

CS177

Stack buffer overflow

whoami

- @publicqi
- CTF player @Shellphish @W&M @Straw_Hat
- Binary exploitation {User | Kernel} land
- Beginner level of other categories {IOT | Web | ...}
- Playing CTFs since Nov 2019


Binary exploitation

- What does it do?
 - Jailbreak/root your phone
 - Take control of a remote server
 - Make yourself root on csil machines
 - Escape from a virtual machine
 - Own someone's phone with a message
 - Own someone's PC if they clicked into your website
 - ...

Tools recommended

- pwndbg – an awesome gdb plugin
- pwntools – a python library that wraps lots of functions
- Ghidra – Free open source reverse engineering tool

Resources recommended

- Youtube @liveoverflow: Binary exploitation series
- pwn.college by ASU: <https://pwn.college/>
- CTF-wiki: <https://ctf-wiki.mahaloz.re/>
- CTFtime: <https://ctftime.org/> 
- BUUOJ: <https://buuoj.cn>