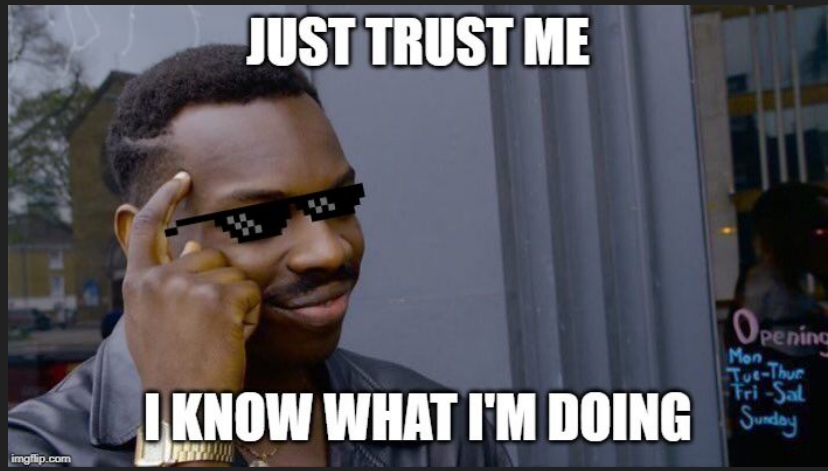
Bring Your Own [Challenges||Capture] The Flag

Eli McRae

Eli McRae (shyft)

- NOT an expert or even good at anything despite credentials indicating otherwise
  - OSCP (soon I promise…)
  - GIAC GNFA (#2556) GCIA (#16095)
  - CompTIA Security+, CySA+, PenTest+ (COMP001008235863)
- 20+ Years of hobbyist hacking experience
  - Fs2600 Fort Smith, AR since 2006
  - Shell On The Border and other CTFs
- 15+ Years of industry-ish experience
  - Computer repair, Developer (kind of), Network engineer (kind of), MSP person (kind of), Pentester (kind of), Teacher (kind of)
- 13 Years Arkansas ANG
  - 8 years Network Control Center at 188th FW
  - 5 years Cyber Warfare Operations dude and Network Specialist at 223rd COS



shyft@shyft.us github.com/ShyftXero linkedin.com/in/eli-mcrae

SOTB History

- JOLT
  - https://web.archive.org/web/20220120202848/https://blog.ecapuano.com/jolthackathon-2017/
  - Share heartwarming about how JOLT changed trajectory of my life…
- Why did SOTB start?
  - Many of the players from the top 3 had ties to Ft Smith
    - /dev/null
    - Jiggawatts
  - Wanted to see if we could do it…

SOTB Challenge Development Standards and Struggles

- Development Standards
  - Don’t announce until at least 1-3 challenges per hour of the event are fully developed.
  - Don’t announce until human logistics are 50% resolved (venue, food options, swag, etc.)
- Struggles
  - Fs2600 growth was negative for a while
  - Existing members don’t have the same free time as they used to
  - It’s hard to always have interesting ideas…
  - Human Logistics is hard… sotb_2018 && sotb_2019

The Problem

We want a solution that implements the following:

- Allows players to contribute to the challenges of the event without compromising the “integrity” of the game
- Allows players contributions to be rewarded / acknowledged in some way
- Allows some form of interplayer transactions that can contribute towards winning **
- Allows for something else I guess…

No other ctf framework offered these capabilities. ***

Our Solution -> https://byoctf.com

These slides -> https://byoctf.com/slides

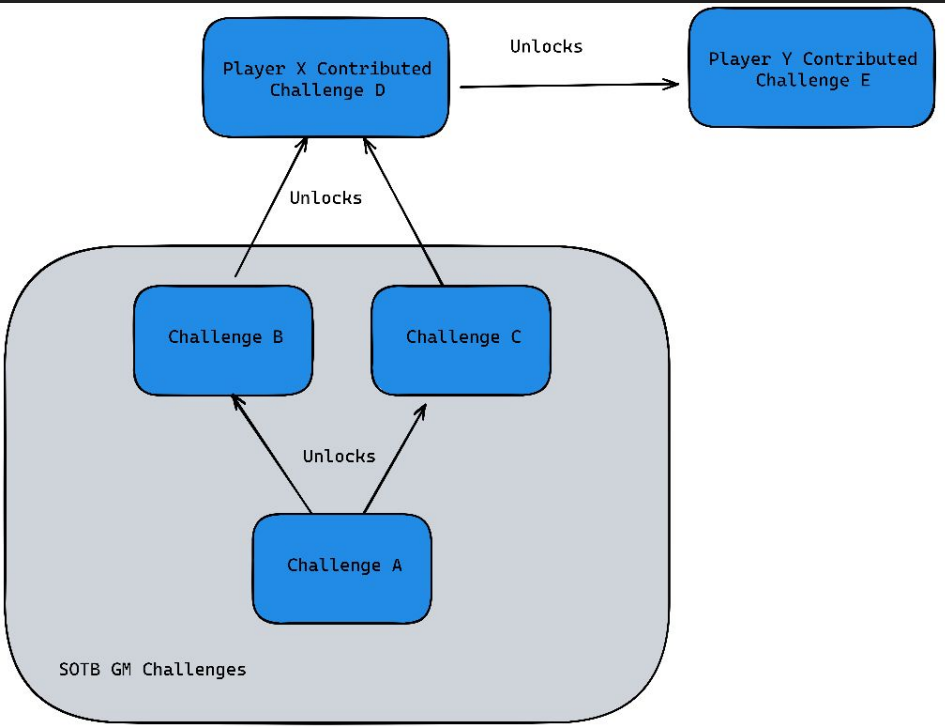
Key Features

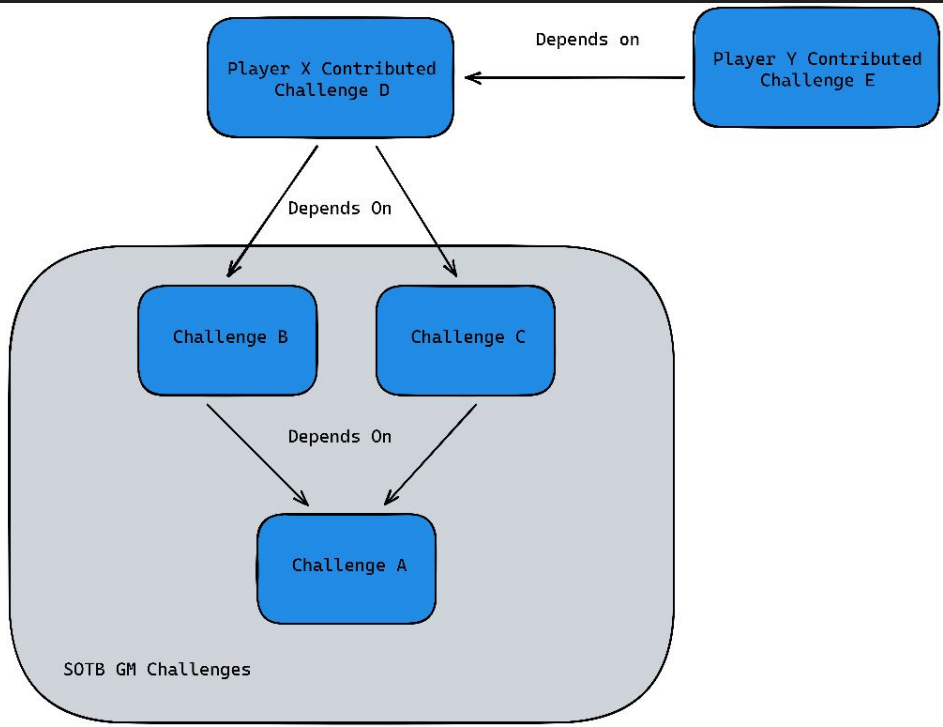
- User contributed challenges meaning GMs aren’t barred from playing.
  - Players can earn points by other players solving the challenges they built.
  - Flags can be validated either internally or externally (if you don't trust us to not look at flags)
- Inter-player transactions via ‘tips’ and Metagames
  - An economy is born; Hopefully you will do something interesting with this.
- Flag-oriented
  - A challenge is one or more flags allowing partial completion
  - A single flag can be part of one or more challenges
  - Bonus flags are not bound to a challenge
  - Reactive points (first blood, decaying points, maybe some others to come)
- Discord-based
  - Haven’t really looked but also haven’t seen it before…

Features Continued…

- Externally validated flags
  - You don’t have to give the GMs the flag if you don’t trust them but you will have to run an external validation server.
  - These challenges are tagged as externally validated.
  - GMs will see the sha256 of the flag but not the flag itself.
  - Flags are submitted slightly differently : `!esub <chall_id> <flag>`
  - https://github.com/ShyftXero/byoctf_ext_validation
- Challenge dependency
  - User contributed challenges can depend upon or extend any other ***existing*** challenge **
  - Ex: Challenge [D] becomes available by solving [C || B] both of which have become available by solving [A]
  - Player can create Challenge E which becomes available by solving D

Two ways to think about the dependencies





Team	
id	int
members	User
name	str
password	str

Tag	
id	int
name	str
challenges	Challenge
flags	Flag

User	
id	int
name	str
challenges	Challenge
solves	Solve
team	Team
sent_transactions	Transaction
recipient_transactions	Transaction
authored_flags	Flag
ratings	Rating

Challenge	
id	int
title	str
flags	Flag
author	User
description	str
parent	Challenge
children	Challenge
tags	Tag
release_time	datetime
visible	bool
hints	Hint
byoc	bool
byoc_ext_url	str
unsolved	bool
byoc_ext_value	float
solve	Solve
transaction	Transaction
ratings	Rating

Flag	
id	int
challenges	Challenge
description	str
solves	Solve
flag	str
value	float
unsolved	bool
bonus	bool
tags	Tag
author	User
byoc	bool
transaction	Transaction
reward_capped	bool

Rating	
id	int
user	User
challenge	Challenge
value	int

Hint	
id	int
text	str
cost	float
challenge	Challenge
transactions	Transaction

Transaction	
id	int
value	float
sender	User
recipient	User
type	str
message	str
time	datetime
solve	Solve
flag	Flag
challenge	Challenge
hint	Hint

Solve	
id	int
time	datetime
flag	Flag
user	User
value	float
transaction	Transaction
challenge	Challenge
flag_text	str

The Next Shell On The Border (sometime in 2023)

- Does this mean the next SOTB will be entirely user-contributed challenges?
  - No. We will still have our challenges for people to solve.

- For what? Just use ctfd like you always did.
  - Ok… It seemed like a good idea at the time…
  - Cool story from JOLT about abuse of trust here…

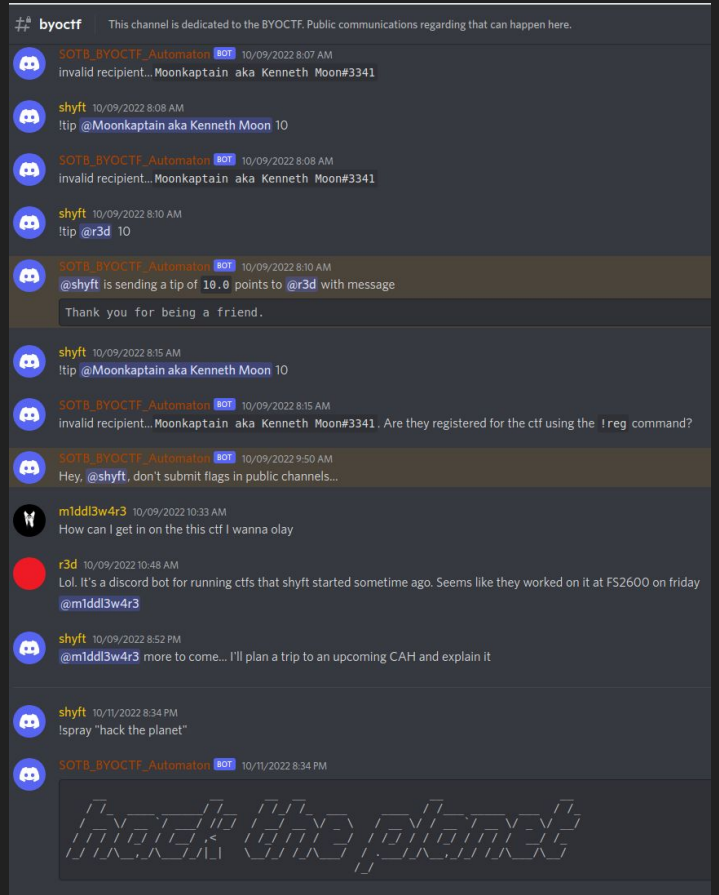
Common Criticisms

- Top 3 so far
  - Impossible-to-solve challenges? (malice)
  - Trivial challenges and a race to the bottom? (do unto others as they do unto you)
  - Legit but over or undervalued challenges? (honest mistake)
  - GMs will cheat
  - What else can you think of?
- Let’s also talk about the technical controls available and in-place.
  - We won’t cheat / can’t really win
  - Disabling or capping byoc reward payout (honest mistake)
  - Disabling challenge (do unto others as they do unto you)
  - Disabling user (malice)
  - Please don’t make us use these tools
  - Same old rules are still there… “don’t hack the scoreboard”

https://github.com/ShyftXero/byoctf_discord#common-criticisms-of-the-byoc-concept

How Does This Implementation Work?

- Discord bot on the Arkansas Hackers discord -> https://krime.life
- Most commands are restricted to DMs with the bot
- Must register to play/view/interact
  - DM bot
  - !reg <teamname> <teampass>



Example

- By default, it costs `50%` of the total challenge value (sum of flags) to post a challenge.
- By default, your reward for the solve of a flag which is part of your challenge is `25%` of that flags value.

- You build a challenge with 2 flags.
  - flag 1 is worth 150 points and
  - flag 2 is 50 points
  - for a total of `200` points
- It will cost you `100` points to post it via `!byoc_commit` so you do.
  - Now you are down `100` points
- When the first solve comes in for flag 1, you will get a reward of `37.5` points
  - Now you are only down `62.5` points.
- When the second solve for flag 1 comes in, you will get another reward of `37.5` points
  - Now you are only down `25` points.
- When the first solve comes in for flag 2, you will get a reward of `12.5` points
  - Now you are only down `12.5` points.
- When the third solve for flag 1 solve for flag 1 comes in, you will get another reward of `37.5` points
  - At this point you have earned back your commit fee and have turned a profit of `25` points

Here’s what another example looks like on the backend

```
~/byoctf_discord on master
❯ ./ctrl_ctf.py trans
```

Trans ID	Value	Type	Sender	Recipient	Message	Time
1	1000.0	seed	BYOCTF_Automaton#7840	shyft#0760		2022-11-22 19:15:49.242313
2	1000.0	seed	BYOCTF_Automaton#7840	notfie#4785		2022-11-22 19:15:49.242351
3	1000.0	seed	BYOCTF_Automaton#7840	Combaticus#8292		2022-11-22 19:15:49.242383
4	1000.0	seed	BYOCTF_Automaton#7840	0xDrMalloc#4492		2022-11-22 19:15:49.242415
5	10.0	hint buy	shyft#0760	BYOCTF_Automaton#7840	bought hint ID 2 for challenge ID 1	2022-11-22 19:15:49.258029
6	1.0	byoc hint reward	BYOCTF_Automaton#7840	0xDrMalloc#4492	hint buy from shyft#0760	2022-11-22 19:15:49.258303
7	10.0	hint buy	Combaticus#8292	BYOCTF_Automaton#7840	bought hint ID 2 for challenge ID 1	2022-11-22 19:15:49.263232
8	1.0	byoc hint reward	BYOCTF_Automaton#7840	0xDrMalloc#4492	hint buy from Combaticus#8292	2022-11-22 19:15:49.263429
9	50.0	hint buy	notfie#4785	BYOCTF_Automaton#7840	bought hint ID 5 for challenge ID 5	2022-11-22 19:15:49.265620
10	5.0	byoc hint reward	BYOCTF_Automaton#7840	Combaticus#8292	hint buy from notfie#4785	2022-11-22 19:15:49.265806
11	30.0	hint buy	Combaticus#8292	BYOCTF_Automaton#7840	bought hint ID 4 for challenge ID 2	2022-11-22 19:15:49.268093
12	110.0	solve	BYOCTF_Automaton#7840	Combaticus#8292	FLAG{asdf} is part of: challenge 1	2022-11-22 19:15:49.275705
13	25.0	byoc reward	BYOCTF_Automaton#7840	0xDrMalloc#4492	Combaticus#8292 of secondteam submitted FLAG{asdf} for challenge challenge 1	2022-11-22 19:15:49.280957
14	100.0	solve	BYOCTF_Automaton#7840	notfie#4785	FLAG{asdf} is part of: challenge 1	2022-11-22 19:15:49.289106
15	25.0	byoc reward	BYOCTF_Automaton#7840	0xDrMalloc#4492	notfie#4785 of bestteam submitted FLAG{asdf} for challenge challenge 1	2022-11-22 19:15:49.294491
16	220.0	solve	BYOCTF_Automaton#7840	Combaticus#8292	FLAG{ASDF} is part of: challenge 1	2022-11-22 19:15:49.302046
17	50.0	byoc reward	BYOCTF_Automaton#7840	0xDrMalloc#4492	Combaticus#8292 of secondteam submitted FLAG{ASDF} for challenge challenge 1	2022-11-22 19:15:49.309508
18	330.0	solve	BYOCTF_Automaton#7840	notfie#4785	FLAG{zxcv} is part of:	2022-11-22 19:15:49.317435
19	75.0	byoc reward	BYOCTF_Automaton#7840	Combaticus#8292	notfie#4785 of bestteam submitted FLAG{zxcv} for challenge __bonus__	2022-11-22 19:15:49.321793
20	100.0	solve	BYOCTF_Automaton#7840	AyKay#3420	FLAG{asdf} is part of: challenge 1	2022-11-22 19:15:49.327922
21	25.0	byoc reward	BYOCTF_Automaton#7840	0xDrMalloc#4492	AyKay#3420 of fourthteam submitted FLAG{asdf} for challenge challenge 1	2022-11-22 19:15:49.332800
22	200.0	solve	BYOCTF_Automaton#7840	AyKay#3420	FLAG{ASDF} is part of: challenge 1	2022-11-22 19:15:49.337883
23	50.0	byoc reward	BYOCTF_Automaton#7840	0xDrMalloc#4492	AyKay#3420 of fourthteam submitted FLAG{ASDF} for challenge challenge 1	2022-11-22 19:15:49.341926
24	220.0	solve	BYOCTF_Automaton#7840	AyKay#3420	FLAG{qwer} is part of: challenge 3 challenge 2	2022-11-22 19:15:49.346883
25	50.0	byoc reward	BYOCTF_Automaton#7840	notfie#4785	AyKay#3420 of fourthteam submitted FLAG{qwer} for challenge challenge 2	2022-11-22 19:15:49.351023
26	300.0	solve	BYOCTF_Automaton#7840	AyKay#3420	FLAG{zxcv} is part of:	2022-11-22 19:15:49.355600
27	75.0	byoc reward	BYOCTF_Automaton#7840	Combaticus#8292	AyKay#3420 of fourthteam submitted FLAG{zxcv} for challenge __bonus__	2022-11-22 19:15:49.359470
28	220.0	solve	BYOCTF_Automaton#7840	AyKay#3420	FLAG{jkl} is part of: challenge 6	2022-11-22 19:15:49.363984
29	50.0	byoc reward	BYOCTF_Automaton#7840	0xDrMalloc#4492	AyKay#3420 of fourthteam submitted FLAG{jkl} for challenge challenge 6	2022-11-22 19:15:49.367694
30	10.0	tip	shyft#0760	Combaticus#8292	Thank you for being a friend.	2022-11-22 19:45:19.126803
31	200.0	byoc commit	shyft#0760	BYOCTF_Automaton#7840	submitted challenge "r3d's multi-flag challenge"	2022-12-03 02:43:20.587505

Benefits of byoctf (even if you don’t want to submit chals)

- Challenge format standardization
- Gentle on-ramp to GM your own thing
- Some other benefit here.

Let’s build/port some challenges

What you'll need

- BYOCTF Challenge Validator -> https://validator.byoctf.com
- TOML syntax refresher -> https://toml.io/en/
- External validator code for ext validation https://github.com/ShyftXero/byoctf_ext_validation
- https://www.uuidgenerator.net/version4

What goes into building cool/good challenges?

- If we didn't discuss challenge design earlier ->
  - https://github.com/ShyftXero/byoctf_discord#notes-or-guidance-for-developing-challenges
  - Think along the lines of cvss but inverted
  - https://www.beyondsecurity.com/vulnerability-assessment-requirements-cvss-explained

- Know what you want the players to know/prove/learn from your challenge
- Understand where this challenge is in relation to other challenges and your audience (you won't ever get this "right")
  - Binary to ascii conversion - low 25 points?
  - Base64 conversion - low 50 points?
  - Classic binary exploitation methods - medium 100-200 points?
  - Newer Binary exploitation methods - High 300-400 points?
  - Execute full kill chain with bespoke exploit on a target - High 500 points?

Simple Single-Flag Challenge

```
author = "Combaticus#8292"
challenge_title = "r3d's challenge"
challenge_description = """good luck finding my flag at validator.byoctf.com"""
tags = [ "pentest",]
uuid = "1f495409-a84b-43a2-bf8e-90fd979024f4"
[[flags]]
flag_title = "r3d flag"
flag_value = 200
flag_flag = "FLAG{this_is_a_flag_from_r3d}"

[[hints]]
hint_cost = 10
hint_text = "the flag is easy"
```

Simple Single-Flag Challenge with a Dependency

- Requirement:
  - existing challenges need to exist… otherwise you won't know their IDs
  - you can't get these IDs until they are committed to the game

```
author = "Combaticus#8292"
challenge_title = "r3d's child challenge"
challenge_description = "good luck finding my flag; download the file from https://transfer.sh/4jiaJ2/chall.dat"
uuid = "c8b524a6-d646-4c03-ac2e-10da3f9b7ce0"
tags = [ "pentest",]
depends_on = [ 6, 7,] # these challenges need to be solved before this challenge is viewable or solvable
[[flags]]
flag_title = "r3d dependent flag "
flag_value = 200
flag_flag = "FLAG{here_is_a_flag} "

[[hints]]
hint_cost = 10
hint_text = "What did you do to solve that other challenge?"
```

Challenge with multiple flags

This is like having different flags for user access and root access for a server.

```
author = "Combaticus#8292"
challenge_title = "r3d's multi-flag challenge"
challenge_description = "good luck hacking into and finding my flags at 3.43.54.28"
tags = [ "pentest", "web",]
uuid = "e66622ea-ac8e-4bcd-a873-a485f4a3724b"
[[flags]]
flag_title = "flag 1 "
flag_value = 100
flag_flag = "FLAG{this_is_flag_1_for_multiflag}"

[[flags]]
flag_title = "flag 2"
flag_value = 300
flag_flag = "FLAG{this_is_flag_2_for_multiflag}"

[[hints]]
hint_cost = 25
hint_text = "Both of the the flags are easy"
```

Self-hosted externally validated challenge

```
author = "Combaticus#8292"
challenge_title = "r3d's externally validated challenge"
challenge_description = "good luck finding my flag. At http://1.2.3.4/hackme "
uuid='2e9e73a9-3e02-4db9-871e-fe5ffde1deb0'
tags = [ "coding",]
external_challenge_value = 250
external_validation = true
external_validation_url = "http://localhost:5000/validate"
# If you don't trust us to not look at the flags you submit, you can host a validation server on some public server and the bot can validate against that.
# I'd use a domain rather than IP because there's no public mechanism to update challenges... These are limited to one flag per challenge. sorry... It will send a post to your endpoint similar to {'challenge_id':<some_id>, 'flag':<some_flag>} . It will expect a response of {'flag':'correct'} or {'flag':'incorrect'} a basic implementation of that functionality will be provided.
# YOU WILL HAVE TO MENTION IN THE CHALLENGE WHETHER OR NOT THIS IS AN EXTERNALLY VALIDATED CHALLENGE.
# There's a different command to validate those flags. !byoc_ext <chall_id> <flag>; we use the validation url (must end in /validate with no trailing slash).
# feel free to extend the server we provide... You can host all of the flags for all of your challenges in the single flags.json file.
# you won't know a challenge ID to serve as the key until you commit your challenge. Currently, there is no first blood reward for externally validated challenges.

[[hints]]
hint_cost = 25
hint_text = "the flag is also easy"
```

Your Thoughts