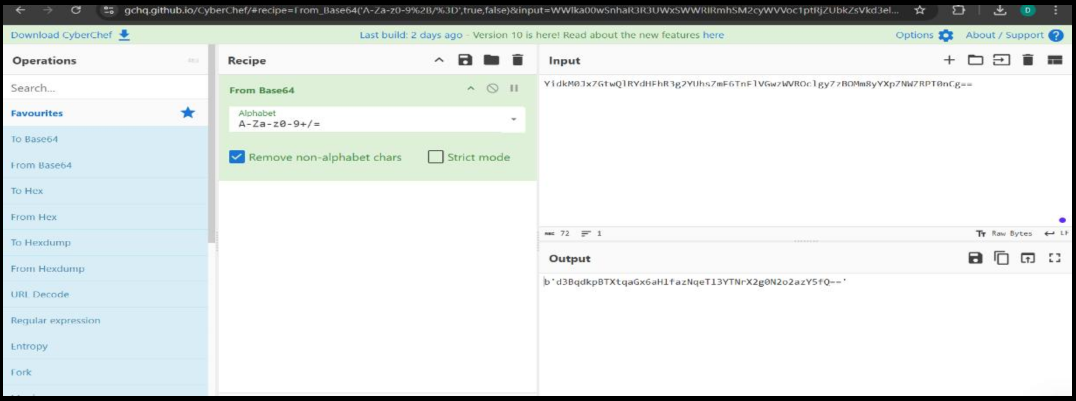
Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

```
YidkM0JxZGtwQlRYdHFhR3g2YUhsZmF6TnFlVGwzWVROclgyZzBOMm8yYXpZNWZRPT0nCg==
```

```
b'd3BqdkpBTXtqaGx6aHlfazNqeTl3YTNrX2g0N2o2azY5fQ=='
```

3) use base 64 and rot 13 bruteforce to decode it.


gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=WWlka00wSnhaR3R3UWxSWWRIRmhSM2cyWVVoc1ptRjZUbkZsVkd3el...
Download CyberChef
Last build: 2 days ago · Version 10 is here! Read about the new features here
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Recipe
Input
Output
72
1
Raw Bytes
LF

From Base64

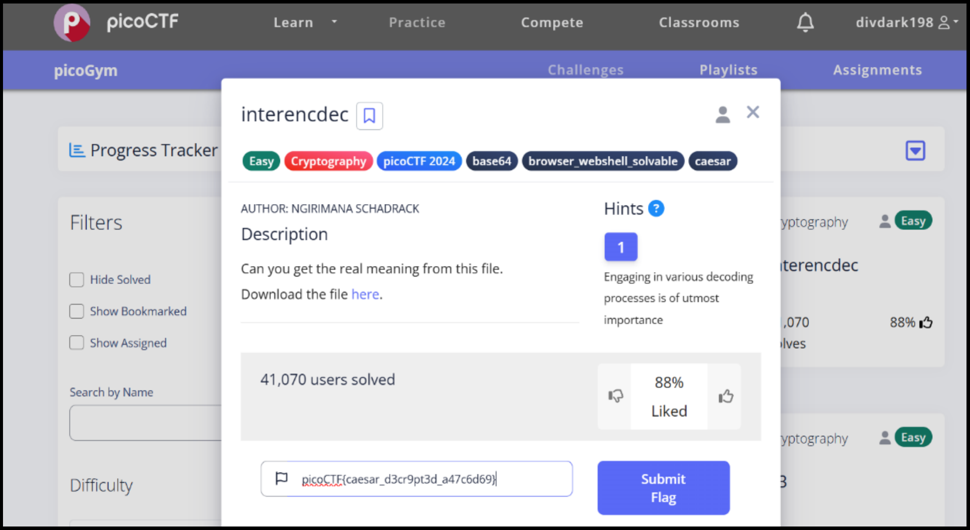
Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

```
YidkM0JxZGtwQlRYdHFhR3g2YUhsZmF6TnFlVGwzWVROclgyZzBOMm8yYXpZNWZRPT0nCg==
```

```
b'd3BqdkpBTXtqaGx6aHlfazNqeTl3YTNrX2g0N2o2azY5fQ=='
```

4) after this we will get our flag.



interencdec

Easy | Cryptography | picoCTF 2024 | base64 | browser_webshell_solvable | caesar

AUTHOR: NGIRIMANA SCHADRACK

Description

Can you get the real meaning from this file.
Download the file here.

Hints

1

Engaging in various decoding processes is of utmost importance

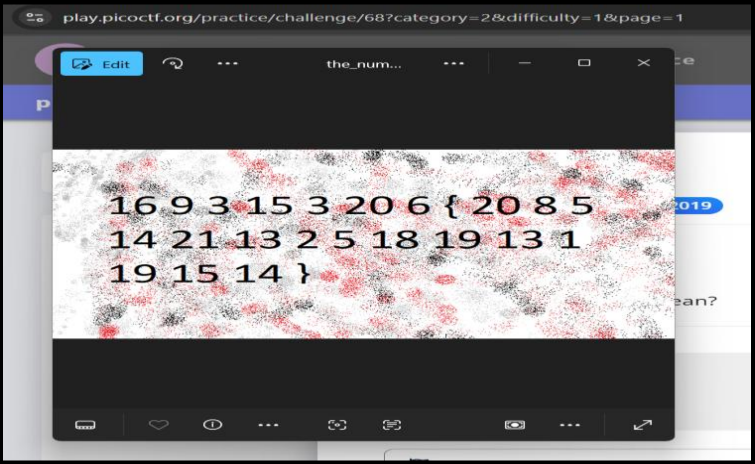
41,070 users solved

88% Liked

picoCTF{caesar_d3cr9pt3d_a47c6d69}

2) Steps for 2nd CTF

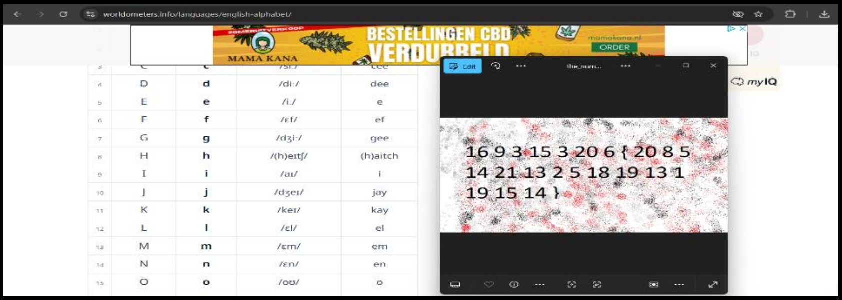
1) we will download the .jpg from challenge.



play.picoctf.org/practice/challenge/68?category=2&difficulty=1&page=1

16 9 3 15 3 20 6 { 20 8 5
14 21 13 2 5 18 19 13 1
19 15 14 }

2) we will decode it using its letters in the no. form.

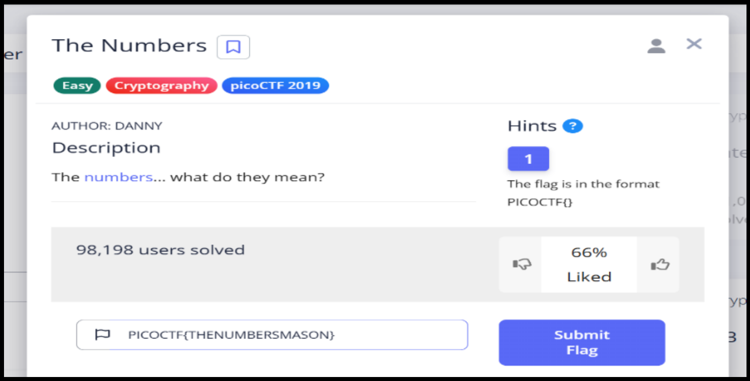


worldometers.info/languages/english-alphabet/

3	C	c	/siː/	cee
4	D	d	/diː/	dee
5	E	e	/iː/	e
6	F	f	/ɛf/	ef
7	G	g	/dʒiː/	gee
8	H	h	/(h)eɪtʃ/	(h)aitch
9	I	i	/aɪ/	i
10	J	j	/dʒeɪ/	jay
11	K	k	/keɪ/	kay
12	L	l	/ɛl/	el
13	M	m	/ɛm/	em
14	N	n	/ɛn/	en
15	O	o	/oʊ/	o

16 9 3 15 3 20 6 { 20 8 5
14 21 13 2 5 18 19 13 1
19 15 14 }

3) than we will get the flag.



The Numbers

AUTHOR: DANNY

Description

The numbers... what do they mean?

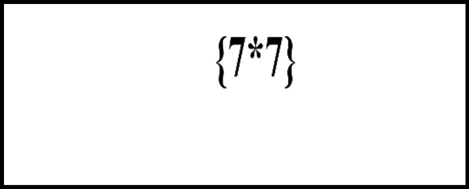
The flag is in the format PICOCTF{}

PICOCTF{THENUMBERSMASON}

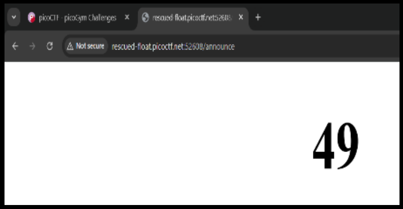
3) Steps for 3rd CTF

1) a search bar will appear after launching inctance.

2) now we will check the ssti1 vulnerability.

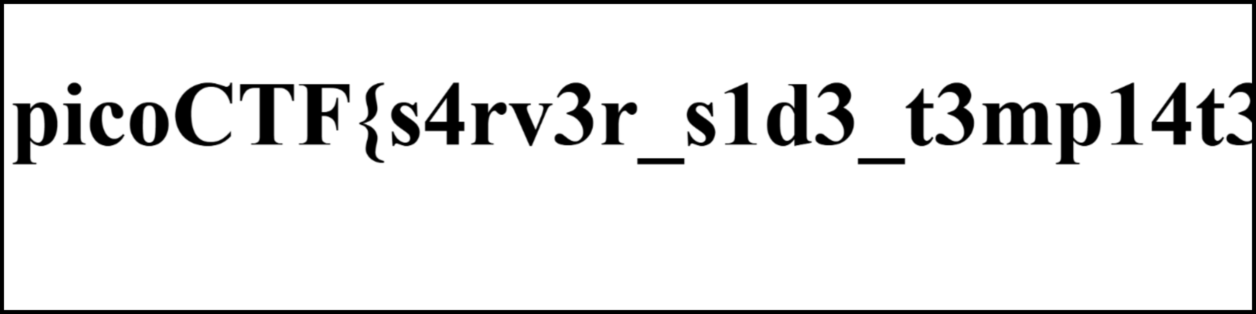


{7*7}


picoCTF - picoGym Challenges
rescued-float.picoctf.net:52608/
Not secure
rescued-float.picoctf.net:52608/announce

49

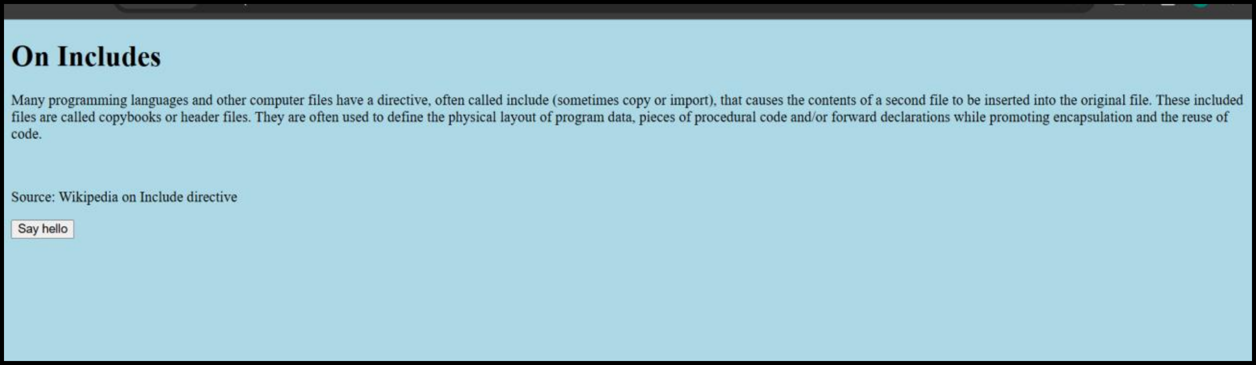
3) now we will use SSTI1 exploit command to exploit it and get the flag using ls and cat (filename) command in exploit command.



picoCTF{s4rv3r_s1d3_t3mp14t3

4) Steps for 4th CTF

1) after starting the machine we get on the website.

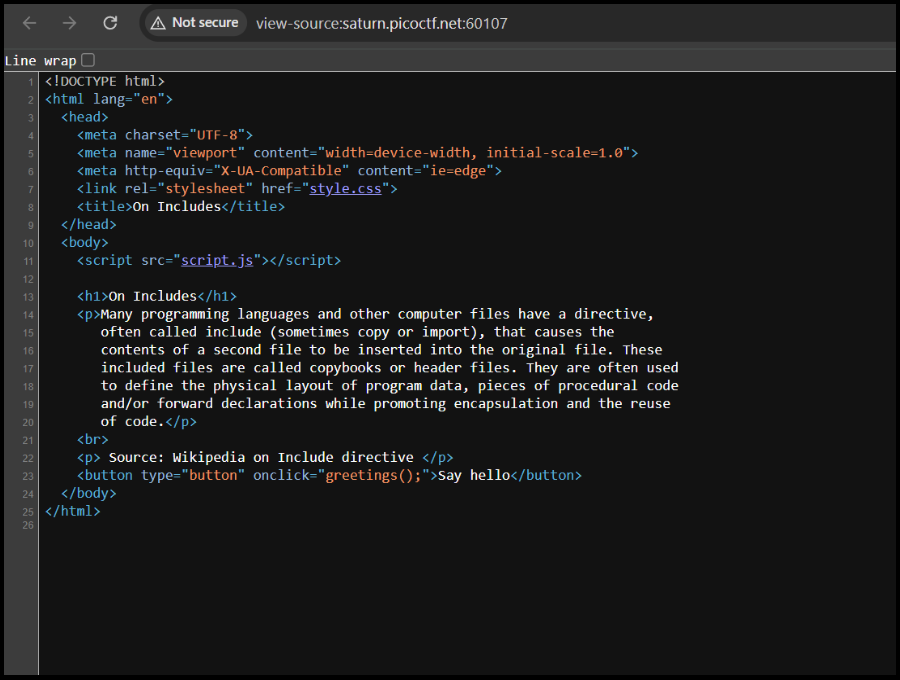


On Includes

Many programming languages and other computer files have a directive, often called include (sometimes copy or import), that causes the contents of a second file to be inserted into the original file. These included files are called copybooks or header files. They are often used to define the physical layout of program data, pieces of procedural code and/or forward declarations while promoting encapsulation and the reuse of code.

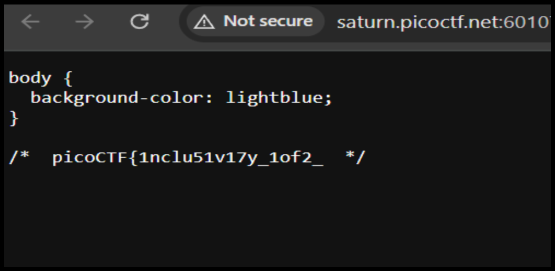
Source: Wikipedia on Include directive

2) we will check for its source code for vulnerability.

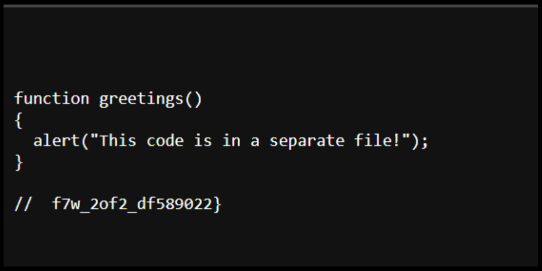


```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <link rel="stylesheet" href="style.css">
    <title>On Includes</title>
  </head>
  <body>
    <script src="script.js"></script>

    <h1>On Includes</h1>
    <p>Many programming languages and other computer files have a directive,
       often called include (sometimes copy or import), that causes the
       contents of a second file to be inserted into the original file. These
       included files are called copybooks or header files. They are often used
       to define the physical layout of program data, pieces of procedural code
       and/or forward declarations while promoting encapsulation and the reuse
       of code.</p>
    <br>
    <p> Source: Wikipedia on Include directive </p>
    <button type="button" onclick="greetings();">Say hello</button>
  </body>
</html>
```

3) in script.js and styple.css we will get our flag in two parts.



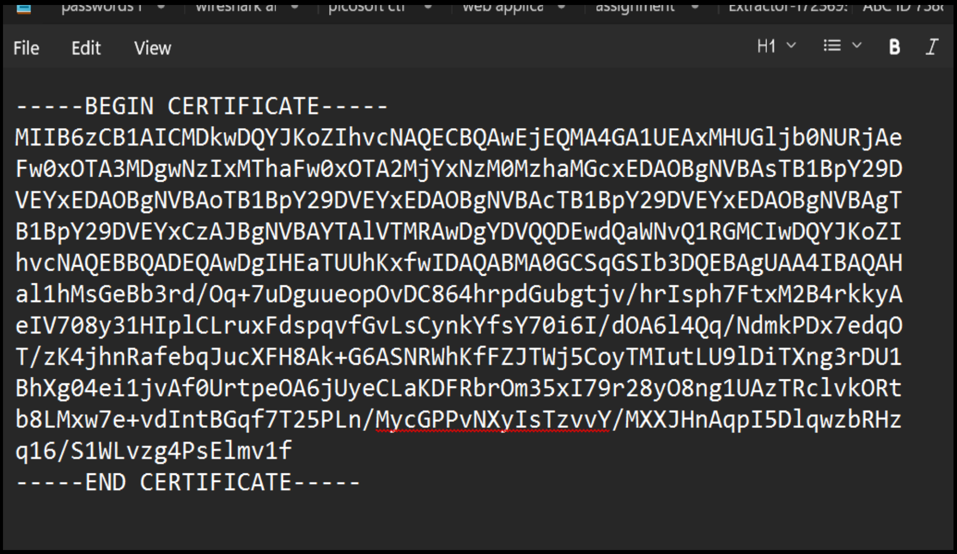
```
body {
  background-color: lightblue;
}

/*  picoCTF{1nclu51v17y_1of2_  */
```



```
function greetings()
{
  alert("This code is in a separate file!");
}

//  f7w_2of2_df589022}
```

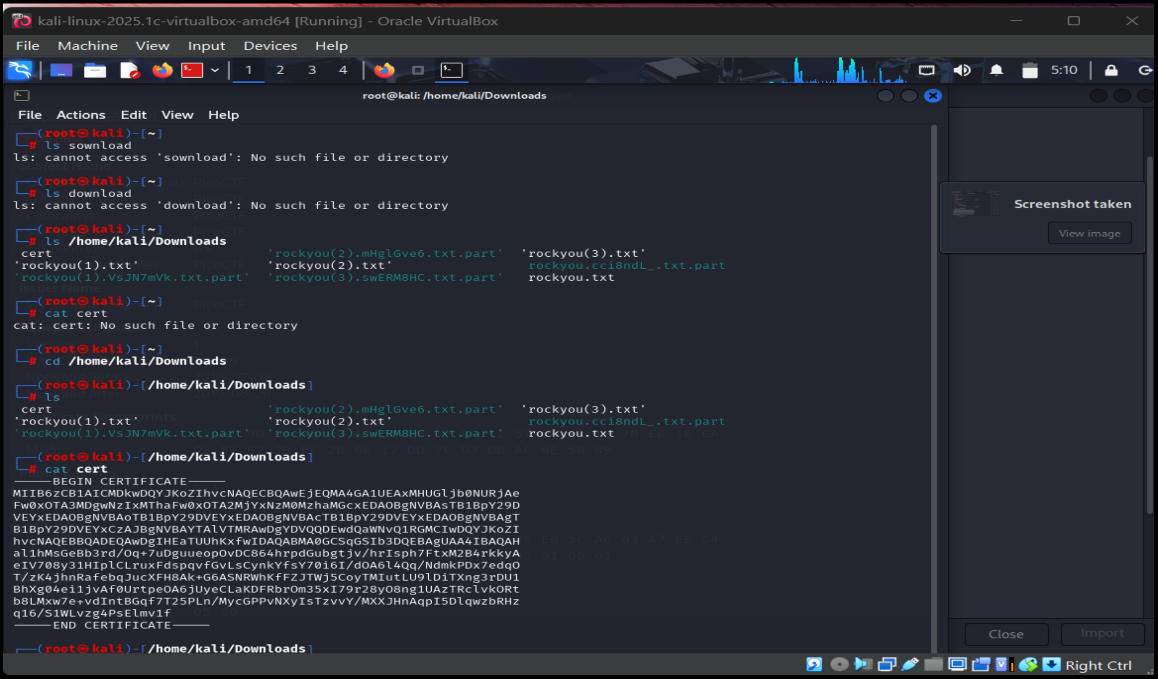
5) Steps for 5th CTF

1) in this first download the doc. That contain random strings.

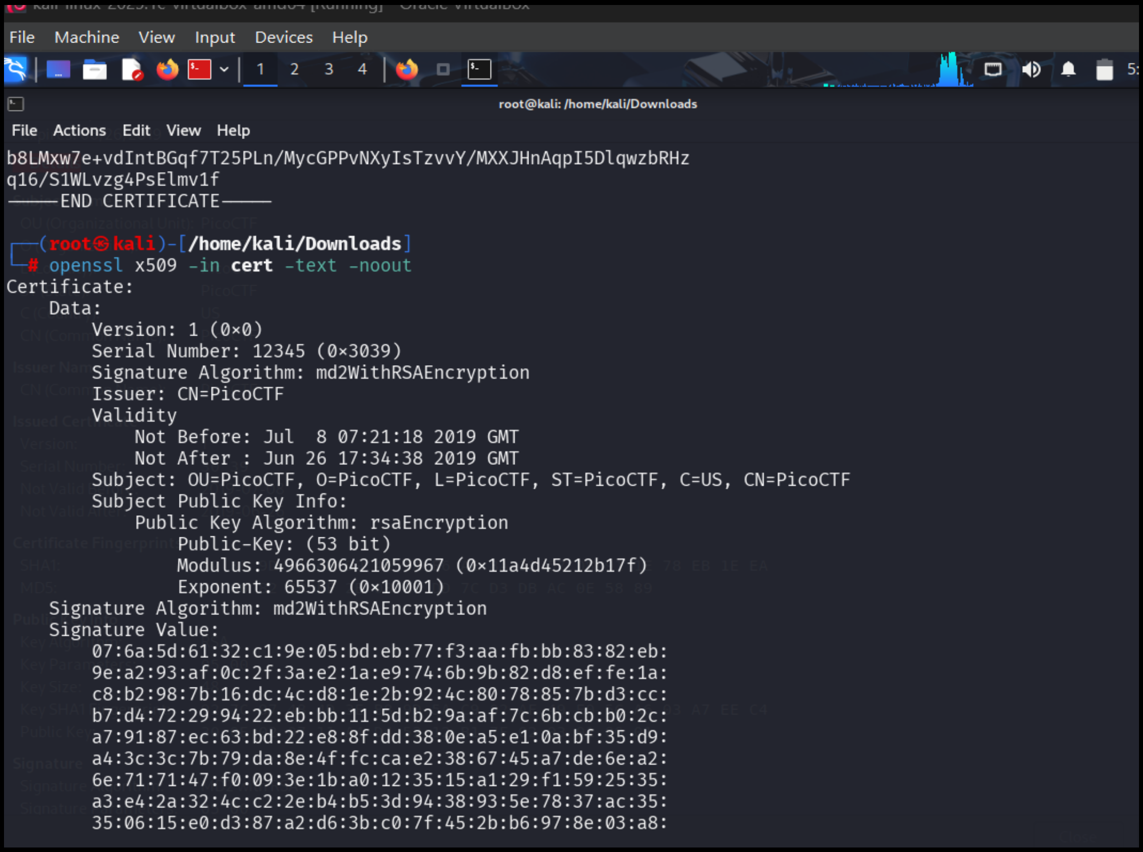


```
-----BEGIN CERTIFICATE-----
MIIB6zCB1AICMDkwDQYJKoZIhvcNAQECBQAwEjEQMA4GA1UEAxMHUGljb0NURjAe
Fw0xOTA3MDgwNzIxMThaFw0xOTA2MjYxNzM0MzhaMGcxEDAOBgNVBAsTB1BpY29D
VEYxEDAOBgNVBAoTB1BpY29DVEYxEDAOBgNVBAcTB1BpY29DVEYxEDAOBgNVBAgT
B1BpY29DVEYxCzAJBgNVBAYTAlVTMRAwDgYDVQQDEwdQaWNvQ1RGMCIwDQYJKoZI
hvcNAQEBBQADEQAwDgIHEaTUUhKxfwIDAQABMA0GCSqGSIb3DQEBAgUAA4IBAQAH
al1hMsGeBb3rd/Oq+7uDguueopOvDC864hrpdGubgtjv/hrIsph7FtxM2B4rkkyA
eIV708y31HIplCLruxFdspqvfGvLsCynkYfsY70i6I/dOA6l4Qq/NdmkPDx7edqO
T/zK4jhnRafebqJucXFH8Ak+G6ASNRWhKfFZJTWj5CoyTMIutLU9lDiTXng3rDU1
BhXg04ei1jvAf0UrtpeOA6jUyeCLaKDFRbrOm35xI79r28yO8ng1UAzTRclvkORt
b8LMxw7e+vdIntBGqf7T25PLn/MycGPPvNXyIsTzvvY/MXXJHnAqpI5DlqwzbRHz
q16/S1WLvzg4PsElmv1f
-----END CERTIFICATE-----
```

2) we will use linux openssl command to get the info of document.



```
┌──(root㉿kali)-[~]
└─# ls sownload
ls: cannot access 'sownload': No such file or directory

┌──(root㉿kali)-[~]
└─# ls download
ls: cannot access 'download': No such file or directory

┌──(root㉿kali)-[~]
└─# ls /home/kali/Downloads
 cert                          'rockyou(2).mHglGve6.txt.part'  'rockyou(3).txt'
'rockyou(1).txt'               'rockyou(2).txt'                 rockyou.cci8ndL_.txt.part
'rockyou(1).VsJN7mVk.txt.part' 'rockyou(3).swERM8HC.txt.part'   rockyou.txt

┌──(root㉿kali)-[~]
└─# cat cert
cat: cert: No such file or directory

┌──(root㉿kali)-[~]
└─# cd /home/kali/Downloads

┌──(root㉿kali)-[/home/kali/Downloads]
└─# ls
 cert                          'rockyou(2).mHglGve6.txt.part'  'rockyou(3).txt'
'rockyou(1).txt'               'rockyou(2).txt'                 rockyou.cci8ndL_.txt.part
'rockyou(1).VsJN7mVk.txt.part' 'rockyou(3).swERM8HC.txt.part'   rockyou.txt

┌──(root㉿kali)-[/home/kali/Downloads]
└─# cat cert
-----BEGIN CERTIFICATE-----
MIIB6zCB1AICMDkwDQYJKoZIhvcNAQECBQAwEjEQMA4GA1UEAxMHUGljb0NURjAe
Fw0xOTA3MDgwNzIxMThaFw0xOTA2MjYxNzM0MzhaMGcxEDAOBgNVBAsTB1BpY29D
VEYxEDAOBgNVBAoTB1BpY29DVEYxEDAOBgNVBAcTB1BpY29DVEYxEDAOBgNVBAgT
B1BpY29DVEYxCzAJBgNVBAYTAlVTMRAwDgYDVQQDEwdQaWNvQ1RGMCIwDQYJKoZI
hvcNAQEBBQADEQAwDgIHEaTUUhKxfwIDAQABMA0GCSqGSIb3DQEBAgUAA4IBAQAH
al1hMsGeBb3rd/Oq+7uDguueopOvDC864hrpdGubgtjv/hrIsph7FtxM2B4rkkyA
eIV708y31HIplCLruxFdspqvfGvLsCynkYfsY70i6I/dOA6l4Qq/NdmkPDx7edqO
T/zK4jhnRafebqJucXFH8Ak+G6ASNRWhKfFZJTWj5CoyTMIutLU9lDiTXng3rDU1
BhXg04ei1jvAf0UrtpeOA6jUyeCLaKDFRbrOm35xI79r28yO8ng1UAzTRclvkORt
b8LMxw7e+vdIntBGqf7T25PLn/MycGPPvNXyIsTzvvY/MXXJHnAqpI5DlqwzbRHz
q16/S1WLvzg4PsElmv1f
-----END CERTIFICATE-----

┌──(root㉿kali)-[/home/kali/Downloads]
```



File Machine View Input Devices Help
1 2 3 4
root@kali: /home/kali/Downloads
File Actions Edit View Help

```
b8LMxw7e+vdIntBGqf7T25PLn/MycGPPvNXyIsTzvvY/MXXJHnAqpI5DlqwzbRHz
q16/S1WLvzg4PsElmv1f
-----END CERTIFICATE-----

┌──(root㉿kali)-[/home/kali/Downloads]
└─# openssl x509 -in cert -text -noout
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 12345 (0x3039)
        Signature Algorithm: md2WithRSAEncryption
        Issuer: CN=PicoCTF
        Validity
            Not Before: Jul  8 07:21:18 2019 GMT
            Not After : Jun 26 17:34:38 2019 GMT
        Subject: OU=PicoCTF, O=PicoCTF, L=PicoCTF, ST=PicoCTF, C=US, CN=PicoCTF
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (53 bit)
                Modulus: 4966306421059967 (0x11a4d45212b17f)
                Exponent: 65537 (0x10001)
    Signature Algorithm: md2WithRSAEncryption
    Signature Value:
        07:6a:5d:61:32:c1:9e:05:bd:eb:77:f3:aa:fb:bb:83:82:eb:
        9e:a2:93:af:0c:2f:3a:e2:1a:e9:74:6b:9b:82:d8:ef:fe:1a:
        c8:b2:98:7b:16:dc:4c:d8:1e:2b:92:4c:80:78:85:7b:d3:cc:
        b7:d4:72:29:94:22:eb:bb:11:5d:b2:9a:af:7c:6b:cb:b0:2c:
        a7:91:87:ec:63:bd:22:e8:8f:dd:38:0e:a5:e1:0a:bf:35:d9:
        a4:3c:3c:7b:79:da:8e:4f:fc:ca:e2:38:67:45:a7:de:6e:a2:
        6e:71:71:47:f0:09:3e:1b:a0:12:35:15:a1:29:f1:59:25:35:
        a3:e4:2a:32:4c:c2:2e:b4:b5:3d:94:38:93:5e:78:37:ac:35:
        35:06:15:e0:d3:87:a2:d6:3b:c0:7f:45:2b:b6:97:8e:03:a8:
```

3) now we will get the certificate info. In this we get the modulus value that can be use to find factors which will give us the value of a and b.

4) after getting our value this will be our flag