

advanced-potion-maker

advanced-potion-making 



Medium Forensics picoMini by redpwn

AUTHOR: BIGC

Description

Ron just found his own copy of advanced potion making, but its been corrupted by some kind of spell. Help him recover it!

Hints

(None)

CHALLENGE ENDPOINTS

Download advanced-potion-making [advanced-potion-making](#)

8,238 users solved



64% Liked



 picoCTF{FLAG}

Submit Flag

Attached file: advanced-potion-making

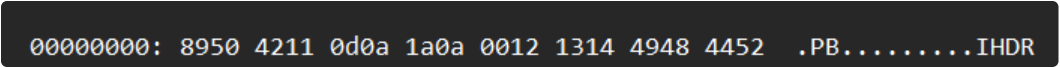
My first instincts

```
$ file advanced-potion-making
advanced-potion-making: data
```

Which yielded nothing, this usually prompts me to analyze what type of data is inside, so...

- 1. **Strings & hex dump** – nothing human-readable in the strings output, but the first few bytes in the hex dump look *almost* like a PNG:

```
$ xxd -g1 -l 16 advanced-potion-making > APM-hex.txt
```



Based on these sources, a real PNG should look like this:

```
[00000000] 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 .PNG.....IHDR
[00000016] 00 00 00 20 00 00 00 20 01 00 00 00 00 5B 01 47 .....[.G
[00000032] 59 00 00 00 04 67 41 4D 41 00 01 86 A0 31 E8 96 Y....gAMA...1..
[00000048] 5F 00 00 00 5B 49 44 41 54 78 9C 2D CC B1 09 03 _...[IDATx.-...
[00000064] 30 0C 05 D1 EB D2 04 B2 4A 20 0B 7A 34 6F 90 15 0.....J..z4o..
[00000080] 3C 82 C1 8D 0A 61 45 07 51 F1 E0 8A 2F AA EA D2 <....aE.Q.../...
[00000096] A4 84 6C CE A9 25 53 06 E7 53 34 57 12 E2 11 B2 ..l..%S..S4W...
[00000112] 21 BF 4B 26 3D 1B 42 73 25 25 5E 8B DA B2 9E 6F !.K&=.Bs%^....o
[00000128] 6A CA 30 69 2E 9D 29 61 6E E9 6F 30 65 F0 BF 1F j.0i..)an.o0e...
[00000144] 10 87 49 2F D0 2F 14 C9 00 00 00 00 49 45 4E 44 ..I/./.....IEND
[00000160] AE 42 60 82
-- Sector 1 -- Assuming 512 Bytes ---
```

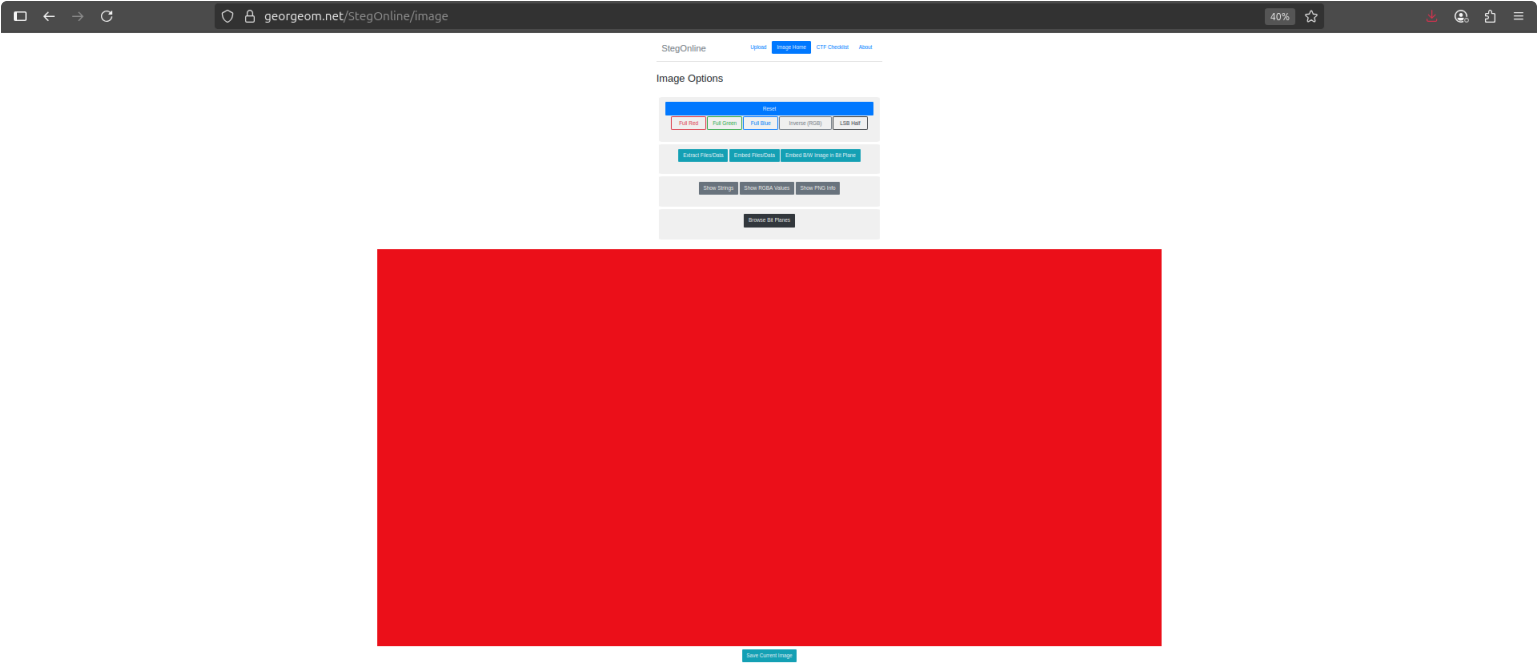
- 2. **Assumption** – If the rest of the file is intact, fixing those bytes should give a valid PNG the usual tools can parse.

Only **5** bytes are off, so using `hexeditor` I changed those values to conform with standard

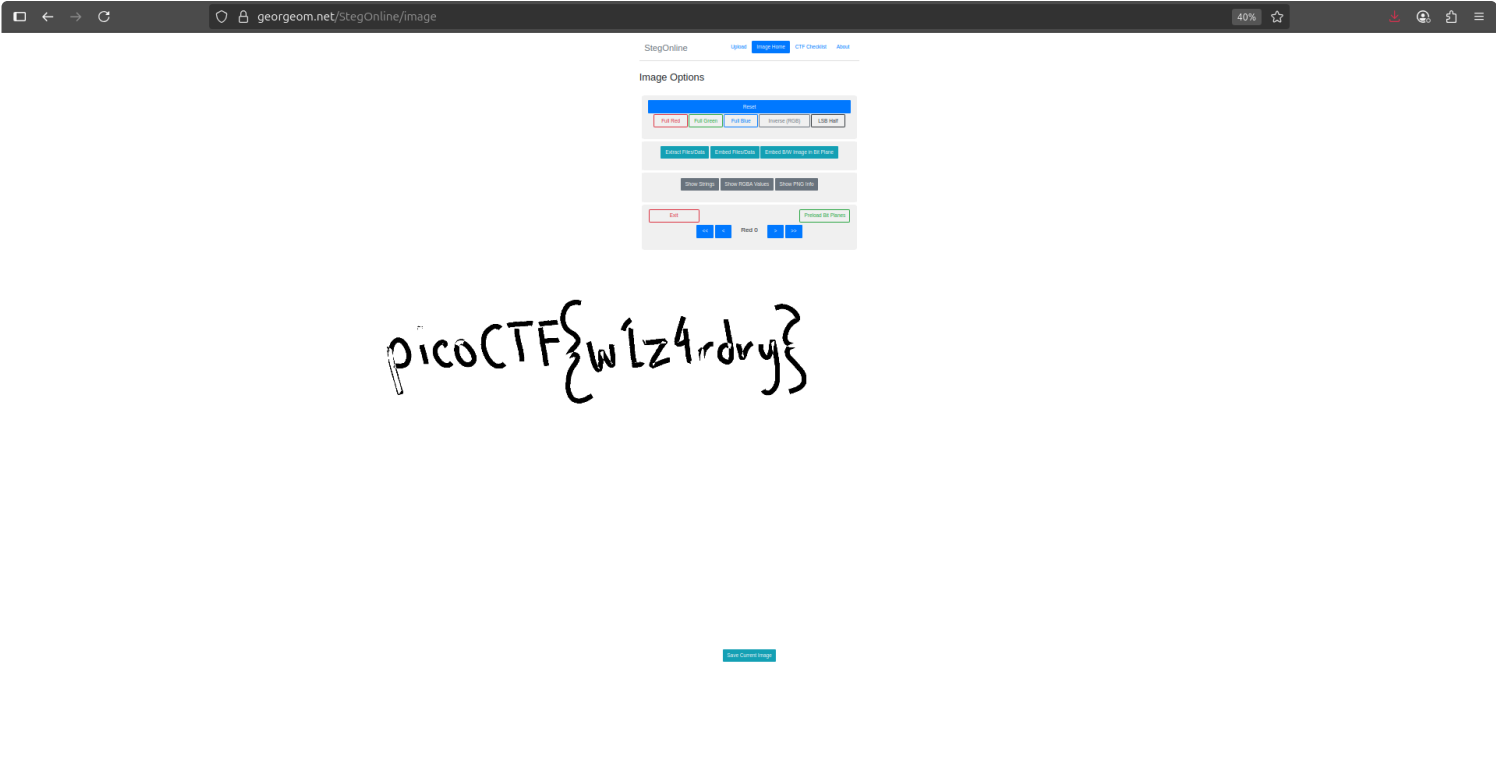


At this point the image opens—and it’s just a red canvas. The flag clearly isn’t in the visible pixels, so we shift to steganography.

Classic trick for this author: data embedded in the *least-significant bit* (LSB) of one colour channel.



1. choose **browse Bit Planes** → **Red 0** (that's the lowest bit of the red channel).
2. Boom—black text on white background spells out:



picoCTF{w1z4rdry}

advanced-potion-making



Medium Forensics picoMini by redpwn

AUTHOR: BIGC
Description

Ron just found his own copy of advanced potion making, but its been corrupted by some kind of spell. Help him recover it!

Hints
(None)

CHALLENGE ENDPOINTS

Download advanced-potion-making advanced-potion-making

8,240 users solved

64% Liked

picoCTF{FLAG}

Submit Flag