PICOCTF 2023

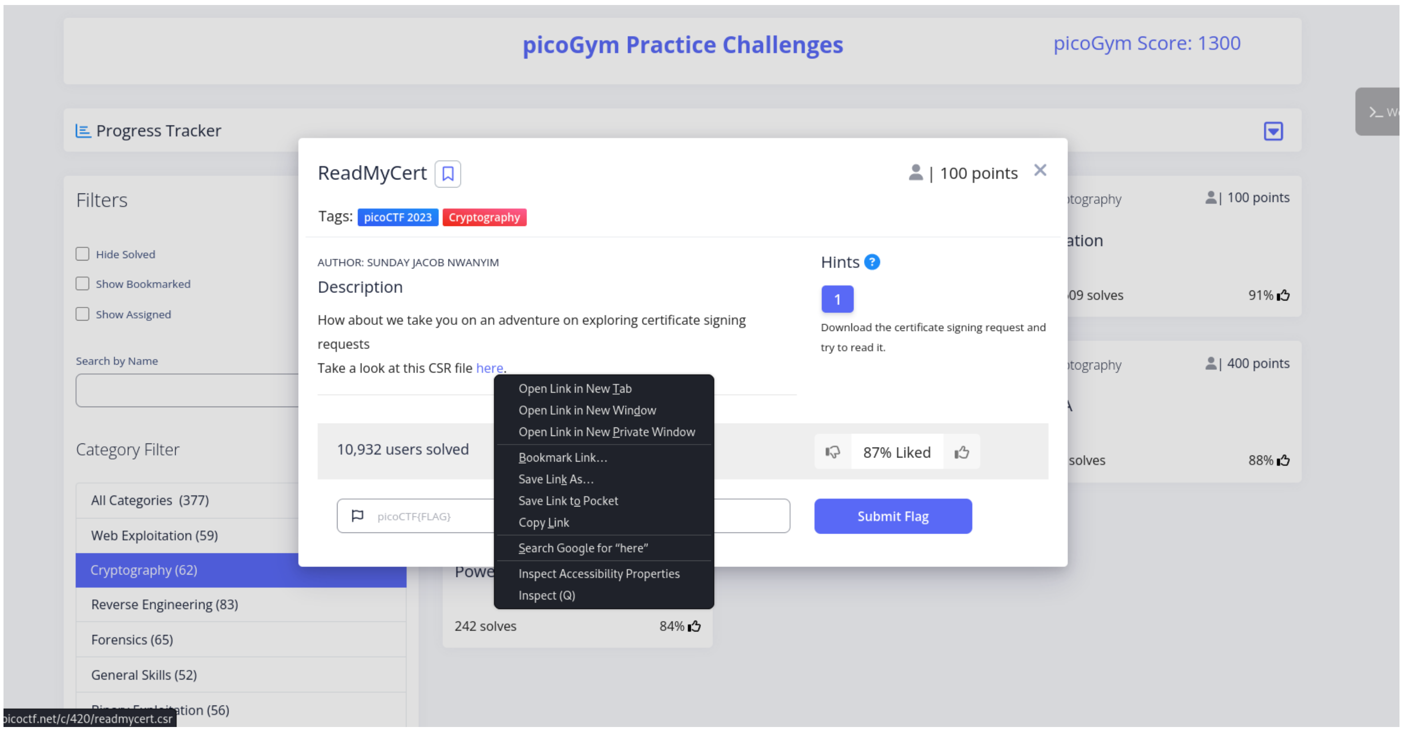
CATEGORY : Cryptography

CHALLENGE : ReadMyCert

PONTS : 100

WRITEUP

First I copy the link of the file



ReadMyCert

Tags: picoCTF 2023 Cryptography

100 points

AUTHOR: SUNDAY JACOB NWANYIM

Description

How about we take you on an adventure on exploring certificate signing requests

Take a look at this CSR file here.

Hints

1

Download the certificate signing request and try to read it.

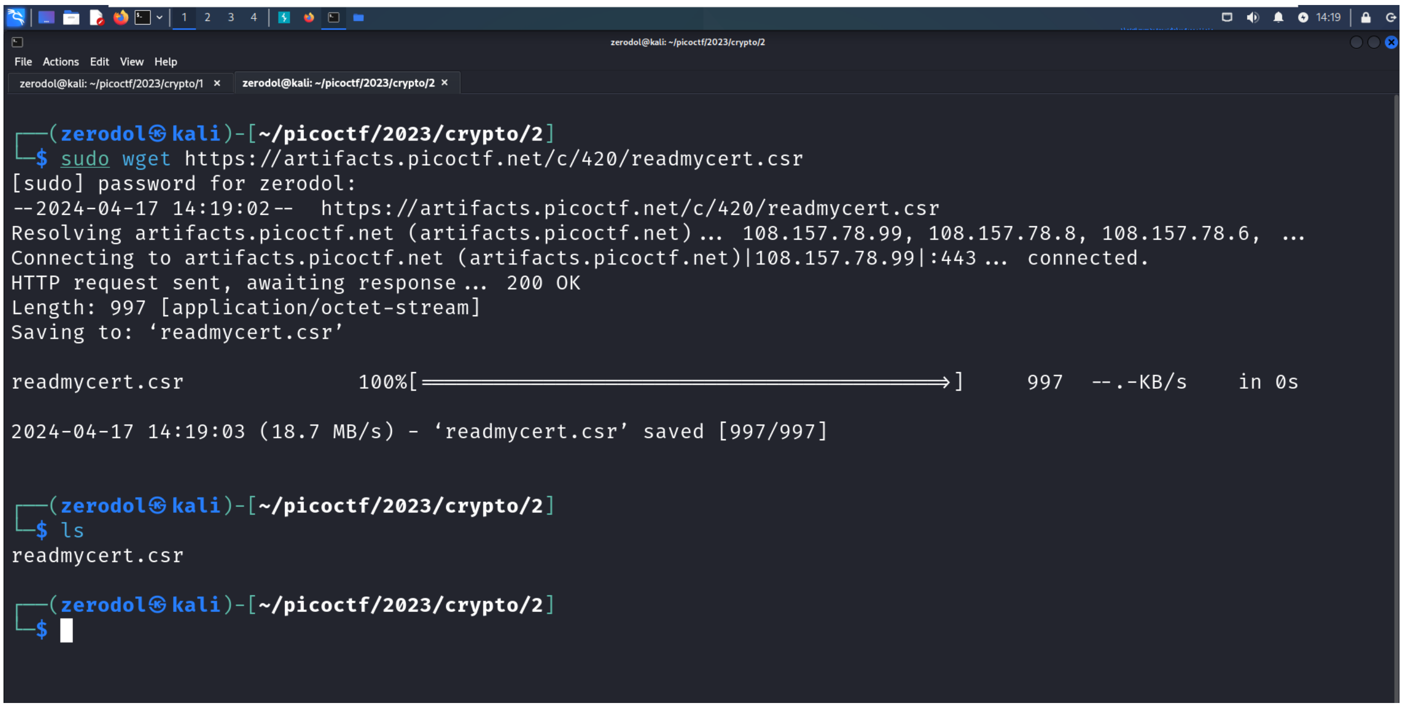
10,932 users solved

87% Liked

picoCTF{FLAG}

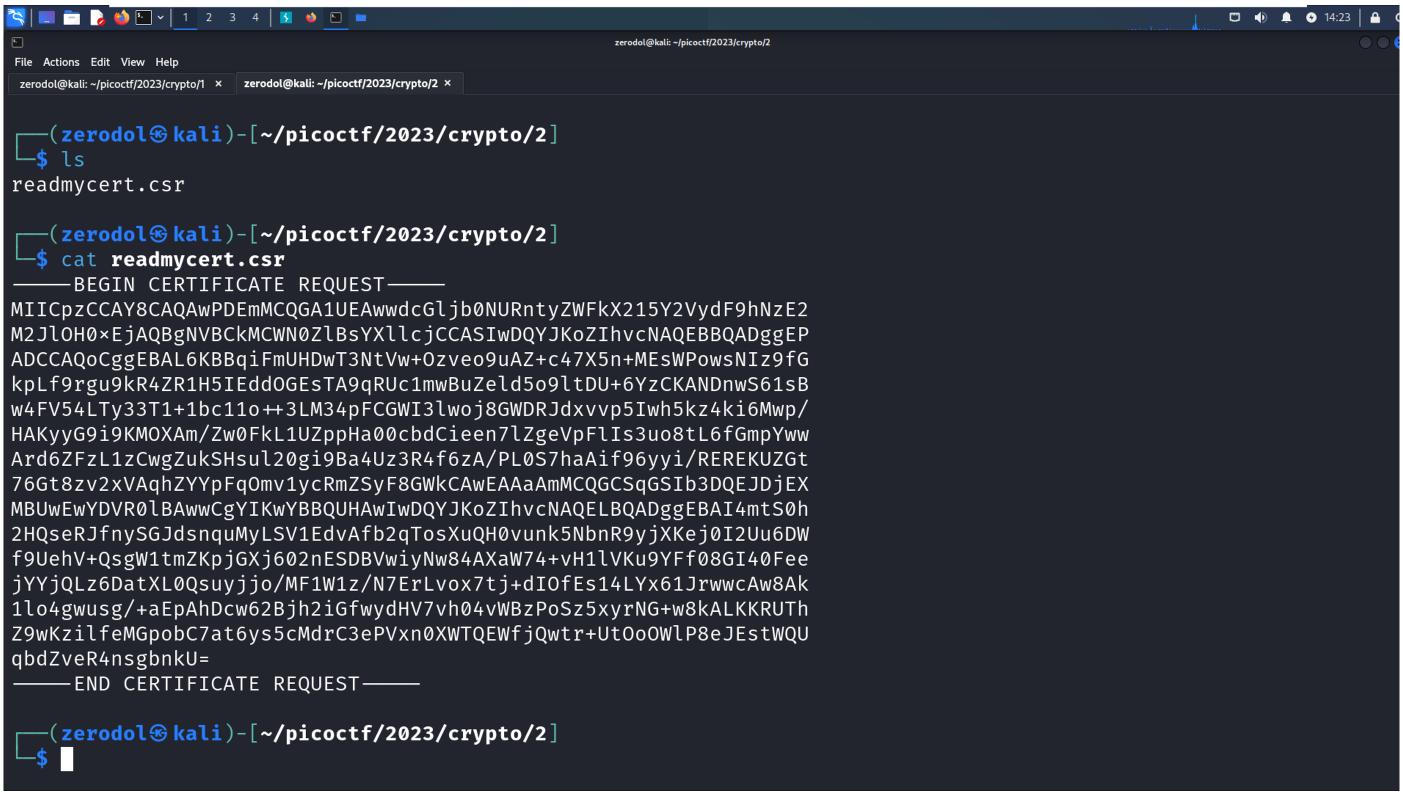
Submit Flag

Next I download the file using the **wget** command. We have a **csr** file named **readmycert.csr**



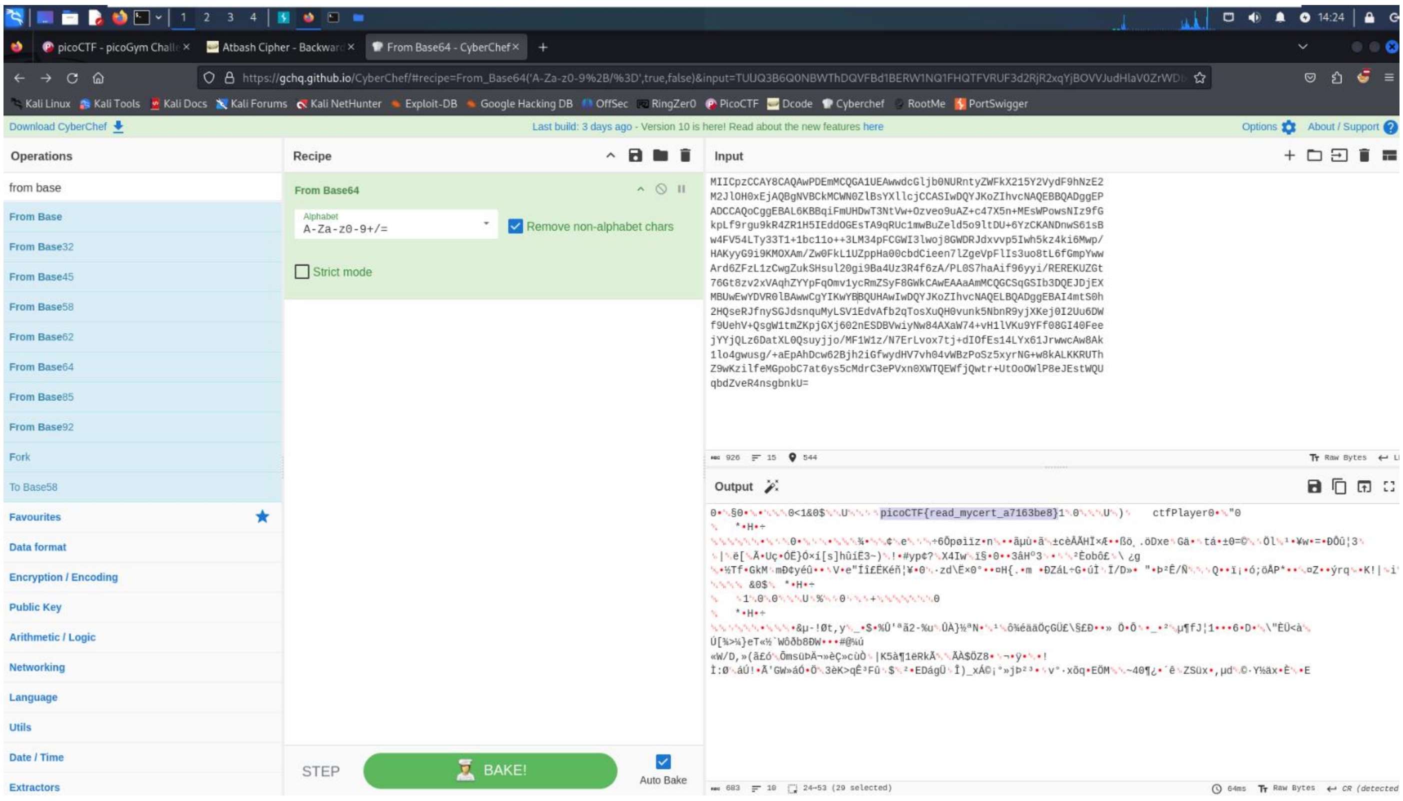
```
┌──(zerodol㉿kali)-[~/picoctf/2023/crypto/2]
└─$ sudo wget https://artifacts.picoctf.net/c/420/readmycert.csr
[sudo] password for zerodol:
--2024-04-17 14:19:02--  https://artifacts.picoctf.net/c/420/readmycert.csr
Resolving artifacts.picoctf.net (artifacts.picoctf.net)... 108.157.78.99, 108.157.78.8, 108.157.78.6, ...
Connecting to artifacts.picoctf.net (artifacts.picoctf.net)|108.157.78.99|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 997 [application/octet-stream]
Saving to: 'readmycert.csr'

readmycert.csr            100%[===========================================>]     997  --.-KB/s    in 0s

2024-04-17 14:19:03 (18.7 MB/s) - 'readmycert.csr' saved [997/997]


┌──(zerodol㉿kali)-[~/picoctf/2023/crypto/2]
└─$ ls
readmycert.csr

┌──(zerodol㉿kali)-[~/picoctf/2023/crypto/2]
└─$ 
```

I display the content of the file with the cat command and we have something that seems to be encrypted in base64. But, no rush, we can check that with our **cyberchef (https://gchq.github.io/CyberChef)**



```
┌──(zerodol㉿kali)-[~/picoctf/2023/crypto/2]
└─$ ls
readmycert.csr

┌──(zerodol㉿kali)-[~/picoctf/2023/crypto/2]
└─$ cat readmycert.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICpzCCAY8CAQAwPDEmMCQGA1UEAwwdcGljb0NURntyZWFkX215Y2VydF9hNzE2
M2JlOH0xEjAQBgNVBCkMCWN0ZlBsYXllcjCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAL6KBBqiFmUHDwT3NtVw+Ozveo9uAZ+c47X5n+MEsWPowsNIz9fG
kpLf9rgu9kR4ZR1H5IEddOGEsTA9qRUc1mwBuZeld5o9ltDU+6YzCKANDnwS61sB
w4FV54LTy33T1+1bc11o++3LM34pFCGWI3lwoj8GWDRJdxvvp5Iwh5kz4ki6Mwp/
HAKyyG9i9KMOXAm/Zw0FkL1UZppHa00cbdCieen7lZgeVpFlIs3uo8tL6fGmpYww
Ard6ZFzL1zCwgZukSHsul20gi9Ba4Uz3R4f6zA/PL0S7haAif96yyi/REREKUZGt
76Gt8zv2xVAqhZYYpFqOmv1ycRmZSyF8GWkCAwEAAaAmMCQGCSqGSIb3DQEJDjEX
MBUwEwYDVR0lBAwwCgYIKwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggEBAI4mtS0h
2HQseRJfnySGJdsnquMyLSV1EdvAfb2qTosXuQH0vunk5NbnR9yjXKej0I2Uu6DW
f9UehV+QsgW1tmZKpjGXj602nESDBVwiyNw84AXaW74+vH1lVKu9YFf08GI40Fee
jYYjQLz6DatXL0Qsuyjjo/MF1W1z/N7ErLvox7tj+dIOfEs14LYx61JrwwcAw8Ak
1lo4gwusg/+aEpAhDcw62Bjh2iGfwydHV7vh04vWBzPoSz5xyrNG+w8kALKKRUTh
Z9wKzilfeMGpobC7at6ys5cMdrC3ePVxn0XWTQEWfjQwtr+UtOoOWlP8eJEstWQU
qbdZveR4nsgbnkU=
-----END CERTIFICATE REQUEST-----

┌──(zerodol㉿kali)-[~/picoctf/2023/crypto/2]
└─$ 
```

On **cyberchef** (https://gchq.github.io/CyberChef) we choose **"from base64"** and we paste our encrypted content. Bingo we can see the flag : **picoCTF{read_mycert_a7163be8}**



Recipe: From Base64 — Alphabet: A-Za-z0-9+/= — Remove non-alphabet chars [✓] — Strict mode [ ]

Input

```
MIICpzCCAY8CAQAwPDEmMCQGA1UEAwwdcGljb0NURntyZWFkX215Y2VydF9hNzE2
M2JlOH0xEjAQBgNVBCkMCWN0ZlBsYXllcjCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAL6KBBqiFmUHDwT3NtVw+Ozveo9uAZ+c47X5n+MEsWPowsNIz9fG
kpLf9rgu9kR4ZR1H5IEddOGEsTA9qRUc1mwBuZeld5o9ltDU+6YzCKANDnwS61sB
w4FV54LTy33T1+1bc11o++3LM34pFCGWI3lwoj8GWDRJdxvvp5Iwh5kz4ki6Mwp/
HAKyyG9i9KMOXAm/Zw0FkL1UZppHa00cbdCieen7lZgeVpFlIs3uo8tL6fGmpYww
Ard6ZFzL1zCwgZukSHsul20gi9Ba4Uz3R4f6zA/PL0S7haAif96yyi/REREKUZGt
76Gt8zv2xVAqhZYYpFqOmv1ycRmZSyF8GWkCAwEAAaAmMCQGCSqGSIb3DQEJDjEX
MBUwEwYDVR0lBAwwCgYIKwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggEBAI4mtS0h
2HQseRJfnySGJdsnquMyLSV1EdvAfb2qTosXuQH0vunk5NbnR9yjXKej0I2Uu6DW
f9UehV+QsgW1tmZKpjGXj602nESDBVwiyNw84AXaW74+vH1lVKu9YFf08GI40Fee
jYYjQLz6DatXL0Qsuyjjo/MF1W1z/N7ErLvox7tj+dIOfEs14LYx61JrwwcAw8Ak
1lo4gwusg/+aEpAhDcw62Bjh2iGfwydHV7vh04vWBzPoSz5xyrNG+w8kALKKRUTh
Z9wKzilfeMGpobC7at6ys5cMdrC3ePVxn0XWTQEWfjQwtr+UtOoOWlP8eJEstWQU
qbdZveR4nsgbnkU=
```

926 15 544

Output

```
0••§0•••0<1&0$•U••picoCTF{read_mycert_a7163be8}1•0••U•)•    ctfPlayer0••"0
•   *•H•÷
••••0••••¾•¢•e••÷6Õpøiïz•n•••âµù•ã•±cèÅÄHÏ×Æ••ßö¸.öDxe•Gä••tá•±0=©••Öl•¹•¥w•=•ÐÔû¦3•
•|•ë[•Ä•Uç•ÓË}Ó×í[s]hûíË3~)•!•#yp¢?•X4Iw•ï§•0••3âHº3•••²Èobô£•\ ¿g
••½Tf•GkM•mÐ¢yéû•••V•e"Íî£ËKéñ¦¥•0••zd\Ë×0°••¤H{.•m •ÐZáL÷G•úÌ•Ï/D»• "•Þ²Ê/Ñ•••Q••ï¡•ó;öÅP*•••¤Z••ýrq••K!|•i
••  &0$•  *•H•÷
•   •1•0•0••U•%••0•••+•••••0
•   *•H•÷
•••••&µ-!Øt,y•_•$•%Û'ªã2-%u•ÛÀ}½ªN•••¹•ô¾éäãÖçGÜ£\§£Ð••» Ö•Õ••_•²•µ¶fJ¦1•••6•D••\"ÈÜ<à•
Ú[¾>¼}eT«½`Wôðb8ÐW•••#@¾ú
«W/D,»(ã£ó•ÕmsüÞÄ¬»èÇ»cùÒ•|K5à¶1ëRkÄ••ÄÀ$ÖZ8••¬•ÿ•••!
Ì:Ø•áÚ!•Ä'GW»áÓ•Ö•3èK>qÊ³Fû•$•²•EDágÜ•Ì)_xÁ©¡°»jÞ²³••v°·xõq•EÖM••~40¶¿•´ê•ZSüx•,µd•©·Y½äx•È••E
```

683 10 24-53 (29 selected) 64ms Raw Bytes CR (detected