

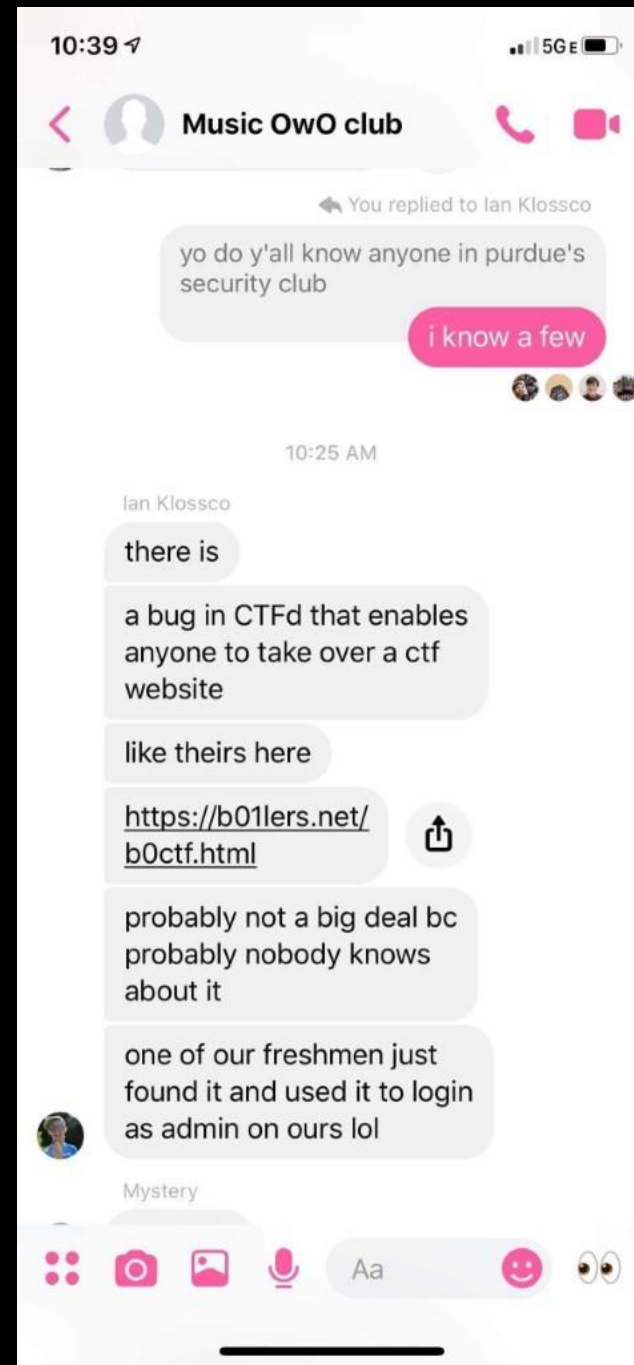


b01lers & SIGPwny



# YOU HACKED US

- We weren't even vulnerable...



# There was permission...

We did set it up for the demo, but you did still hack us...



hey hey! i'm from uiuc's security club

Hey Austin told me you were gonna message

You can now call each other and see information like Active Status and when you've read messages.



we were thinking up of things to demo for our first meeting and though that teasing the purdue/uiuc rivalry might have good entertainment value

We're talking rn in our officers chat about spinning back up a vulnerable instance of ctf

4:49 PM **ian5v** yes

**ian5v** it was noticeably smaller the second of the two times i went

**ian5v** hackathons are largely good for free food and to learn a new skill

**ian5v** or if you have a specific project idea in mind

5:19 PM **Jesse** but it's also Purdue 🤢

5:20 PM **Husincostan** Purdue is actually pretty nice tho ngl

**Husincostan** But it's also Purdue

sigpwny

# general

General discussion about SigPwny and its activities.

October 27, 2018

# welcome

# announcements

TEXT CHANNELS

# general



# random

# hangouts

# i-made-a-thing

# ask-for-help-here

# learning-resources

# pwny-ctf

# seminar

VOICE CHANNELS

General

3:43 PM **ian5v** yo.... let's go win purdue's CTF

**ian5v** <https://boilerctf.com/>

3:43 PM **Pranav** fuck purdue

3:43 PM **ian5v** looks like it's internal

**ian5v** you gotta play solo tho

**ian5v** no rules against external agents tho

**ian5v** don't use a name that ties back to uiuc

**ian5v** @Evan @seb

**ian5v** HECK it's constrained to purdue.edu

3:54 PM **Jesse** i have a purdue.edu

3:55 PM **ian5v** yooooo

3:55 PM **Jesse** wait nvm

**Jesse** it got deleted lmfao

3:55 PM **ian5v** lol

3:57 PM **Jesse** i can try to get one though

**Jesse** got some friends

3:58 PM **ian5v** oh i wonder if

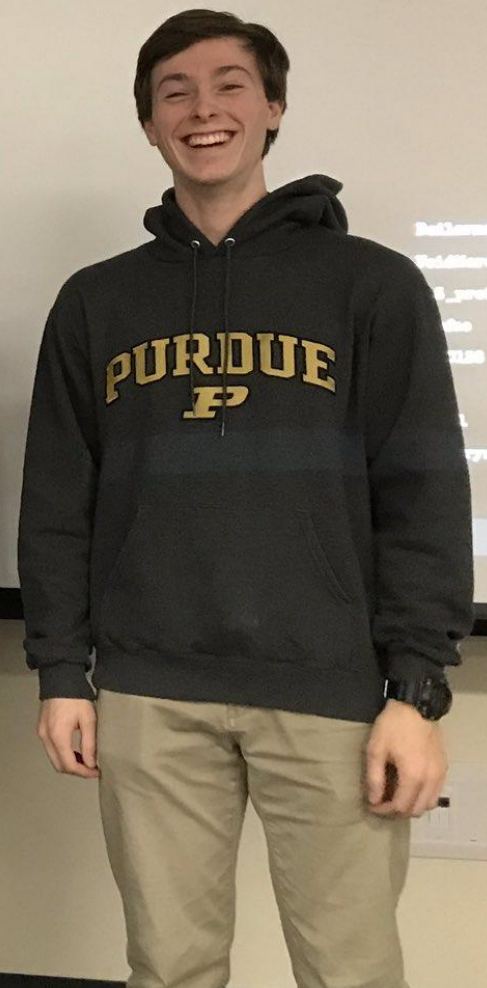
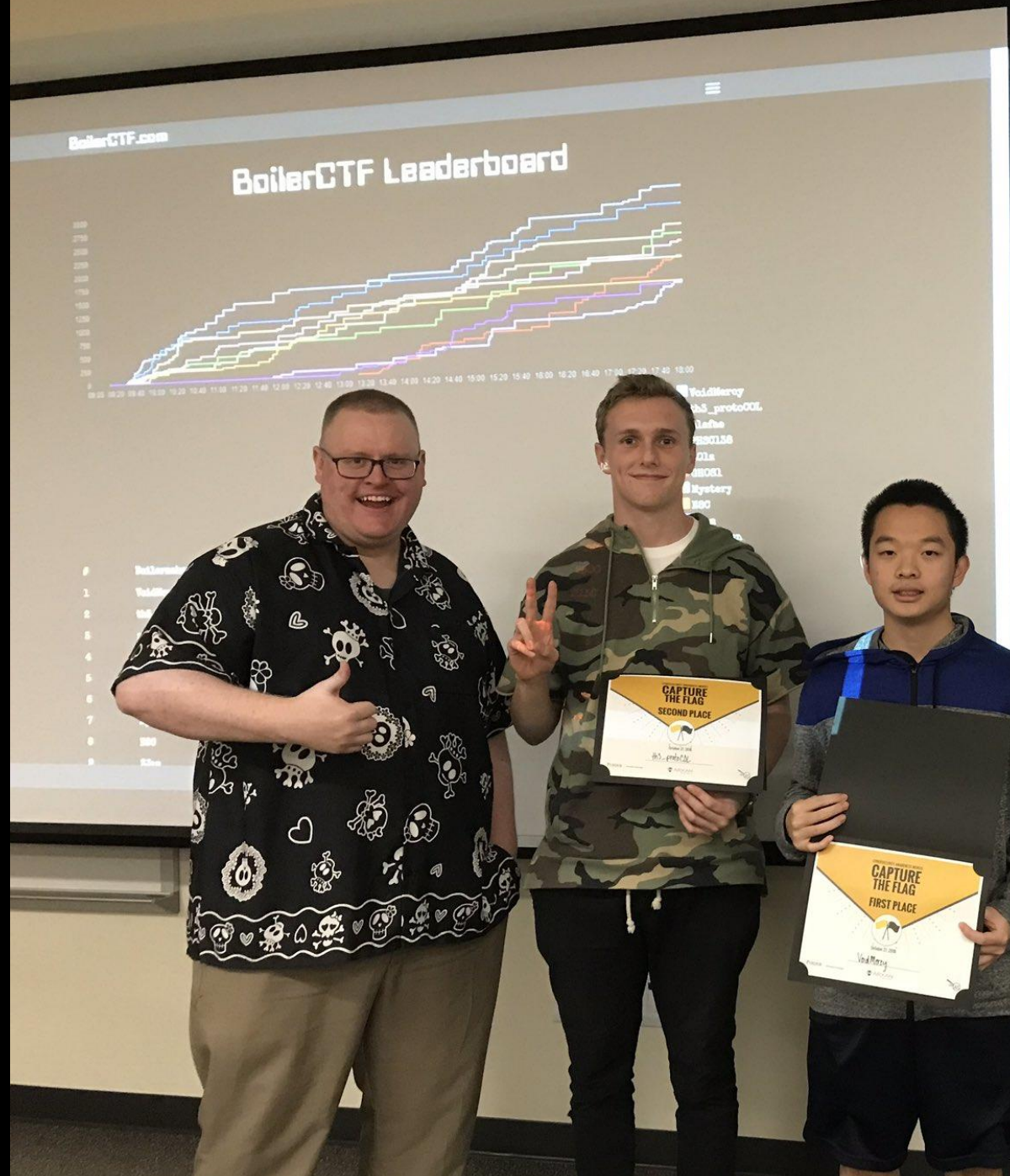
**ian5v** it's client side checking

3:58 PM **Jesse** wait

**Jesse** LOL

**Jesse** NO VERIFICATION NEEDED

3:59 PM **ian5v** OH lmao



A cartoon illustration of Bugs Bunny from Looney Tunes. He is standing in the center, wearing a long, flowing brown cape with orange and grey trim around the neck. He has a serious, determined expression with his eyes narrowed. The background is a light blue sky with a few dark green trees at the bottom. The text "OF COURSE YOU KNOW THIS MEANS WAR!" is overlaid at the bottom in a bold, white, sans-serif font with a black outline.

**OF COURSE YOU KNOW THIS MEANS WAR!**





# How to assert dominance

And how to protect yourselves from hackers

# Part #1: The Plan

# #pwny-ctf

The screenshot shows a Discord server interface for the server named "sigpwny". The left sidebar lists channels under "TEXT CHANNELS" and "VOICE CHANNELS". The "pwny-ctf" channel is selected and highlighted. The main window displays the message history for this channel, showing several bot announcements from "CTFd".

**Channel List:**

- TEXT CHANNELS
  - # welcome
  - # announcements
  - # general
  - # random
  - # hangouts
  - # i-made-a-thing
  - # ask-for-help-here
  - # learning-resources
  - # pwny-ctf
  - # seminar
- VOICE CHANNELS
  - General

**Message History:**

- 10:23 AM:** BOT CTFd: Xavier solved SIGPwny Discord (50) (Last Wednesday at 10:23 AM)
- 10:08 PM:** BOT CTFd: skagawa solved Welcome to SIGPwny! (50) (Last Wednesday at 10:08 PM)
- 10:36 PM:** BOT CTFd: yiE solved Inspect Me (0) (Last Wednesday at 10:36 PM)
- January 23, 2020**
- 11:54 AM:** BOT CTFd: skagawa solved Inspect Me (0) (Last Thursday at 11:54 AM)
- 11:56 AM:** BOT CTFd: skagawa solved How to Save and Exit Vim? (50) (Last Thursday at 11:56 AM)
- 12:00 PM:** BOT CTFd: skagawa solved B/A 1: Source (20) (Last Thursday at 12:00 PM)
- January 24, 2020**

# The Idea

- Jump into first place on SIGPwny's internal CTF at once
- The catch: only '[@illinois.edu](mailto:illinois.edu)' emails can register


## Register

Only email addresses under illinois.edu may register ×

Don't use important passwords! People may try to hack this site \*wink\*.

User Name

Email

Password

# Logging In

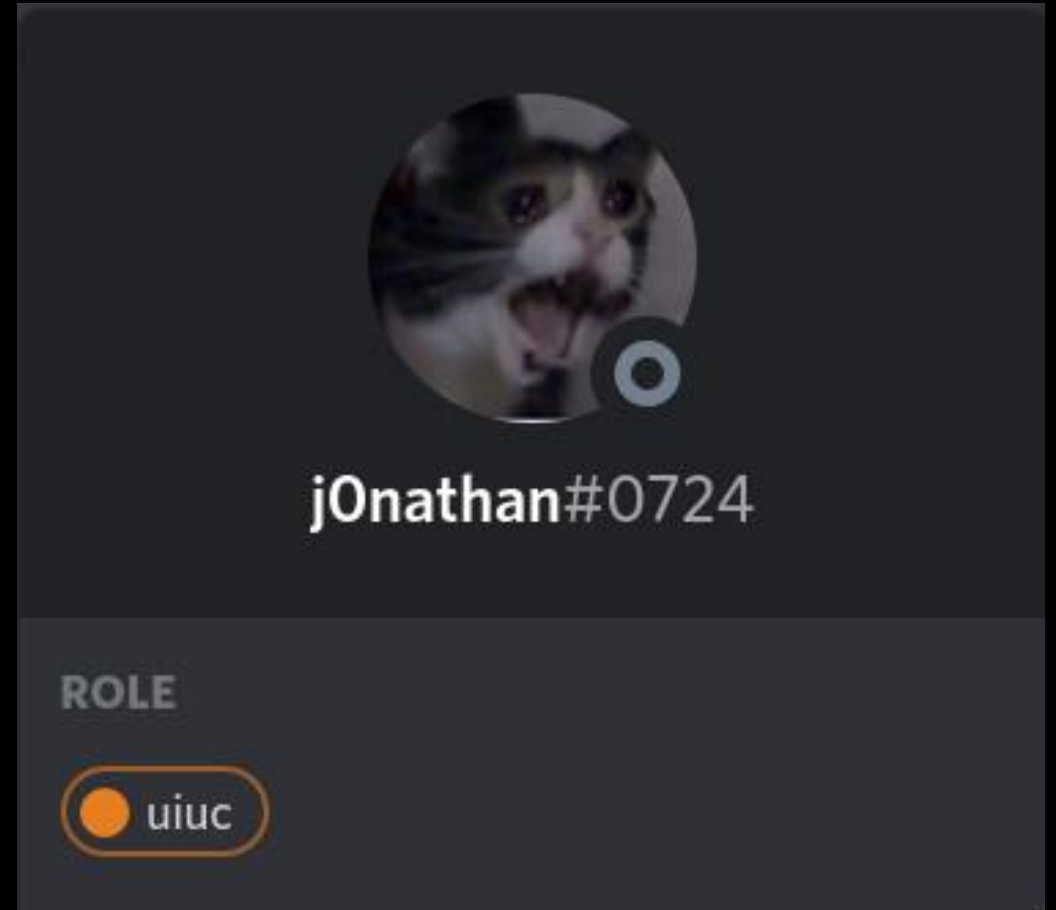
- Inspired by a critical Google vulnerability: <https://medium.com/bugbountywriteup/how-i-broke-into-google-issue-tracker-667b9e33e931>
- We acquired an '@illinois.edu' email and created our account - 'jonathan'.

# Part #2: Enter Jonathan

# j0nathan

Some challenges required a Discord account/talking to an admin

Trapezoid.asm - 5000pt chal that we needed to solve, the files were in a private channel.



A screenshot of a Discord user profile for the user j0nathan#0724. The profile features a circular avatar of a cat with its mouth open, a small grey circle with a white dot next to it, and the text 'j0nathan#0724' below the avatar. Underneath the name, the word 'ROLE' is displayed in a light grey font. Below 'ROLE', there is a single role named 'uiuc', which is represented by an orange circle and the text 'uiuc' inside a rounded rectangular button.

## OpSec

Password Manager 50	Venmo 50	Enable 2FA 50	Safe Browsing 50
Cleanup 50	Find Something Embarrassing 100	SMS 100	Meeting Flag 200

So... about opsec.



# Challenge Solutions

File: /home/novafacing/Downloads/sol\_soc\_3.py

```
1 import requests
2
3 my_discord_snowflake_id = "473743276248399873" #insert your ID
4 webhook_url = "https://discordapp.com/api/webhooks/568263559817986059/4TuyweDapREC3QNuZptFf-gHDA24ek8RLi4lF5S1ZsBoLbs0l1Zr2oHhbkqTZ6mY7oA1" #from challenge description
5
6 requests.post(webhook_url, data='{"content": "<@' + my_discord_snowflake_id + '>',"username": "kuilin"}', headers={"Content-Type": "application/json"})
```

# Juicy Gossip!



**ian5v** 09/01/2019

for a super small org like sigpwny used to be (*cough* because the culture wasn't friendly so people didn't stay *cough*)  
idk if it was super effective i didn't really have a good read  
mostly ppl didn't do stuff so meeting quality was poor  
i've also seen a 10 person board for a ~150 person club  
which worked pretty effectively



**Husincostan** 09/01/2019

From what I've seen in my time here, exec board for sigpwny seems to make more sense  
Most of the decisions we've made are kinda made together instead of being decided by one person  
Having an exec board is also probably nice to avoid situation where we have one head with certain bias (like overly aggressive to acm or whatever)

# Social Engineering Prevention (?)



Aaron 09/01/2019

Are we validating UIUC students in any way? We should ask them to send us an email from their UIUC email

I just think the inevitable "I SE'd myself into SigPwny's restricted chat" is probably not good, no matter how unimportant that is in terms of content revealed

Moved this from [#general](#)

[@Josh](#)

# Fundraising Discussion!



**Josh** 08/28/2019

Does the sigpwny name have enough weight for this to be appealing to companies? I mean I have no experience in this kind of thing, but we aren't exactly huge



**ian5v** 08/28/2019

i think the whole idea of a resume book stinks a little



**Pranav** 08/28/2019

I really does



**Thomas** 08/28/2019

it should be open to all takers



**ian5v** 08/28/2019

but

the model of "suck corporate dick for money" sucks. (note: "sucking dick" is a shitty phrase) (edited)



**Thomas** 08/28/2019

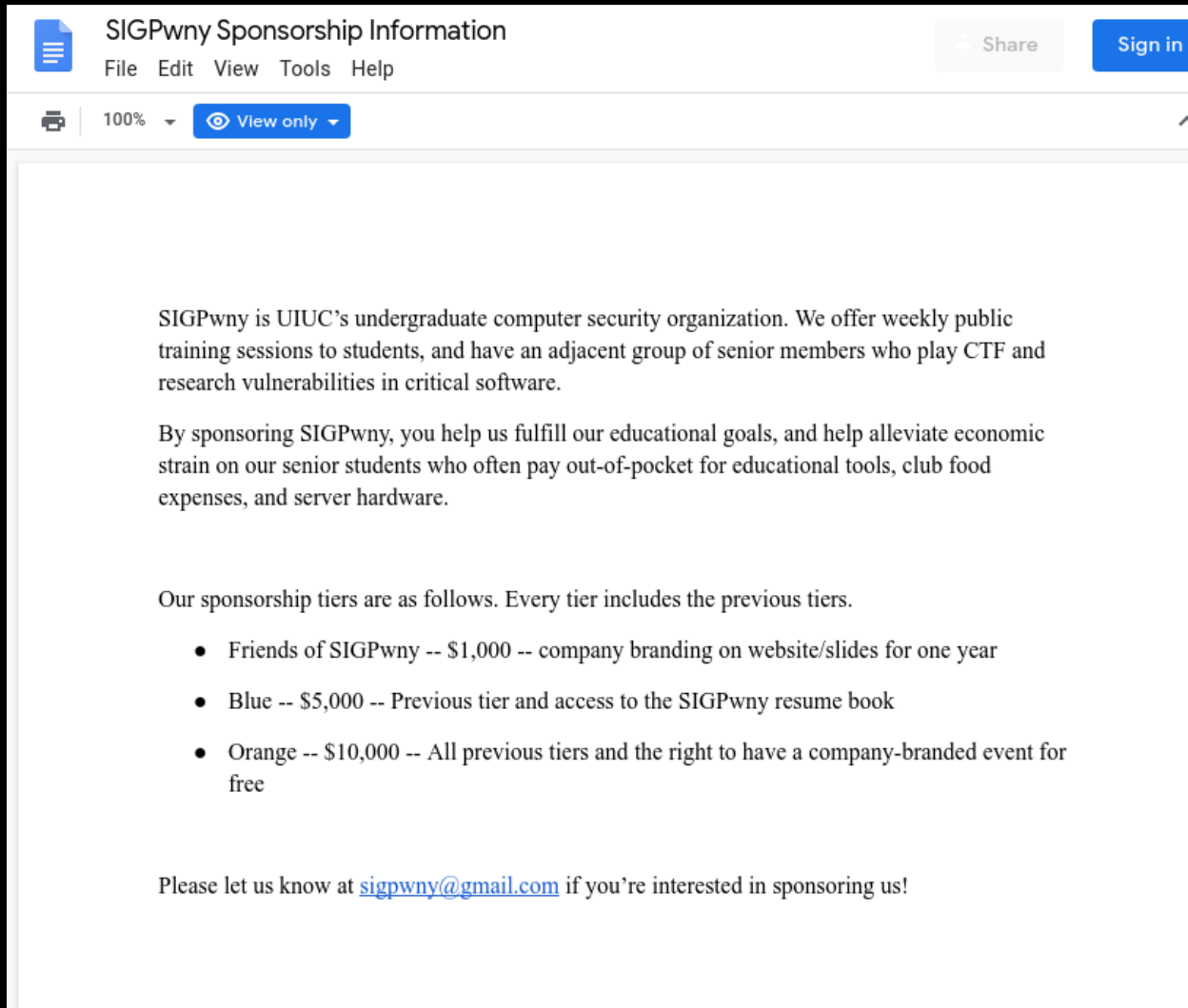
true



**ian5v** 08/28/2019

there should be budgets for school clubs.  
if schools got as much funding as corporations made....

# Fundraising Documents!



The image shows a screenshot of a Google Docs document titled "SIGPwny Sponsorship Information". The document is in "View only" mode and is displayed at 100% zoom. The content of the document is as follows:

SIGPwny is UIUC's undergraduate computer security organization. We offer weekly public training sessions to students, and have an adjacent group of senior members who play CTF and research vulnerabilities in critical software.

By sponsoring SIGPwny, you help us fulfill our educational goals, and help alleviate economic strain on our senior students who often pay out-of-pocket for educational tools, club food expenses, and server hardware.

Our sponsorship tiers are as follows. Every tier includes the previous tiers.

- Friends of SIGPwny -- \$1,000 -- company branding on website/slides for one year
- Blue -- \$5,000 -- Previous tier and access to the SIGPwny resume book
- Orange -- \$10,000 -- All previous tiers and the right to have a company-branded event for free

Please let us know at [sigpwny@gmail.com](mailto:sigpwny@gmail.com) if you're interested in sponsoring us!

# Fixing OpSec

- Verify people in person
- Multiple layers of security
- Share Google documents with specific users/groups
- Careful with sharing challenge solutions – DM or decide if its okay being public

# Part #3: Easy Money

# Free Solves: PicoCTF

- PicoCTF writeups are available
- <https://github.com/0e85dc6eaf/CTF-Writeups/tree/master/PicoCTF%202018>


Inspect Me	Pwny BigO	0	picoCTF{ur_4_rea
What's My Name?	Pwny BigO	1	picoCTF{w4lt3r_w
Forensics Warmup 2	Pwny BigO	2	picoCTF{extensio
General Warmup 2	Pwny BigO	3	picoCTF{11011}
strings	Pwny BigO	4	picoCTF{sTrIngS_
Crypto warmup 2	Pwny BigO	5	picoCTF{this_is_
The vault	Pwny BigO	6	picoCTF{w3lc0m3_
logon	Pwny BigO	7	picoCTF{l0g1ns_a
buttons	Pwny BigO	8	picoCTF{button_b
Here's johnny	Pwny BigO	9	picoCTF{J0hn_1\$_
reversing warmup 2	Pwny BigO	10	picoCTF{th4t_w4s
grep 1	Pwny BigO	11	picoCTF{grep_and
forensics warmup 1	Pwny BigO	12	picoCTF{welcome_
general warmup 1	Pwny BigO	13	picoCTF{A}
net cat	Pwny BigO	14	picoCTF{NETcat_i
rsa-madlibs	Pwny BigO	15	picoCTF{d0_u_kn0



# Free Solves: Over the Wire

- Natas & Bandit Over the Wire flags available
- <https://github.com/axiomiety/otw/blob/master/natas.passwords>
- <https://github.com/axiomiety/otw/blob/master/bandit.passwords>

Branch: master ▾ otw / bandit.passwords

 axiomiety password updates

1 contributor

24 lines (24 sloc) | 999 Bytes

```
1 bandit1:boJ9jbbUNNfktD7800psq0ltutMc3MY1
2 bandit2:CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
3 bandit3:UmHadQclWmgdLOKQ3YNgjWxGoRMB5luK
4 bandit4:pIwrPrtpN36QITSp3EQaw936yaFoFgAB
5 bandit5:koReB0KuIDDepwhWk7jZC0RTdopnAYKh
6 bandit6:DXjZPULLxYr17uwoI01bNLQbtFemEgo7
7 bandit7:HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
8 bandit8:cvX2JJJa4CFALtqS87jk27qwqGhBM9pLV
9 bandit9:UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhr
10 bandit10:truKldjsbJ5g7yyJ2X2R0o3a5HQJFuLk
11 bandit11:IFukwKGSFW8M0q3IRFqrxE1hxTNEbUPR
12 bandit12:5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
13 bandit13:8ZjyCRiBWFYkneahHwxCV3wb2a10RpYL
14 bandit14:4yoYUJ5y0k0YlSh1DzateTPHiqyU3b2e
```

# Old Oaken Bucket

## boilerctf: old-oaken-bucket

Nov 5, 2018

### PEDA may be useful

It's a script that makes gdb easier to use (run these in your shell)

```
git clone https://github.com/longld/peda.git ~/peda
echo "source ~/peda/peda.py" >> ~/.gdbinit
echo "DONE! debug your program with gdb and enjoy"
```

### Some GDB basics you'll need

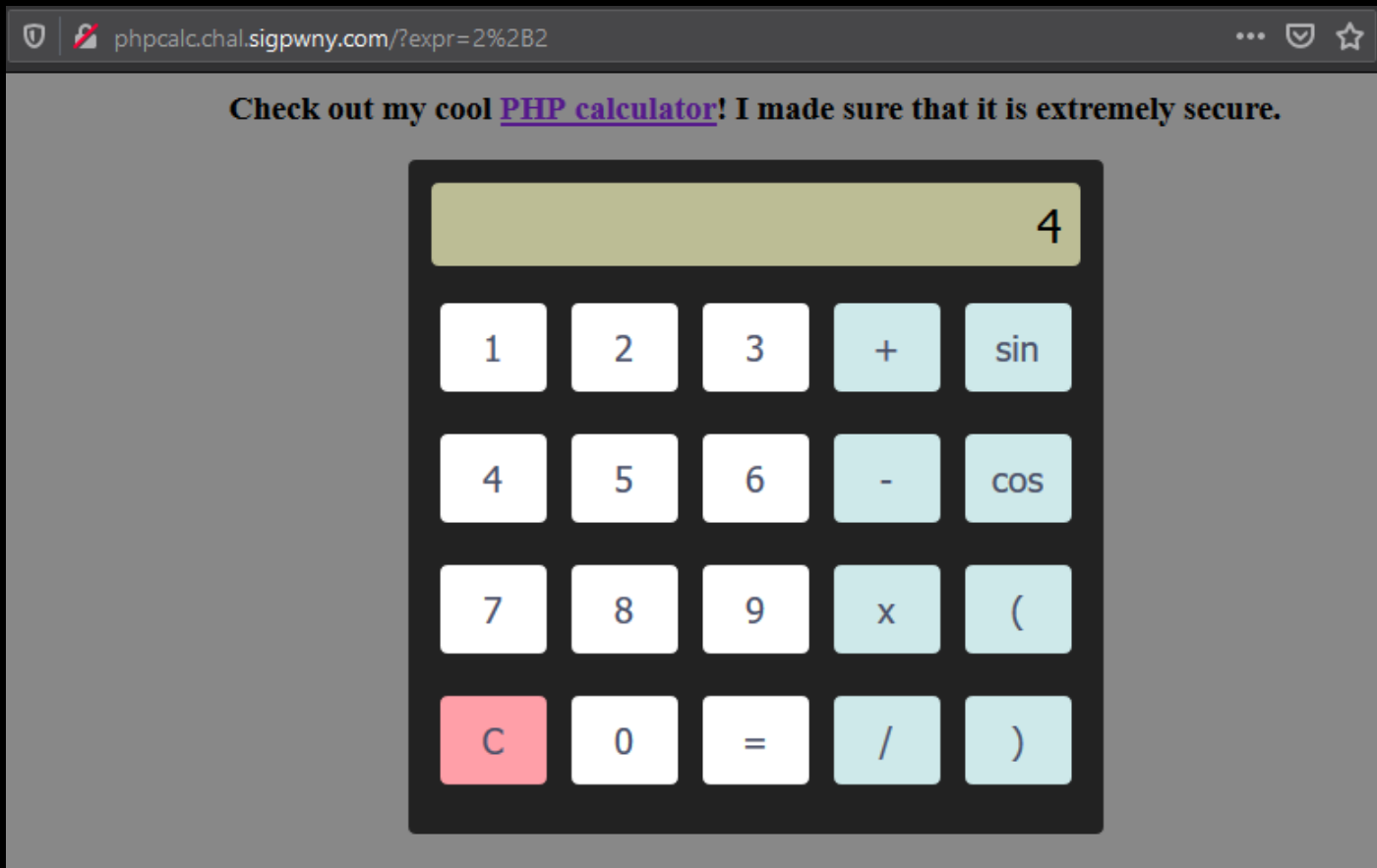
- `gdb old-oaken-bucket`
- `break * 0x4005f6` set a breakpoint on the main function. the binary is stripped, if you're curious why read [this](#)
- `run AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA` # starts the program and runs until it hits the breakpoint
- `ni` # next instruction – steps in assembly.
- `c` continue until the next breakpoint or the program ends

[Simple reversing challenge from an internal Purdue ctf that i \\*ahem\\*d my way into. Download link.](#)

```
~/workspace/playground/bucket
└─ ls
old-oaken-bucket* solver.py
~/workspace/playground/bucket
└─ ls -l old-oaken-bucket
-rwxr-xr-x 1 nat nat 6344 Oct 27 2018 old-oaken-bucket*
~/workspace/playground/bucket
└─ python2 solver.py
WARNING | 2020-01-25 16:20:45,543 | angr.analyses.disassembly_utils | Your version of
capstone does not support MIPS instruction groups.
29971608406721428983539903359161723172023448547023777466310451980115587448701
~/workspace/playground/bucket
└─ p
>>> import binascii
>>> s = hex(29971608406721428983539903359161723172023448547023777466310451980115587448
701)[2:]
>>> binascii.unhexlify(s)
b'BCTF{h@h_fal53_f1@gs_ar3_funny?}'
>>>
```

# Part #4: Some Challenges

# PHPCalc



- We broke it.
- We managed to encode `exec("command")`, if command is 7 or fewer characters.

# PHPCalc – Shell Commands

**whoami :**

www-data

**ls -C:**

flag.php index.php styles.css

**ls -lra:**

drwxrwxrwx 1 www-data www-data 4096 Jan 28 16:47 .

**rm \*:**

Don't worry we didn't run it. But it would work.

# Discord SE 10

- Given a link to an image, get an invite to the discord server.
- [https://cdn.discordapp.com/attachments/568224176905650220/568234865644797963/how\\_to\\_solve.png](https://cdn.discordapp.com/attachments/568224176905650220/568234865644797963/how_to_solve.png)

```
* How to solve
```

```
* Nobody gets this one.
```

January 27, 2020

9:06 AM **Chofhe** I was clicking through Sigpwny's slides, and ran into your discord hacking one. That's always fun. Do you know if there are any tools out there to just extract available information about discord servers/etc? I know there used to be BetterDiscord, but that's out of date and can be selfbotty.

I'm also curious about the last slide - could you describe what the advanced tricks are / describe what the challenge might be?

11:04 AM **kuilin** Not that I know of, but the node inspector in the client itself would be the easiest to use, imo - the network tab is right there and that logs *all* the data

**kuilin** ...hm, maybe not websocket data, but that's savable in other ways

**kuilin** On the last slide I was referring to actually reading through the minified JS, setting breakpoints, inspecting variables, etc, to identify what the code does. B&A 9 is solvable only by logging raw websocket events, because even though you don't have access to view anything on the UI, the server config and any changes to it is still broadcast, and B&A 10 involves replicating the initial handshake, which is slightly harder, as all channel infos, including their topics, are sent there. That's solved by either repeating the initial calls or making Discord time out and reconnect. Or, hm, I suppose joining the server with the breakpoints up would work too, but I haven't tested that

**kuilin** SE 10 is a very wacky one that I'm sorta disappointed nobody's solved. Have you seen the hints for that one yet?

11:13 AM **Chofhe** No, I'm not a student at Illinois, I've just been clicking around some. :/

11:14 AM **kuilin** Social Engineering 10

Title: Social Engineering 10: Uninvited

Info: Here is a link to an image that was uploaded to a public Discord server's #general text channel: [https://cdn.discordapp.com/attachments/568224176905650220/568234865644797963/how\\_to\\_solve.png](https://cdn.discordapp.com/attachments/568224176905650220/568234865644797963/how_to_solve.png) Join the Discord server. (Note: This is not a steganography problem.)

Hint (-0 points): There are two separate ideas that need to be used together to solve this.

Hint (-50 points): Try creating a few Discord servers. Is there a relationship between a Discord server's automatically-created #general channel's snowflake and the server snowflake?

Hint (-100 points): The invite link you're supposed to use to join was not created by a user or bot.

Points: 250

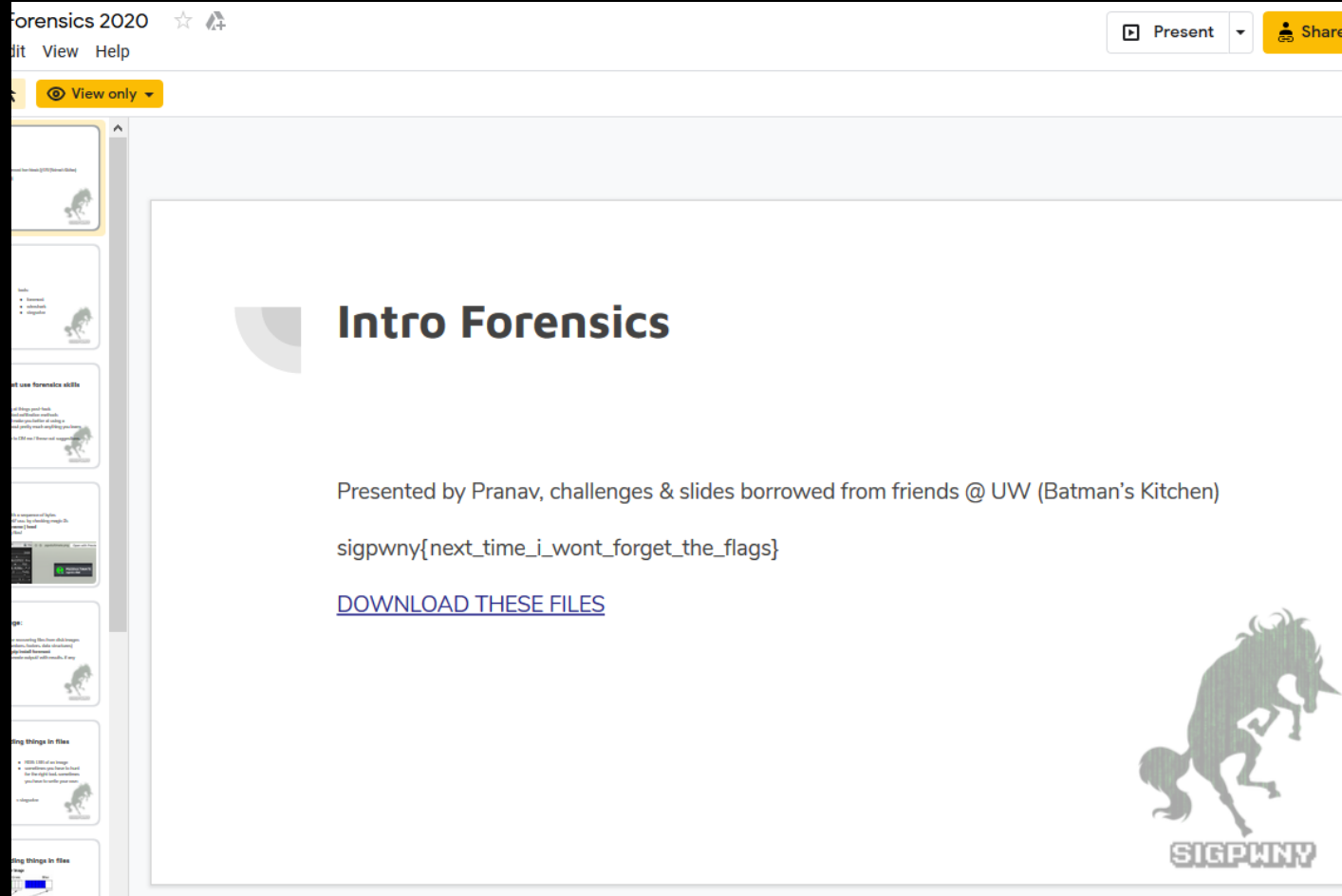
\* How to solve

\* Nobody gets this one.

**kuilin** Mentally subtract the points if you want :P

11:15 AM **Chofhe** 😊 Will do.

# Meeting Flags



The screenshot shows a Beamer presentation slide titled "Intro Forensics". The slide content includes:

- Presented by Pranav, challenges & slides borrowed from friends @ UW (Batman's Kitchen)
- sigpwny{next\_time\_i\_wont\_forget\_the\_flags}
- [DOWNLOAD THESE FILES](#)
- A logo of a horse in the bottom right corner with the text "SIGPWNY" below it.

The slide is displayed in a Beamer viewer window with a "View only" button and "Present" and "Share" buttons in the top right corner.

- Make slides private, or don't have the flag in the slides



# Impossible Challenges



Ones that involved seeing someone in person



OpSec



Web Chals were DOWN :(



Meeting Flags



Game Hacking



Game Hacking Montage

b01lers

# B01lers

## About Us

- Founded Fall 2014 by Professor Payer
- 3 different advisors since then
- Current Advisor: Antonio Bianchi – Member of Shellphish and OOO
- Grown rapidly – undergrad and grad student members

# Resources

# #resources

- Channel on Discord
- <https://discord.gg/jrUGtYe>

# resources

4:08 PM **nsnc** You'll never need this... but cool gui tool for editing and reading ATARI binaries: <https://github.com/robmcmullen/omnivore/releases> (edited) September 20, 2019

7:59 PM **nsnc** <https://ctf101.org/> (edited) September 24, 2019

12:51 PM **ZJam** Rsa Ctf tool: <https://github.com/Ganapati/RsaCtfTool> September 25, 2019

12:53 PM **PHSC** PHP Magic Hashes: <https://github.com/spaze/ashes> September 30, 2019

7:40 PM **ZJam** File Signature Table: [https://www.garykessler.net/library/file\\_sigs.html](https://www.garykessler.net/library/file_sigs.html) (edited) October 9, 2019

1:52 PM **GHOS1** Buffer overflow tutorial by Turkstra <https://turkeyland.net/projects/overflow/index.php>

5:05 PM **ZJam** Online Stego Tool: <https://aperisolve.fr/> October 10, 2019

1:31 PM **nsnc** Steg toolkit: <https://github.com/DominicBreuker/stego-toolkit> (edited) October 20, 2019

12:56 AM **GHOS1** Excellent presentaion on heap attacks <http://homes.sice.indiana.edu/yh33/Teaching/1433-2016/lec13-HeapAttacks.pdf>

3:01 PM **A0su** Brief heap gitbook <https://heap-exploitation.dhavalKapil.com/> November 1, 2019

1:56 PM **A0su** CSAW Challenges <https://365.csaw.io/> November 11, 2019

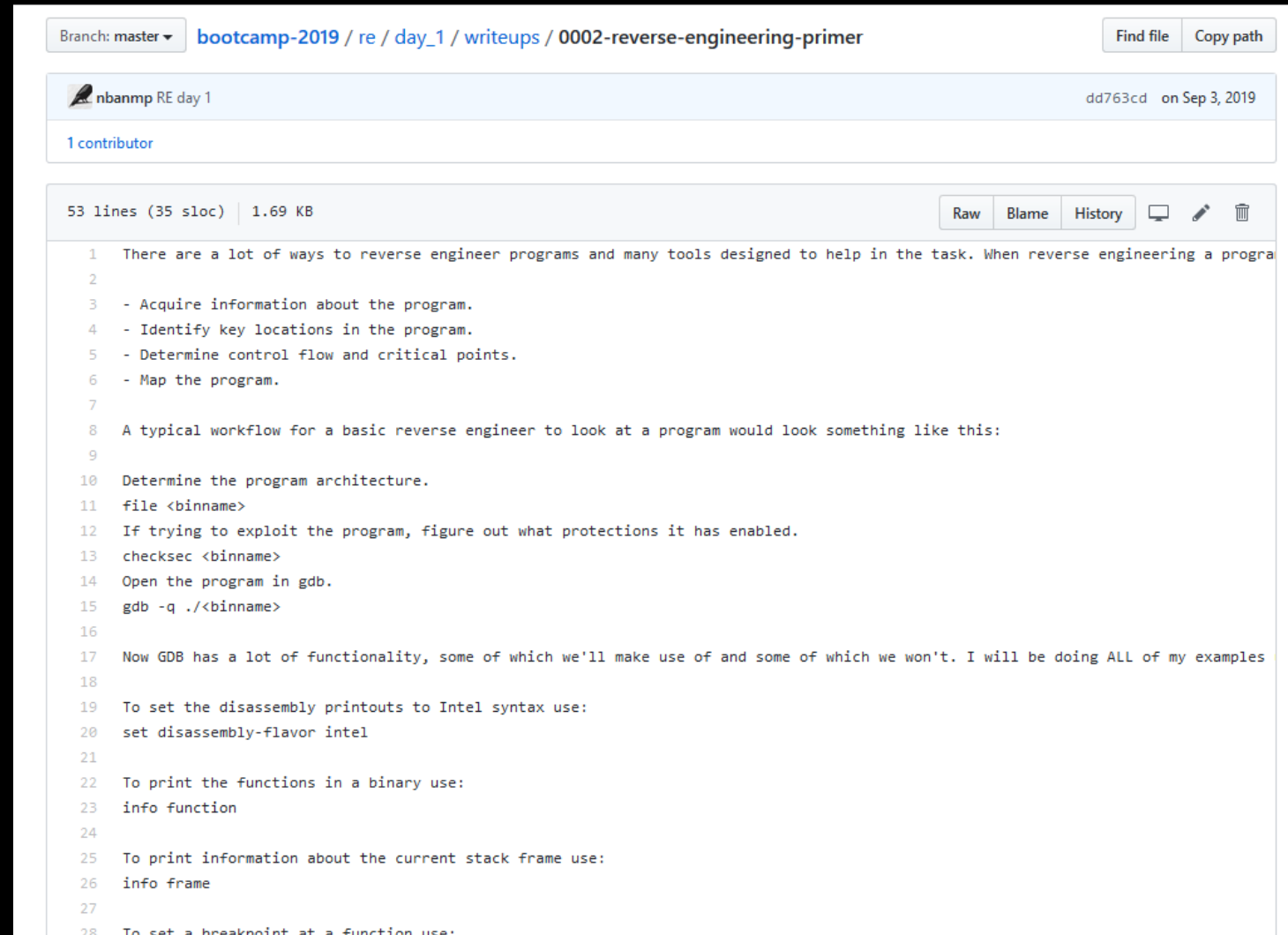
6:44 PM **nsnc** Pintool: <https://github.com/wagi/pintool> January 16, 2020

4:24 PM **maczilla** Past RPISEC Courses in RE: <https://github.com/JeremyBlackthorne/RPISEC-Courses> January 22, 2020

3:12 PM **nsnc** Kernel Exploitation: [https://github.com/ctf-wiki/ctf-wiki/blob/master/docs/pwn/linux/kernel/ref/13\\_lecture.pdf](https://github.com/ctf-wiki/ctf-wiki/blob/master/docs/pwn/linux/kernel/ref/13_lecture.pdf) (edited)

# bootcamp

- <https://github.com/b01lers/bootcamp-2019>
- Training material from Fall 2019

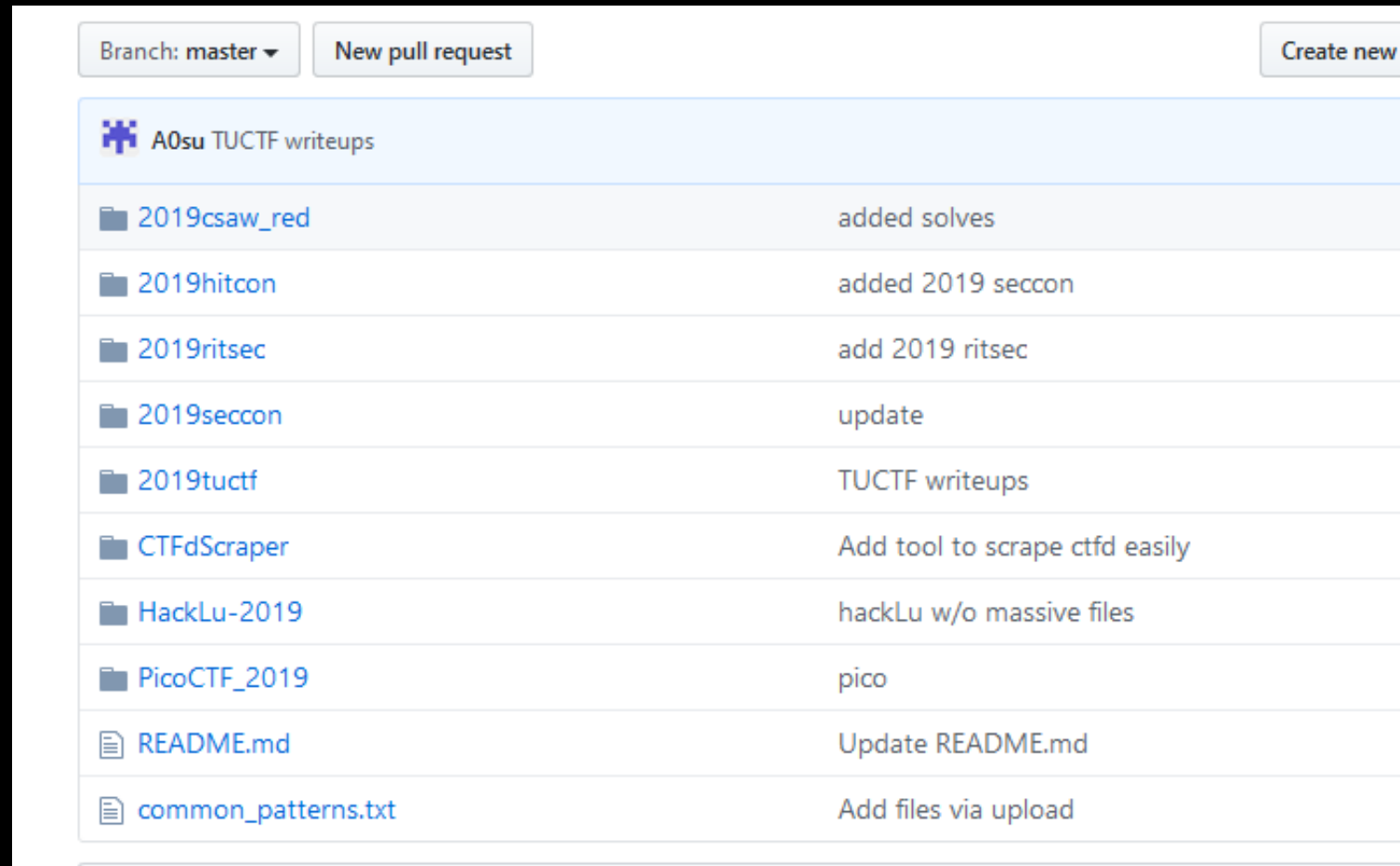


The screenshot shows a GitHub repository page for the file '0002-reverse-engineering-primer' in the 'bootcamp-2019' repository. The page is on the 'master' branch. The file was committed by 'nbanmp' on Sep 3, 2019. The file contains 53 lines of text (35 sloc) and is 1.69 KB in size. The content of the file is as follows:












```
1  There are a lot of ways to reverse engineer programs and many tools designed to help in the task. When reverse engineering a program
2
3  - Acquire information about the program.
4  - Identify key locations in the program.
5  - Determine control flow and critical points.
6  - Map the program.
7
8  A typical workflow for a basic reverse engineer to look at a program would look something like this:
9
10 Determine the program architecture.
11 file <binname>
12 If trying to exploit the program, figure out what protections it has enabled.
13 checksec <binname>
14 Open the program in gdb.
15 gdb -q ./<binname>
16
17 Now GDB has a lot of functionality, some of which we'll make use of and some of which we won't. I will be doing ALL of my examples
18
19 To set the disassembly printouts to Intel syntax use:
20 set disassembly-flavor intel
21
22 To print the functions in a binary use:
23 info function
24
25 To print information about the current stack frame use:
26 info frame
27
28 To set a breakpoint at a function use:
```

# b01lers Library

- <https://github.com/b01lers/b01lers-library>
- Previous CTF Challenges
- Some have writeups



Branch: master ▾ New pull request Create new

 A0su TUCTF writeups	
 2019csaw_red	added solves
 2019hitcon	added 2019 secon
 2019ritsec	add 2019 ritsec
 2019secon	update
 2019tuctf	TUCTF writeups
 CTfDScraper	Add tool to scrape ctfD easily
 HackLu-2019	hackLu w/o massive files
 PicoCTF_2019	pico
 README.md	Update README.md
 common_patterns.txt	Add files via upload

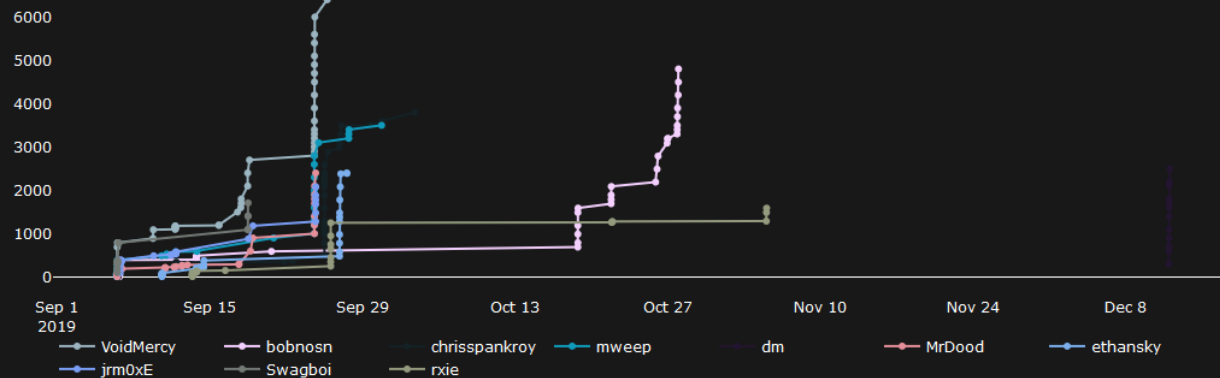
Internal CTF



# Internal CTF

## Scoreboard

Current Champions



- <http://internal.b01lers.net:6698>
- Only @purdue.edu and @illinois.edu emails may register
- Create an account

# Bootcamp

## BOOTCAMP

Dev Tools Part 1 10	Dev Tools Part 2.5 10	Dev Tools Part 4 10	HTTP Methods 1 10
HTTP Methods 2 10	Puke Brute 10	SQL Part 1 10	SQL Part 2 10
Dev Tools Part 2 10	Classical Crypto 2 10	Classical Crypto 1 10	Classical Crypto 3 10
Classical Crypto 4 10	Classical Crypto 5 10	XOR 1 10	XOR 2 10
XOR 3 10	XOR 4 10	RSA 1 10	RSA 2 10

Powered by CTFd

- Start with this category
- Easier
- Writeups and tutorials available:
- <https://github.com/b01lers/bootcamp-2019>

# Misc / Recon



Recon: No hints for you.



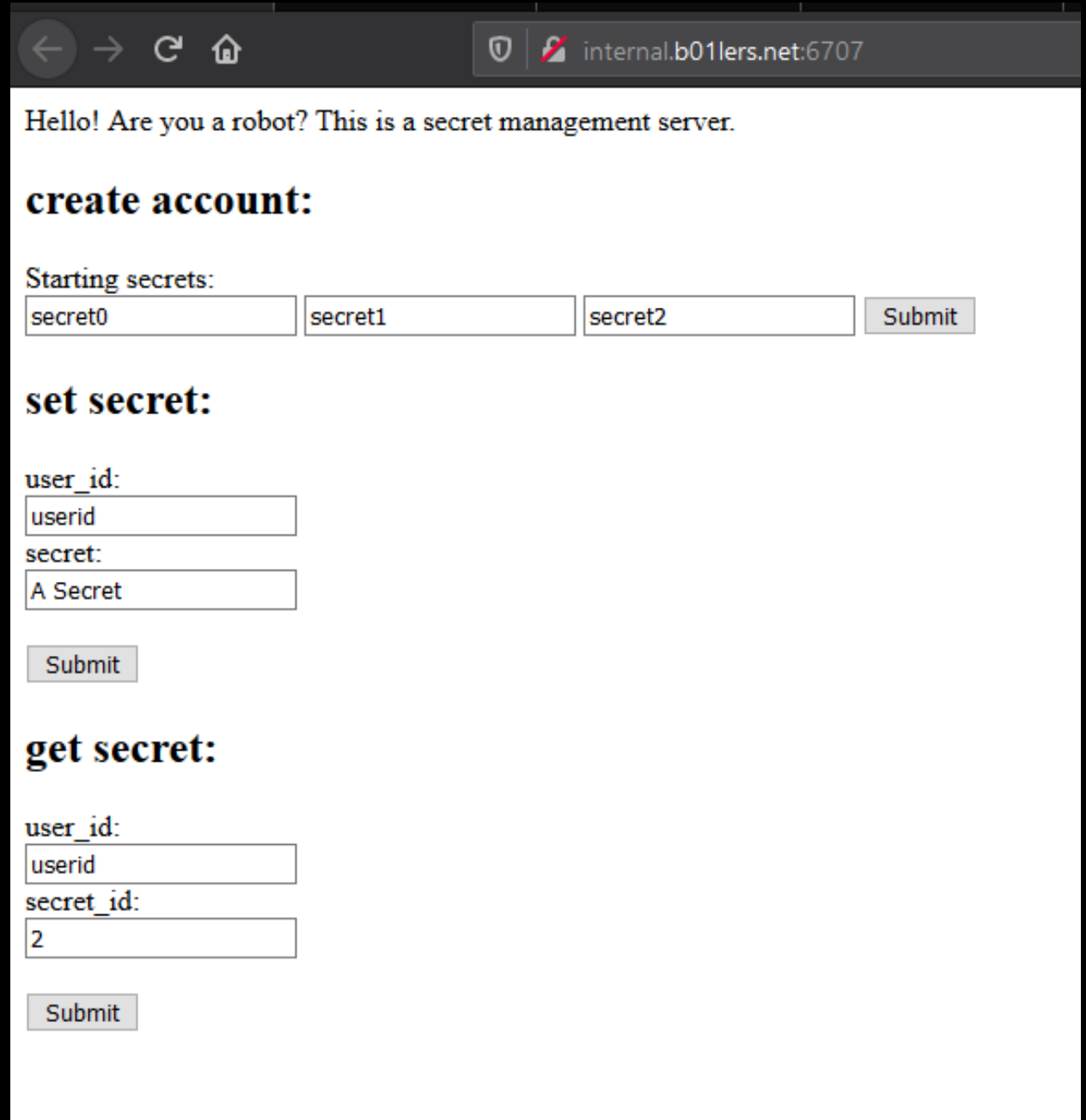
Forensics



Random Chals

# Web

- 2 Chals:
  - Python Pirates
  - Python IS Secure
- Check Bootcamp as well
- Leak the Source
- Find a Bug
- Postman/Curl



The screenshot shows a web browser window with the address bar displaying "internal.b01lers.net:6707". The page content includes a greeting, three sections for account management, and a "Submit" button for each section.

Hello! Are you a robot? This is a secret management server.

**create account:**

Starting secrets:

**set secret:**

user\_id:

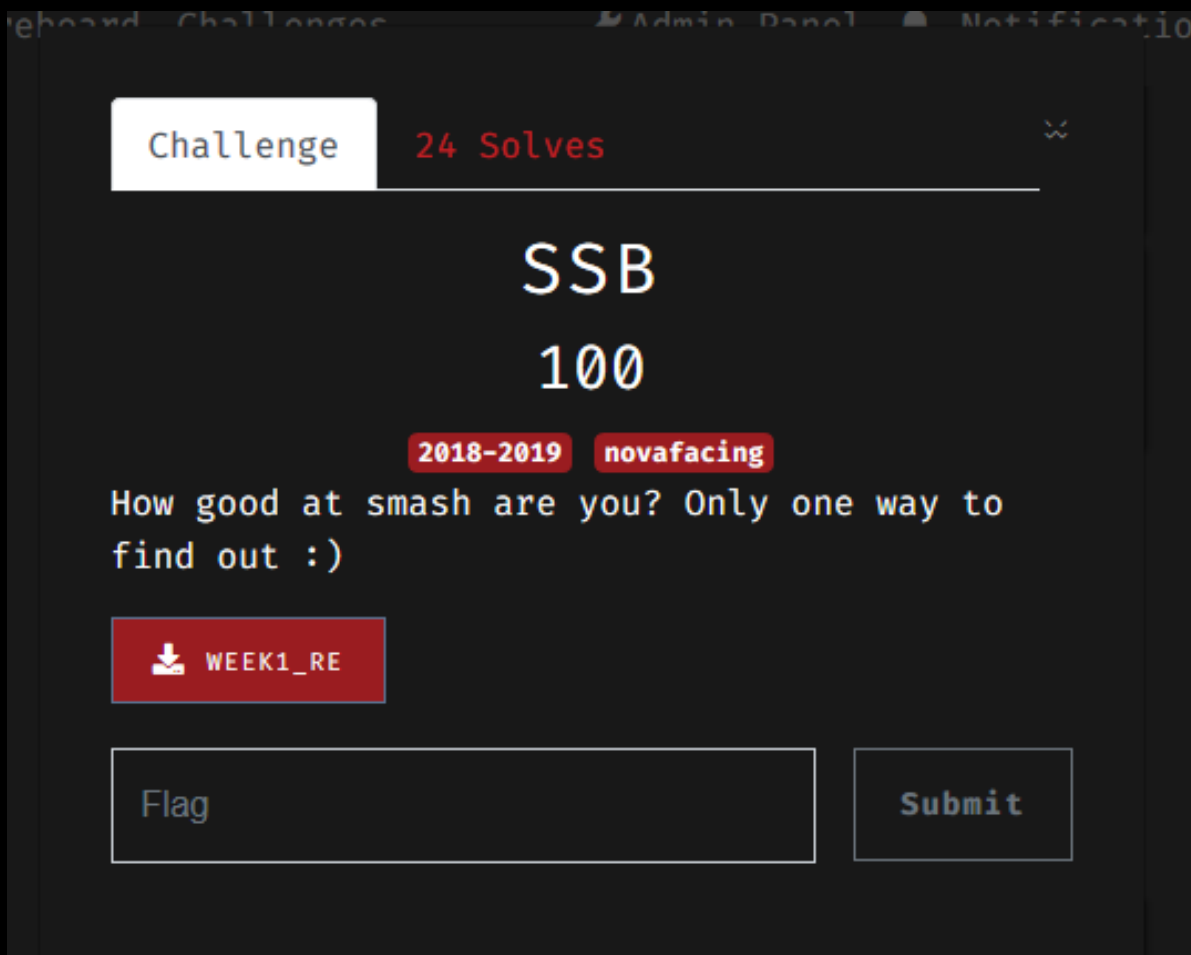
secret:

**get secret:**

user\_id:

secret\_id:

# RE



The screenshot shows a challenge page with the following elements:

- Challenge name: **SSB**
- Points: **100**
- Tags: **2018-2019** and **novafacing**
- Description: "How good at smash are you? Only one way to find out :)"
- Download button: **WEEK1\_RE**
- Input field: **Flag**
- Submit button: **Submit**

- GDB
- Ghidra
- Also helpful: strings/ltrace
- Look at bootcamp RE tutorials

# Crypto



ROT



SUBSTITUTION



CLASSICAL  
CIPHERS



RSA



DOUBLE DES

# PWN



Will always involve writing scripts



pwntools



Also uses RE skills



Buffer Overflow



printf



Heap

Public CTF



# B01lers CTF

- <https://ctf.b01lers.net>
- Mar 14 00:00 UTC – Mar 16 00:00 UTC
- Actual testing!
- PWN, RE, CRYPTO, WEB, More!
- Balanced Difficulty!



b01lers CTF