

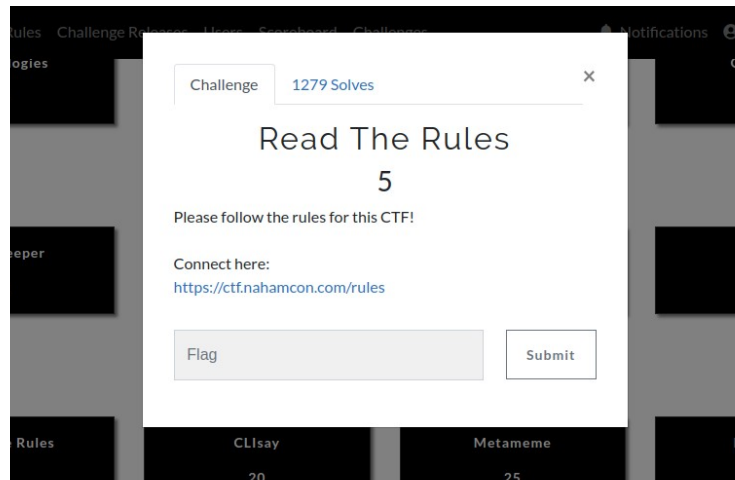
NahamCon CTF writeup

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



#WarmUp challenges

Read the rules



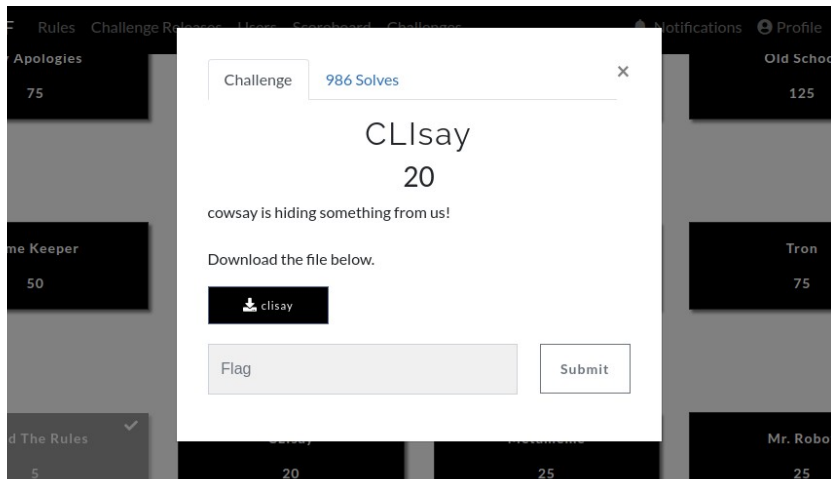
Steps to get the flag:

- Open page
- Analyze page source

Flag: flag{we_hope_you_enjoy_the_game}

```
160 <p>
161     Flags for this competition will follow the format: <b>flag{</b>, with words joined together with underscores inside the curly braces. If you look
162     closely, you can even find a flag on this page!<br>
163     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
164     different flag format.
165 </p>
166 <h1> Support </h1>
167
168 <p>
169     If you need to ask for help on any challenges or need some support, you can join the NahamCon Discord Server <a
170     href="https://discord.gg/ucCz7uh">https://discord.gg/ucCz7uh</a>.
171 </p><h1> Prizes </h1><p>
172     Thanks to the support from you the community and our sponsors, we are pleased to offer prizes to the winners of NahamCon CTF!
173 </p><ul>
174 <li> 1st Place - $500 USD </li>
175 <li> 2nd Place - $250 USD </li>
176 <li> 3rd Place - $100 USD </li>
177 </ul><p></p><!-- Thank you for reading the rules! Your flag is: -->
178 <!--      flag{we_hope_you_enjoy_the_game}      -->
179 </div>
180
181 </main>
182
183 <footer class="footer">
184     <div class="container text-center">
185         <a href="https://ctfd.io" class="text-secondary">
186             <small class="text-muted">Powered by CTFD</small>
187         </a>
188     </div>
189 </footer>
190
191 <script defer src="/themes/core/static/js/vendor.bundle.min.js?d=25aef801"></script>
192 <script defer src="/themes/core/static/js/core.min.js?d=25aef801"></script>
193 <script defer src="/themes/core/static/js/helpers.min.js?d=25aef801"></script>
194
195 <script defer src="/themes/core/static/js/pages/main.min.js?d=25aef801"></script>
196
197
198
199
200
201
```

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}

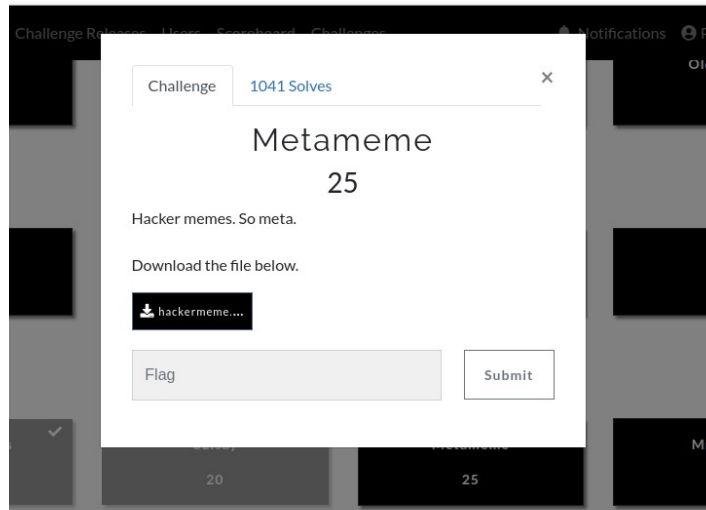
```
~/NahamsecCTF$ file clisay
clisay: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, i
nterpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=70e60678f1c0b75ea3aae2a4e8e1e89
78e3c6fc0, for GNU/Linux 3.2.0, not stripped

~/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



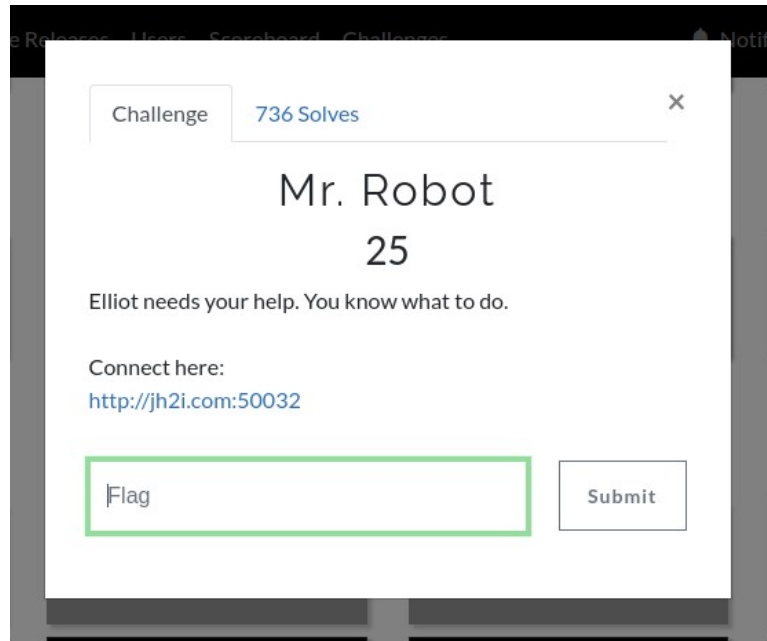
Steps to get the flag:

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

Flag: flag{N0t_7h3_4cTuaL_Cr3At0r}

```
ExifTool Version Number      : 11.16
File Name                    : hackermeme.jpg
Directory                   : .
File Size                    : 372 kB
File Modification Date/Time  : 2020:06:12 21:45:49+03:00
File Access Date/Time       : 2020:06:12 21:46:15+03:00
File Inode Change Date/Time  : 2020:06:12 21:46:05+03:00
File Permissions             : rw-rw-r--
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : None
X Resolution                 : 1
Y Resolution                 : 1
XMP Toolkit                  : Image::ExifTool 10.80
Creator                      : flag{N0t_7h3_4cTuaL_Cr3At0r}
Image Width                  : 1920
Image Height                 : 1080
Encoding Process              : Progressive DCT, Huffman coding
Bits Per Sample              : 8
Color Components              : 3
```

Mr. Robot



Steps to get the flag:

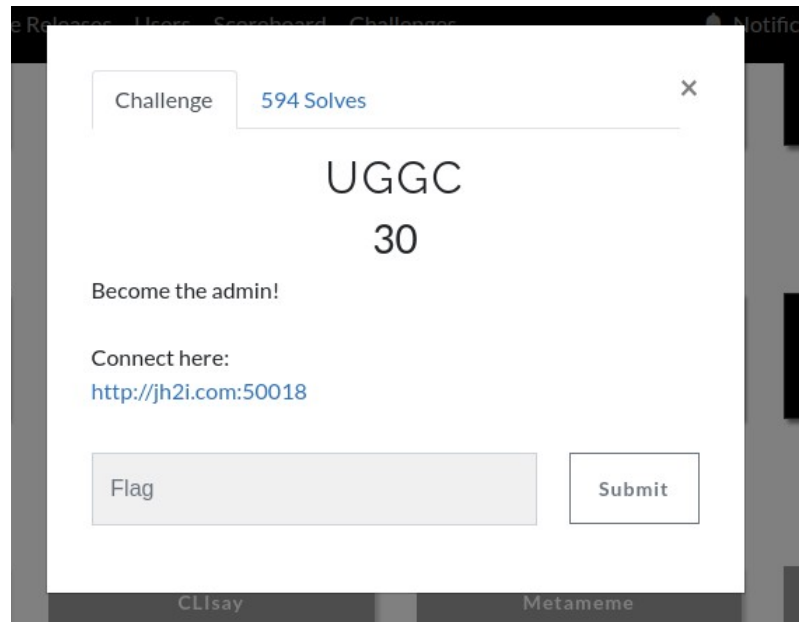
- Open site
- Manually type a url to open robots.txt

Flag: flag{welcome_to_robots.txt}



← → ↻ ⓘ Not secure | jh2i.com:50032/robots.txt
flag{welcome_to_robots.txt}

UGGC



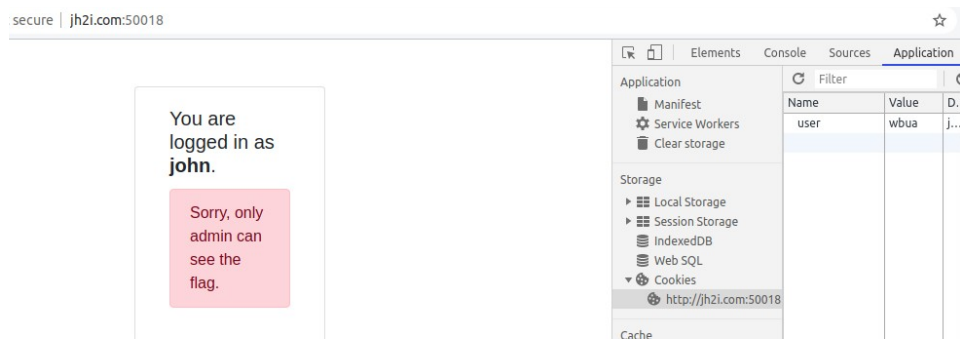
Steps to get the flag:

- 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}



Please choose a username to login.



You are
logged in as
john.

Sorry, only
admin can
see the
flag.

The Network tab shows a list of requests. The first request is 'login' to 'http://jh2i.com:50018/login' with a status of 302 FOUND. The 'Headers' panel is expanded, showing the following details:

- General:**
 - Request URL: http://jh2i.com:50018/login
 - Request Method: POST
 - Status Code: 302 FOUND
 - Remote Address: 161.35.252.71:50018
 - Referrer Policy: no-referrer-when-downgrade
- Response Headers:**
 - Content-Length: 209
 - Content-Type: text/html; charset=utf-8
 - Date: Fri, 12 Jun 2020 18:56:31 GMT
 - Location: http://jh2i.com:50018/
 - Server: Werkzeug/1.0.1 Python/3.6.9
 - Set-Cookie: user=mbua; Path=
- Request Headers:**
 - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

← → ↻ ⓘ Not secure | jh2i.com:50018

You are
logged in as
admin.

Congratulations
here is your flag!

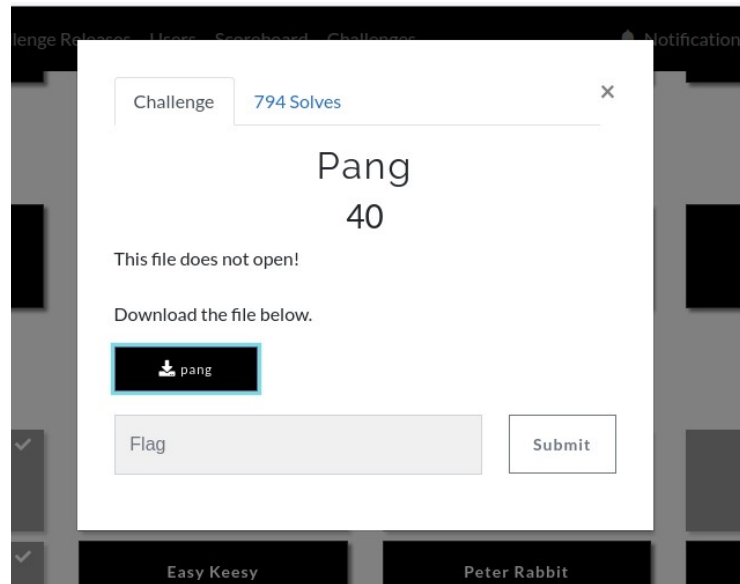
flag{H4cK_
aLL_7H3_
C0okI3s}

The Application tab shows the 'Cookies' section for 'http://jh2i.com:50018'. A single cookie is listed:

Name	Value	D.	P.	E.	S.	H.	S.	P.
user	nqzva	j...	/	S..	9			M.

The 'Storage' section on the left shows 'Local Storage', 'Session Storage', 'IndexedDB', 'Web SQL', and 'Cookies' (selected). The 'Cache' section shows 'Cache Storage' and 'Application Cache'. The 'Background Services' section shows 'Background Fetch', 'Background Sync', 'Notifications', 'Payment Handler', 'Periodic Background Sync', and 'Push Messaging'. The 'Frames' section shows 'top'.

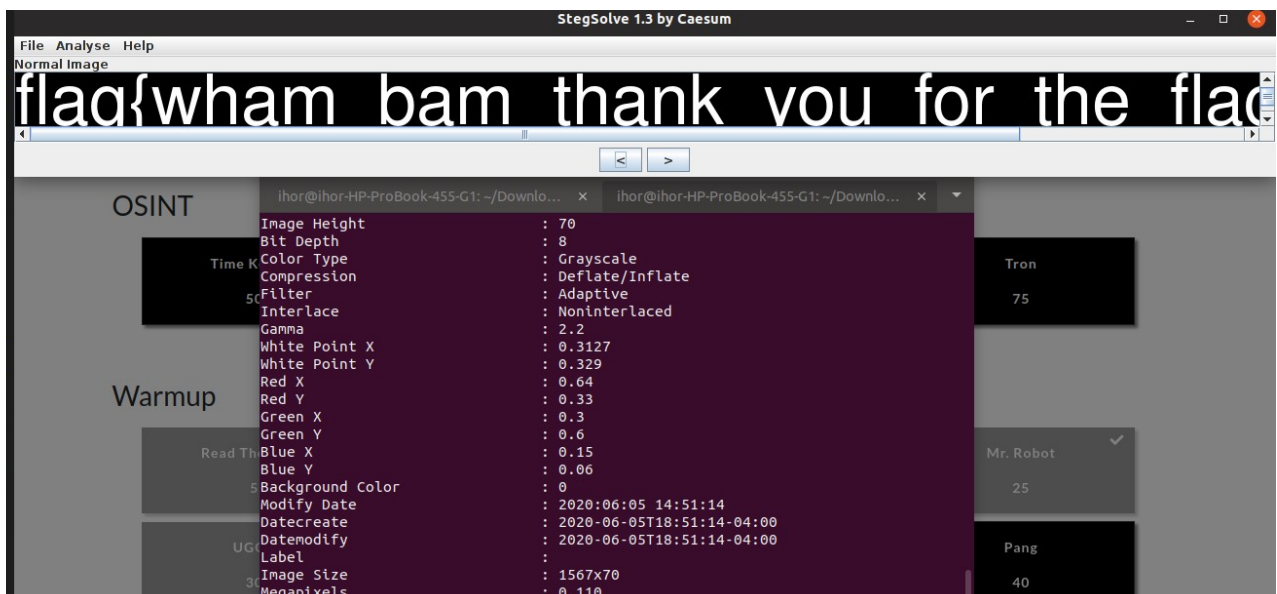
Pang



Steps to get the flag:

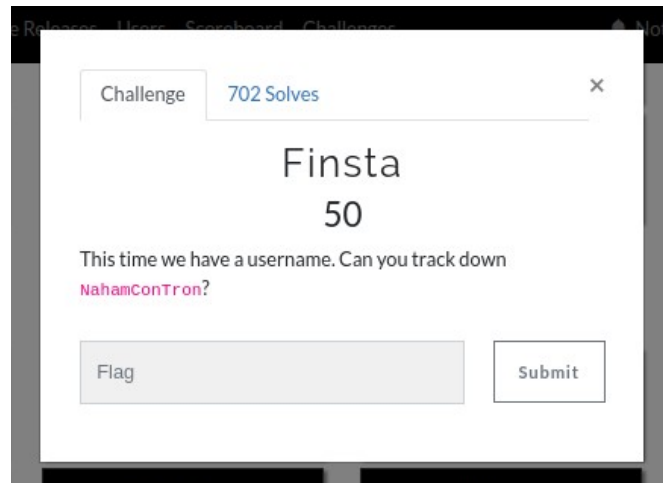
- Use Stegsolve.jar to get the flag: `java -jar Stegsolve.jar`. When Stegsolve is ready, select an image (pang) using File → Open

Flag: `flag{wham_bam_thank_you_for_the_flag_maam}`



OSINT

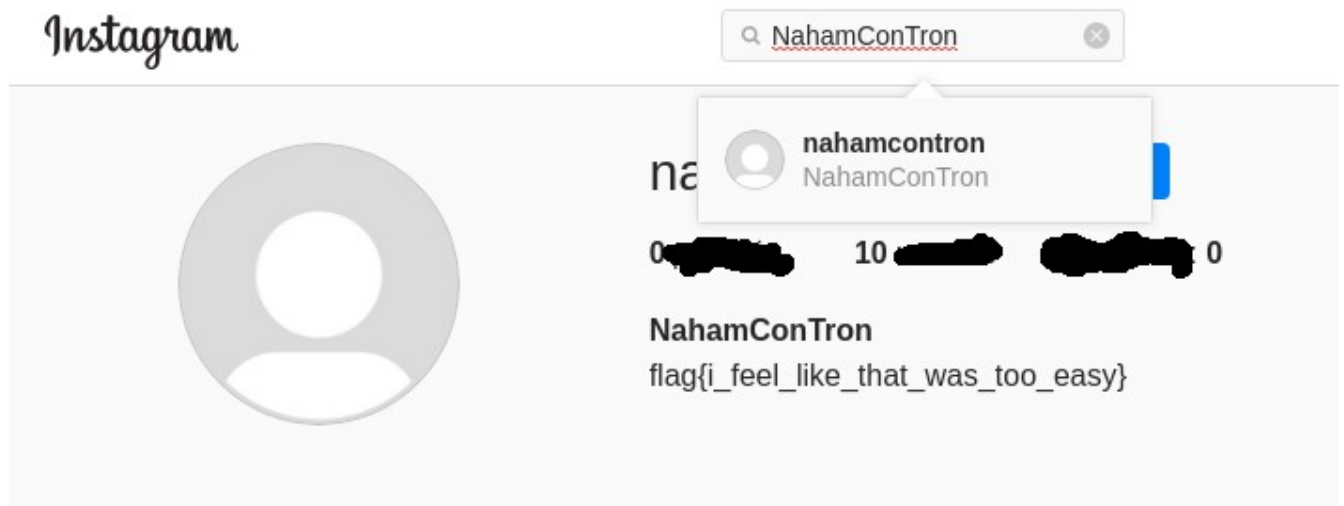
Finsta



Steps to get the flag:

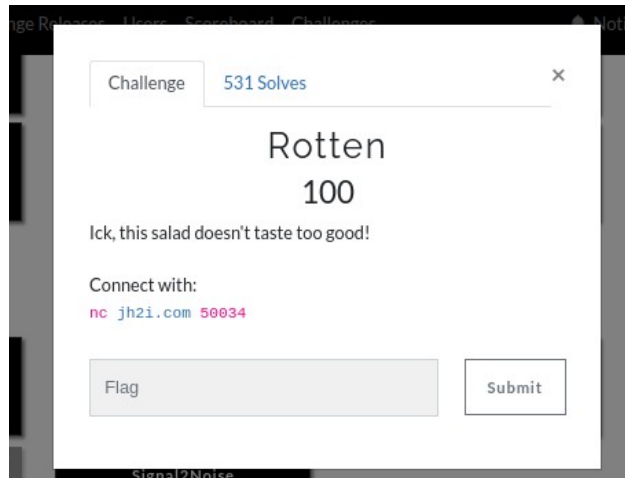
- Use Instagram search to look for the NahamConTron

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}

```
NahamsecCTF$ echo "send back this line exactly. no flag here, just filler." | nc jh2i.com 50034
send back this line exactly. no flag here, just filler.
bnwm kjlt cqr b urwn ngjlcuh. lqajlcna 16 xo cqn oujp rb 'f'
```

About ROT13

```
xjsi gfhp ymnx qnsj jcfhyqd. hmfwfhyjw 0 tk ymj kqfl nx 'k'
jveu srth kyzj czev vortkcp. tyrirtkvi 1 fw kyv wcrx zj 'c'
qclb zyai rfgq jglc cyvarjw. afypyarcp 2 md rfc dbye gq 'y'
coxn lkmu drsc vsxo ohkmdvi. mrkbkmdob 3 yp dro pvkq sc 'q'
iudt rgsa jxyi bydu unqsjbo. sxqhsjjuh 4 ev jxu vbqw yi '{'
lxgw utvd mabl ebqx xqtvmer. vatktvmxk 5 hy max yetz bl 'g'
xjsi gfhp ymnx qnsj jcfhyqd. hmfwfhyjw 6 tk ymj kqfl nx 't'
frao onpx guvf yvar rknpgyl. punenpgre 7 bs gur synt vf 'j'
lxgw utvd mabl ebqx xqtvmer. vatktvmxk 8 hy max yetz bl 'i'
xjsi gfhp ymnx qnsj jcfhyqd. hmfwfhyjw 9 tk ymj kqfl nx 'd'
coxn lkmu drsc vsxo ohkmdvi. mrkbkmdob 10 yp dro pvkq sc 'y'
```



ROT2

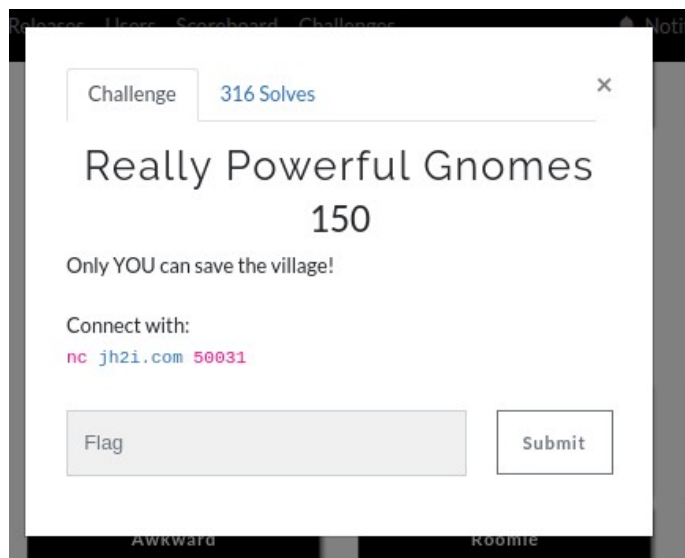


```
zluk ihjr aopz spul lehjasf. johyhjaly 0 vm aol mshn pz 'm'
lxgw utvd mabl ebqx xqtvmer. vatktvmxk 1 hy max yetz bl 'e'
send back this line exactly. character 2 of the flag is 'a'
eqzp nmow ftue xuzq qjmofox. otmdmofqd 3 ar ftq rxms ue 's'
kwfv tsuc lzak dafw wpsuldq. uzsjsulwj 4 gx lzw xdsy ak 'f'
nzly wvxf ocdn gdiz zsvxogt. xcvmvxozm 5 ja ocz agvb dn 'i'
zhluk ihjr aopz spul lehjasf. johyhjaly 6 vm aol mshn pz 'v'
htcs qprz iwxx axct tmprian. rwpgprrtg 7 du iwt uapv xh 'l'
nzly wvxf ocdn gdiz zsvxogt. xcvmvxozm 8 ja ocz agvb dn 'i'
zhluk ihjr aopz spul lehjasf. johyhjaly 9 vm aol mshn pz 'f'
eqzp nmow ftue xuzq qjmofox. otmdmofqd 10 ar ftq rxms ue 'a'
```

```
xjsi gfhp ymnx qnsj jcfhyqd. hmfwfhyjw 0 tk ymj kqfl nx 'k'
jveu srth kyzj czev vortkcp. tyrirtkvi 1 fw kyv wcrx zj 'c'
qclb zyai rfgq jglc cyvarjw. afypyarcp 2 md rfc dbye gq 'y'
coxn lkmu drsc vsxo ohkmdvi. mrkbkmdob 3 yp dro pvkq sc 'q'
iudt rgsa jxyi bydu unqsjbo. sxqhsjjuh 4 ev jxu vbqw yi '{'
lxgw utvd mabl ebqx xqtvmer. vatktvmxk 5 hy max yetz bl 'g'
xjsi gfhp ymnx qnsj jcfhyqd. hmfwfhyjw 6 tk ymj kqfl nx 't'
frao onpx guvf yvar rknpgyl. punenpgre 7 bs gur synt vf 'j'
lxgw utvd mabl ebqx xqtvmer. vatktvmxk 8 hy max yetz bl 'i'
xjsi gfhp ymnx qnsj jcfhyqd. hmfwfhyjw 9 tk ymj kqfl nx 'd'
coxn lkmu drsc vsxo ohkmdvi. mrkbkmdob 10 yp dro pvkq sc 'y'
nzly wvxf ocdn gdiz zsvxogt. xcvmvxozm 11 ja ocz agvb dn 'p'
iudt rgsa jxyi bydu unqsjbo. sxqhsjjuh 12 ev jxu vbqw yi '}'
yktj hgiq znay 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 buxqziv. zexoxzqbo 15 lc qeb cixd fp 'l'
bnwm kjlt cqrh urwn ngjlcuh. lqajalcna 16 xo cqn oujp rb 'f'
frao onpx guvf yvar rknpgyl. punenpgre 17 bs gur synt vf 'j'
lxgw utvd mabl ebqx xqtvmer. vatktvmxk 18 hy max yetz bl 'r'
yktj hgiq znay rotk kdgizre. ingxgizkx 19 ul znk lrgm oy 'u'
jveu srth 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 'a'

jveu srth kyzj czev vortkcp. tyrirtkvi 24 fw kyv wcrx zj 'r'
ugpf dcmn vjku nkgp gzcevna. ejctcevgf 25 qh vjg hnci ku 'g'
myhx vuwe nbcm fchy yruwnfs. wbuluwnyl 26 iz nby zfua cm 'm'
nzly wvxf ocdn gdiz zsvxogt. xcvmvxozm 27 ja ocz agvb dn 'v'
nzly wvxf ocdn gdiz zsvxogt. xcvmvxozm 28 ja ocz agvb dn 'm'
rdmc azbj sgfr khnd dwzbskx. bgzqzbsdq 29 ne sgd ekzf hr 'r'
eqzp nmow ftue xuzq qjmofox. otmdmofqd 30 ar ftq rxms ue 'j'
```

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}

```
What would you like to do?
Gold: 146525
Weapon level

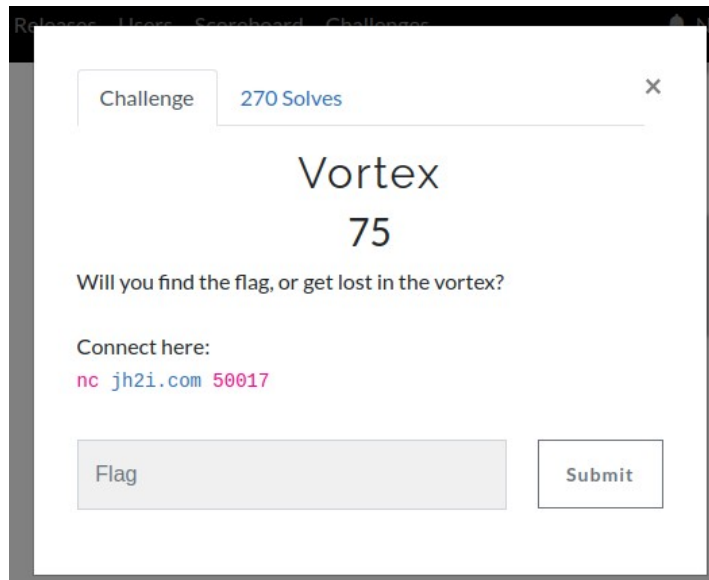
YAYYY!!! You have defeated the gnomes and saved the villagers
Here's your flag: flag{it_was_in_fact_you_that_was_really_powerful}

What would you like to do?
Gold: 46525
Weapon level: 10

1. Defeat the gnomes (level 10)
2. Fight a dragon (level 7)
3. Raid the cyclops (level 5)
4. Plunder the pirates (level 3)
5. Go on a journey (level 1)
6. Browse the shop
7. End journey
>
```

Miscellaneous

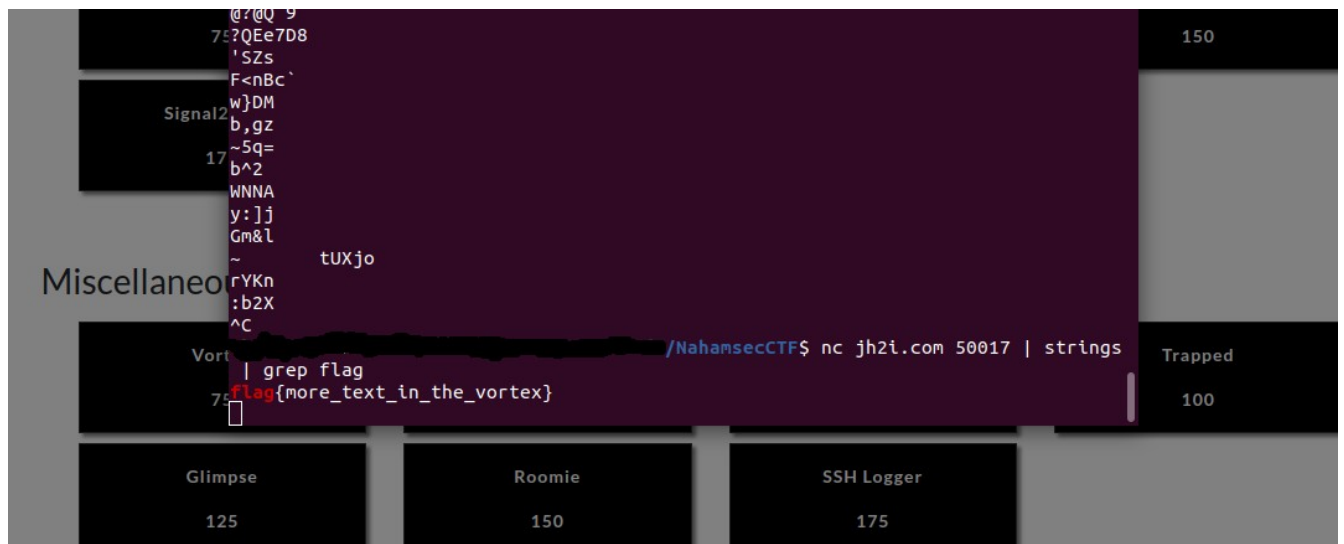
Vortex



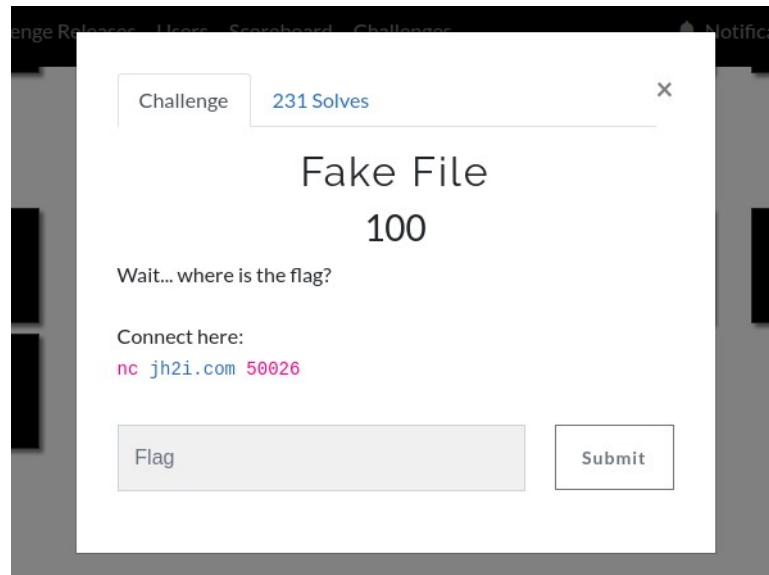
Steps to get the flag:

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

Flag: flag{more_text_in_the_vortex}



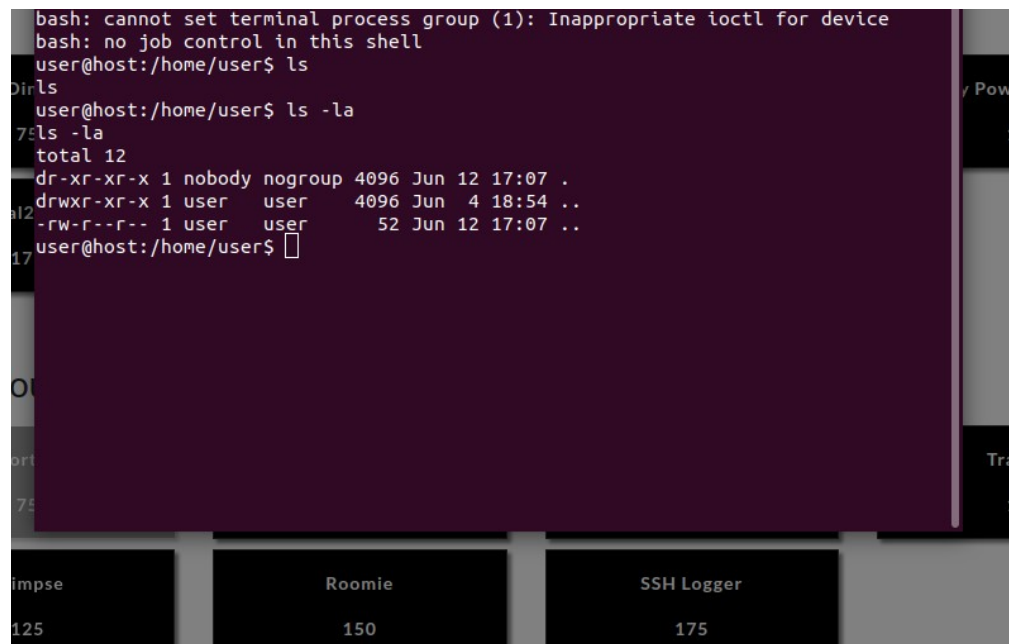
Fake file



Steps to get the flag:

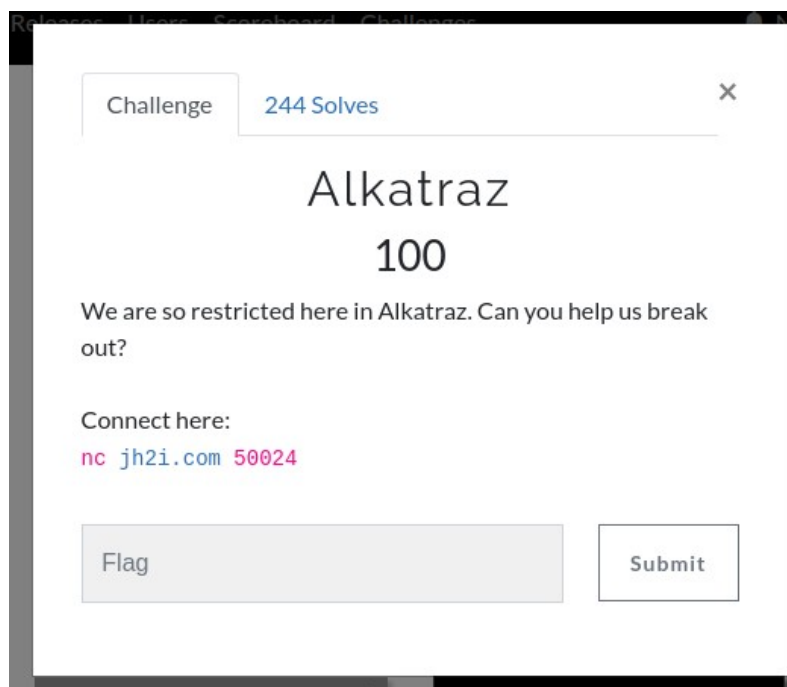
- Connect to the target server
- Use 'ls -la' to look around. It seems that there is a fake file '..'
- It is not available using cat/less/more. We should use 'find' to bypass the restrictions (see the screenshot below)

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$
```

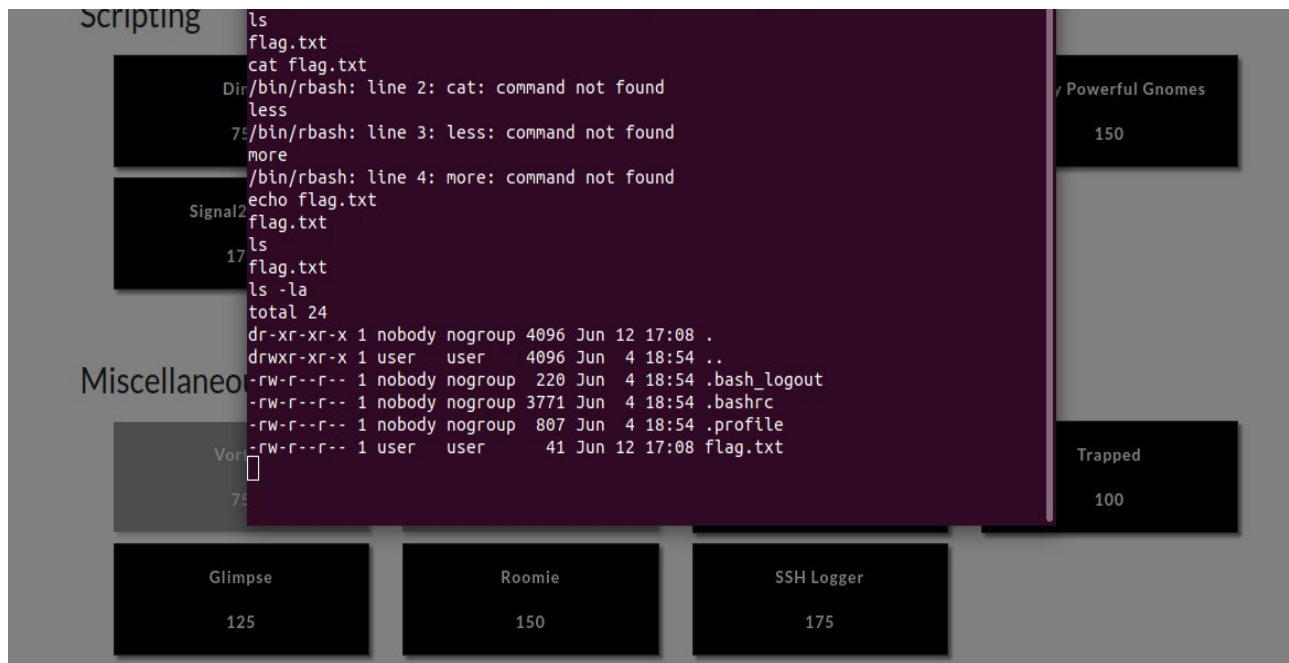
Alkatraz



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)

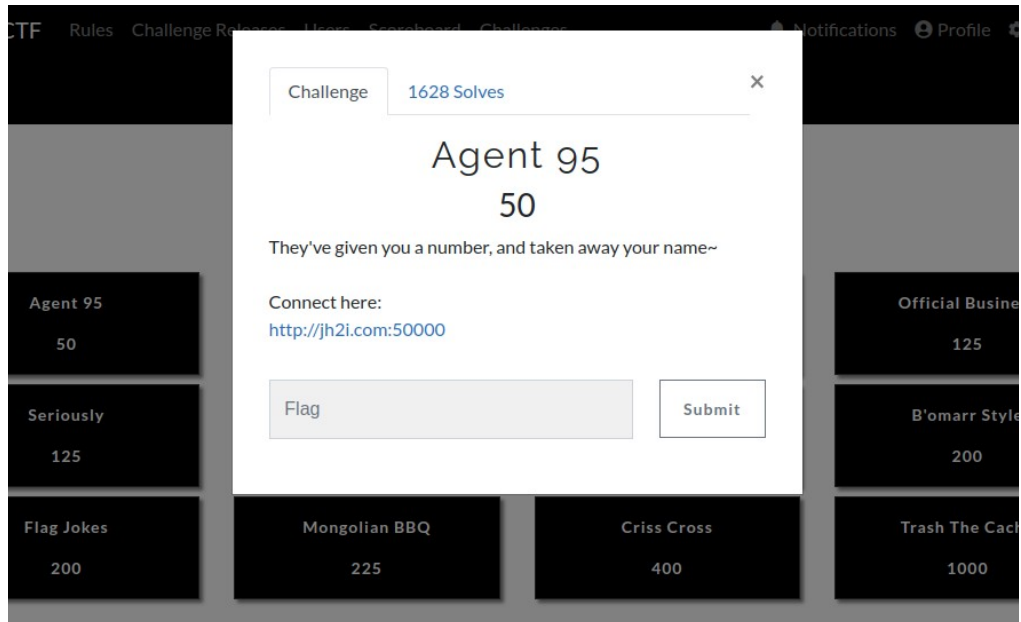
Flag: flag{congrats_you_just_escaped_alkatraz}



```
/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 directory
```


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}

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!



/tos/user-agent-string

Versionnummer 5 wurde nicht zuende entwickelt. Mozilla, auf dem auch die neueren Netscape Versionen basieren, wahlweise den Gecko-Browser Mozilla Firefox oder den Netscape-Browsererkennung.

Internet Explorer

Am Ende der Neunziger Jahre der Netscape Navigator, zu welcher Netscape-Version der Microsoft Internet Explorer „MSIE“ folgte in Klammern erst an zweiter Stelle, dann Netscape 2.0:

Mozilla/2.0 (compatible; MSIE 3.0; Windows 95)

Ab Version 8.0 gab der Internet Explorer immer nur die Versionsnummer an, wischenzeitlich sowohl in technischer Hinsicht als auch in der Versionsnummer. Er wurde auch die Version der Browser-Engine Trident angegeben:

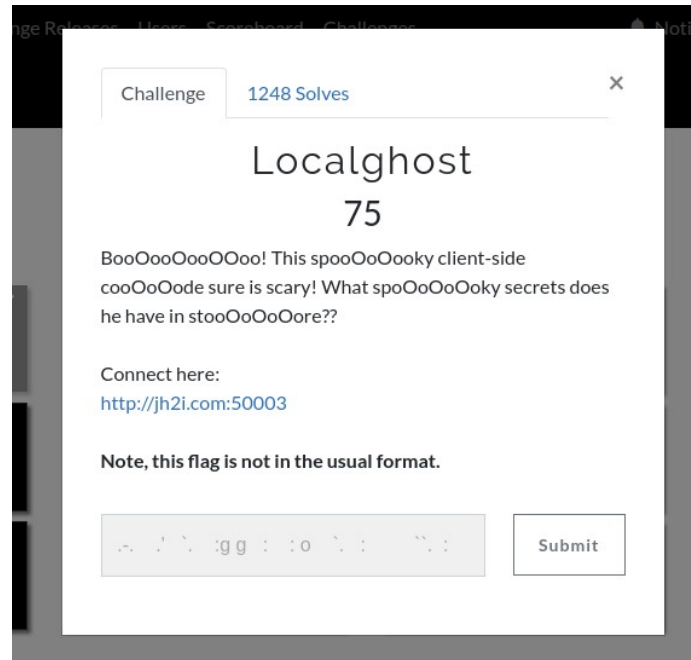
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)

Ab Version 9.0 beginnt die Browsererkennung 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:“ identifizierbar 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}
<div style="text-align:center">
<br><br><br><br>
<b> NOT CHALLENGE RELATED:</b><br>THANK YOU to Digital Ocean for supporting NahamCon and NahamCon CTF!
<p>

</p>
</div>
~$
```

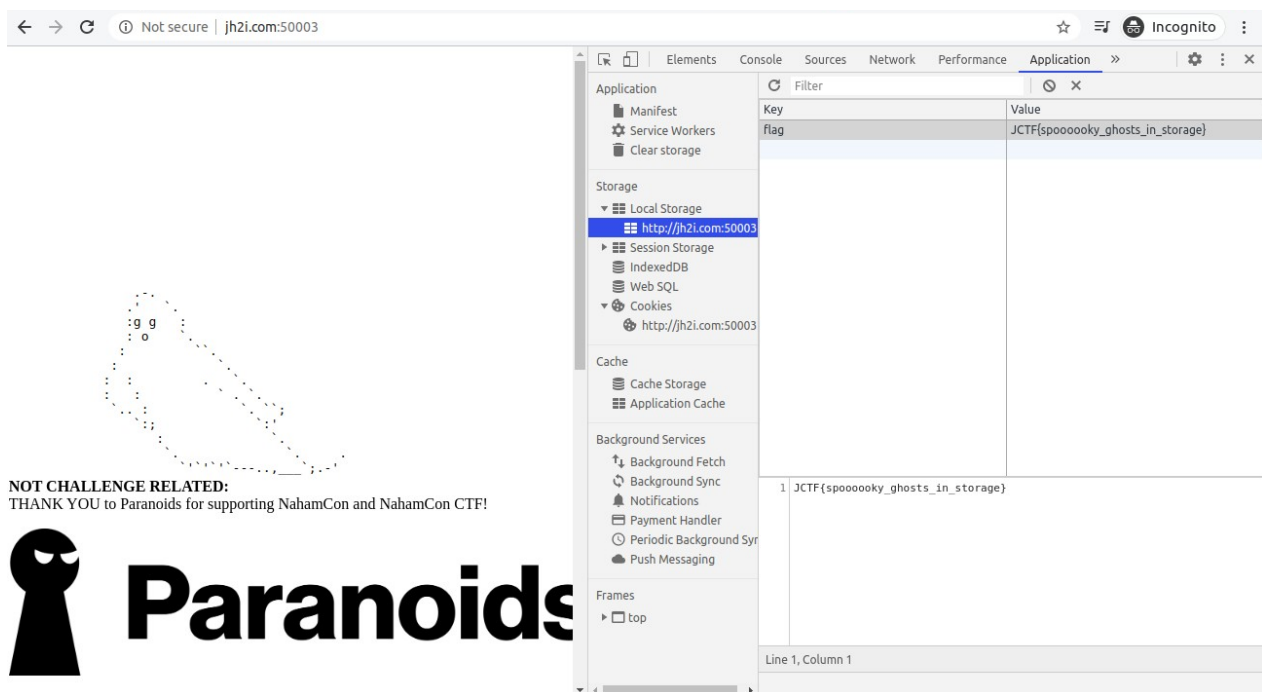
Localghost



Steps to get the flag:

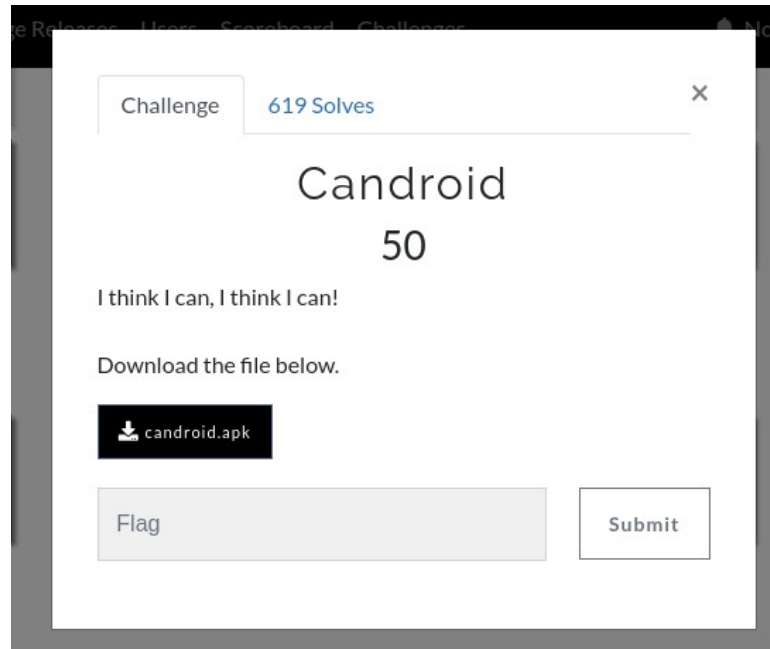
- Open the site
- Check local storage

Flag: JCTF{spooooooky_ghosts_in_storage}



Mobile

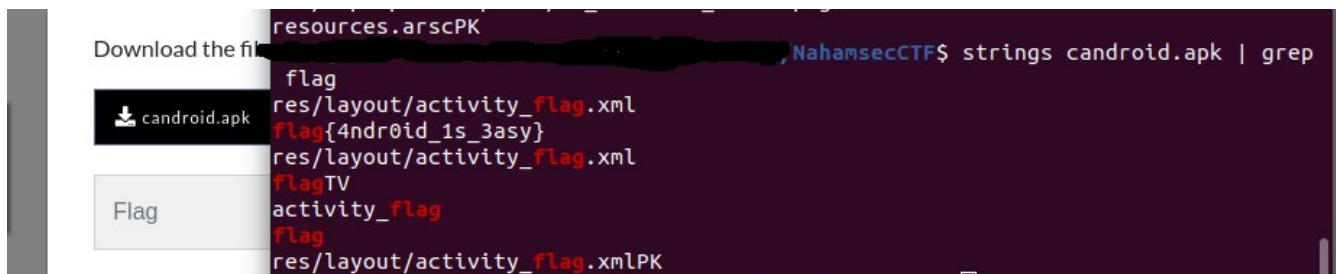
Candroid

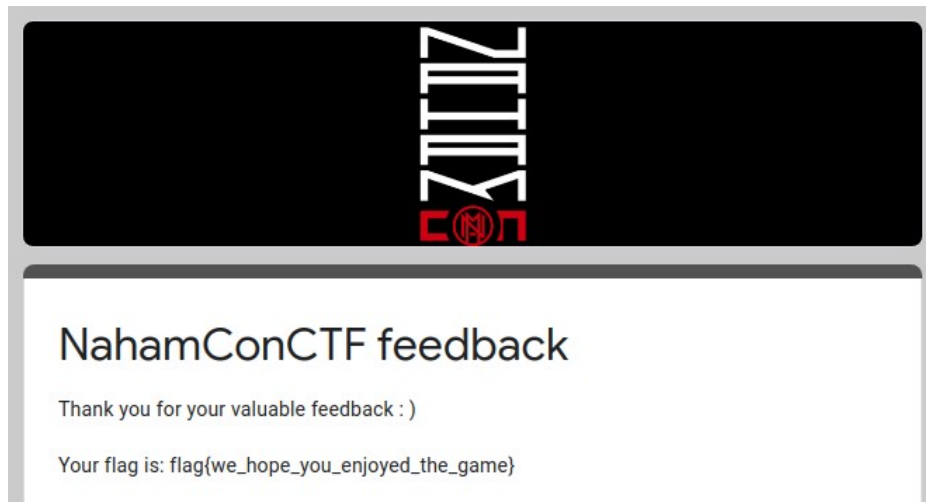


Steps to get the flag:

- 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!