

WiCyS 2023



#role-join WiCyS
#signin wicys



ROCHESTER INSTITUTE OF TECHNOLOGY
STUDENT CHAPTER

Follow Our Socials



@Wicysrit



Fill out our highlight form!



@WiCySRIT

https://docs.google.com/forms/d/e/1FAIpQLSfpTbloIAIASQNOoyIAor2_8mE4KPzLthHvtVMzJLNMoFkt7A/viewform?usp=sf_link

Wicys Conference

Conference Dates: **April 11-13 2024**
Location: Gaylord Opryland Resort in
Nashville, Tennessee

Applications Open: **September 11**
Applications Close: **November 6**
Notification of Status: **December 18**



Intro To CTF

What is a CTF?

A Capture The Flag (CTF) competition is where participants solve challenges to find hidden flags.

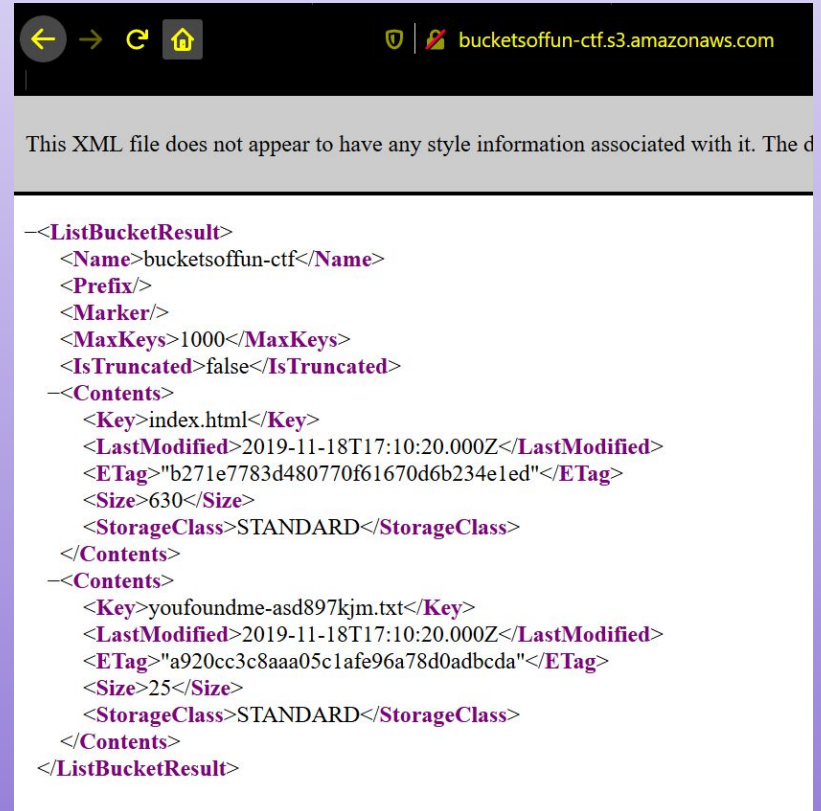


Categories

crypto forensics
web reversing
pwn networking
osint misc

Web Category

The “Web” category has participated identify and exploit vulnerabilities in websites to find those hidden challenges.



```
← → ↻ 🏠 bucketsoffun-ctf.s3.amazonaws.com

This XML file does not appear to have any style information associated with it. The d

<!--ListBucketResult-->
  <Name>bucketsoffun-ctf</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>>false</IsTruncated>
  <!--Contents-->
    <Key>index.html</Key>
    <LastModified>2019-11-18T17:10:20.000Z</LastModified>
    <ETag>"b271e7783d480770f61670d6b234e1ed"</ETag>
    <Size>630</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <!--Contents-->
    <Key>youfoundme-asd897kjm.txt</Key>
    <LastModified>2019-11-18T17:10:20.000Z</LastModified>
    <ETag>"a920cc3c8aaa05c1afe96a78d0adbcd"</ETag>
    <Size>25</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>
```

Crypto Category

The “Crypto” category has participants decipher encoded messages to find those hidden flags.

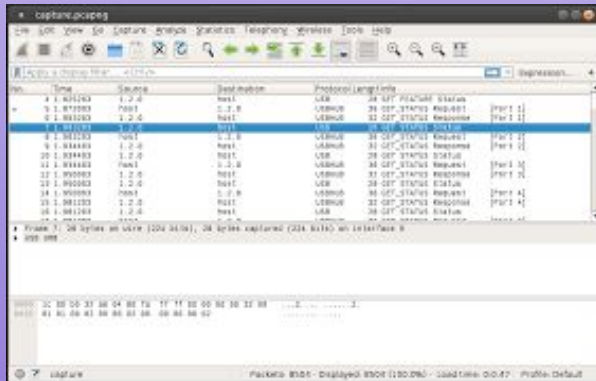
```
Plain text: aa
```

```
Encrypted output:
```

```
48 27 47 36 81 22 21 34
```


Forensics Category

The “Forensics” category has participants analyze information from computer files, memory dumps, or network traffic to find those hidden flags.



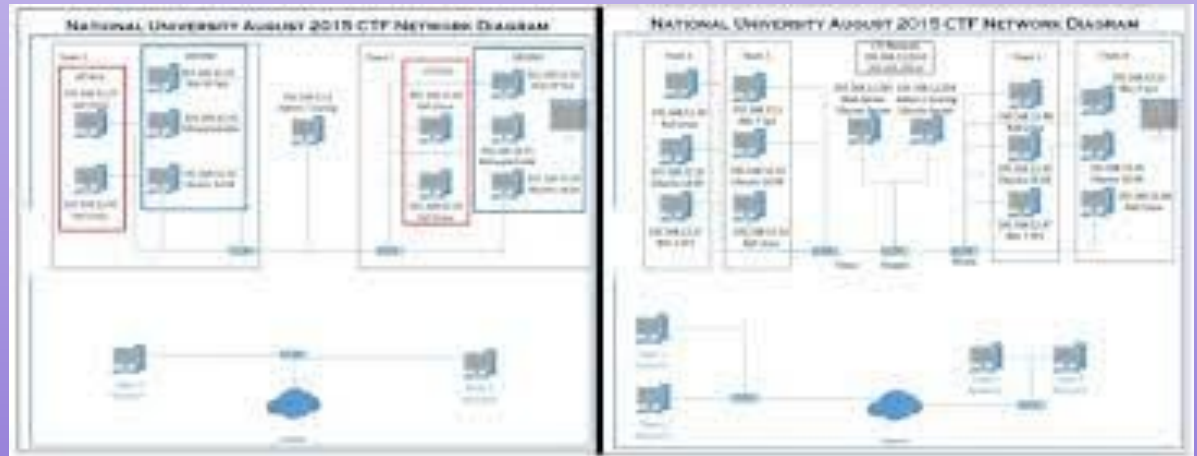
Reversing Category

The “Reversing” category has participants dissecting and decoding programs or binaries to find those hidden flags.



Networking Category

The “Networking” category has participants analyze, manipulate, and exploit network communication to find those hidden flags.



OSINT Category

The “OSINT” category has participants gather public information to solve challenges and get those hidden flags.



15.8K 95.9K 477.6K

Sergio Quintana ✓
@svjournalist

Replying to @JackMa and @iwriterealgood

Where are these supplies headed in the US?
I'm a reporter in San Francisco.
If they're headed here, I'd love to see the flights land if possible.

10:27 PM · Mar 15, 2020 from San Francisco, CA · Twitter for iPhone

PWN Category

The “PWN” category has participants exploit vulnerabilities in binary software to gain unauthorized access and find those hidden flags.

```
root@kali:~# file Baby
Baby: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically link
ed, interpreter /lib/ld-linux.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=a71c01623
6eb290c36be6e6fa1c8c525b296996f, not stripped
root@kali:~# checksec Baby
[*] '/root/Baby'
Arch:      i386-32-little
RELRO:     Partial RELRO
Stack:     No canary found
NX:        NX disabled
PIE:       No PIE (0x8048000)
RWX:       Has RWX segments
root@kali:~#
```



MISC Category

The “MISC” category has participates solve challenges that do not fit in other categories. This category tests a wide range of problem-solving skills.

```

--(Register Overview)---
EAX=00000012  ESI=00000181  DS=01DD  ES=01DD  FS=0000  GS=0000  SS=01DD  Real
EBX=000001A0  EDI=0000016F  CS=01DD  EIP=00000134  C0 Z1 S0 00 A0 P1 D0 I1 T0
ECX=00000000  EBP=00005A65
EDX=00008470  ESP=0000FFFC                                5233334

--(Data Overview  Scroll: page up/down)---
01DD:012F  31 2D 46 47 49 75 F5 5A 68 48 49 58 25 41 29 CD  1-FGiU.ZhHIX%A)
01DD:013F  21 68 53 4C 58 34 53 CD 21 43 54 46 7B 67 30 30  !hSLX45.!(CTF{g00
01DD:014F  64 6F 31 64 44 4F 53 2D 46 54 57 70 0D 0D 0D 0D  do1d05-FTW)...
01DD:015F  0E 49 49 34 7F 5C 0D 70 35 48 12 57 3D 0E 0D 29  .II4.\.p5K.W=.
01DD:016F  16 50 5B 2D 60 7C 30 67 76 50 59 30 6F 6E 51 30  .P[.|@gvPY0on00
01DD:017F  67 65 5A 30 77 59 35 3E 44 30 67 5D 68 28 28 58  geZ0wY5>00g]h+(X
01DD:018F  2D 6B 26 34 60 50 5B 30 2F 2C 36 34 22 50 34 41  -k&4"P[0/,64"P4A
01DD:019F  50 C3 0D 54 68 65 20 46 6F 6F 62 61 6E 69 7A 65  P..The Foobanize

--(Code Overview  Scroll: up/down)---
01DD:012F  312D      xor [di],bp      ss:[016F]=5016
01DD:0131  46      inc si
01DD:0132  47      inc di
01DD:0133  49      dec cx
01DD:0134  75F5    jne 0000012B($-b)  (no jmp)
01DD:0136  5A      pop dx

```

```

root@zion:/home/neo# file spurious
spurious: data
root@zion:/home/neo# xxd spurious | head -4
00000000: 7f45 4c4c 0201 0100 0000 0000 0000 0000  .ELL.....
00000010: 0300 3e00 0100 0000 f005 0000 0000 0000  ..>.....
00000020: 4000 0000 0000 0000 9819 0000 0000 0000  @.....
00000030: 0000 0000 4000 3800 0900 4000 1d00 1c00  ....@.8...@....
root@zion:/home/neo# echo "00000000: 7f45 4c46" | xxd -r - spurious
root@zion:/home/neo# file spurious
spurious: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dyn
terpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sh
d7b90483089cfe61ed03f3066, not stripped
root@zion:/home/neo# ./spurious
Your flag: g7qqta0UkjwJ1tbcN6Dwl6ej

```

```

root@zion:/home/neo# file spurious.zip
spurious.zip: Zip archive data, at least v2.0 to extract
root@zion:/home/neo# unzip -l spurious.zip
Archive:  spurious.zip
  Length      Date    Time    Name
-----
 8409      2020-05-18  22:05    spurious
-----
 8409
 1 file
root@zion:/home/neo# unzip spurious.zip
Archive:  spurious.zip
[spurious.zip] spurious password:
password incorrect--reenter:
skipping: spurious_      incorrect password

```


Join our CTF



Demo Time

ctf-demo.wicysrit.org

WiCyS CTFd

ctf.wicysrit.org