RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **SBX3-TIL4**

Offensive Capture the Flag 101 - Guided Beginner CTF

Irvin Lemus
Director of Content Development
Pacific Hackers Association
@infosecirvin

Sandra Stibbards
Owner and President, Camelot Investigations

Rod Soto
President & Co-Founder
Pacific Hackers Association
@rodsoto

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

PACIFIC HACKERS ASSOCIATION

Why Am I here?

- Do you know what CTF stands for?
- Do you want to know what a CTF is?
- Should I be playing CTF games?
- Should my employees be playing CTF games?

What is a CTF?

- Capture The Flag.
- Military Term.
- Test your Knowledge and Abilities.
- Real-life Scenarios.
- Cyber is not Different.
  - Involves computer security challenges.

Types of Challenges

- Web Application Attacks.
- Cryptography.
- Forensics (PCAP Analysis, File Analysis).
- OSINT.
- Malware Reverse Engineering.
- Coding / Scripting / Encoding / Decoding.
- Simple Trivia.

CTF Types

- **Jeopardy Style.**
- Attack & Defend.
- King of the Hill.
- DFIR – Digital Forensics & Incident Response.
- OSITN – Open-Source Intelligence.

Web	Crypto	Forensics	Reverse	Misc	Pwn
1	165	100	50	50	50
150	150	150	100	100	150
204	150	150	150	165	200
203	200	200	200	150	250
206	257	200	300	200	323
318	334	250	300	300	440
325	400	347	400		
	430	350			

Why Does it Matter?

- It is a great environment to learn and develop skills.
- It allows players the possibility to attack and exploit targets otherwise forbidden and unlawful in real life.
- Forces players to cooperate and share knowledge in multi-stage/exploitation challenges.
- Expose professionals in real-life scenarios.
- The skills learned are transferable and likely to improve performance.
- CTF is the BEST training method for people trying to break into the security industry.

Where do I Start?

- This class :)
- Security Conferences (RSA, BSides, BlackHat, DEFCON, Local Meetups).
  - NoQRTR CTF at Dark Arts Village (Sandbox) - https://www.noqrtrctf.com/
  - Pacific Hackers Meetup - https://www.meetup.com/pacifichackers/
- CFT Time - https://ctftime.org/
- Create your Own.
  - https://ctfd.io/
  - https://tryhackme.com/
  - https://www.hackthebox.com/

PACIFIC HACKERS ASSOCIATION

What should I Bring?

- A computer loaded with Security Tools. (Not Corporate or Personal).
- Willingness to Learn.
- Patience and Tolerance to Frustration.
- Open Mind.
- Friends for Support.
  - Even better, a Team.

CTF Tools

- Live Linux Distributions (Kali, Parrot, Security Onion, etc.)
- Virtualization Software.
  - VMWare.
  - VirtualBox.
- Windows with Linux Subsystem Installed.
- Online Resources.
  - CyberChef - https://gchq.github.io/CyberChef/
  - CTF Walkthroughs.

PACIFIC HACKERS ASSOCIATION

Tips for Success

- Do not get FRUSTRATED or QUIT.
- Choose an area where you have strengths or skills that will allow you to get into the competition quickly.
- Pick a Team with Diverse Background.
  - Network administration, malware analysis, developer/coder, forensics.
  - Know your team's strengths.
- Communication is the Key.
  - Slack/Discord.
- Patience and Tolerance.
- Write Notes and Save Resources.
- **There is NO Cheating in Hacking**.

PACIFIC HACKERS ASSOCIATION

Summary

- Play as many CTFs as you can.
- Attend Conferences and Hacker meetups.
- Join or Create a Team.
- Develop your skills in that which you enjoy when it comes to hacking.
- Join us at the DarkArts.io Sandbox at RSA Conference 2022; there are several CTFs you can play.

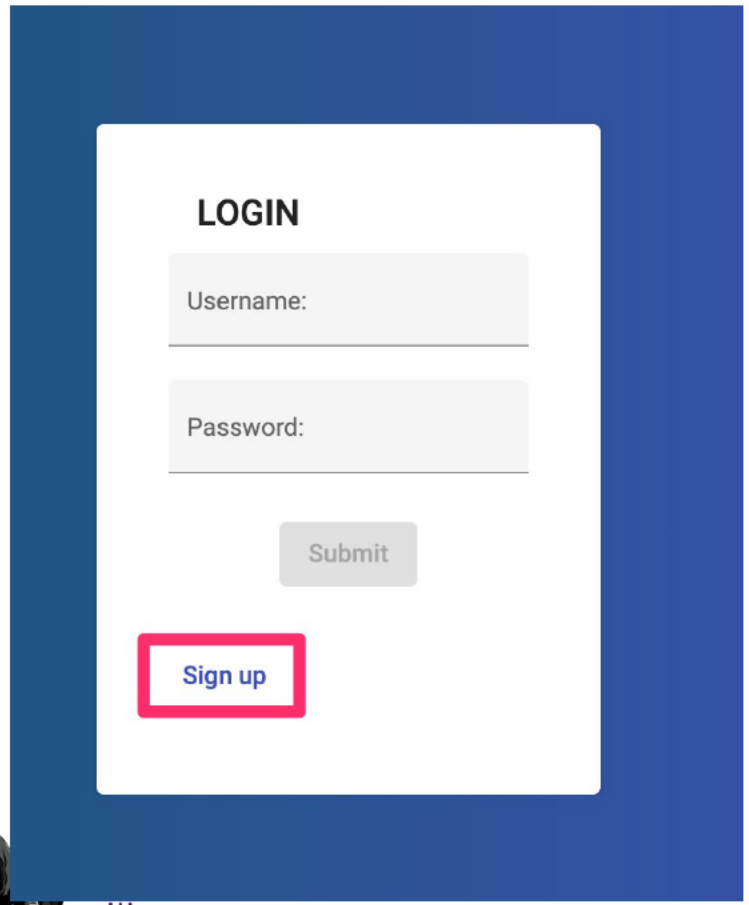
RSAConference2022

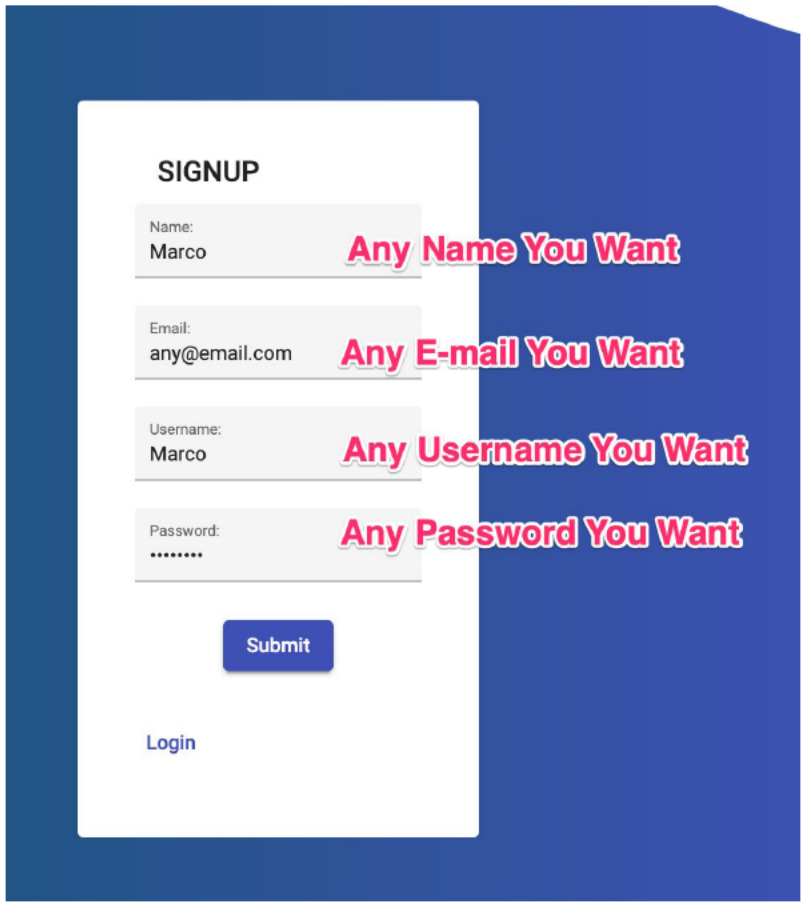
CTF Walkthrough.

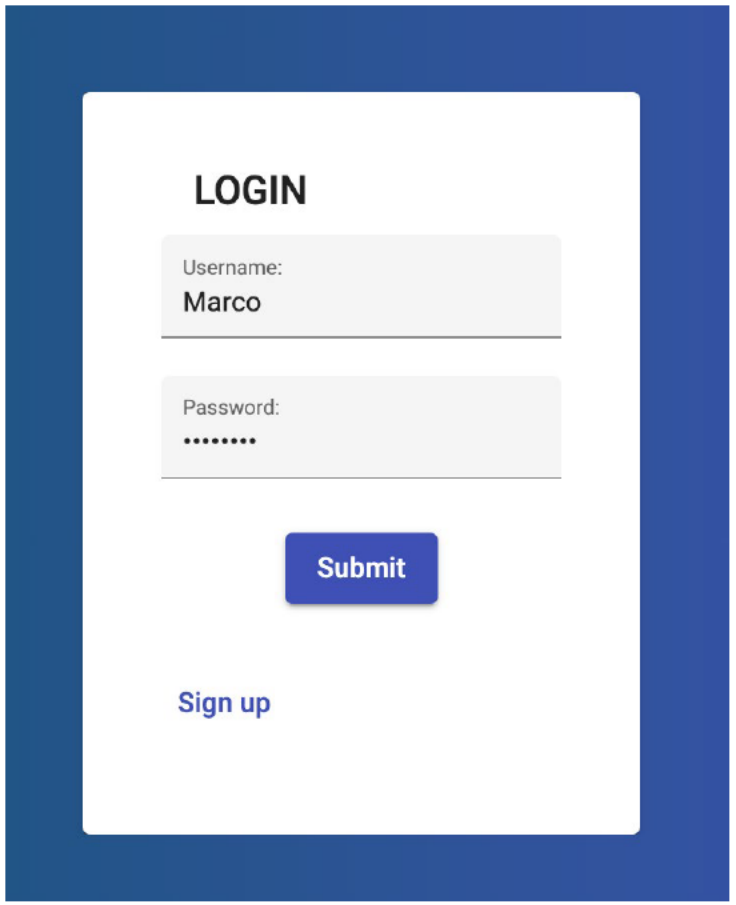
Let The CTF Begin.

Access The CTF

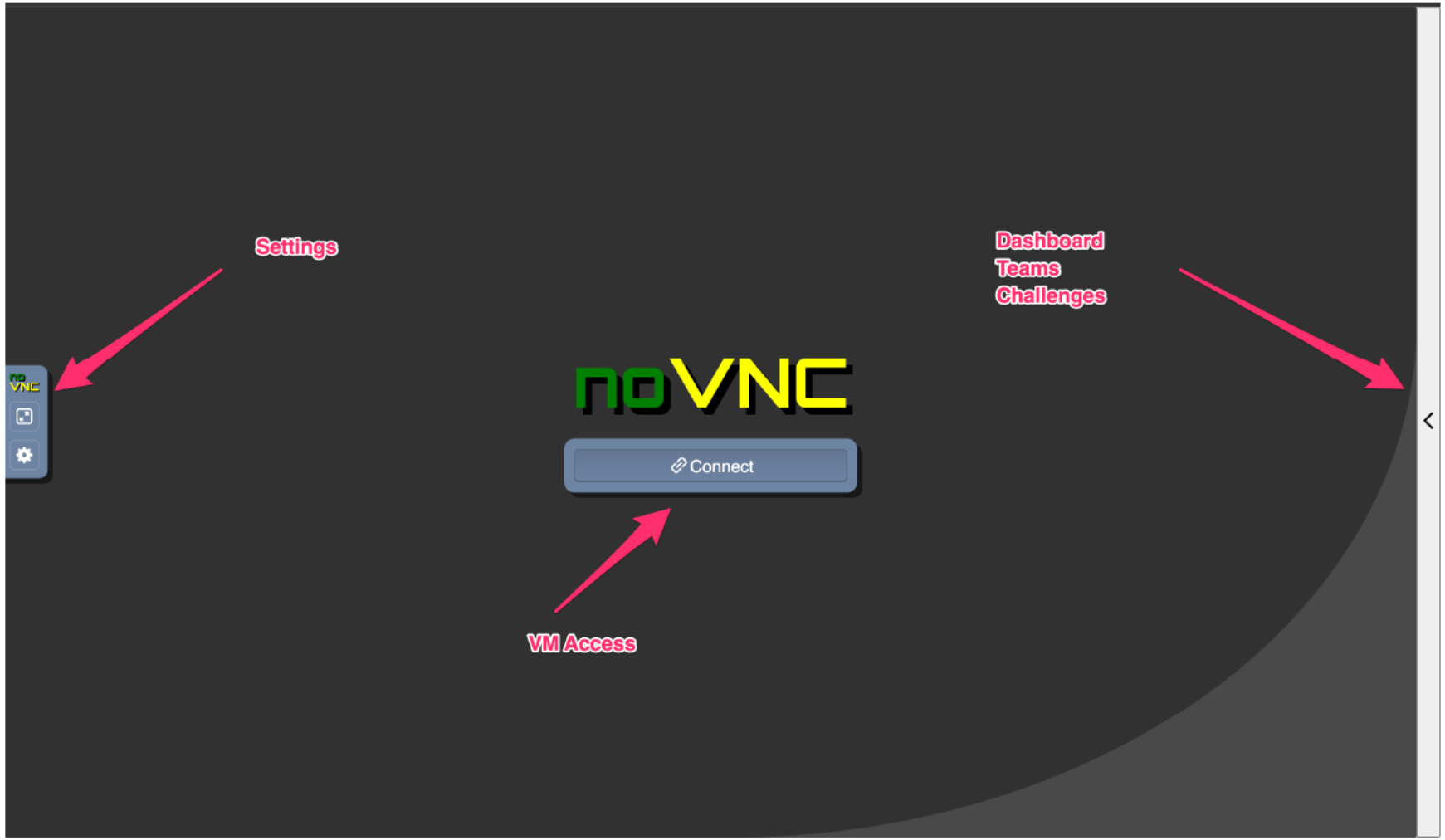
- https://rsa.baycyber.net/



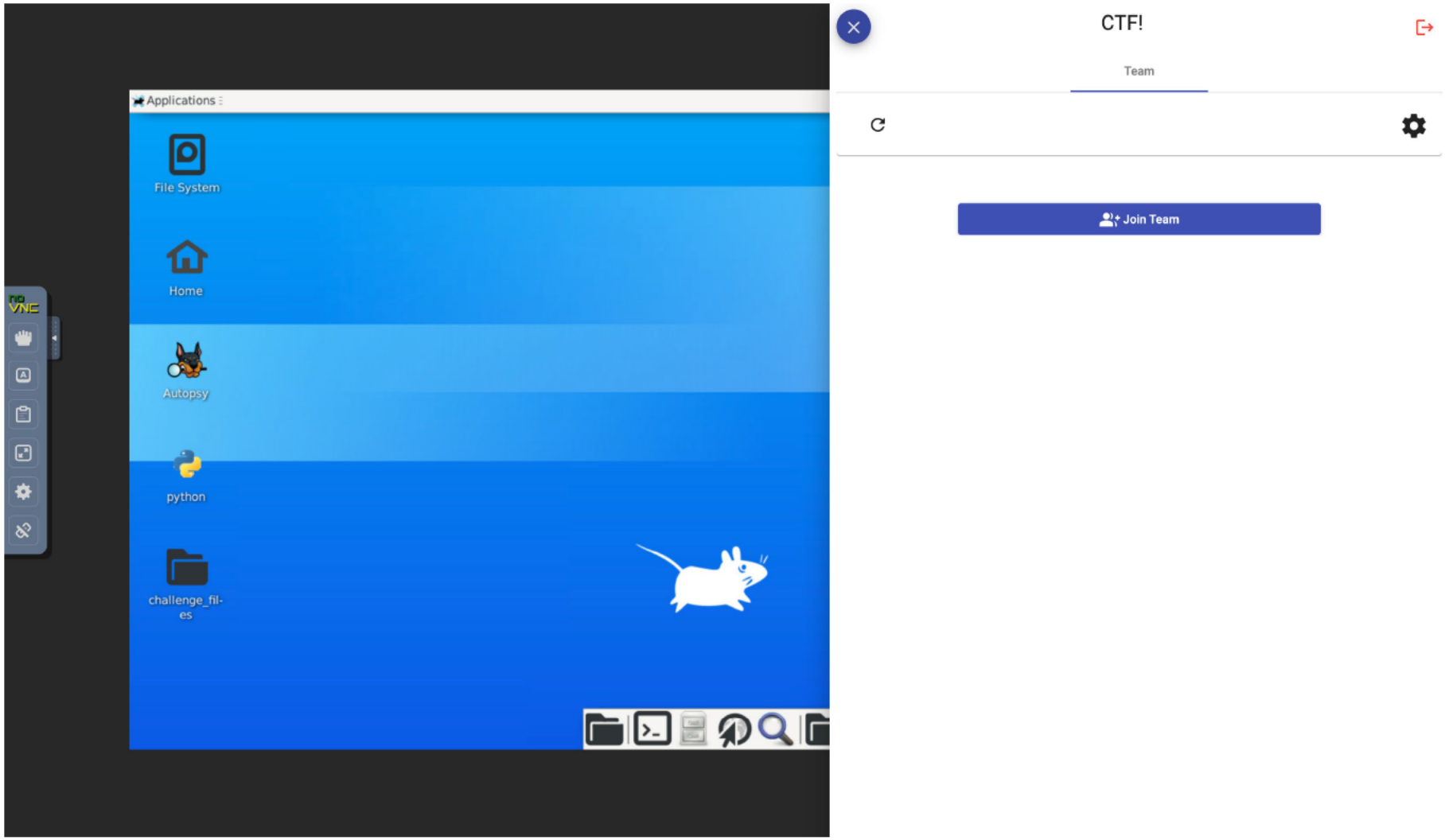




The Environment (1)



The Environment (2)



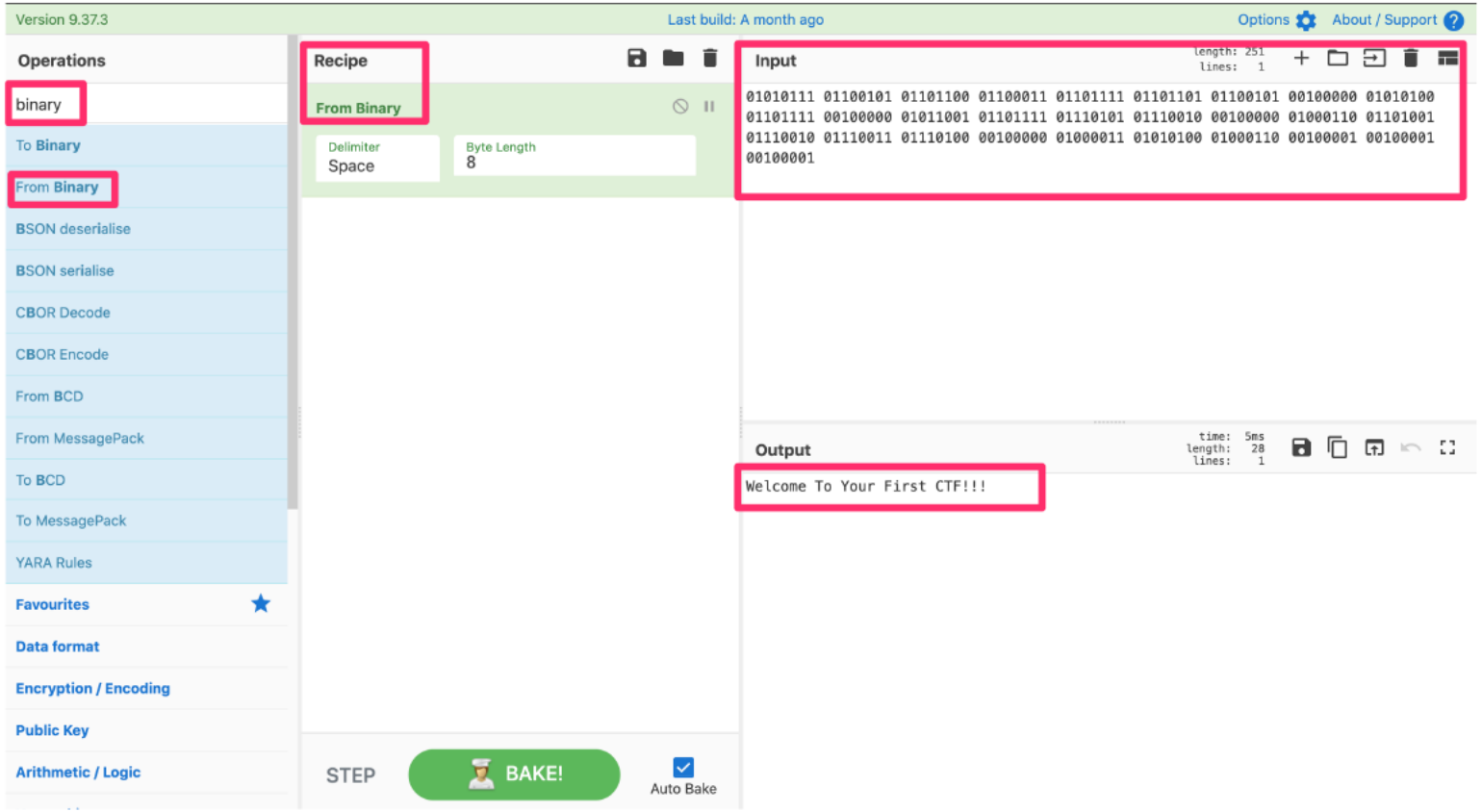
Challenges

- Cryptography
- OSINT
- Network Analysis
- Threat Intel & Malware Analysis
- WebApp & SQLi Attacks

Cryptography

- All Questions can be answer by Using **CyberChef**

https://gchq.github.io/CyberChef/

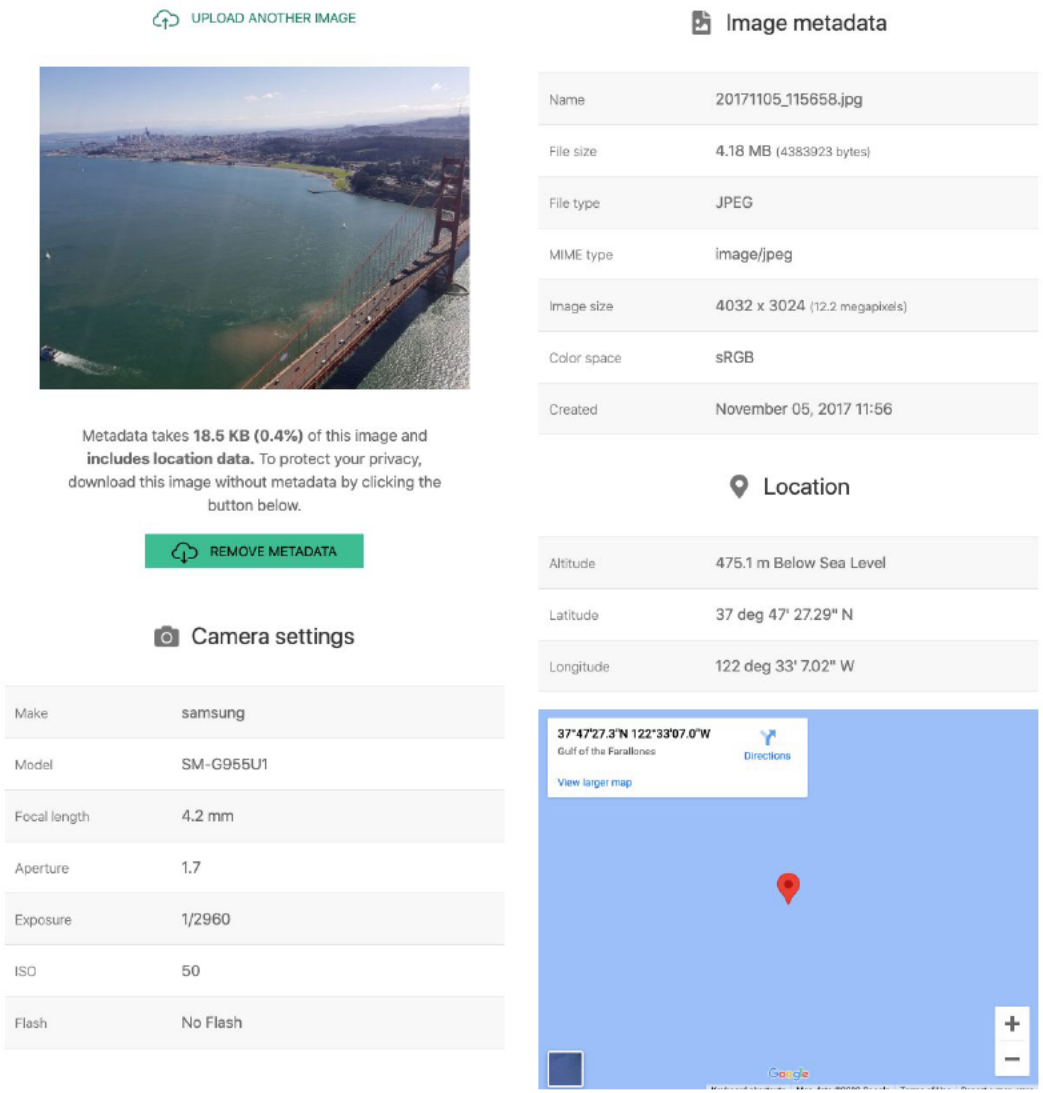


OSINT (1)

- Use file “20171105_115658.jpg” to answer the OSINT Challenges.
- Hint: https://jimpl.com/

OSINT (2)

- A1) 2017:11:05 11:56:58 UTC
- A2) 4032x3024
- A3) samsung
- A4) SM-G955U1
- A5) 37.7909, -122.5519



References

- https://www.csoonline.com/article/3341318/top-tools-and-resources-for-running-a-capture-the-flag-competition.html
- https://www.csoonline.com/article/3257659/10-questions-to-answer-before-running-a-capture-the-flag-ctf-contest.html
- https://zaratec.github.io/ctf-practice/
- https://ctfd.io/
- https://ctftime.org/
- https://www.meetup.com/pacifichackers/
- https://www.hackthebox.com/
- https://tryhackme.com/
- https://www.noqrtrctf.com/

PACIFIC HACKERS ASSOCIATION