

GreyHat CTF Meetings (FALL 2020)

Problems will be listed in order from easy to hard. Highlight (or copy-paste) the hints to see their content. All problems are property of their respective owners. We will go over the problems during weekly CTF meetings (Tuesday at 7PM on BlueJeans).

Week 7 - How to Burp

Important: download Burp Suite Community Edition

Problem: "Postbook" from [Hacker101 CTF](#)

Link: <http://34.94.3.143/c71dd5d07b/>

Hints: There are 7 flags on this website.

- The person with username "user" has a very easy password... user // password
- Try viewing your own post and then see if you can change the ID
- You should definitely use "Inspect Element" on the form when creating a new post
- $189 * 5$
- ***You can edit your own posts, what about someone else's?***
- The cookie allows you to stay signed in. Can you figure out how they work so you can sign in to user with ID 1?
- Deleting a post seems to take an ID that is not a number. Can you figure out what it is?

Week 6 - Reverse Engineering

1. Vault Door 3 (picoCTF)
 - a. This vault uses for-loops and byte arrays. The source code for this vault is here: [VaultDoor3.java](#)
 - b. Hints

2. ASM2 (picoCTF)
 - a. What does `asm2(0xb,0x2e)` return? Submit the flag as a hexadecimal value (starting with '0x'). NOTE: Your submission for this question will NOT be in the normal flag format. [Source](#)
 - b. Hints

3. Rock (CSAW 2016)
 - a. Never forget the people's champ.
<https://365.csaw.io/files/1639472fcee4b79aa1908e9732f0b962/rock>
 - b. Write-up:
<https://github.com/VulnHub/ctf-writeups/blob/master/2016/csaw/rock.md>
4. Bananascript (CSAW 2016)

- a. Not too sure how to Interpret this, the lab member who wrote this "forgot" to write any documentation. This shit, and him, is bananas. B, A-N-A-N-A-S.
- b. <https://365.csaw.io/files/5bcb4f49ba2c42d5e507f602a8e8d0d9/banana.script>
- c. <https://365.csaw.io/files/100a60a8f4efce78dec38fe1fe6ed8b0/monkeyDo>
- d. Write-up: <https://ctftime.org/writeup/7620>

Week 5 - Server-side Web

1. Irish Name Repo (picoCTF 2018)
 - a. There is a website running at <http://2018shell2.picoctf.com:52135>. Do you think you can log us in? Try to see if you can login!
 - b. Hints
2. Flask Skeleton Key (picoCTF 2018)
 - a. Nice! You found out they were sending the Secret_key: 385c16dd09098b011d0086f9e218a0a2. Now, can you find a way to log in as admin? <http://2018shell2.picoctf.com:48263>.
 - b. Hints
3. Shia (CSAW 2017)
 - a. To access, create an account on <https://365.csaw.io> and visit <https://365.csaw.io/challenges#shia>.
4. Orangev2 (CSAW 2017)
 - a. To access, create an account on <https://365.csaw.io> and visit <https://365.csaw.io/challenges#orangev2>

Week 4 - Pwn

Some prerequisite knowledge on computer memory (à la CS 2110) may help with these problems. See [this video series by LiveOverflow](#) for tutorials. Also, from now on, we'll do 4 problems per week: (easy/hard) high-school CTF // (easy/hard) collegiate CTF. Problems will still be listed in order of difficulty

Note: the flags in problems 1-3 will be dummy/redacted flags because pwn problems usually have shell servers to give the actual flag. #4 is from CSAW 2020, so the server is still up.

1. Buffer overflow 1 (picoCTF)
 - a. Okay now you're cooking! This time [sic] can you overflow the buffer and return to the flag function in this [program](#)? You can find it in /problems/buffer-overflow-1_2_86cbe4de3cdc8986063c379e61f669ba on the shell server. [Source](#).
 - b. Hints

- [REDACTED]
- [REDACTED]
2. Buffer overflow 2 (picoCTF)
 - a. Alright, this time you'll need to control some arguments. Can you get the flag from this [program](#)? You can find it in `/problems/buffer-overflow-2_4_ca1cb0da49310dd45c811348a235d257` on the shell server. [Source](#).
 - b. Hints

[REDACTED]
 3. Small Boi (CSAW Quals 2019)
 - a. you were a baby boi earlier, can you be a small boi now?
`https://github.com/r4j0x00/ctf-writeups/raw/master/csaw2019/pwn/small_boi/small_boi`
 - b. Hints

[REDACTED]
 4. feather (CSAW Quals 2020)
 - a. I made a brand-new filesystem archive format that I think will supercede tar! Could you help me test it out? `nc pwn.chal.csaw.io 5017`. Libc2.31 md5: 10fdeb77eea525914332769e9cd912ae
 - b. Files
 - i. https://drive.google.com/drive/folders/1lr6Kxw4Fuy95E4chqtTgQq0u_AtoYkC1?usp=sharing
 - c. Write-up
 - i. <https://ptr-yudai.hatenablog.com/entry/2020/09/14/181939#Pwn-450pts-feather-6-solves>

Week 3 - CSAW Quals 2020

Starts **Friday, September 11th at 4PM**

BlueJeans open all weekend (see Slack for link)

Will go over some problems Monday 6:30PM

Week 2 - Neil and Tilly's Crypto Corner

Use Google to help! Don't feel like you have to attempt/solve all 5 of these—I wanted to include problems that appeal to everyone so there is a wide range of difficulty.

1. Touch Base - 100 points - TJCTF 2019
 - a. Decode this string for an easy flag!
Encoded: `dGpj dGZ7ajJzdF9zMG0zX2I0c2U2NH0=`
 - b. Hints

[REDACTED]

 - c. Write-up

2. ZOR - 200 points - picoCTF 2014

- a. Daedalus has encrypted their blueprints! Can you get us the password?

Two files: [zor.py](#), [encrypted](#)

- b. Hints

- c. Write-up

i. <https://ashwinvbs.gitbooks.io/picoctf-2014-writeup/content/chapter19.html>

3. Easy as RSA - 300 points - TJCTF 2019

- a. Decrypt this for a quick flag!

n: 379557705825593928168388035830440307401877224401739990998883

e: 65537

c: 29031324384546867512310480993891916222287719490566042302485

- b. Hints

- c. Write-up

i. <https://ctftime.org/writeup/14547>

4. Super Safe RSA 3 - 400 points - picoCTF 2018 (challenge)

- a. The more primes, the safer.. right.?? Connect with `nc

2018shell12.picoctf.com 35072` (command line shell)

- b. Hints

- c. Write-up

i. <https://tcode2k16.github.io/blog/posts/picoctf-2018-writeup/cryptography/#super-safe-rsa-3>

5. Magic Padding Oracle - 500 points - picoCTF 2018

- a. Can you help us retrieve the flag from this crypto service? `nc

2018shell13.picoctf.com 24933`

Source:

<https://2018shell1.picoctf.com/static/71aba0dacd85657a2ab6d0f4e576bcc5/pkcs7.py>

- b. Hints

- c. Write-up

i. https://github.com/Dvd848/CTFs/blob/master/2018_picoCTF/Magic%20Padding%20Oracle.md

Week 1 - Misc. picoCTF problems

Selections from picoCTF 2019 (misc. categories)

This week is a hodgepodge of categories, meant to give an introduction into what types of problems CTFs may offer. picoCTF is a high-school level competition from CMU. Flags look like this: `picoCTF{this_is_a_flag}` (you'll know it when you see it).

1. Client-side-again - 100 points - web
 - a. Can you break into this super secure portal?
<https://2019shell1.picoctf.com/problem/49886/> ([link](#)) or
<http://2019shell1.picoctf.com:49886>
 - b. Hints

 - c. Write-up
 - i. https://github.com/Dvd848/CTFs/blob/master/2019_picoCTF/Client-side-again.md
2. Mr. Worldwide - 200 points - crypto
 - a. A musician left us a message. What's it mean?
 - b. `picoCTF{(35.028309, 135.753082)(46.469391, 30.740883)(39.758949, -84.191605)(41.015137, 28.979530)(24.466667, 54.366669)(3.140853, 101.693207)_(9.005401, 38.763611)(-3.989038, -79.203560)(52.377956, 4.897070)(41.085651, -73.858467)(57.790001, -152.407227)(31.205753, 29.924526)}`
 - c. Hints

 - d. Write-up
 - i. https://github.com/Dvd848/CTFs/blob/master/2019_picoCTF/Mr-Worldwide.md
3. Flag Shop - 300 points - overflow
 - a. There's a flag shop selling stuff, can you buy a flag? Source. Connect with ``nc 2019shell1.picoctf.com 29250``. [Source code download](#)
 - b. Hints

 - c. Write-up
 - i. https://github.com/Dvd848/CTFs/blob/master/2019_picoCTF/flag_shop.md
4. Empire1 - 400 points - web
 - a. Psst, Agent 513, now that you're an employee of Evil Empire Co., try to get their secrets off the company website. <https://2019shell1.picoctf.com/problem/37779/>. Can you first find the secret code they assigned to you?
 - b. Hints


[REDACTED]

c. Write-up

- i. https://github.com/Dvd848/CTFs/blob/master/2019_picoCTF/Empire1.md