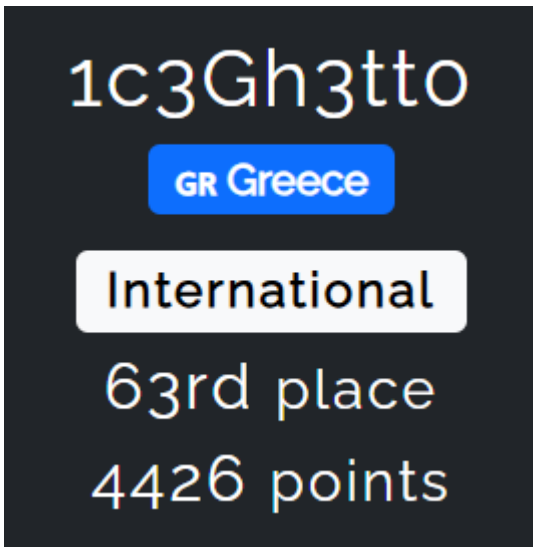
JUK3

1C3GH3TTO – JUKE WRITEUPS

BrunnerCTF 2025



Categories

Crypto

The Cryptographic Kitchen!


solve.py

Encrypted and Desperate


solve.py

Forensics

Memory Loss

BrunnerCTF 2025 / Memory Loss

1. `$ python3 Giannis/CTF/volatility3/vol.py -f memoryloss.dmp windows.filescan.FileScan | grep -i "\.png\|\.jpeg\|\.jpg\|\.bmp\"`
2. `$ python3 Giannis/CTF/volatility3/vol.py -f memoryloss.dmp -o extracted_images windows.dumpfiles.DumpFiles --virtaddr 0xb207c3ab6c40`
3. open the image and view the flag

New Order

BrunnerCTF 2025 / New Order

1. unzip the doc file
2. $ olevba word/vbaProject.bin --deobf
3. take this vba script and deobfuscate it
4. from the result decode base64 and find a link
5. download the content of this link and find another base64, which while decoding you can notice the flag

deobf.py

Misc

The Yeast Key


solve.py

```
C:\Users\User\Desktop>python solve.py
brunner{1i0n3l_p0i14n3_m4573r_0f_50urd0u6h_p455phr453_15_cr01554n7V4u17!93}
```

Pie Recipe


solve.py

```
C:\Users\User\Desktop>python solve.py
Sums (ASCII codes): [89, 110, 74, 49, 98, 109, 53, 108, 99, 110, 115, 51, 97, 68,
78, 102, 90, 122, 65, 120, 90, 68, 78, 117, 88, 51, 66, 111, 77, 86, 56, 119, 90,
108, 57, 54, 90, 87, 78, 114, 90, 87, 53, 107, 98, 51, 74, 109, 102, 81, 61, 61]
Base64 string: YnJ1bm5lcns3aDNfZzAxZDNuX3BoMV8wZl96ZWNrZW5kb3JmfQ==
Decoded flag: brunner{7h3_g01d3n_ph1_0f_zeckendorf}
```

Bakerman

BrunnerCTF 2025 / Bakerman

1. open the mp3 in hex editor and notice it is actually a zip
2. extract the image from it
3. run `zsteg` command
4. combine the base64 and decode them all together to read the flag

Cake Constellation

After checking all 12:26:3X, I noticed that 12:26:33 was the better viewable, so I changed the script to view only this. after zooming noticed the flag

solve.py

Planes!

Mobile

RivalCakes

After searching in data and sdcard folders, I found the 4 password parts and an image that had some coordinates

```
<string
name="recipe_file">/storage/emulated/0/Download/Cakes/best_cak
e_in_the_world.jpg</string>
```

Then opened what3words and input them to complete the flag

FridayCake

BrunnerCTF 2025 / FridayCake
keywords: apk, mobile

1. `apktool d FridayCake.apk -o FridayCase_output`
2. `ls -la FridayCake_output/smali/dk/brunnerctf/fridaycake/`
3. notice these smali files having verifyCode and decodeFlag
4. `strings FridayCake_output/lib/arm64-v8a/libnative-lib.so | grep -i brunner`
5. find the functions and then use radare2 to view the assembly code
6. when you have everything put them to chatgpt to make you script for decoding
7. fix the flag format and submit


solve.py

```
C:\Users\User\Desktop>python solve.py
raw : ;;FLBD;;csvoofs|Z1v`Vt4e`Gs2e5`G1s`Hs5cc2oh`Ui2t`S2hiu@~
text: ;;EKAC;;brunner Y0u Us3d Fr1d4 F0r Gr4bb1ng Th1s R1ght@~
```

Reverse

Trippi Troppa Chaos

solve.py

```
C:\Users\User\Desktop>python solve.py
brunner{tr4l4l3r0_b0mb4rd1r0_r3v3rs3_3ng1n33r1ng_sk1b1d1_m4st3r}
```