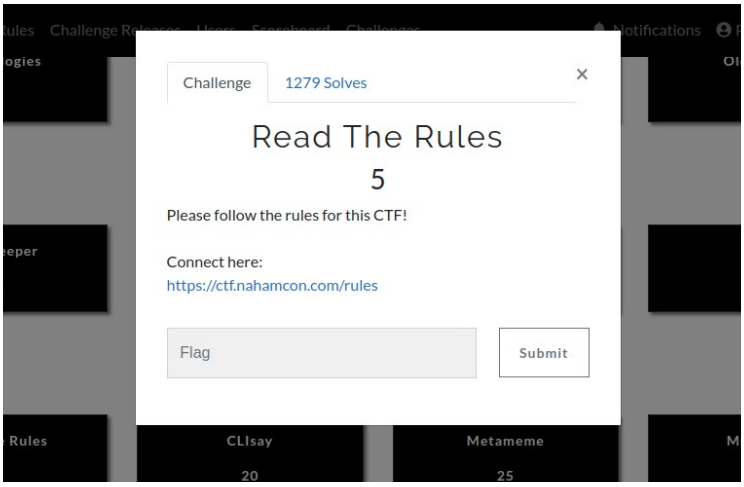
NahamCon CTF writeup

What’s up, folks?! Are you ready for the new writeup? Let’s start.

#WarmUp challenges

Read the rules



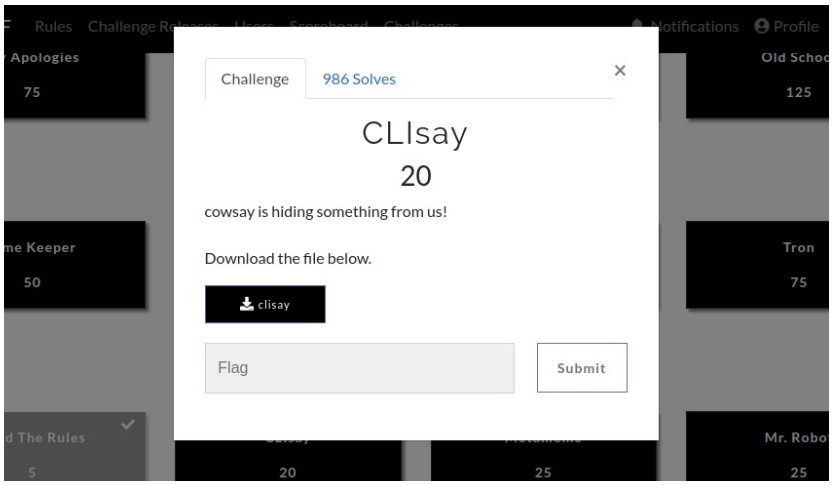
Steps to get the flag:

- Open page
- Analyze page source

Flag: flag{we_hope_you_enjoy_the_game}

```
<p>
        Flags for this competition will follow the format: <b>flag{}</b>, with words joined together with underscores inside the curly braces. If you look closely, you can even find a flag on this page!<br>
        Note: Some of the flags will have a different wrapper or no wrapper for the flag. This is denoted in the challenge description for any that have a different flag format.
</p>
<h1> Support </h1>

<p>
        If you need to ask for help on any challenges or need some support, you can join the NahamCon Discord Server <a href="https://discord.gg/ucCz7uh">https://discord.gg/ucCz7uh</a>.
</p>
<p>
  And you can ping <code>@CTF-Help</code> on the server! One of our CTF Helpers will answer your question or provide assistance, if needed.
</p><h1> Prizes </h1><p>
        Thanks to the support from you the community and our sponsors, we are pleased to offer prizes to the winners of NahamCon CTF!
</p><ul>
<li> 1st Place - $500 USD </li>
<li> 2nd Place - $250 USD </li>
<li> 3rd Place - $100 USD </li>
</ul><p></p><!-- Thank you for reading the rules! Your flag is: -->
<!--         flag{we_hope_you_enjoy_the_game}          -->
    </div>

    </main>

    <footer class="footer">
        <div class="container text-center">
            <a href="https://ctfd.io" class="text-secondary">
                <small class="text-muted">Powered by CTFd</small>
            </a>
        </div>
    </footer>

    <script defer src="/themes/core/static/js/vendor.bundle.min.js?d=25aef801"></script>
    <script defer src="/themes/core/static/js/core.min.js?d=25aef801"></script>
    <script defer src="/themes/core/static/js/helpers.min.js?d=25aef801"></script>


    <script defer src="/themes/core/static/js/pages/main.min.js?d=25aef801"></script>
```

CLISay



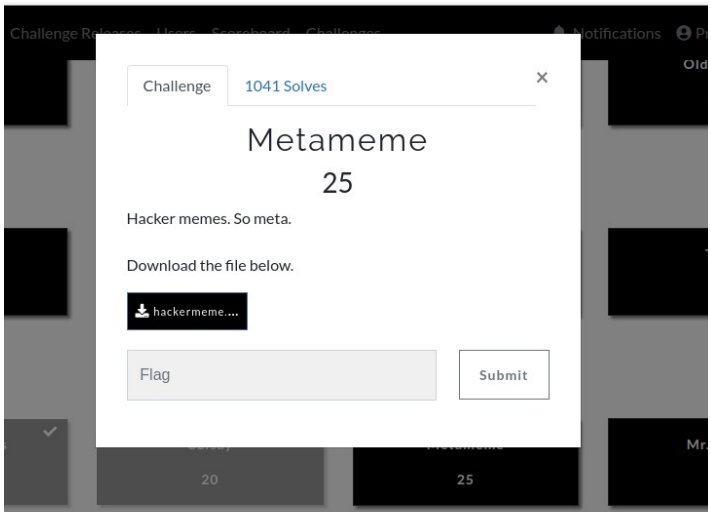
Steps to get the flag:

- Get the file type: “file clisay”
- Retrieve strings from the file: “strings clisay”

Flag: flag{Y0u_c4n_r3Ad_M1nd5}

```
[redacted]/NahamsecCTF$ file clisay
clisay: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, i
nterpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=70e60678f1c0b75ea3aae2a4e8e1e89
78e3c6fc0, for GNU/Linux 3.2.0, not stripped
[redacted]s/NahamsecCTF$ strings clisay
/lib64/ld-linux-x86-64.so.2
libc.so.6
printf
__cxa_finalize
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
flag{Y0u_c4n_
  _____________________________
/ Sorry, I'm not allow to reveal any \
\ secrets...                       /
  -------------------------------
         \   ^__^
          \  (oo)\_______
             (__)\       )\/\
                 ||----w |
                 ||     ||
r3Ad_M1nd5}
:*3$"
```

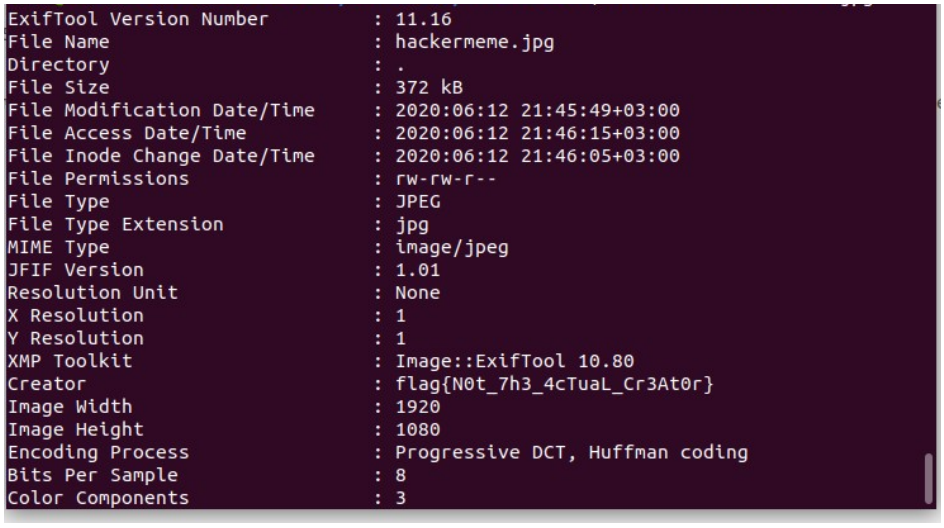
Metameme



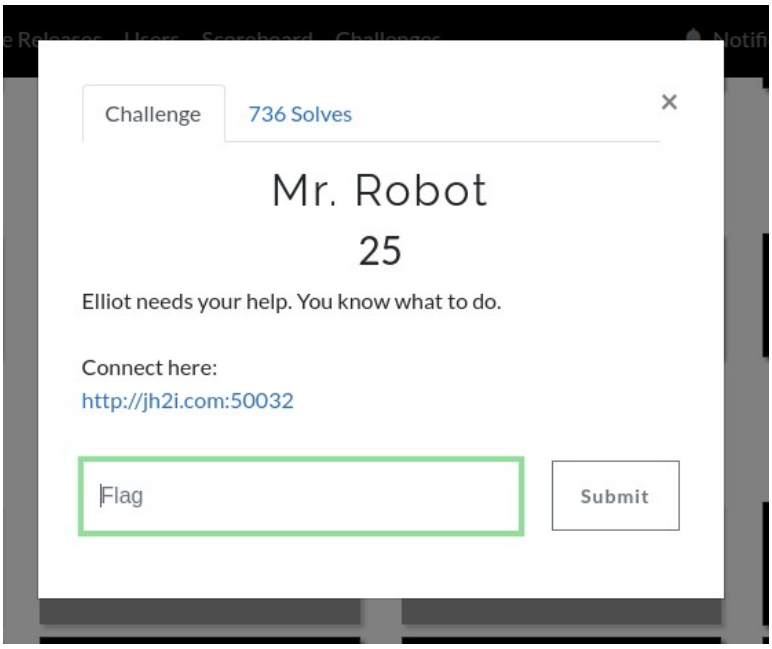
Steps to get the flag:

- Get file metadata using exiftool: “exiftool hackermeme.jpg”

Flag: flag{N0t_7h3_4cTuaL_Cr3At0r}



Mr. Robot

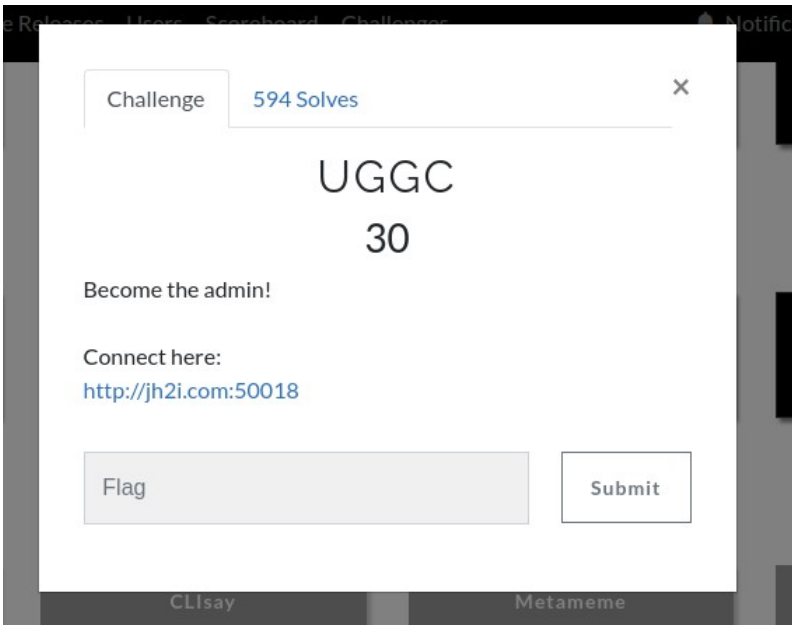


Steps to get the flag:

- Open site
- Manually type a url to open robots.txt

Flag: flag{welcome_to_robots.txt}

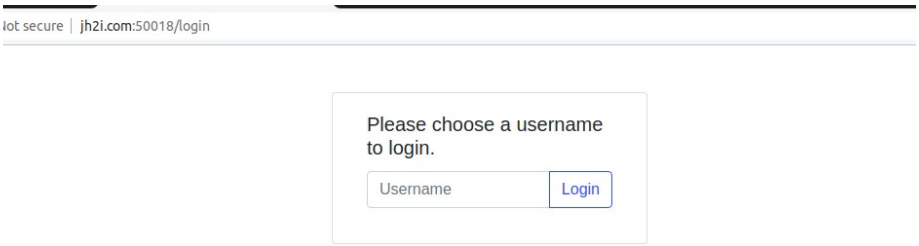
UGGC

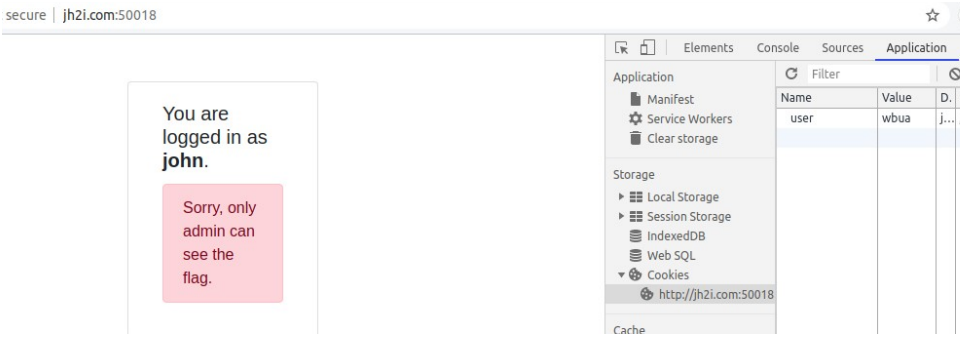


Steps to get the flag:

- Open site
- Analyze source code, application cookies, local storage
- Login with any user name (I used john)
- Analyze cookies once again after login. Change value of the user cookie to admin
- Change the ‘user’ cookie to nqzva and refresh the page

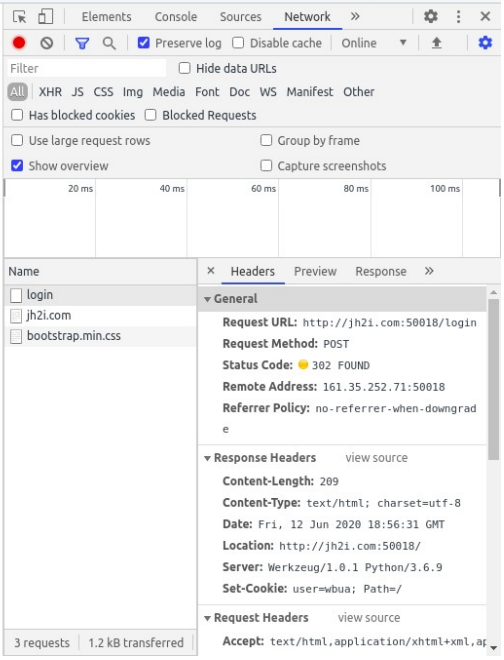
Flag: flag{H4cK_aLL_7H3_C0okI3s}

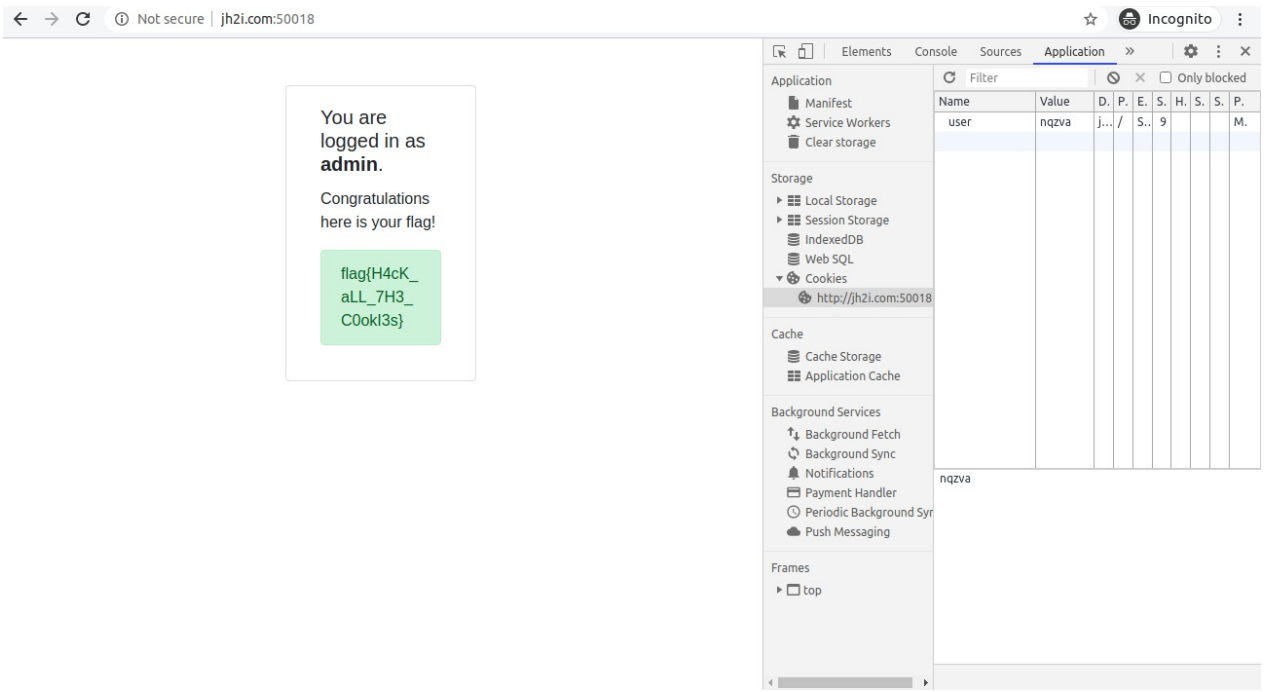




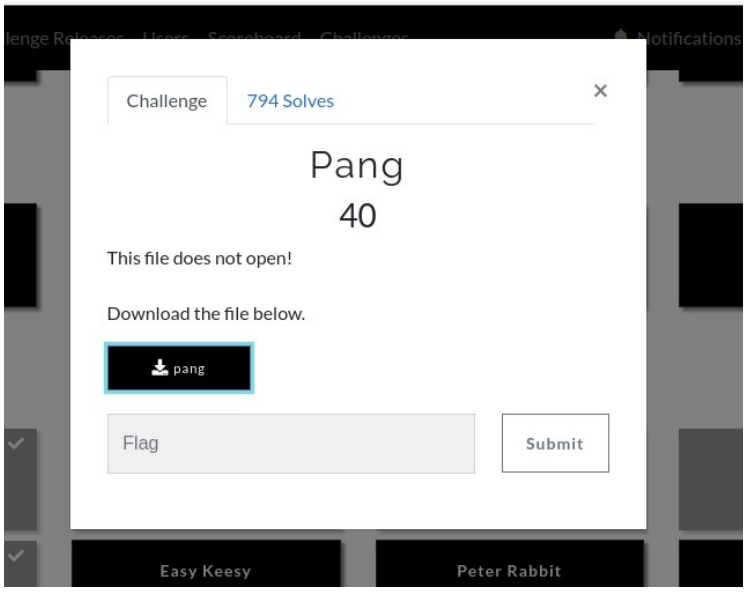
You are logged in as **john**.

Sorry, only admin can see the flag.





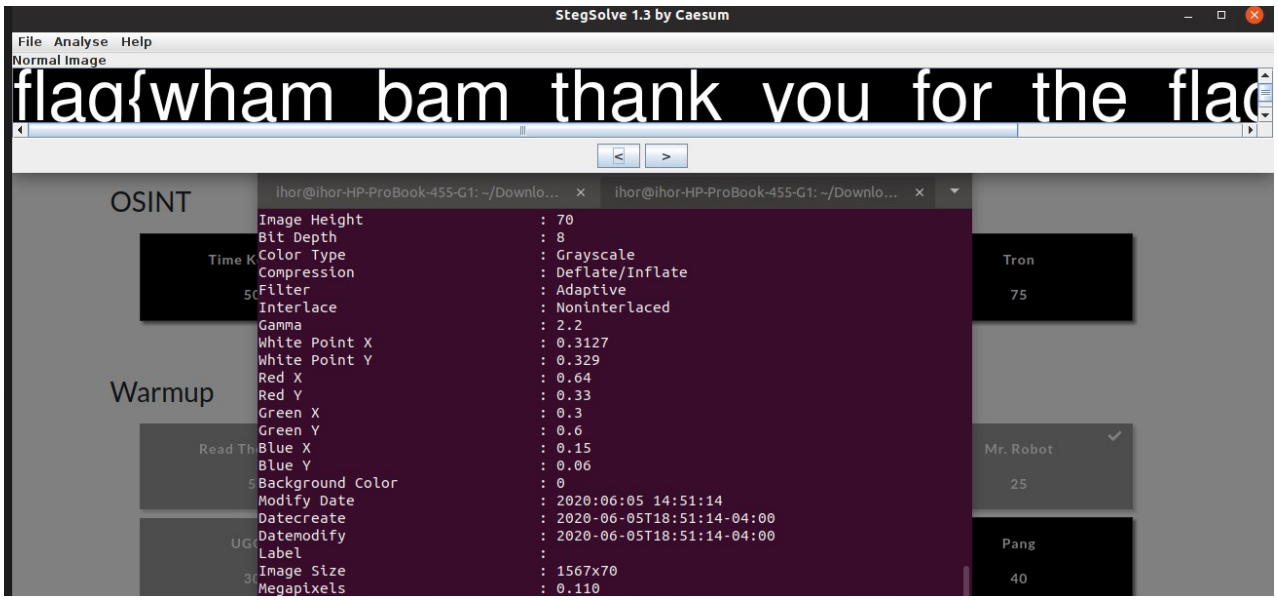
Pang



Steps to get the flag:

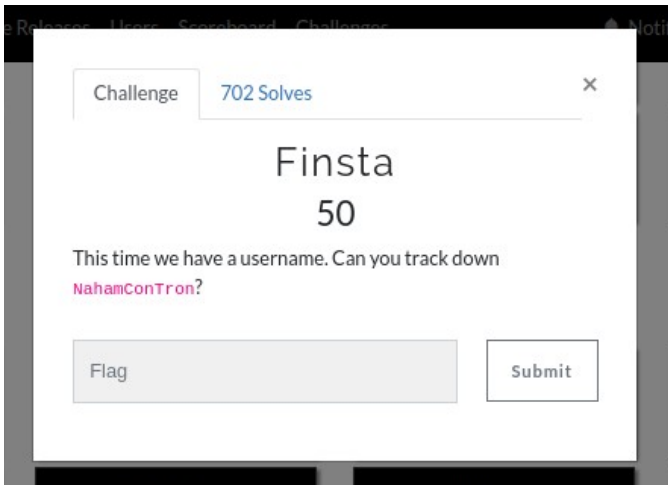
- Use Stegsolve.jar to get the flag: “java -jar Stegsolve.jar”. When Stegsolve is ready, select an image (pang) using File → Open

Flag: flag{wham_bam_thank_you_for_the_flag_maam}



OSINT

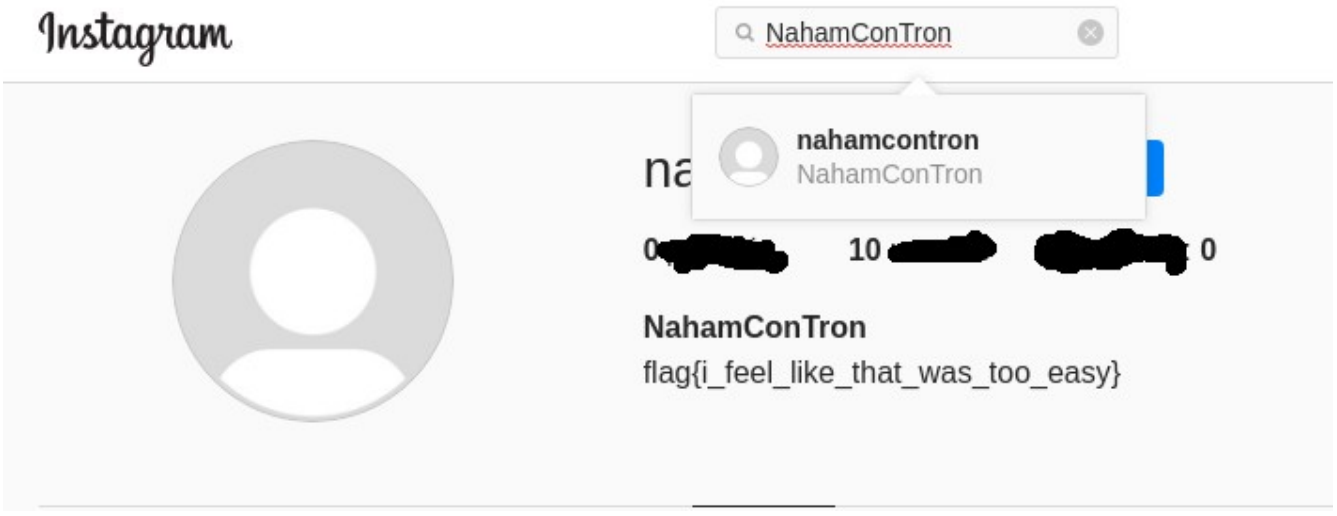
Finsta



Steps to get the flag:

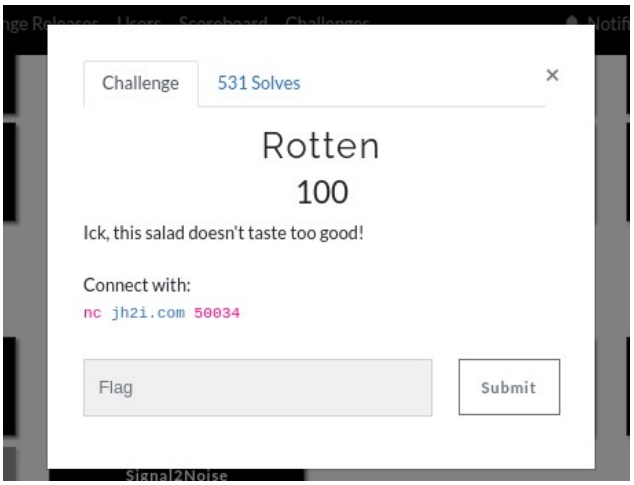
- Use Instagram search to look for the NahamConTron

Flag: flag{i_feel_like_that_was_too_easy}



Scripting

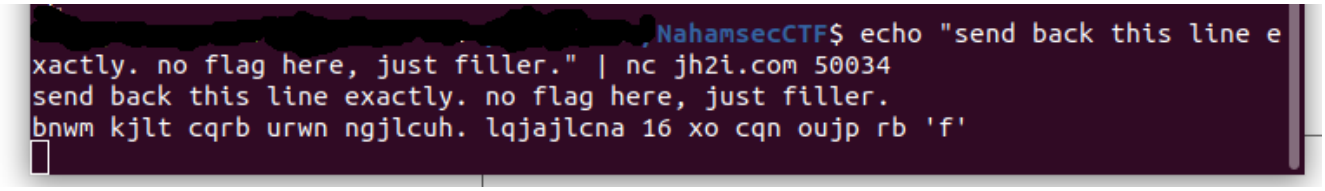
Rotten



Steps to get the flag:

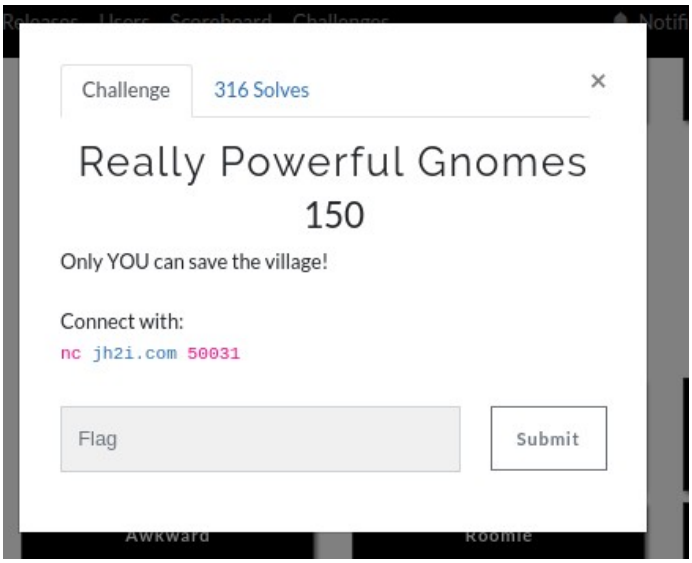
- Connect to the server using nc
- Follow the instructions
- We need to grab 30 letters to recreate a flag (it can be automated using small script, see “Really Powerful Gnomes” challenge)
- Once you’ve got all the letters, decode it using https://rot13.com/

Flag: flag{now_you_know_your_caesars}




```
xjsi gfhp ymnx qnsj jcfhyqd. hmfwfhyjw 0 tk ymj kqfl nx 'k'
jveu srtb kyzj czev vortkcp. tyrirtkvi 1 fw kyv wcrx zj 'c'
qclb zyai rfgq jglc cvyarjw. afypyarcp 2 md rfc djye gq 'y
coxn lkmu drsc vsxo ohkmdvi. mrkbkmdob 3 yp dro pvkq sc 'q'
iudt rqsa jxyi bydu unqsjbo. sxqhqsjuh 4 ev jxu vbqw yi '{'
lxgw utvd mabl ebgx xqtvmer. vatktvmxk 5 hy max yetz bl 'g'
xjsi gfhp ymnx qnsj jcfhyqd. hmfwfhyjw 6 tk ymj kqfl nx 't'
fraq onpx guvf yvar rknpgyl. punenpgre 7 bs gur synt vf 'j'
lxgw utvd mabl ebgx xqtvmer. vatktvmxk 8 hy max yetz bl '_'
xjsi gfhp ymnx qnsj jcfhyqd. hmfwfhyjw 9 tk ymj kqfl nx 'd'
coxn lkmu drsc vsxo ohkmdvi. mrkbkmdob 10 yp dro pvkq sc 'y'
nziy wvxf ocdn gdiz zsvxogt. xcvmvxozm 11 ja ocz agvb dn 'p'
iudt rqsa jxyi bydu unqsjbo. sxqhqsjuh 12 ev jxu vbqw yi '_'
yktj hgiq znoy rotk kdgizre. ingxgizkx 13 ul znk lrgm oy 'q'
kwfv tsuc lzak dafw wpsuldq. uzsjsulwj 14 gx lzw xdsy ak 'f'
pbka yxzh qefp ifkb buxzqiv. zexoxzqbo 15 lc qeb cixd fp 'l'
bnwm kjlt cqrb urwn ngjlcuh. lqjajlcna 16 xo cqn oujp rb 'f'
fraq onpx guvf yvar rknpgyl. punenpgre 17 bs gur synt vf '_'
lxgw utvd mabl ebgx xqtvmer. vatktvmxk 18 hy max yetz bl 'r'
yktj hgiq znoy rotk kdgizre. ingxgizkx 19 ul znk lrgm oy 'u'
jveu srtb kyzj czev vortkcp. tyrirtkvi 20 fw kyv wcrx zj 'l'
coxn lkmu drsc vsxo ohkmdvi. mrkbkmdob 21 yp dro pvkq sc 'b'
send back this line exactly. character 22 of the flag is '_'

jveu srtb kyzj czev vortkcp. tyrirtkvi 24 fw kyv wcrx zj 'r'
ugpf dcem vjku nkpg gzcevna. ejctcevgt 25 qh vjg hnci ku 'g'
myhx vuwe nbcm fchy yruwnfs. wbuluwnyl 26 iz nby zfua cm 'm'
nziy wvxf ocdn gdiz zsvxogt. xcvmvxozm 27 ja ocz agvb dn 'v'
nziy wvxf ocdn gdiz zsvxogt. xcvmvxozm 28 ja ocz agvb dn 'm'
rdmc azbj sghr khmd dwzbskx. bgzqzbsdq 29 ne sgd ekzf hr 'r'
eqzp nmow ftue xuzq qjmofxk. otmdmofqd 30 ar ftq rxms ue '}'
```

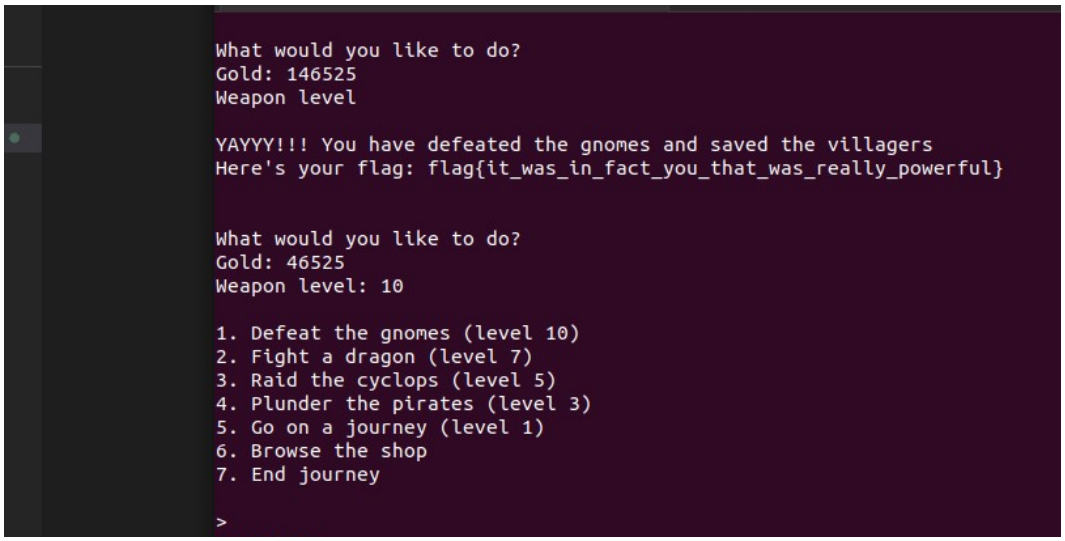
Really Powerful Gnomes



Steps to get the flag:

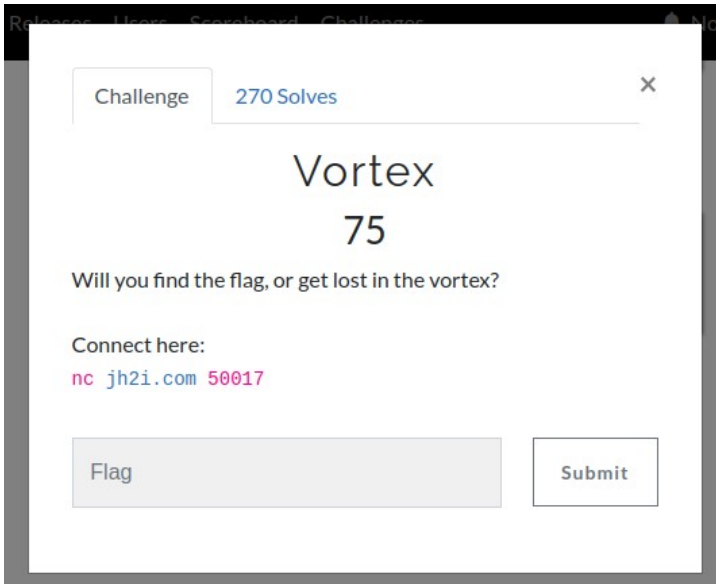
- I created a small python script based on (https://gist.github.com/leonjza/f35a7252babdf77c8421). To get a flag, you need to just run the script. Sometimes, connection to the target server might be dropped and you need to restart the script (script sources are in the 'Gnome Defender' folder)

Flag: flag{it_was_in_fact_you_that_was_really_powerful}



Miscellaneous

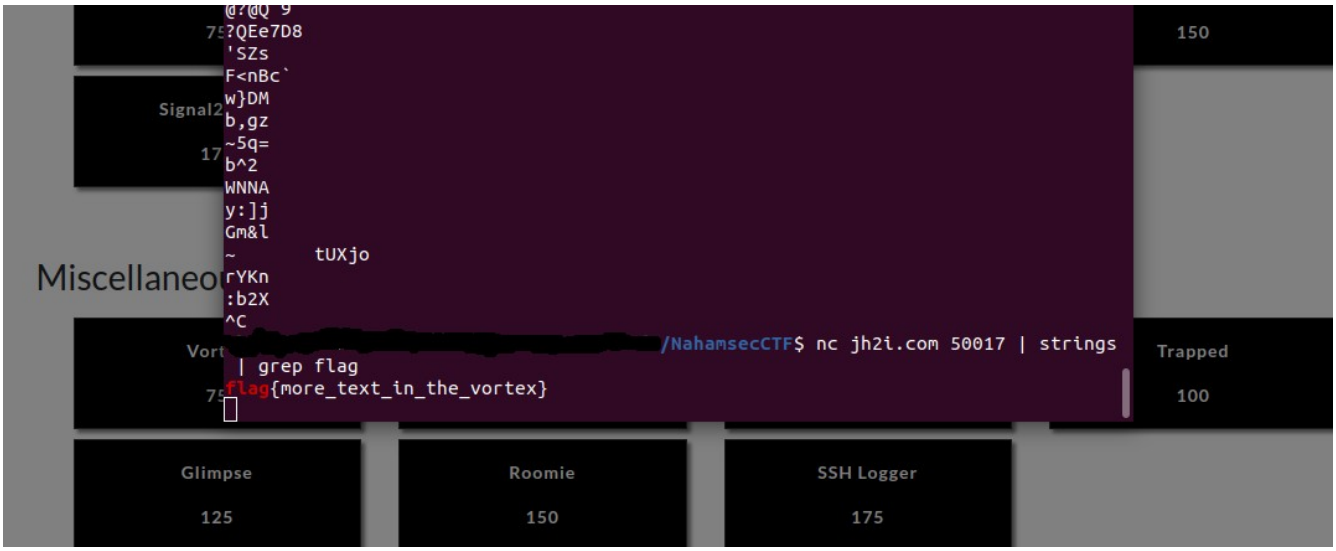
Vortex



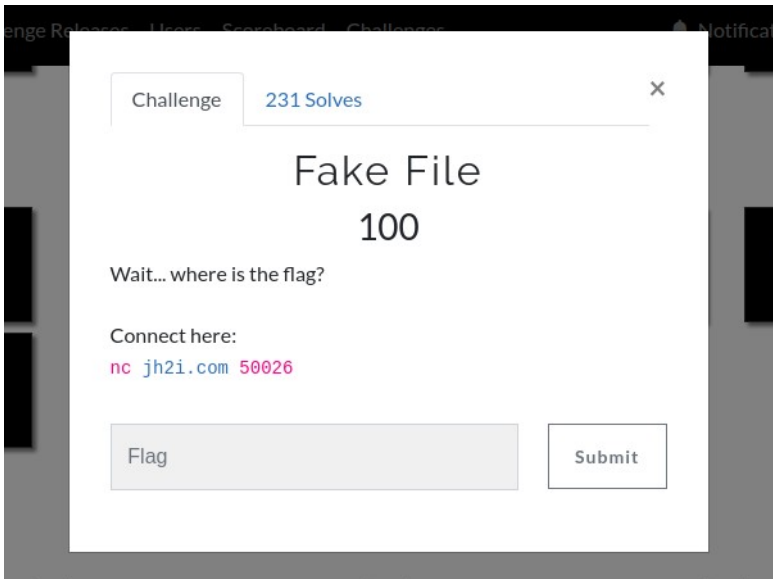
Steps to get the flag:

- Connect to the server using nc
- Use pipes (nc | strings | grep) to get the flag

Flag: flag{more_text_in_the_vortex}



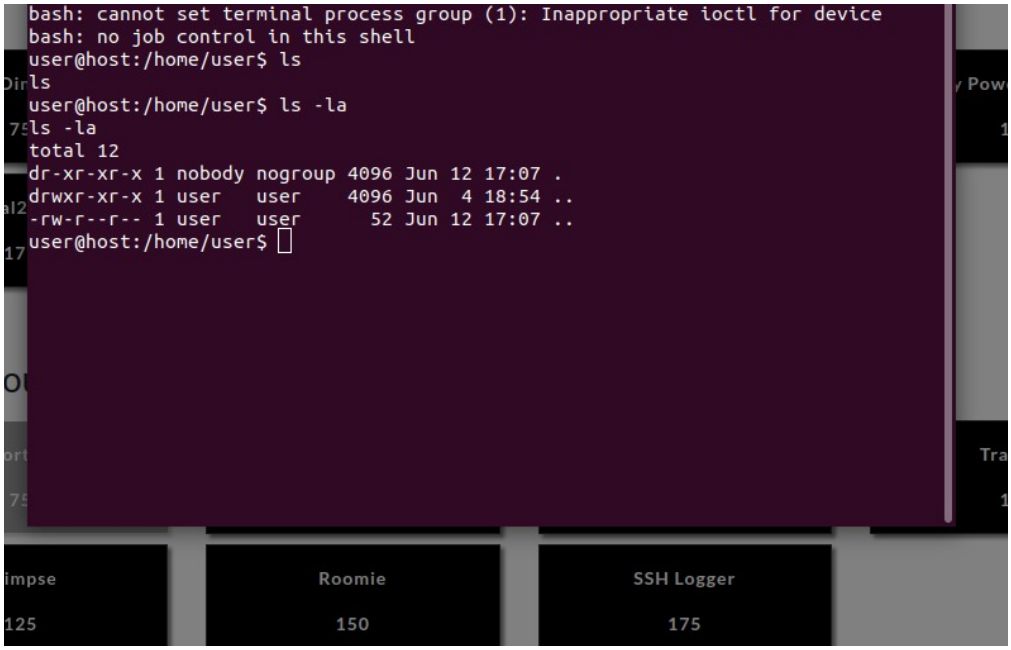
Fake file



Steps to get the flag:

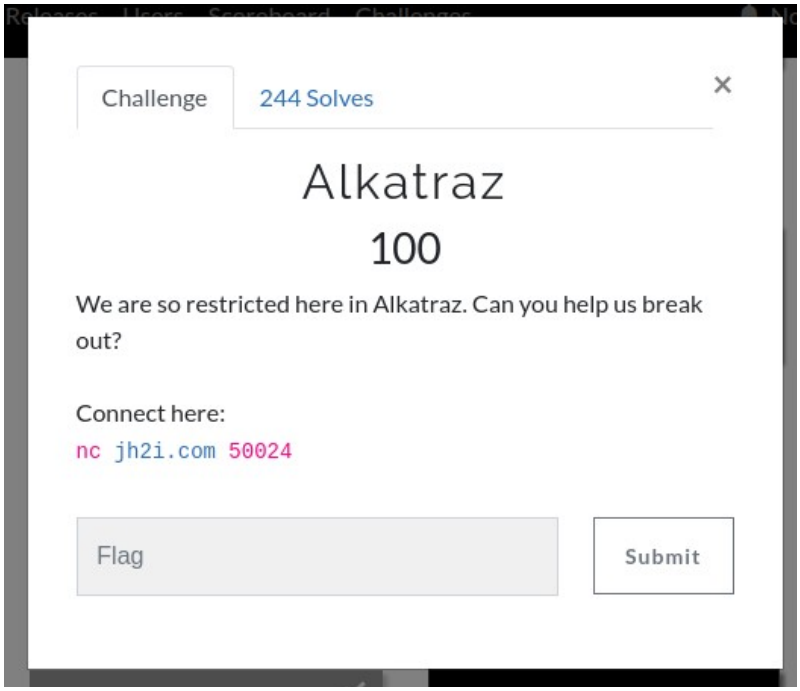
- Connect to the target server
- Use ‘ls -la’ to look around. It seems that there is a fake file ‘..’
- It is not available using cat/less/more. We should use ‘find’ to bypass the restrictions (see the screenshot below)

Flag: flag{we_should_have_been_worried_about_u2k_not_y2k}



```
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
user@host:/home/user$ ls -la
ls -la
total 12
dr-xr-xr-x 1 nobody nogroup 4096 Jun 12 17:08 .
drwxr-xr-x 1 user   user    4096 Jun  4 18:54 ..
-rw-r--r-- 1 user   user      52 Jun 12 17:08 ..
user@host:/home/user$ find . -type f -exec cat {} \;
find . -type f -exec cat {} \;
flag{we_should_have_been_worried_about_u2k_not_y2k}
user@host:/home/user$
```

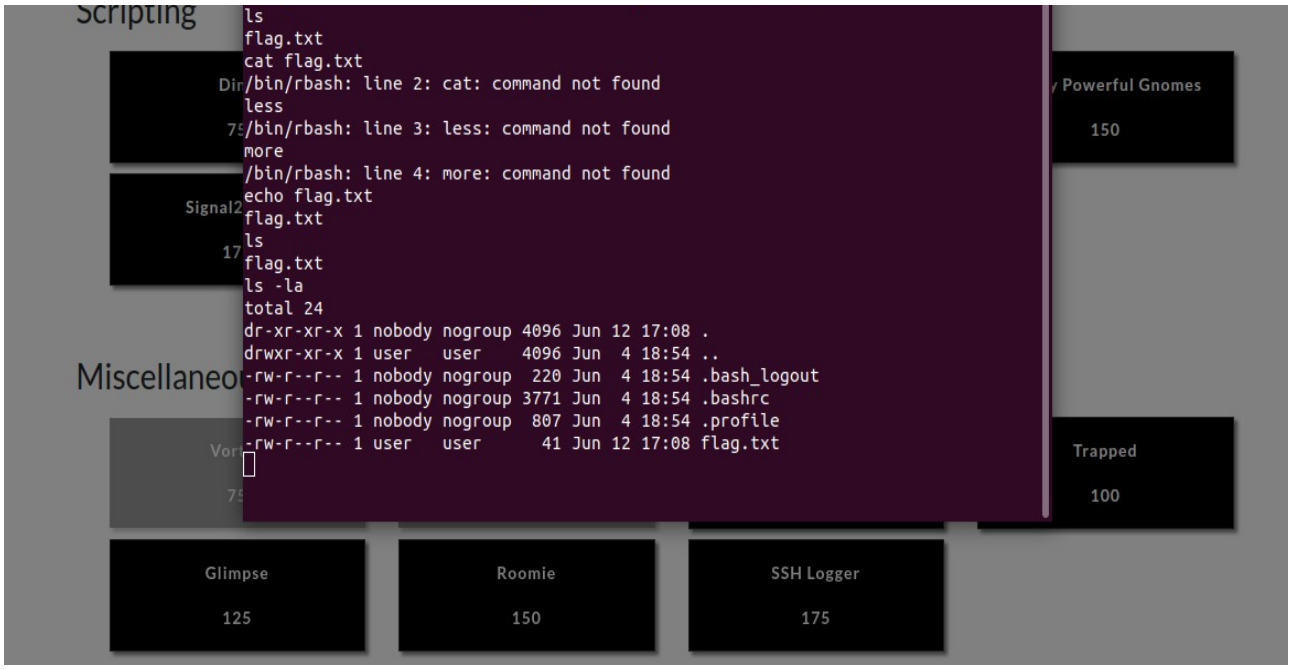
Alkatraz



Steps to get the flag:

- Connect to the target server
- We are in the restricted bash. We cannot use cat/less/more and many other commands but we are good to go with the ‘ls’ (see the screenshot below)

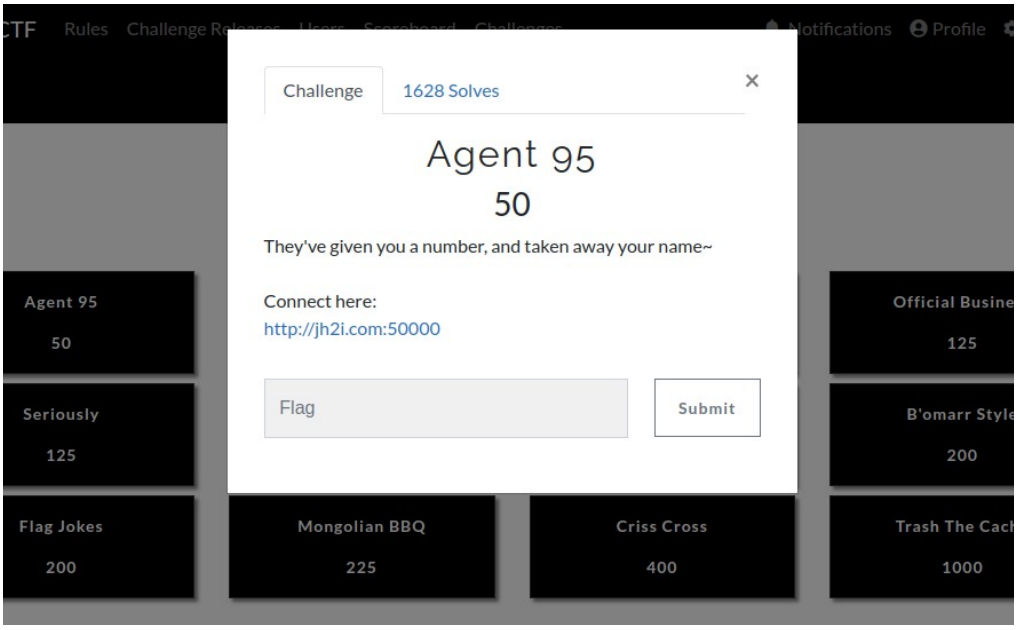
Flag: flag{congrats_you_just_escaped_alkatraz}


Scripting
Powerful Gnomes
150
Signal2
Miscellaneo
Trapped
100
Glimpse
125
Roomie
150
SSH Logger
175
ls
flag.txt
cat flag.txt
/bin/rbash: line 2: cat: command not found
less
/bin/rbash: line 3: less: command not found
more
/bin/rbash: line 4: more: command not found
echo flag.txt
flag.txt
ls
flag.txt
ls -la
total 24
dr-xr-xr-x 1 nobody nogroup 4096 Jun 12 17:08 .
drwxr-xr-x 1 user user 4096 Jun 4 18:54 ..
-rw-r--r-- 1 nobody nogroup 220 Jun 4 18:54 .bash_logout
-rw-r--r-- 1 nobody nogroup 3771 Jun 4 18:54 .bashrc
-rw-r--r-- 1 nobody nogroup 807 Jun 4 18:54 .profile
-rw-r--r-- 1 user user 41 Jun 12 17:08 flag.txt


/bin/rbash: line 45: mv: command not found
tee data.txt
/bin/rbash: line 46: tee: command not found
chmod
/bin/rbash: line 47: chmod: command not found
echo "cat flag.txt" > test.sh
/bin/rbash: line 48: test.sh: restricted: cannot redirect output
ls
flag.txt
echo "cat flag.txt" | test.sh
/bin/rbash: line 50: test.sh: command not found
echo "cat flag.txt" | bash
/bin/rbash: line 51: bash: command not found
echo "cat flag.txt" | exec
sh
/bin/rbash: line 54: sh: command not found
ls flag.txt
flag.txt
ls $(< flag.txt)
ls: cannot access 'flag{congrats_you_just_escaped_alkatraz}': No such file or di
rectory

Web

Agent 95

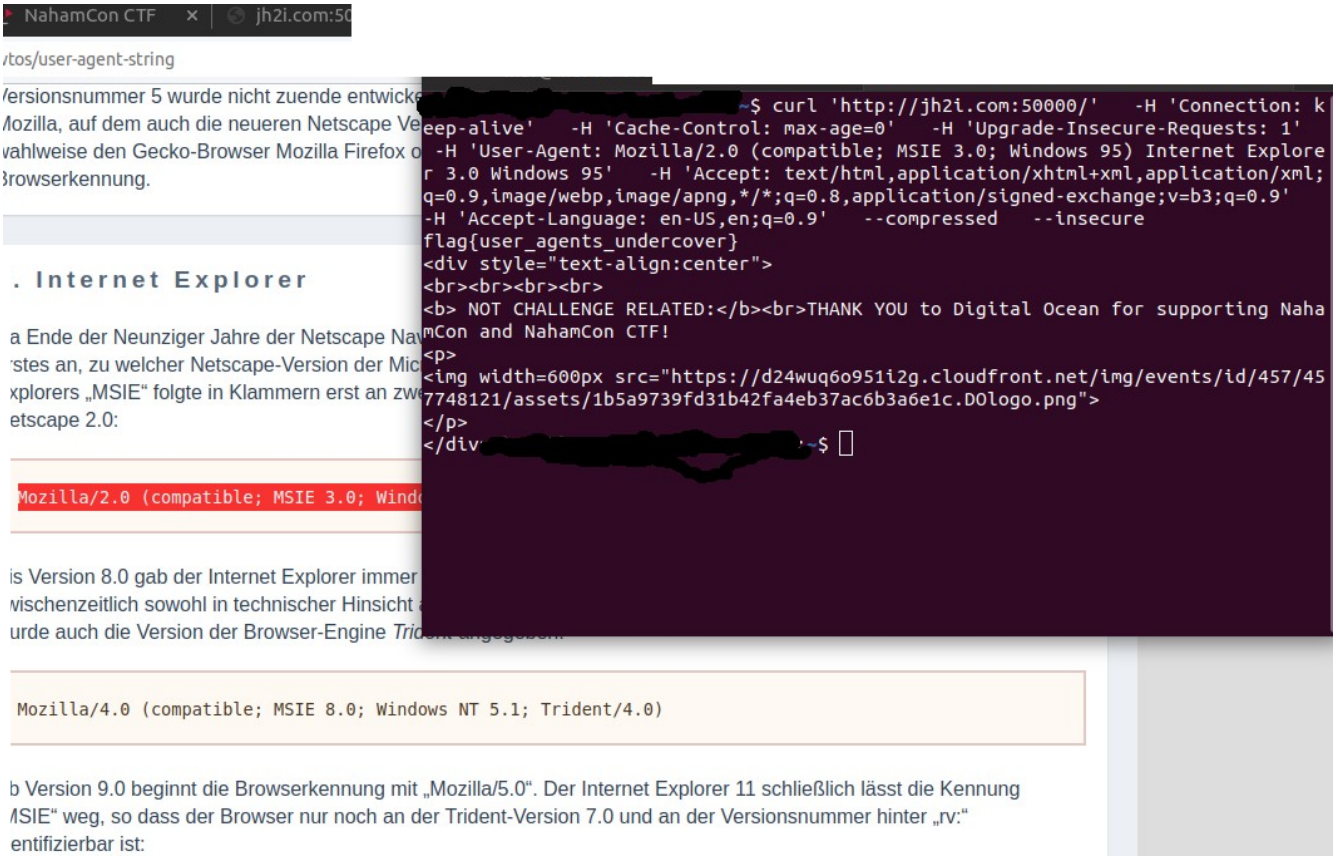


Steps to get the flag:

- Open the target website
- To get the flag we need to use UserAgent header manipulations and pretend that we're using Windows 95. Use any available User Agent header generator (I used https://developers.whatismybrowser.com/ , https://jkip.de/howtos/user-agent-string) and then modify a request to the server in order to get the flag

Flag: flag{user_agents_undercover}


Not secure | jh2i.com:50000
Incognito
You don't look like our agent!
We will only give our flag to our Agent 95! He is still running an old version of Windows...
NOT CHALLENGE RELATED:
THANK YOU to Digital Ocean for supporting NahamCon and NahamCon CTF!
DigitalOcean

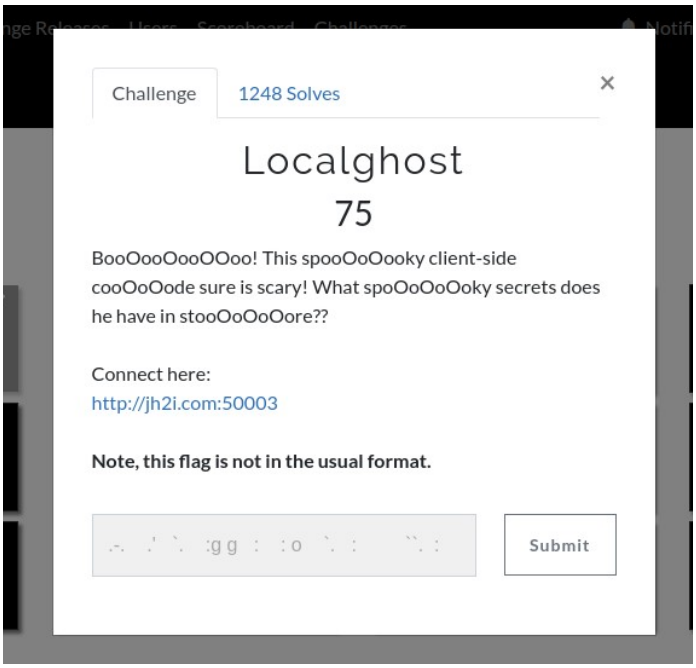

NahamCon CTF
jh2i.com:50
/tos/user-agent-string
/ersionsnummer 5 wurde nicht zuende entwicke
Mozilla, auf dem auch die neueren Netscape Ve
wahlweise den Gecko-Browser Mozilla Firefox o
Browserkennung.
. Internet Explorer
a Ende der Neunziger Jahre der Netscape Na
stes an, zu welcher Netscape-Version der Mic
xplorers „MSIE“ folgte in Klammern erst an zw
etscape 2.0:
Mozilla/2.0 (compatible; MSIE 3.0; Windo
is Version 8.0 gab der Internet Explorer immer
wischenzeitlich sowohl in technischer Hinsicht
urde auch die Version der Browser-Engine Trid
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
b Version 9.0 beginnt die Browserkennung mit „Mozilla/5.0“. Der Internet Explorer 11 schließlich lässt die Kennung
MSIE“ weg, so dass der Browser nur noch an der Trident-Version 7.0 und an der Versionsnummer hinter „rv:“
entifizierbar ist:
~$ curl 'http://jh2i.com:50000/' -H 'Connection: keep-alive' -H 'Cache-Control: max-age=0' -H 'Upgrade-Insecure-Requests: 1' -H 'User-Agent: Mozilla/2.0 (compatible; MSIE 3.0; Windows 95) Internet Explorer 3.0 Windows 95' -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9' -H 'Accept-Language: en-US,en;q=0.9' --compressed --insecure
flag{user_agents_undercover}

 NOT CHALLENGE RELATED:
THANK YOU to Digital Ocean for supporting NahamCon and NahamCon CTF!

<img width=600px src="https://d24wuq6o951i2g.cloudfront.net/img/events/id/457/457748121/assets/1b5a9739fd31b42fa4eb37ac6b3a6e1c.DOlogo.png">

</div
~$

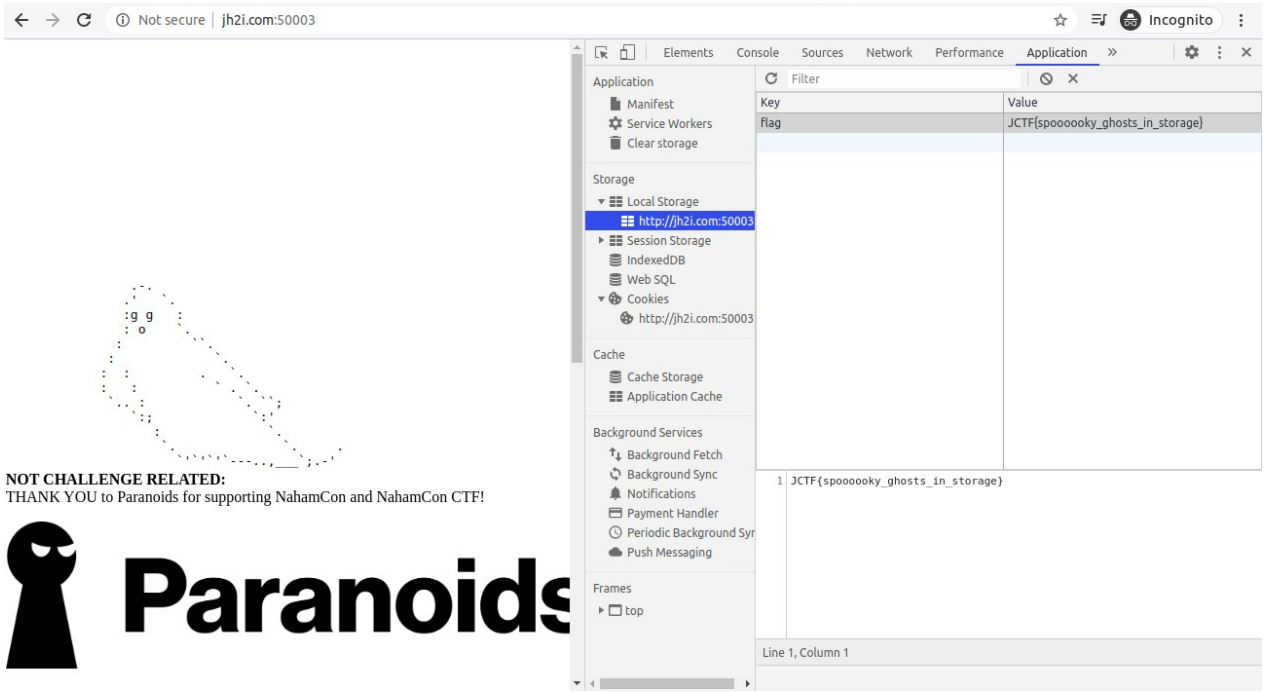
Localghost



Steps to get the flag:

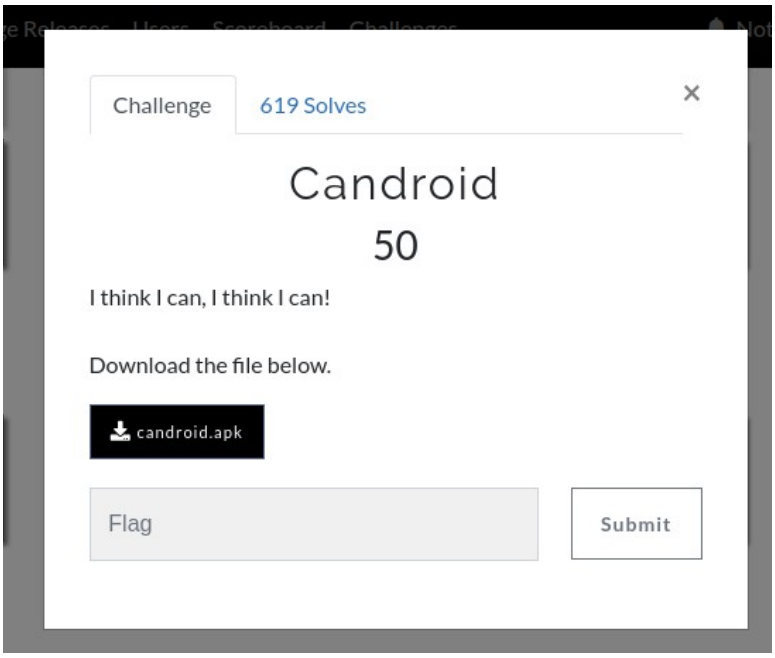
- Open the site
- Check local storage

Flag: JCTF{spoooooky_ghosts_in_storage}



Mobile

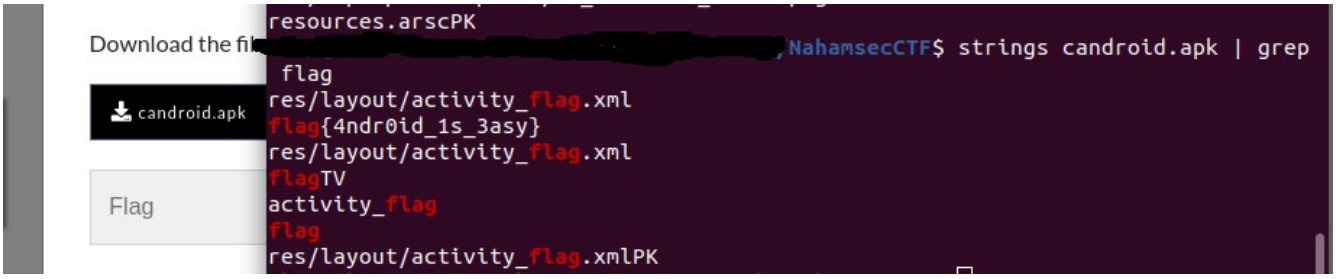
Candroid



Steps to get the flag:

- You have two options: reverse the APK using any tool you want (apktool, dex2jar, APKStudio, https://deapk.vaibhavpandey.com/) or just use ‘strings’ command

Flag: flag{4ndr0id_1s_3asy}



That’s all for today! Thanks for your time! Also, thanks to the all organizers of this event!!! Look forward to compete in the next CTF event from Nahamsec!