

Mason Competitive Cyber

CTFs For Beginners



Proud Sponsors



CACI

EVER VIGILANT



Capture the Flag Competitions



- Usually online
- Jeopardy style
 - Questions worth varying amounts of points
 - Complete tasks to find the answer, called the “flag”
 - Web exploitation
 - Forensics
 - Cryptography
 - Reverse engineering
- Attack/Defense style
 - Option 1: server that everyone tries to control
 - Option 2: protect your own machine, capture other people’s machines

Reverse Engineering

Strcmp 25	memcmp 50	syscall 75	Position Independent 100
hearts 100	malloc 200	fork 400	Nascar Simulator 650

Caffix's Corner (Hard)

fgets all the points 100	turtle sh3lls 100	exploit mitigations 150	turtle sh3lls 2 150
fgets all the points 2 250	fgets all the points 3 350	turtle sh3lls 3 350	turtle sh3lls 4 600

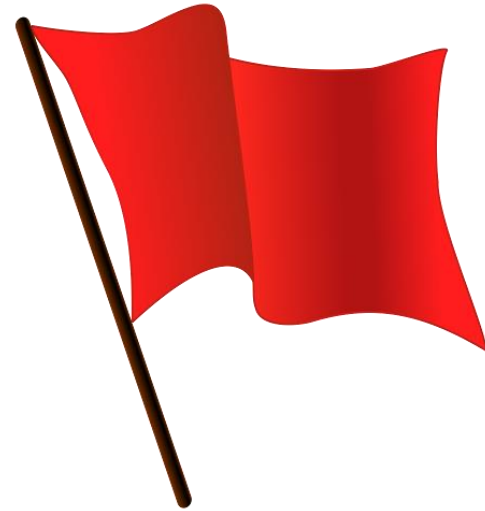
Modern Cryptography

Oracle, but not the TikTok klr 500

What is this Flag thing?



- Normally the solution to the challenge
- Has a specific format unique to the CTF
 - Commonly in the form `flag{The Flag}`
 - For the MasonCC training CTF, format is `masoncc{Flag}`
- Sometimes the flag is already formatted, sometimes it's not
 - You may find a flag in the form `flag{}`
 - Other times flag will need to be put into the flag format
- Example: “What year was the Statue of Liberty Built?”
 - Put you answer in the form `flag{}`
 - In this case, the flag will be the year it was built.
 - `flag{1875}`



Joining Your First CTF



- For Today, we will be joining the MasonCC Training CTF, TCTF
- To get started, go to <https://tctf.competitivecyber.club/> and click on register
 - Choose a Username, password, and Use your @gmu.edu email
 - Choose Wisely, everyone will see it
- After Registering, click challenges
 - Wow, that's a lot of challenges
 - Almost all of them were written by MasonCC Members
 - Contacting the author may help if your stuck

User Name

Your username on the site

Email

Never shown to the public

Password

Password used to log into your account

Submit

Let's Solve a Challenge



- The name of the challenge is “Salad Man”, remember this.
 - Many times, the title and description give you hints
- Let's download the attached file and see what we get.
- File Contents: “synt{Fnynq_zna_vf_orfg_zna}”*
- Not sure where to start? [Google It!](#)
- Alright, so we think it may be a “Caesar Cipher”
- Let's use a website to try and get the flag.
- <https://www.dcode.fr/caesar-cipher>

*example used in slides is different from actual CTF

Challenge


3 Solves

×

Salad Man

50

Remember to submit all flags in the format masoncc{flag}

 encrypted.txt

Flag

Submit

Let's Solve Another One



- This challenge is a Steganography challenge.
 - Steganography is the technique of hiding data in files.
 - Some nice tools to have:
 - Foremost (detects file headers to extract files)
 - Zsteg (Runs an automated set of scripts)
 - strings (looks for strings in the input file)
-
- Let's try running the png through some tools
 - Hey, what's this zip file doing in there?
 - In linux, the unzip command will unzip a file

Challenge


2 Solves

×

Stegosaurus

60

Is there a hidden message in this photo?

 lawandpolicy...

Flag

Submit

Web Challenges



- In web challenges, I like to start by opening the developer tools (F12) and just poking around the site.
- Open the Elements or Sources tab and look at the source html.
 - In HTML, `<!-- Comments Look Like This -->`
- If that yields nothing, try opening the network tab and look at the web requests.
 - You may have to reload the page to see them
 - GET requests are your computer downloading a file from a server
 - POST requests are your computer sending data to a server
 - Pay close attention to the request headers, they often include useful details.

Hidden in Plain Sight



On your own, (or with a friend), try and see if you can solve “Hidden in Plain Sight”

- Use the tips on the last slide, remember, F12 to open the developer panel
- In a couple of minutes, we will solve it as a group.
- Open the Elements tab and look at the source html.
 - In HTML, <!-- Comments Look Like This -->
- If that yields nothing, try opening the network tab and look at the web requests.
 - You may have to reload the page to see them
 - GET requests are your computer downloading a file from a server
 - POST requests are your computer sending data to a server
 - Pay close attention to the request headers, they often include useful details.

Challenge

6 Solves

×

Hidden in Plain Sight

30

<http://sekritskwerl.com:8080/>

Please enter the flag in masoncc{} format

Where to Find CTFs?



- Watch out in the #ctf-watch slack channel for announcements for CTFs
- There are a few long running CTFs that are good practice.
 - PicoCTF is a good beginner oriented CTF
 - Our very own TCTF
 - MicroCorruption-Embedded Security Challenges