CAPTURE THE FLAG WITH TOWER OF HANOI

HTTPS://TOH.NECST.IT

ARMANDO BELLANTE
@IKIGA1
@ARMANDO_BELLANTE

WHOAMI

- B.Sc./M.Sc. in Computer Science and Engineering at Politecnico di Milano;
- Playing hacking competitions (CTFs) with Tower of Hanoi and mhackeroni since 2015;
- Currently pursuing Ph.D. in Quantum Machine Learning and application to Cybersecurity at Politecnico di Milano.

QUANTUMALGORITHMS.ORG

DEFCON

WHOAREWE

- Hackers! We regularly meet and we hack.
  Our crime is that of curiosity.

- Politecnico di Milano CTF Team.
  Part of mhackeroni.
  Cyberchallenge.IT organizers @ Polimi.

- The oldest Italian CTF team…

POLITECNICO MILANO 1863
NECST laboratory

HTTPS://TOH.NECST.IT

@TOWEROFHANOI

TOH@NECST.IT

FIRST…HOW DID I MEET TOH?

APPROACHING A HACKING TEAM IN 2015

- Met them at my first year
  - I didn’t know how to CODE
- Joined their hackmeetings. Hackmeetings are peer meetings…

“Bro that challenge is easy! Just overflow the buffer, overwrite the return address with some code pointer and you’ll highjack the control flow!”

HOW DID I SURVIVE?

- Stubborn as hell
- Kept going to the hackmeetings. Silently learning the language for more than a year…
- Read and practiced a lot (Erickson’s The art of Exploitation + https://root-me.org saved me ❤️) + learned how to search things online properly
- WENT TO EVERY CTF WITH TOH!
- It might be frustrating and damn hard at the beginning. It’ll get better, a lot!

WAIT, ONCE AGAIN, WHAT'S A CTF?

CAPTURE THE FLAG!

- Security competitions
- Try to break into applications/systems to retrieve some secret: a Flag!

flag{this_l00ks_like_4_flag!}

SKILLS IN A CTF TEAM

Reverse Engineering

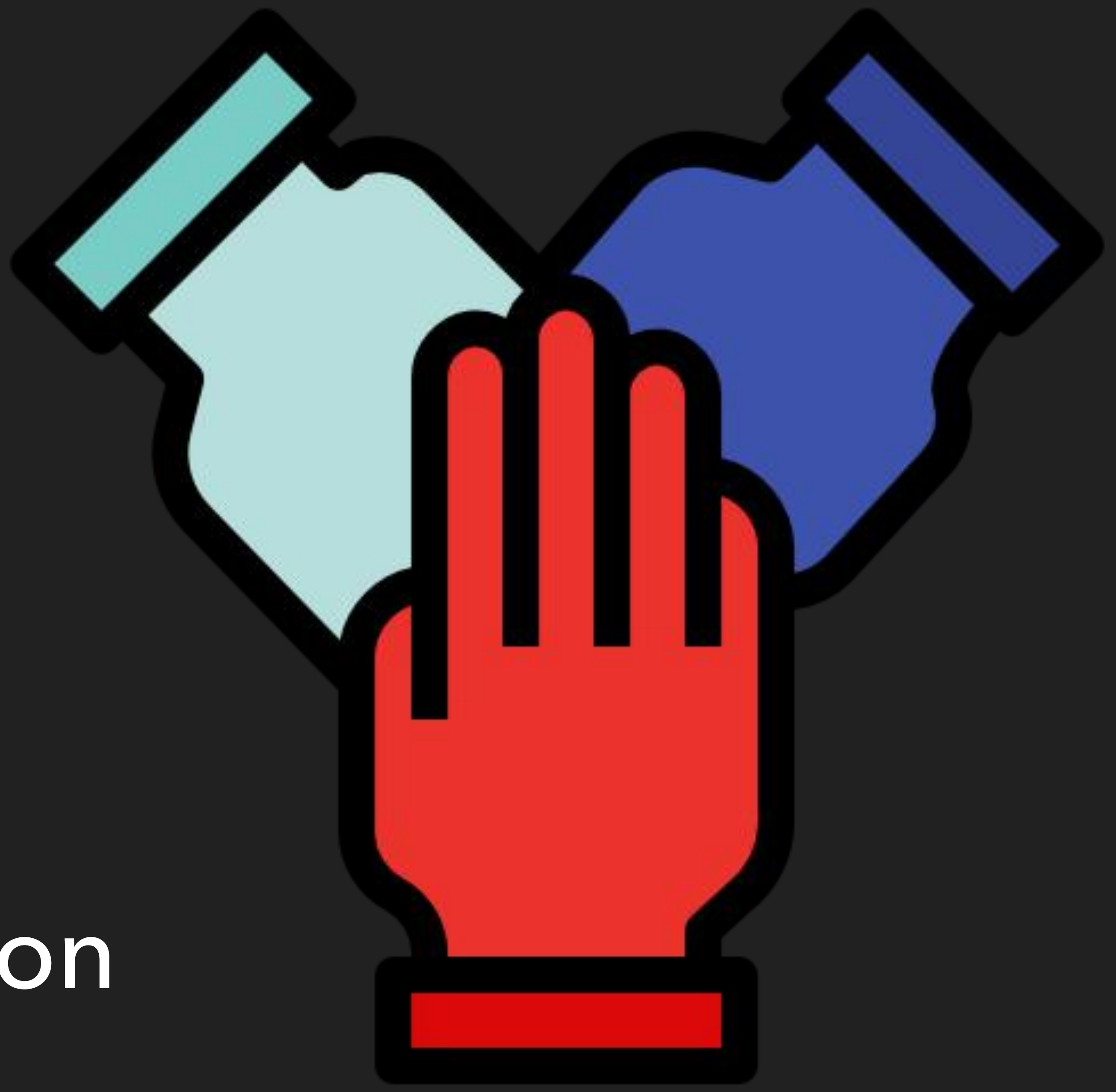
Cryptography

Binary Exploitation

Web Applications

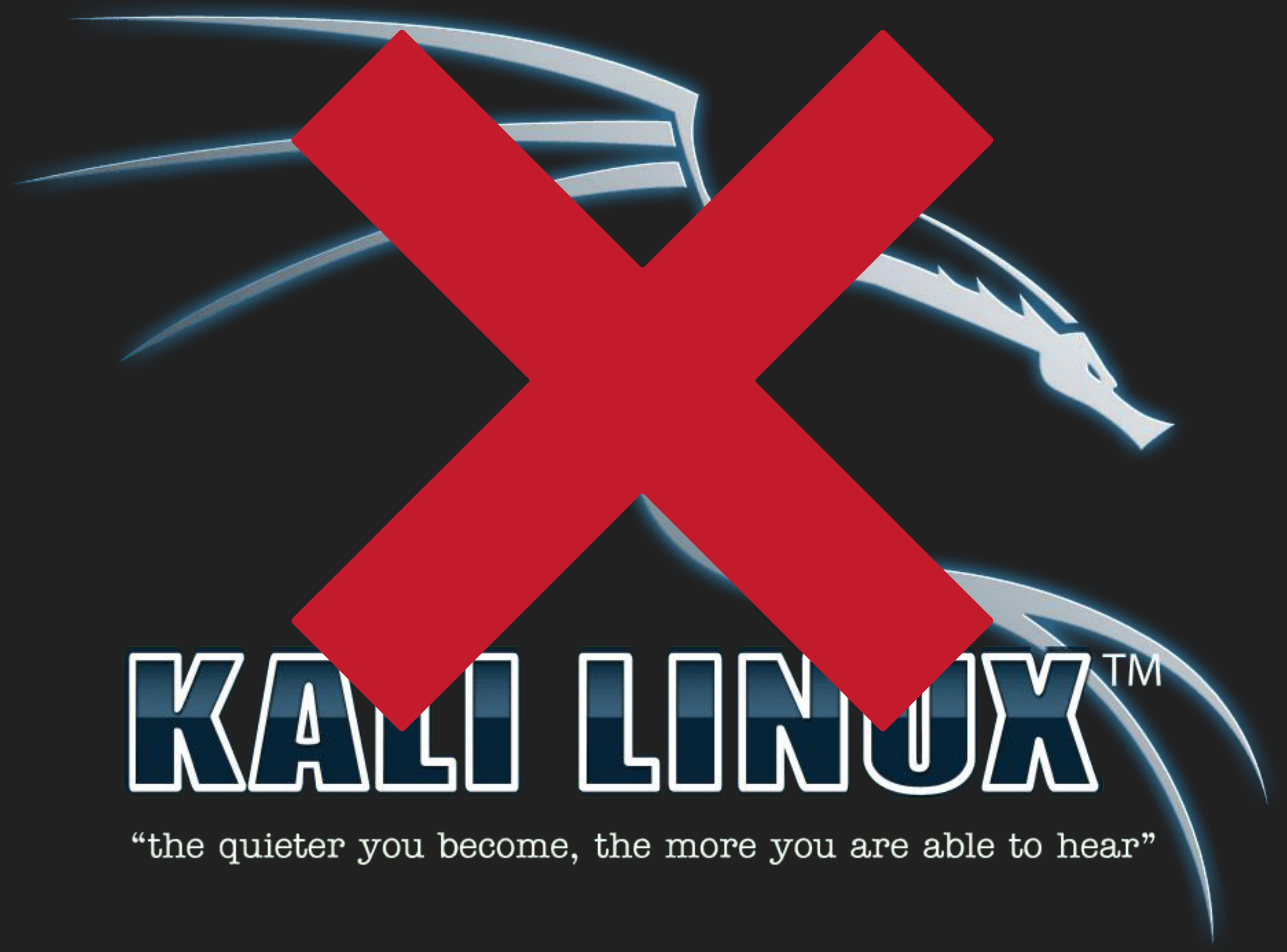
System Administration

Forensics

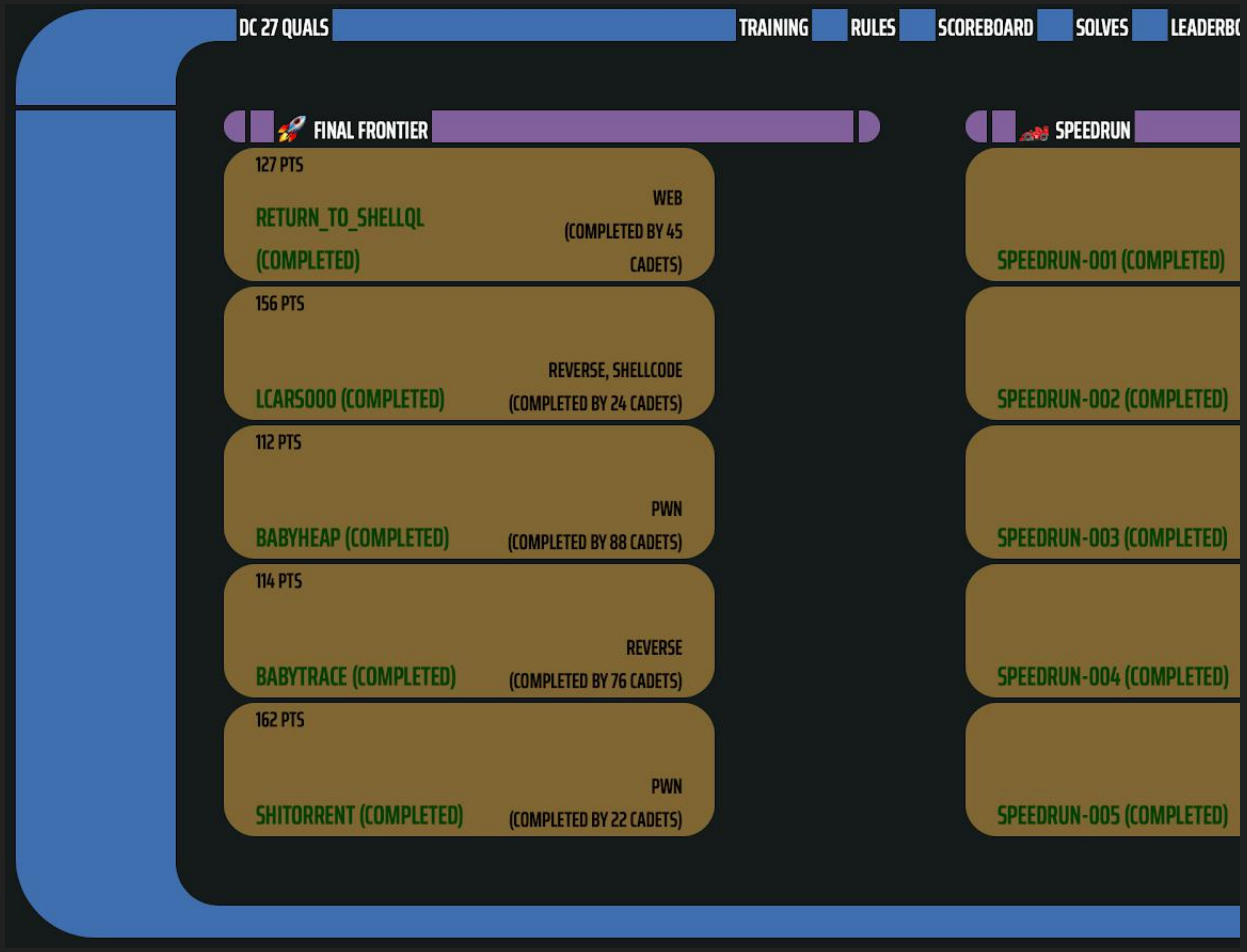


DESIGNING GOOD CHALLENGES

- Focus on some specific vulnerability/ies
- Hardly no bruteforcing required
- No guessing
- Non-exploitable via automatic tools (pff, script kiddies…)



THERE ARE TWO TYPES OF CTFS



127 PTS
RETURN_TO_SHELLQL (COMPLETED)
WEB (COMPLETED BY 45 CADETS)

156 PTS
LCARS000 (COMPLETED)
REVERSE, SHELLCODE (COMPLETED BY 24 CADETS)

112 PTS
BABYHEAP (COMPLETED)
PWN (COMPLETED BY 88 CADETS)

114 PTS
BABYTRACE (COMPLETED)
REVERSE (COMPLETED BY 76 CADETS)

162 PTS
SHITORRENT (COMPLETED)
PWN (COMPLETED BY 22 CADETS)

SPEEDRUN-001 (COMPLETED)

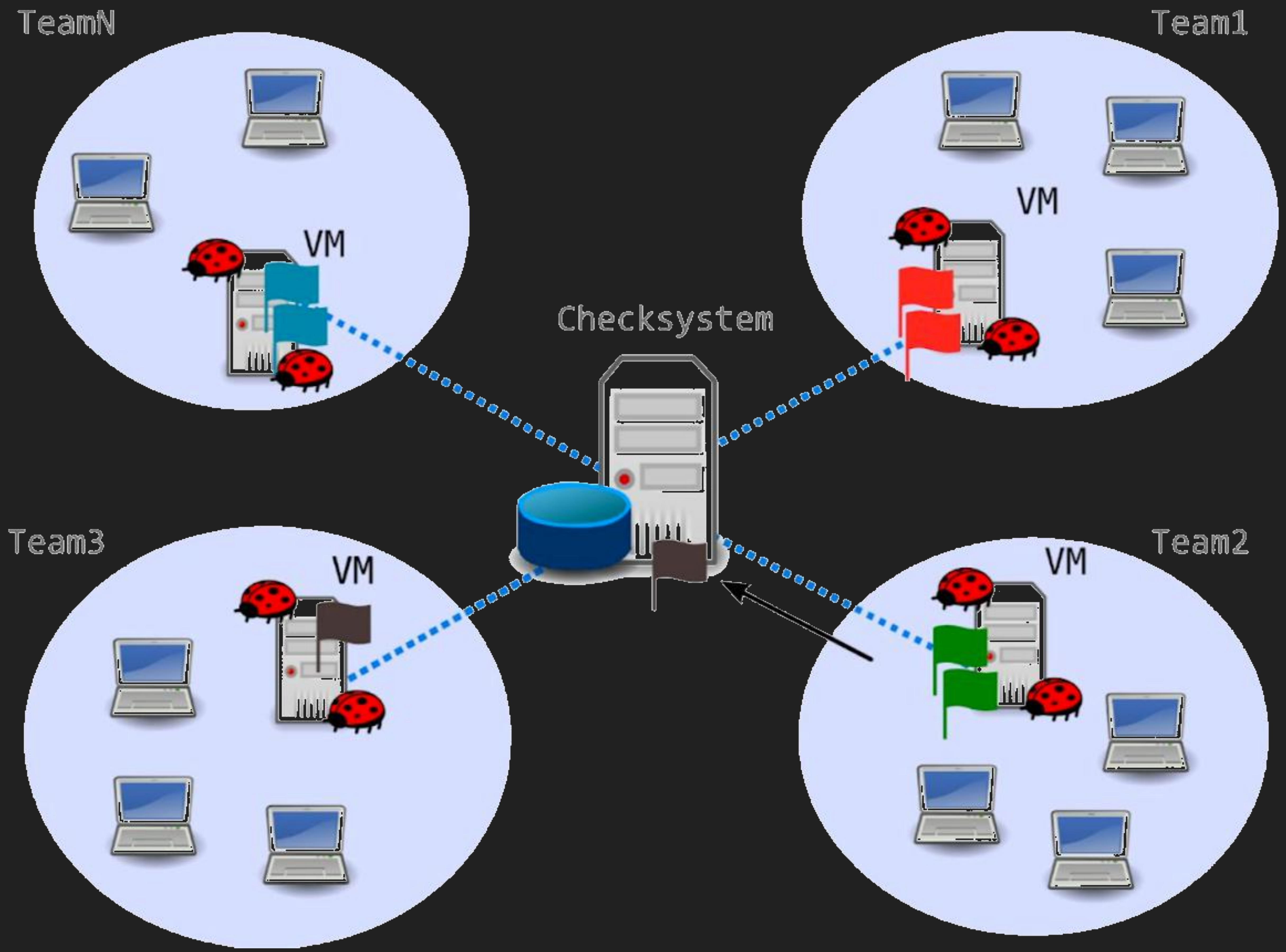
SPEEDRUN-002 (COMPLETED)

SPEEDRUN-003 (COMPLETED)

SPEEDRUN-004 (COMPLETED)

SPEEDRUN-005 (COMPLETED)

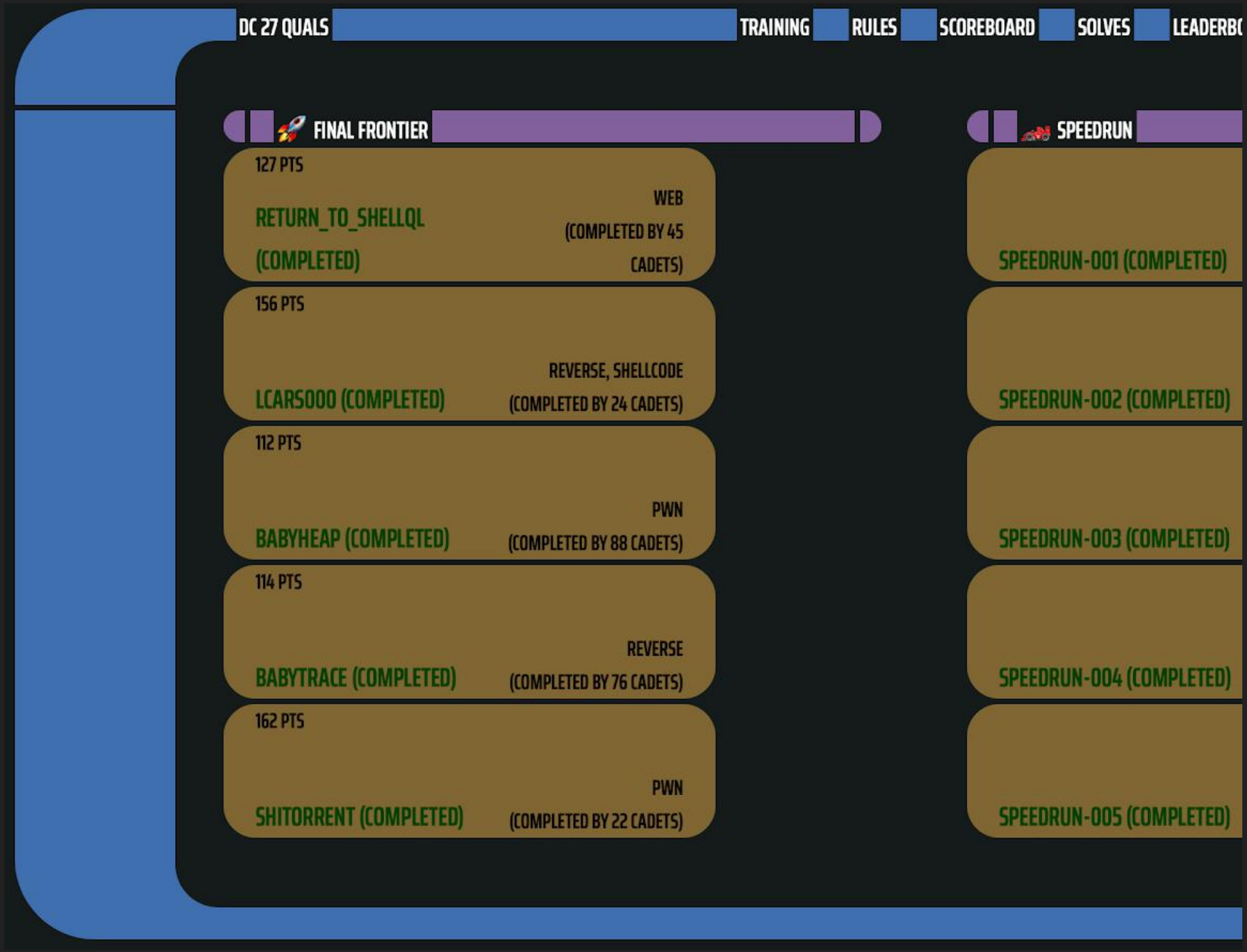
Jeopardy



Attack & Defense

JEOPARDY

- Cathegories
- All vs one!
- Last ~48h
- No need to patch



FINAL FRONTIER

127 PTS
RETURN_TO_SHELLQL (COMPLETED)
WEB (COMPLETED BY 45 CADETS)

156 PTS
LCARS000 (COMPLETED)
REVERSE, SHELLCODE (COMPLETED BY 24 CADETS)

112 PTS
BABYHEAP (COMPLETED)
PWN (COMPLETED BY 88 CADETS)

114 PTS
BABYTRACE (COMPLETED)
REVERSE (COMPLETED BY 76 CADETS)

162 PTS
SHITORRENT (COMPLETED)
PWN (COMPLETED BY 22 CADETS)

SPEEDRUN

SPEEDRUN-001 (COMPLETED)

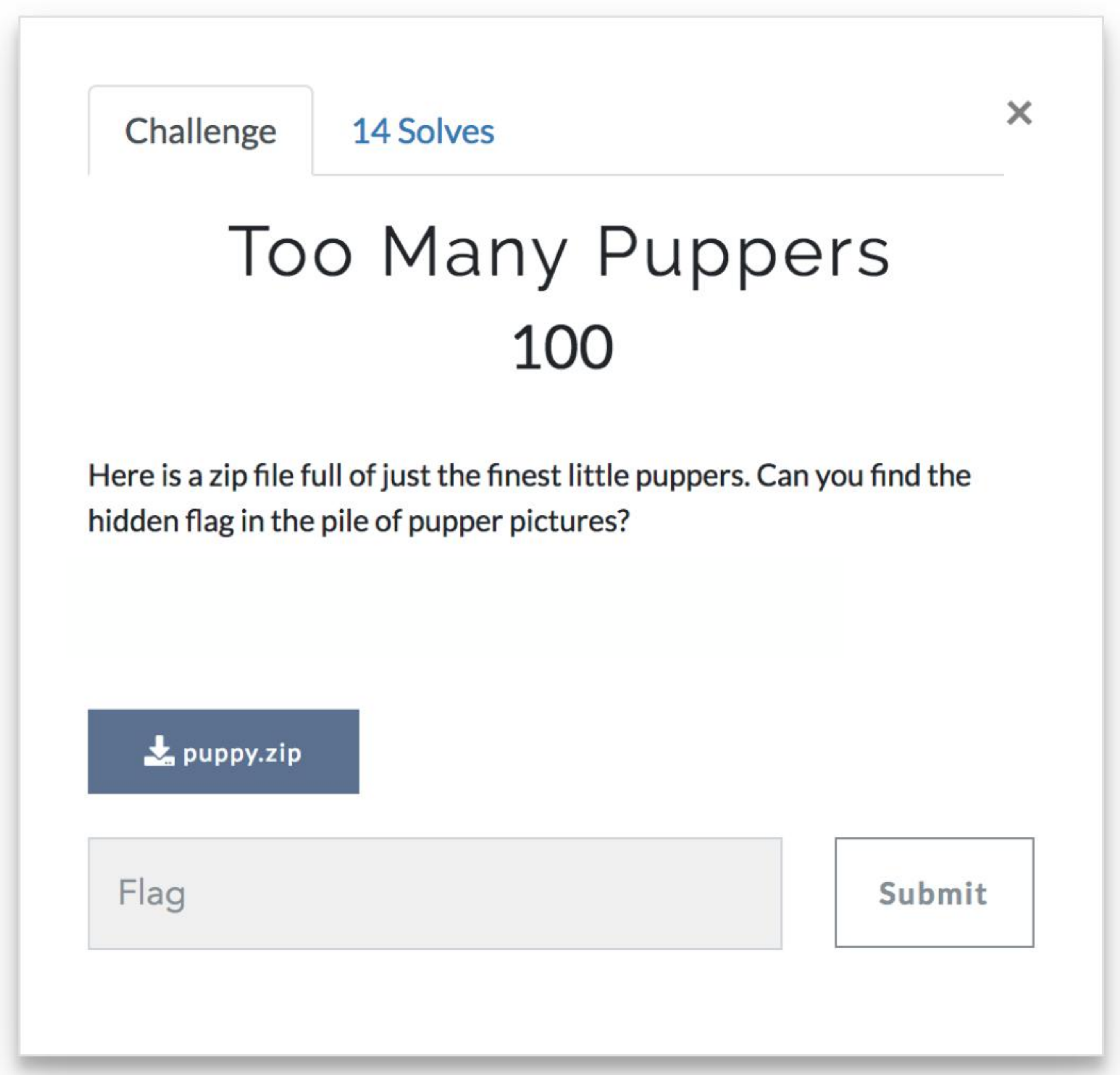
SPEEDRUN-002 (COMPLETED)

SPEEDRUN-003 (COMPLETED)

SPEEDRUN-004 (COMPLETED)

SPEEDRUN-005 (COMPLETED)

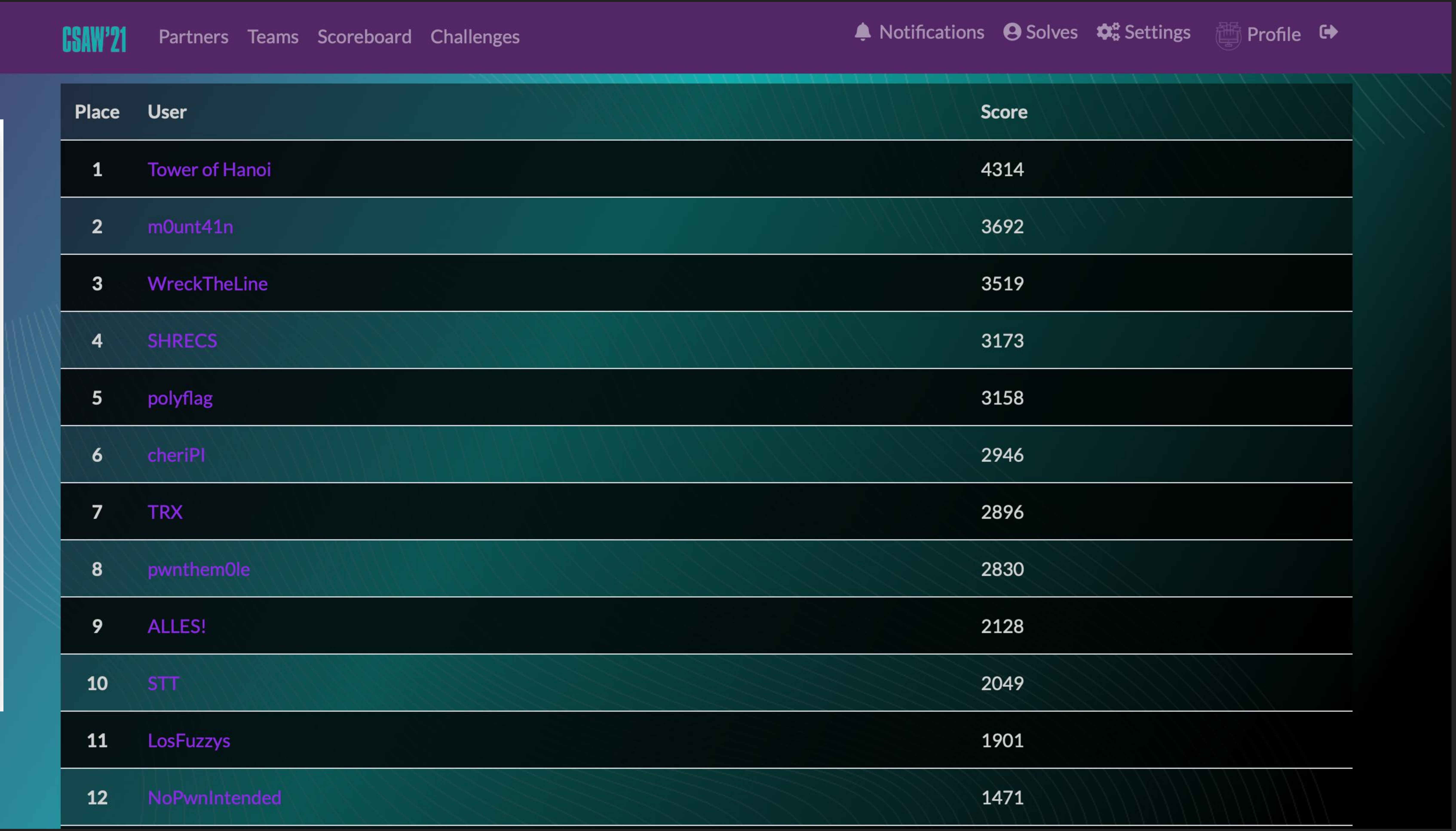
SCORING



Too Many Puppers

100

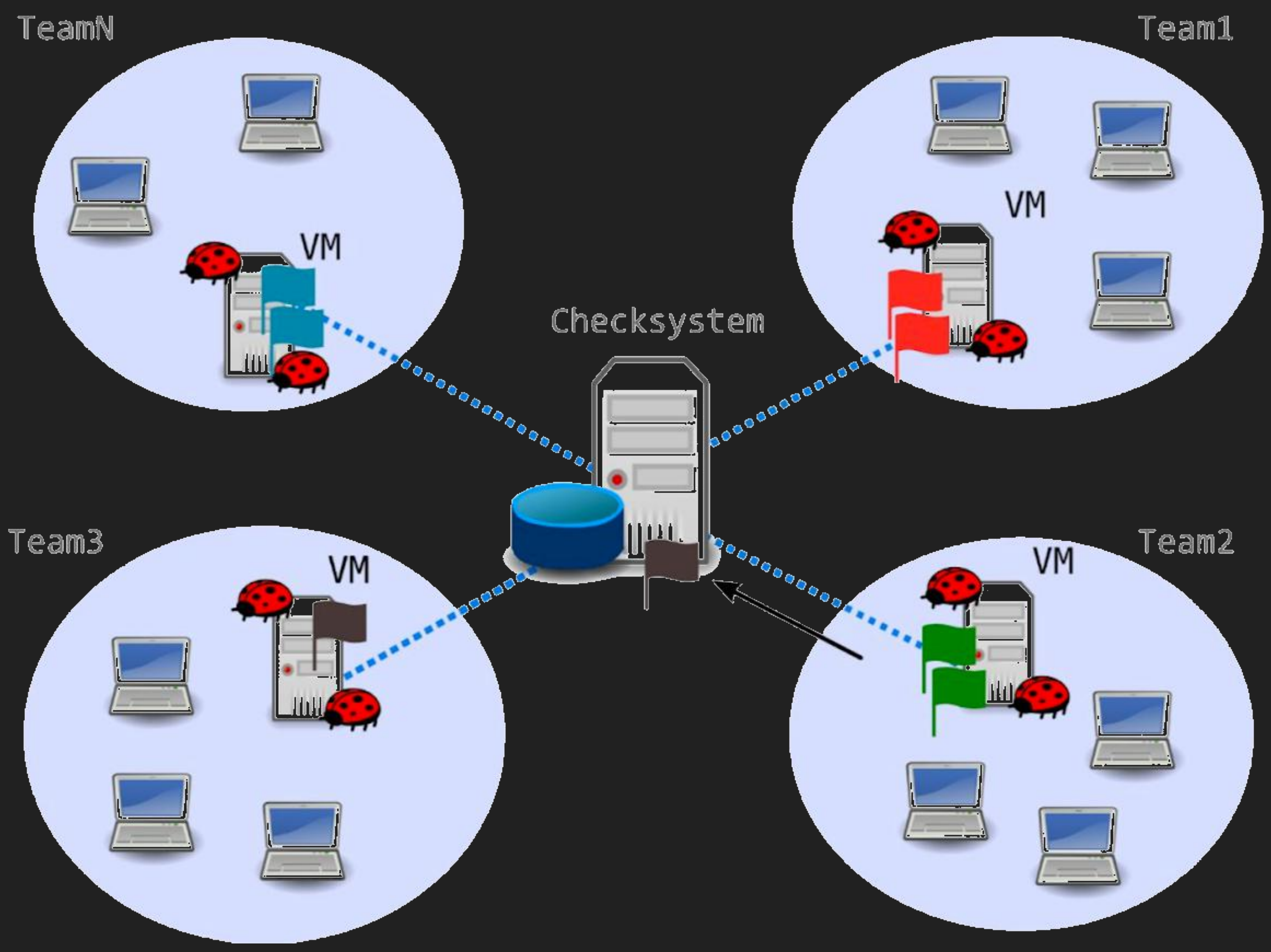
Here is a zip file full of just the finest little puppers. Can you find the hidden flag in the pile of pupper pictures?



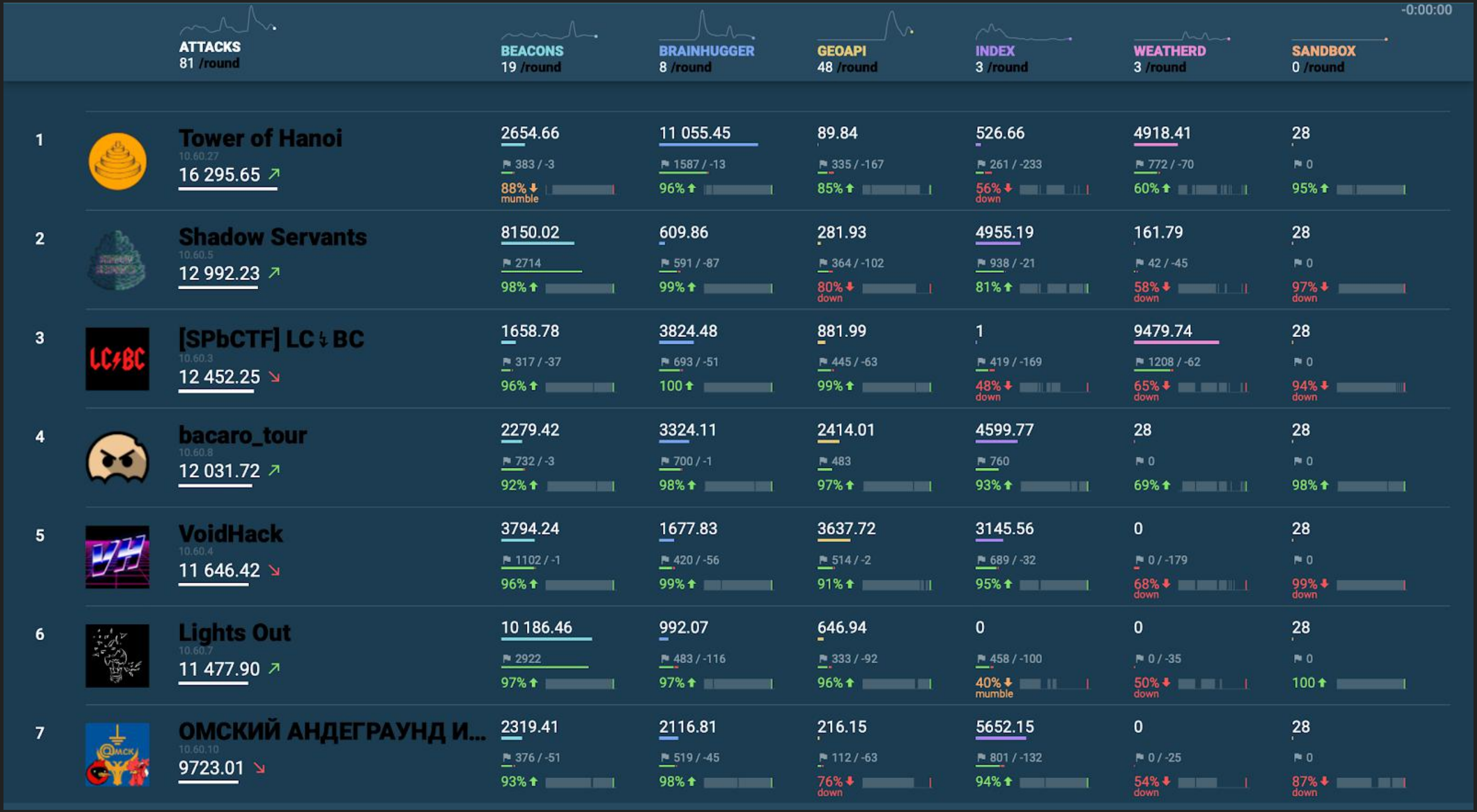
Place	User	Score
1	Tower of Hanoi	4314
2	m0unt41n	3692
3	WreckTheLine	3519
4	SHRECS	3173
5	polyflag	3158
6	cheriPI	2946
7	TRX	2896
8	pwnthem0le	2830
9	ALLES!	2128
10	STT	2049
11	LosFuzzys	1901
12	NoPwnIntended	1471

ATTACK AND DEFENSE

- All vs all!
- Last ~8h
- Need to patch
- Attacks each 'tick'
- Need tools



SCORING



-0:00:00

	ATTACKS 81 /round	BEACONS 19 /round	BRAINHUGGER 8 /round	GEOAPI 48 /round	INDEX 3 /round	WEATHERD 3 /round	SANDBOX 0 /round
1	Tower of Hanoi 10.60.27 16 295.65 ↗	2654.66 ⚑ 383 / -3 88% ↓ mumble	11 055.45 ⚑ 1587 / -13 96% ↑	89.84 ⚑ 335 / -167 85% ↑	526.66 ⚑ 261 / -233 56% ↓ down	4918.41 ⚑ 772 / -70 60% ↑	28 ⚑ 0 95% ↑
2	Shadow Servants 10.60.5 12 992.23 ↗	8150.02 ⚑ 2714 98% ↑	609.86 ⚑ 591 / -87 99% ↑	281.93 ⚑ 364 / -102 80% ↓ down	4955.19 ⚑ 938 / -21 81% ↑	161.79 ⚑ 42 / -45 58% ↓ down	28 ⚑ 0 97% ↓ down
3	[SPbCTF] LC↯BC 10.60.3 12 452.25 ↘	1658.78 ⚑ 317 / -37 96% ↑	3824.48 ⚑ 693 / -51 100 ↑	881.99 ⚑ 445 / -63 99% ↑	1 ⚑ 419 / -169 48% ↓ down	9479.74 ⚑ 1208 / -62 65% ↓ down	28 ⚑ 0 94% ↓ down
4	bacaro_tour 10.60.8 12 031.72 ↗	2279.42 ⚑ 732 / -3 92% ↑	3324.11 ⚑ 700 / -1 98% ↑	2414.01 ⚑ 483 97% ↑	4599.77 ⚑ 760 93% ↑	28 ⚑ 0 69% ↑	28 ⚑ 0 98% ↑
5	VoidHack 10.60.4 11 646.42 ↘	3794.24 ⚑ 1102 / -1 96% ↑	1677.83 ⚑ 420 / -56 99% ↑	3637.72 ⚑ 514 / -2 91% ↑	3145.56 ⚑ 689 / -32 95% ↑	0 ⚑ 0 / -179 68% ↓ down	28 ⚑ 0 99% ↓ down
6	Lights Out 10.60.7 11 477.90 ↗	10 186.46 ⚑ 2922 97% ↑	992.07 ⚑ 483 / -116 97% ↑	646.94 ⚑ 333 / -92 96% ↑	0 ⚑ 458 / -100 40% ↓ mumble	0 ⚑ 0 / -35 50% ↓ down	28 ⚑ 0 100 ↑
7	ОМСКИЙ АНДЕГРАУНД И... 10.60.10 9723.01 ↘	2319.41 ⚑ 376 / -51 93% ↑	2116.81 ⚑ 519 / -45 98% ↑	216.15 ⚑ 112 / -63 76% ↓ down	5652.15 ⚑ 801 / -132 94% ↑	0 ⚑ 0 / -25 54% ↓ down	28 ⚑ 0 87% ↓ down

TEAM ORGANIZATION (A & D)

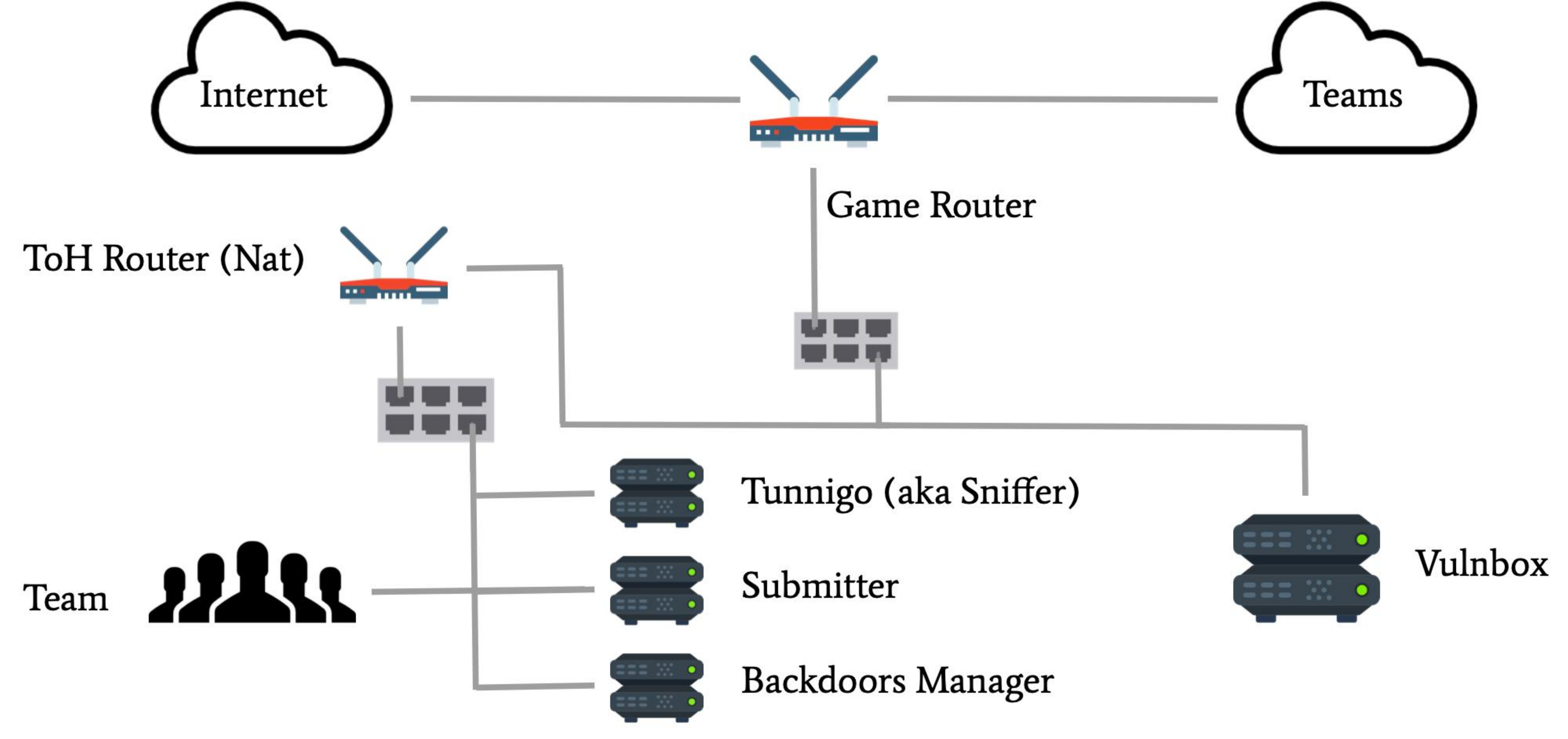
Sysadmins

(❤ Poul)

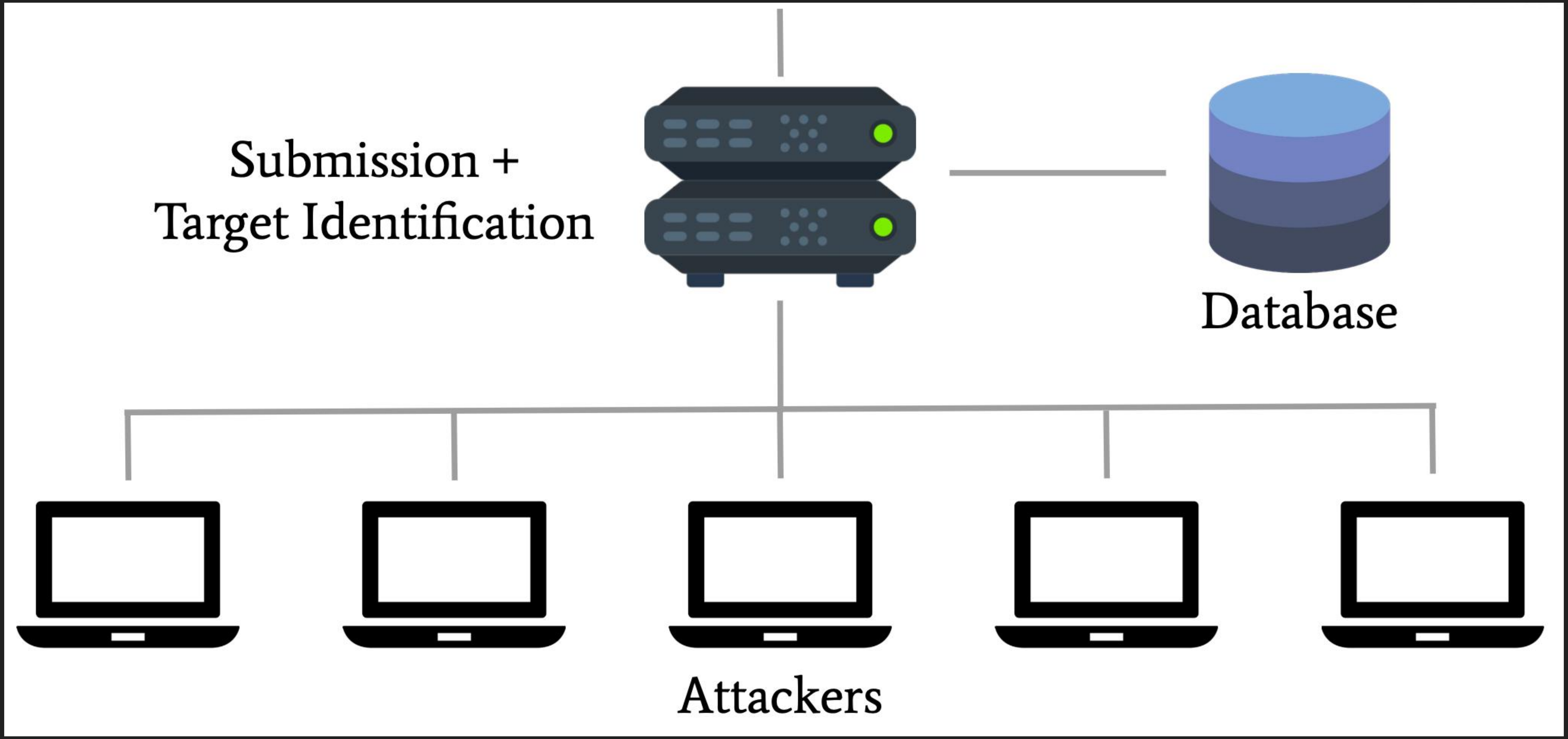
Challenge Solvers

Tool Dev/Deployers

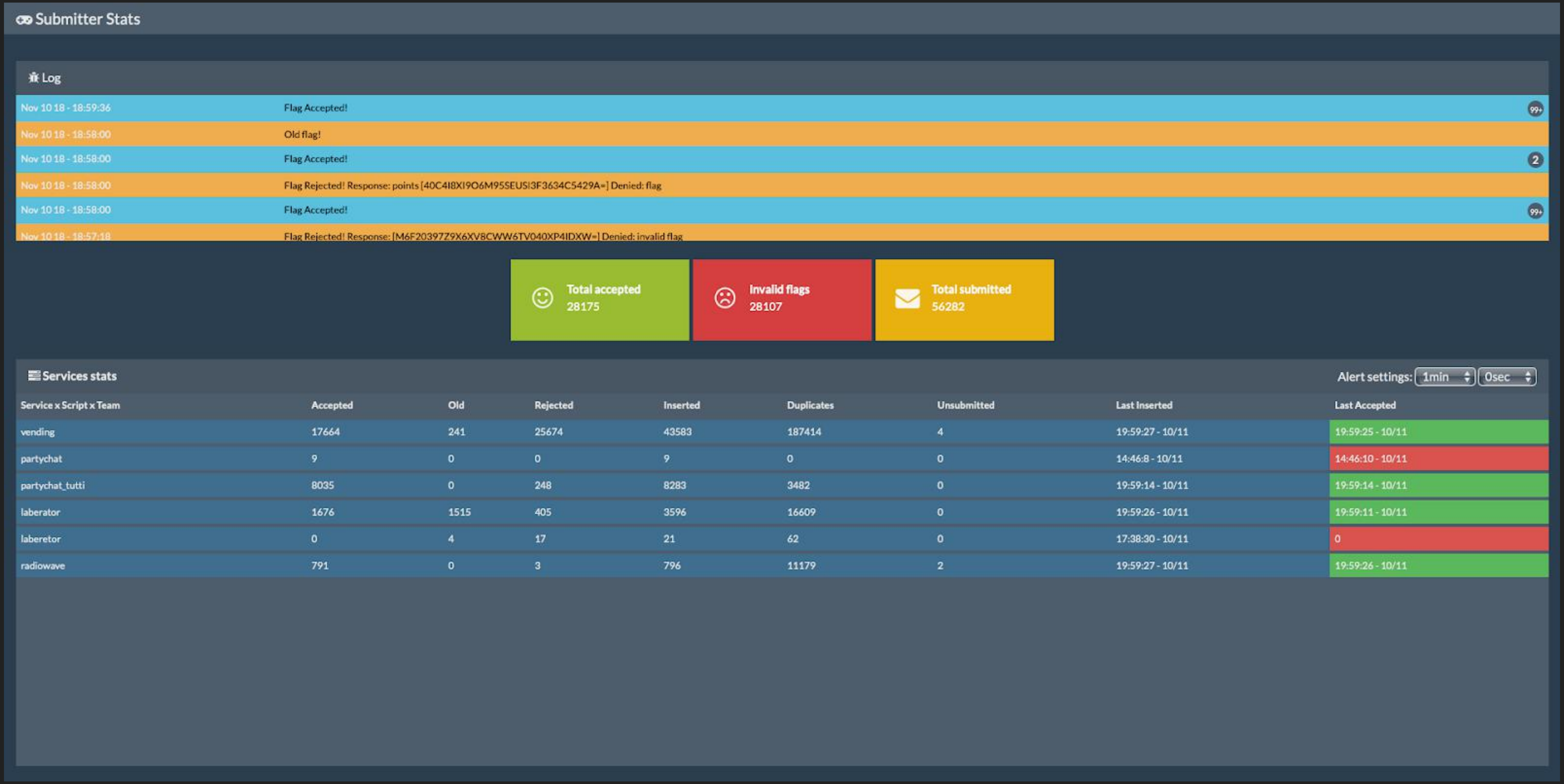
INFRASTRUCTURE AND TOOLS



SUBMITTING FLAGS



SUBMITTING FLAGS



Submitter Stats

Log

```
Nov 10 18 - 18:59:36    Flag Accepted!                                                                    99+
Nov 10 18 - 18:58:00    Old flag!
Nov 10 18 - 18:58:00    Flag Accepted!                                                                    2
Nov 10 18 - 18:58:00    Flag Rejected! Response: points [40C4I8XI9O6M95SEUSI3F3634C5429A=] Denied: flag
Nov 10 18 - 18:58:00    Flag Accepted!                                                                    99+
Nov 10 18 - 18:57:18    Flag Rejected! Response: [M6F20397Z9X6XV8CWW6TV040XP4IDXW=] Denied: invalid flag
```

Total accepted 28175

Invalid flags 28107

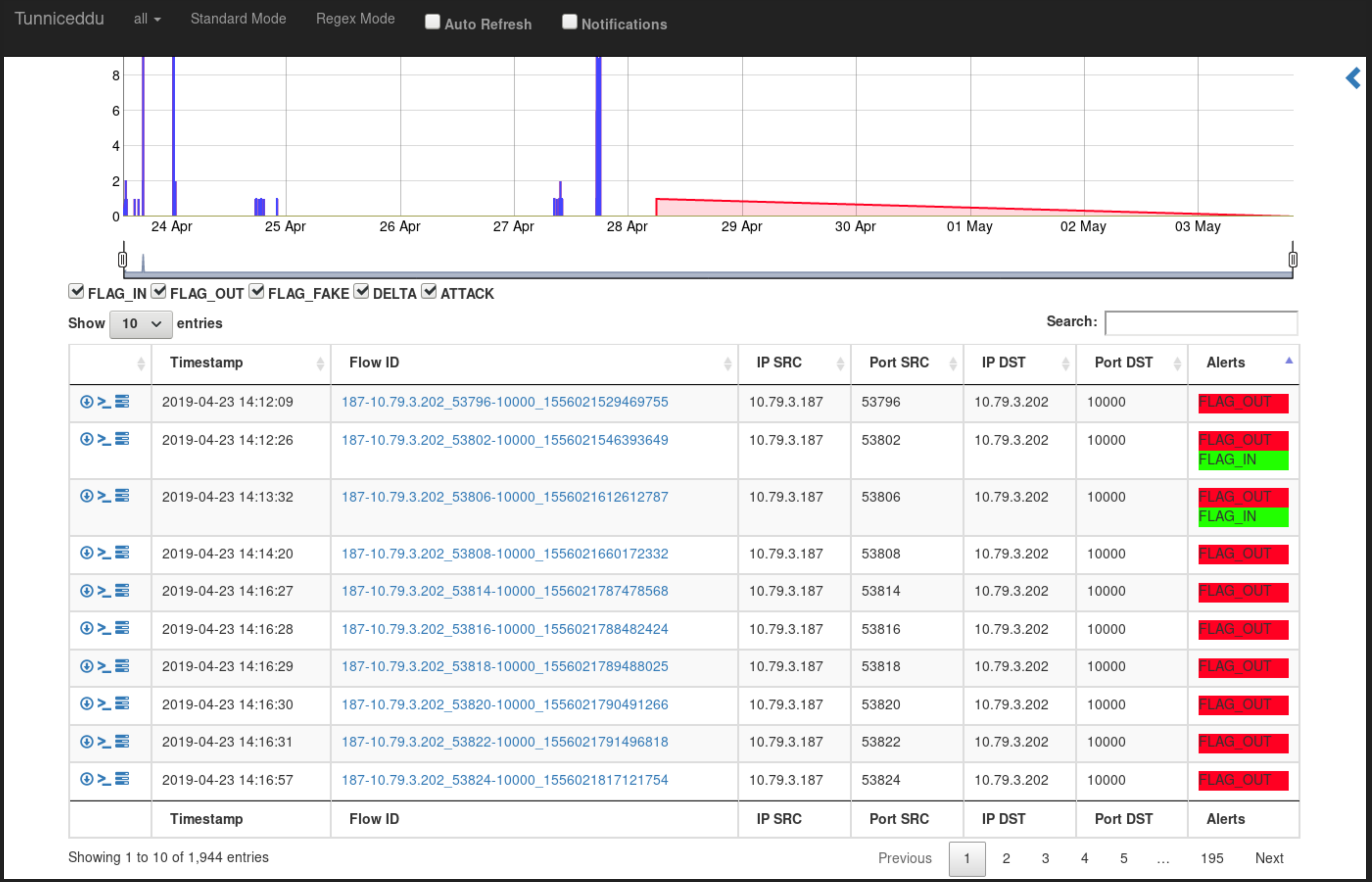
Total submitted 56282

Services stats

Alert settings: 1min 0sec

Service x Script x Team	Accepted	Old	Rejected	Inserted	Duplicates	Unsubmitted	Last Inserted	Last Accepted
vending	17664	241	25674	43583	187414	4	19:59:27 - 10/11	19:59:25 - 10/11
partychat	9	0	0	9	0	0	14:46:8 - 10/11	14:46:10 - 10/11
partychat_tutti	8035	0	248	8283	3482	0	19:59:14 - 10/11	19:59:14 - 10/11
laberator	1676	1515	405	3596	16609	0	19:59:26 - 10/11	19:59:11 - 10/11
laberetor	0	4	17	21	62	0	17:38:30 - 10/11	0
radiowave	791	0	3	796	11179	2	19:59:27 - 10/11	19:59:26 - 10/11

NETWORK ANALYSIS



□ Auto Refresh □ Notifications

☑ FLAG_IN ☑ FLAG_OUT ☑ FLAG_FAKE ☑ DELTA ☑ ATTACK

Show 10 entries

Search:

	Timestamp	Flow ID	IP SRC	Port SRC	IP DST	Port DST	Alerts
	2019-04-23 14:12:09	187-10.79.3.202_53796-10000_1556021529469755	10.79.3.187	53796	10.79.3.202	10000	FLAG_OUT
	2019-04-23 14:12:26	187-10.79.3.202_53802-10000_1556021546393649	10.79.3.187	53802	10.79.3.202	10000	FLAG_OUT FLAG_IN
	2019-04-23 14:13:32	187-10.79.3.202_53806-10000_1556021612612787	10.79.3.187	53806	10.79.3.202	10000	FLAG_OUT FLAG_IN
	2019-04-23 14:14:20	187-10.79.3.202_53808-10000_1556021660172332	10.79.3.187	53808	10.79.3.202	10000	FLAG_OUT
	2019-04-23 14:16:27	187-10.79.3.202_53814-10000_1556021787478568	10.79.3.187	53814	10.79.3.202	10000	FLAG_OUT
	2019-04-23 14:16:28	187-10.79.3.202_53816-10000_1556021788482424	10.79.3.187	53816	10.79.3.202	10000	FLAG_OUT
	2019-04-23 14:16:29	187-10.79.3.202_53818-10000_1556021789488025	10.79.3.187	53818	10.79.3.202	10000	FLAG_OUT
	2019-04-23 14:16:30	187-10.79.3.202_53820-10000_1556021790491266	10.79.3.187	53820	10.79.3.202	10000	FLAG_OUT
	2019-04-23 14:16:31	187-10.79.3.202_53822-10000_1556021791496818	10.79.3.187	53822	10.79.3.202	10000	FLAG_OUT
	2019-04-23 14:16:57	187-10.79.3.202_53824-10000_1556021817121754	10.79.3.187	53824	10.79.3.202	10000	FLAG_OUT
	Timestamp	Flow ID	IP SRC	Port SRC	IP DST	Port DST	Alerts

Showing 1 to 10 of 1,944 entries

Previous 1 2 3 4 5 … 195 Next

BACKDOORING

Cross-compilation
Encrypted communication
& more evil stuff

PWNING SINCE 2004

UCSB iCTF winners in 2004 and 2005.

PWNING SINCE 2004

(2011)

(2012)

(2013)

(2015)

RUCTF

(2017)

(2018)

(2019)

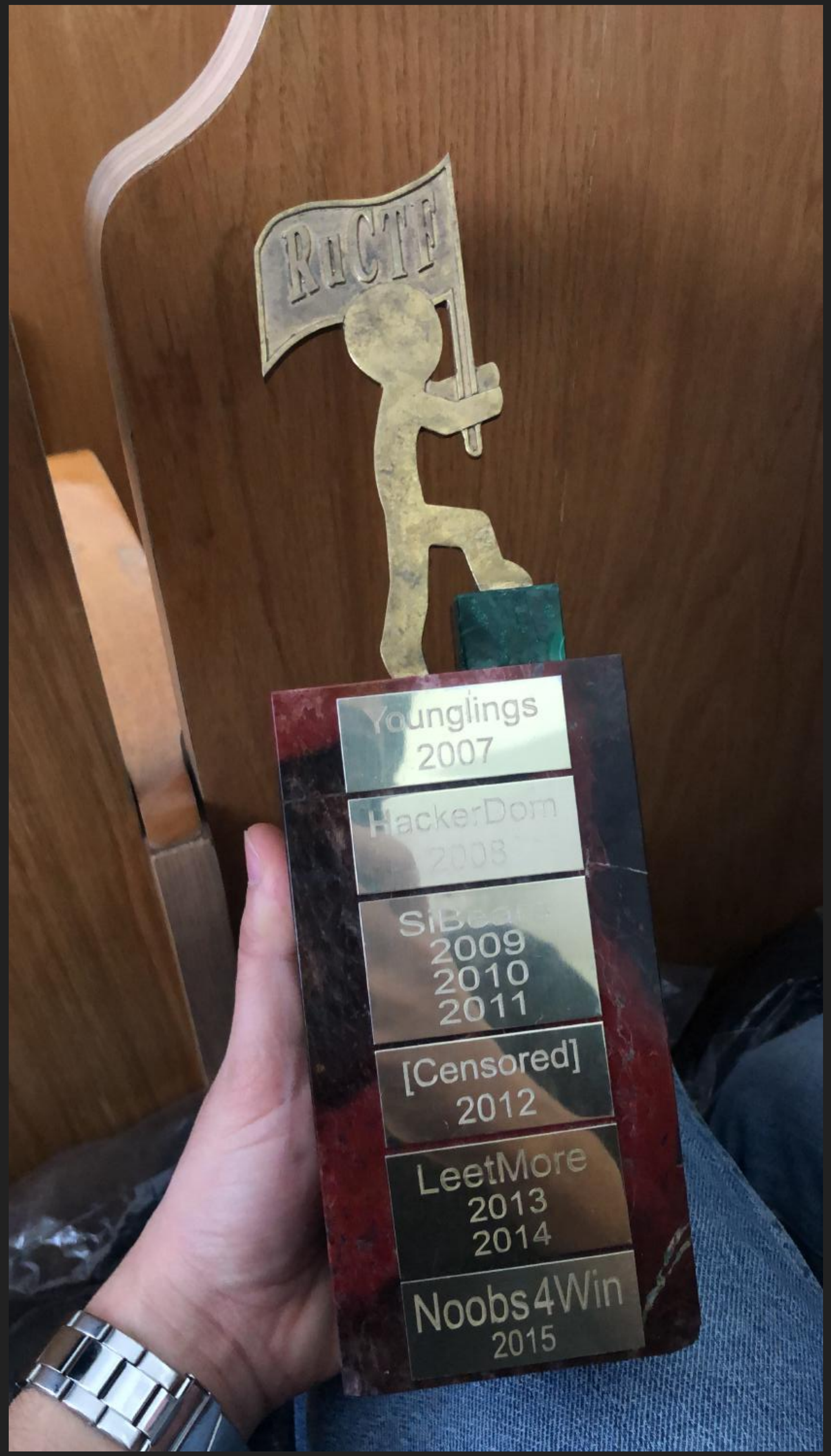
Ekaterinburg, Russia

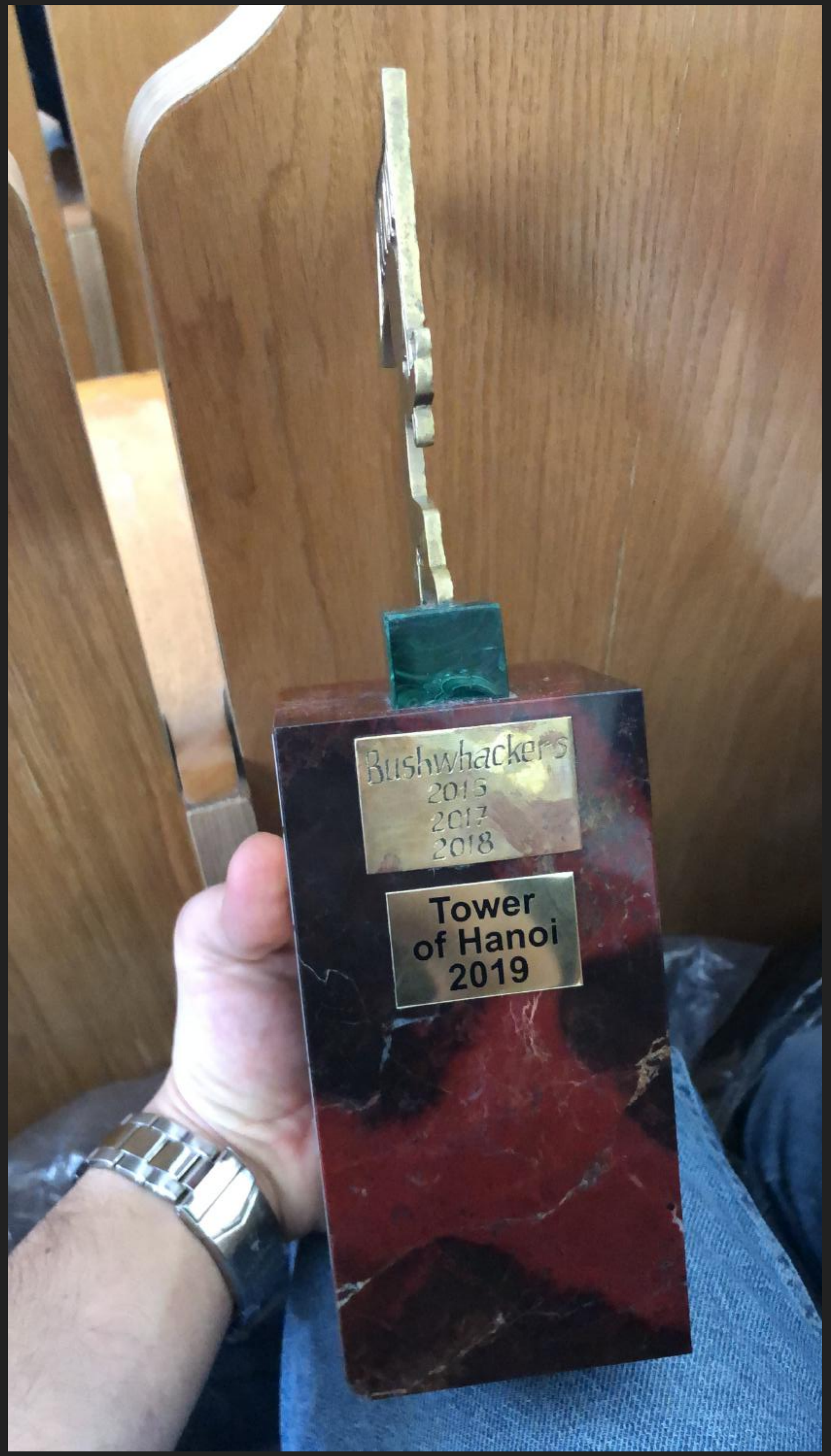
FOR THE FIRST TIME IN 13 YEARS

Ежегодные открытые межвузовские
соревнования и конференция
по информационной безопасности
2019
RuCTF

(2019)

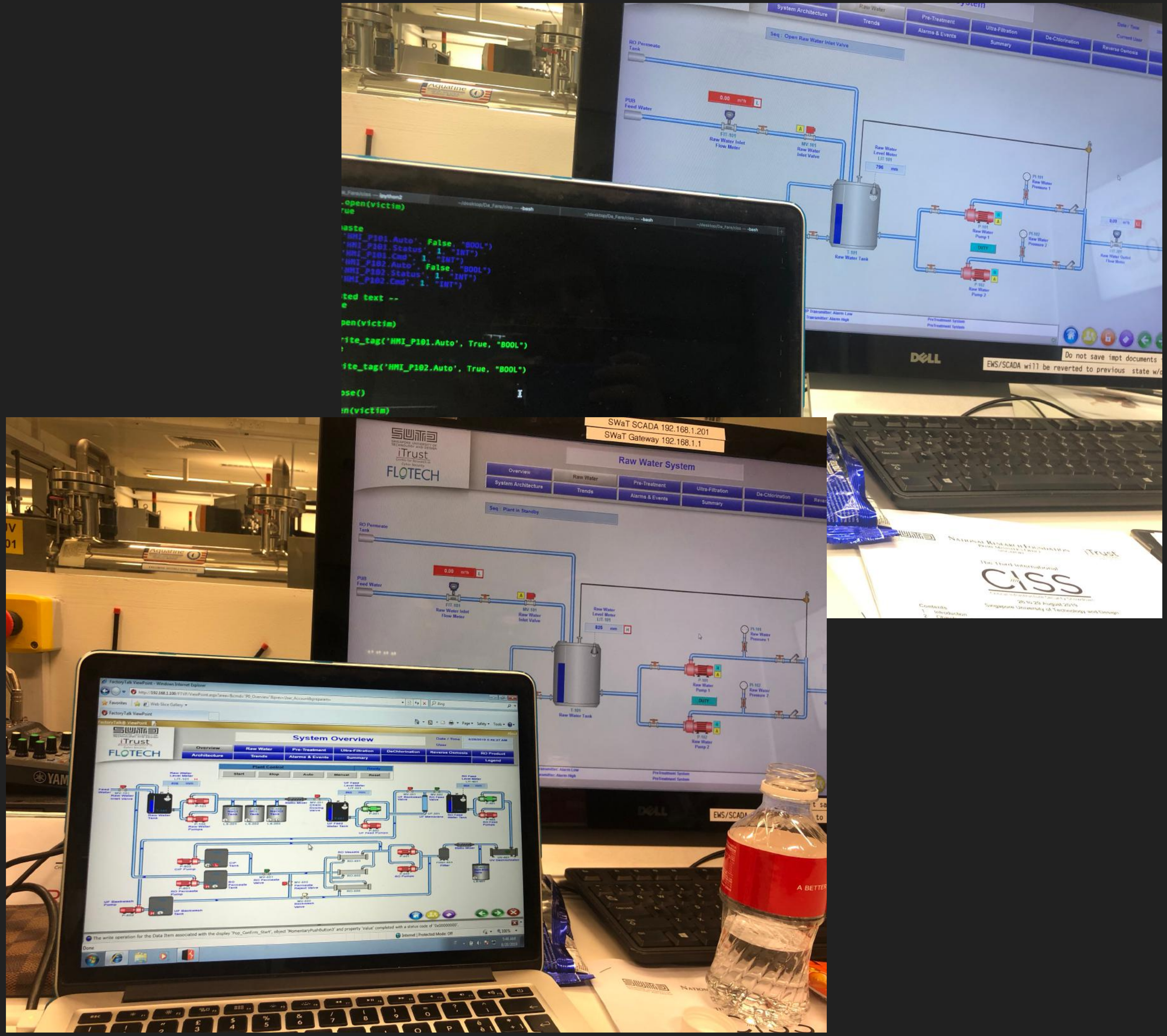
WHOPS…


RuCTF
Younglings
2007
HackerDom
2008
SiBears
2009
2010
2011
[Censored]
2012
LeetMore
2013
2014
Noobs4Win
2015


Bushwhackers
2016
2017
2018
Tower
of Hanoi
2019

NOT ONLY CTFS… HACKING PLANTS IN SINGAPORE!

SUTD University, Singapore



```
.open(victim)
rue

aste
'HMI_P101.Auto', False, "BOOL")
'HMI_P101.Status', 1, "INT")
'HMI_P101.Cmd', 1, "INT")
'HMI_P102.Auto', False, "BOOL")
'HMI_P102.Status', 1, "INT")
'HMI_P102.Cmd', 1, "INT")

ted text --
e

pen(victim)

rite_tag('HMI_P101.Auto', True, "BOOL")

ite_tag('HMI_P102.Auto', True, "BOOL")

ose()

n(victim)
```

FOLLOWING OUR DREAMS: DEFCON CTF CTF ALSO MEANS COMMUNITY

No age limits. No team size limits.

The most famous CTF of all… Every year in Las Vegas!

Only 15 teams can qualify during the year. More than 1000 teams attempt.

mhackeroni
Italia

Tower of Hanoi
Milano

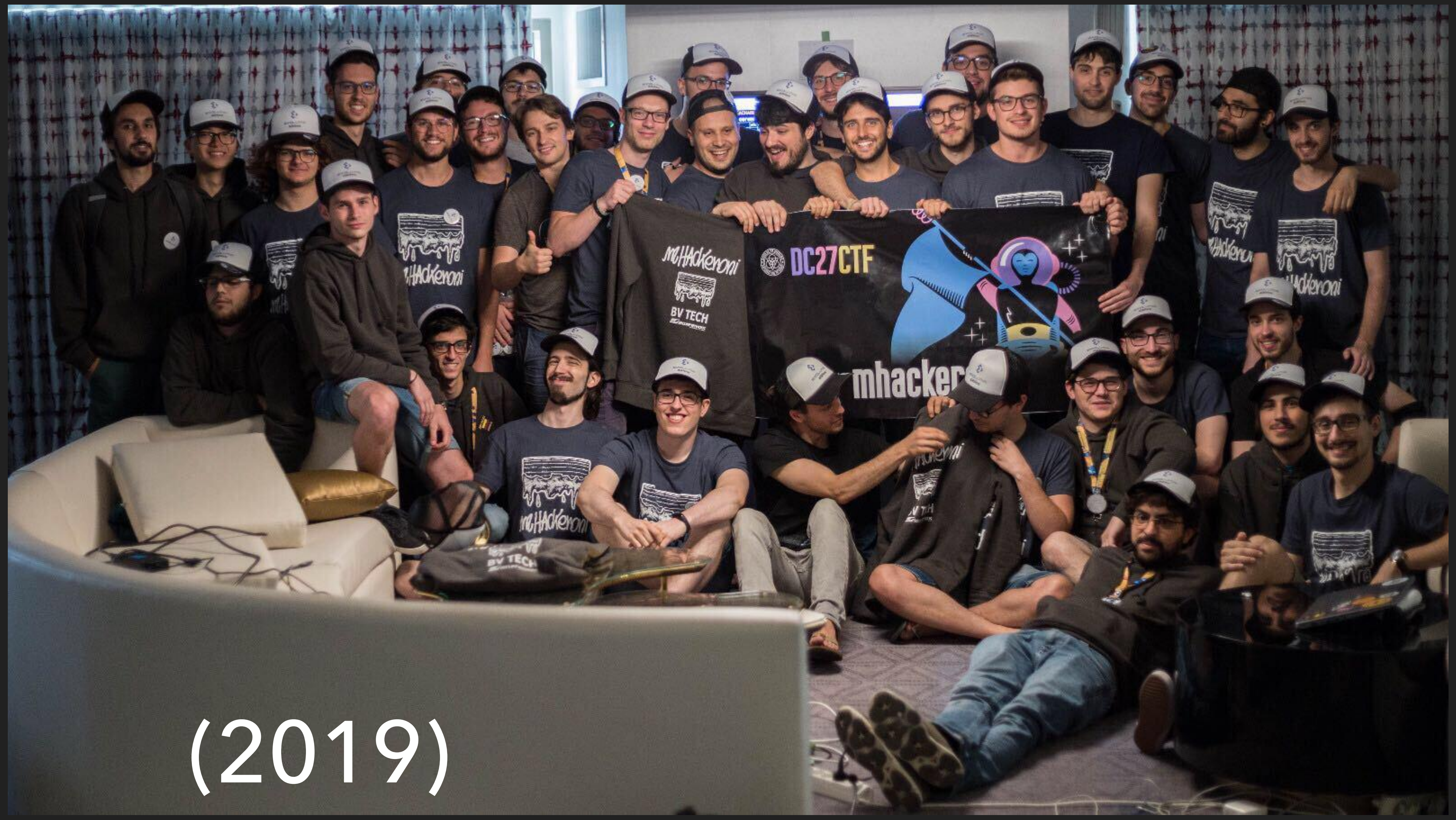
C00kies
Venezia

Spritzers
Padova

The Roman Exploit
Roma

DEFCON CTF

(2018)


(2019)

We managed to play 4 DEFCON CTFs. From 2018 till today.

WONDERING HOW IS IT LIKE?

Las Vegas, Nevada

HOW DO I JOIN TOH?

CYBERCHALLENGE.IT

Free course on infosec.
For 20 young talents

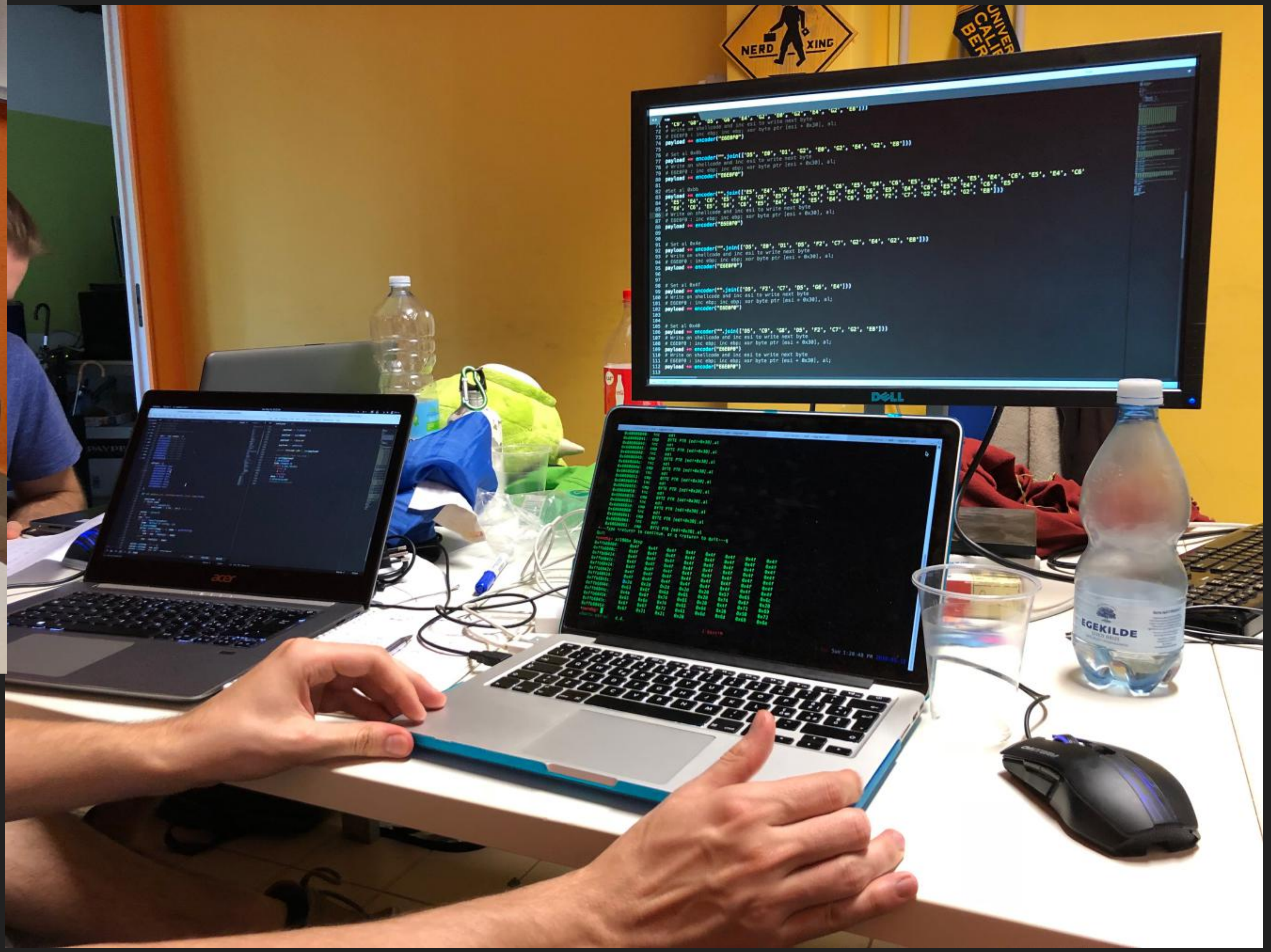
Courses start on the 2nd semester.

Remember how I started? I wish I had this opportunity back then!

Enroll now! Registration open from 02/11/2021 to 14/01/2022.
https://cyberchallenge.it

HACKMEETINGS

We meet every Saturday
here at Polimi in room 3.1.5
We train by playing CTFs, join us!



WE ALSO HAVE A DISCORD SERVER!

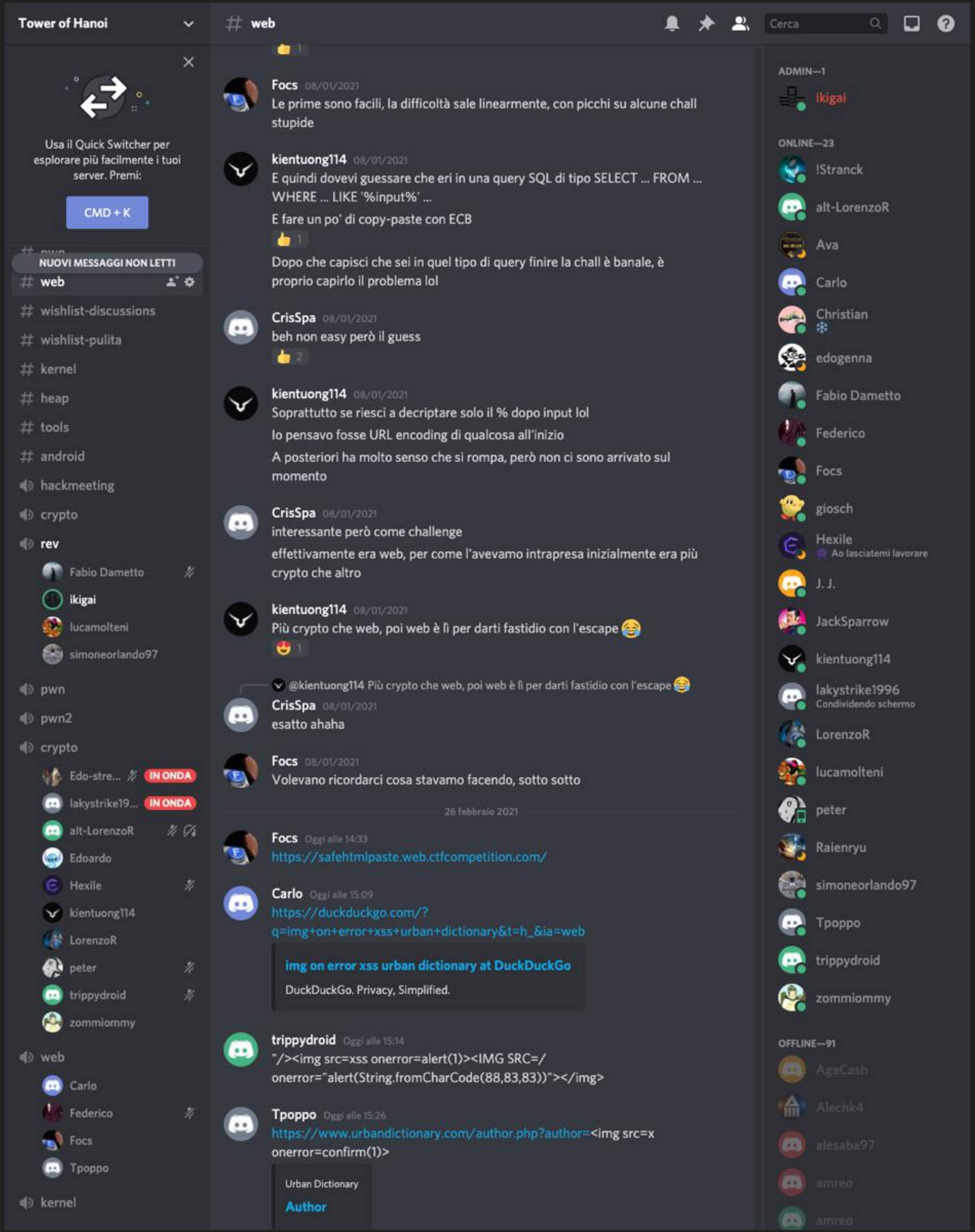
Send us an email at toh@necst.it
to get an invitation!

CONTACT US

HTTPS://TOH.NECST.IT

@TOWEROFHANOI

TOH@NECST.IT



Tower of Hanoi

Usa il Quick Switcher per esplorare più facilmente i tuoi server. Premi:

CMD + K

pwn

NUOVI MESSAGGI NON LETTI

web
wishlist-discussions
wishlist-pulita
kernel
heap
tools
android
hackmeeting
crypto
rev
- Fabio Dametto
- ikigai
- lucamolteni
- simoneorlando97

pwn
pwn2
crypto
- Edo-stre... IN ONDA
- lakystrike19... IN ONDA
- alt-LorenzoR
- Edoardo
- Hexile
- kientuong114
- LorenzoR
- peter
- trippydroid
- zommiommy

web
- Carlo
- Federico
- Focs
- Tpoppo

kernel

web

👍 1

Focs 08/01/2021
Le prime sono facili, la difficoltà sale linearmente, con picchi su alcune chall stupide

kientuong114 08/01/2021
E quindi dovevi guessare che eri in una query SQL di tipo SELECT ... FROM ... WHERE ... LIKE '%input%' ...
E fare un po' di copy-paste con ECB
👍 1
Dopo che capisci che sei in quel tipo di query finire la chall è banale, è proprio capirlo il problema lol

CrisSpa 08/01/2021
beh non easy però il guess
👍 2

kientuong114 08/01/2021
Soprattutto se riesci a decriptare solo il % dopo input lol
Io pensavo fosse URL encoding di qualcosa all'inizio
A posteriori ha molto senso che si rompa, però non ci sono arrivato sul momento

CrisSpa 08/01/2021
interessante però come challenge
effettivamente era web, per come l'avevamo intrapresa inizialmente era più crypto che altro

kientuong114 08/01/2021
Più crypto che web, poi web è lì per darti fastidio con l'escape 😂
😍 1

@kientuong114 Più crypto che web, poi web è lì per darti fastidio con l'escape 😂
CrisSpa 08/01/2021
esatto ahaha

Focs 08/01/2021
Volevano ricordarci cosa stavamo facendo, sotto sotto

26 febbraio 2021

Focs Oggi alle 14:33
https://safehtmlpaste.web.ctfcompetition.com/

Carlo Oggi alle 15:09
https://duckduckgo.com/?q=img+on+error+xss+urban+dictionary&t=h_&ia=web

img on error xss urban dictionary at DuckDuckGo
DuckDuckGo. Privacy, Simplified.

trippydroid Oggi alle 15:14
"/><img src=xss onerror=alert(1)><IMG SRC=/ onerror="alert(String.fromCharCode(88,83,83))"></img>

Tpoppo Oggi alle 15:26
https://www.urbandictionary.com/author.php?author=<img src=x onerror=confirm(1)>

Urban Dictionary
Author

Cerca

ADMIN—1
- ikigai

ONLINE—23
- !Stranck
- alt-LorenzoR
- Ava
- Carlo
- Christian
- edogenna
- Fabio Dametto
- Federico
- Focs
- giosch
- Hexile — Ao lasciatemi lavorare
- J. J.
- JackSparrow
- kientuong114
- lakystrike1996 — Condividendo schermo
- LorenzoR
- lucamolteni
- peter
- Raienryu
- simoneorlando97
- Tpoppo
- trippydroid
- zommiommy

OFFLINE—91
- AgaCash
- Alechk4
- alesaba97
- amreo
- amreo

OK.. BUT HOW DO EXPLOITS HAPPEN?

A TINY BIT…

DEVELOPERS VS ATTACKERS

- Challenge: developers see client as a (cooperative) part of the application

- Developer's Mindset:
  - the user will click on the "Login" button
  - as a result the browser will generate a correct GET request to */login.php?user=foo*
  - the server will process the request
- Attacker's Mindset:
  - we can craft a GET request to send */login.php?user=w|-|4t3v3r* to the server

THE DATA AND CODE PROBLEM

CODE INJECTION PROBLEMS

Conflicting requirements:

- Functional requirement: we need to mix code (e.g., HTML) with data (e.g., the blog comment)
- Security requirement: never mix code and data!!

Consequence: If, at any point, there is a “parsing” routine (e.g., browser’s JavaScript parser) that reacts (e.g., prints something) on some “control sequences” found in data (i.e., no input validation), we have a vulnerability.

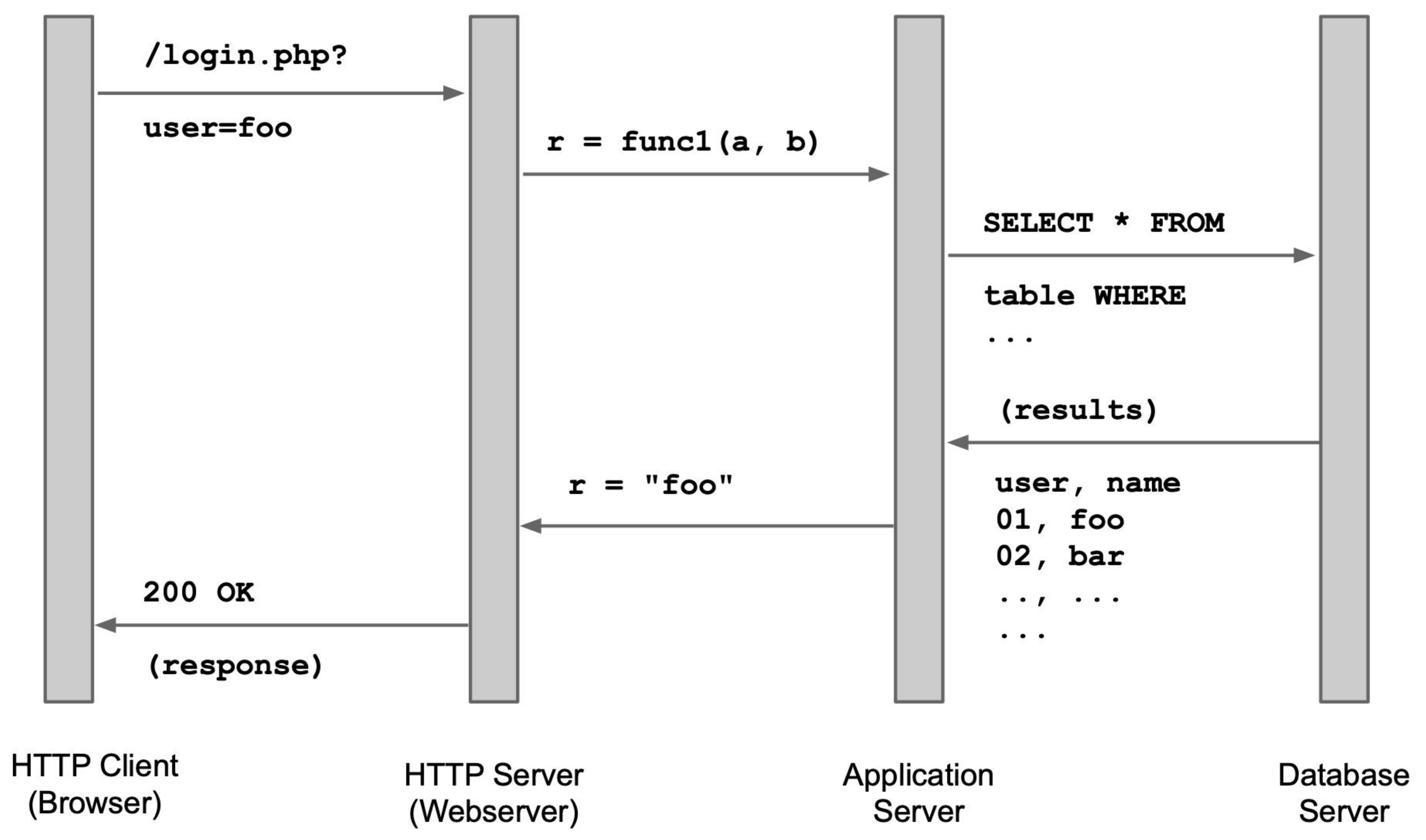
WHAT WILL YOURS SAY?

THE UNTRUSTWORTHY CLIENT

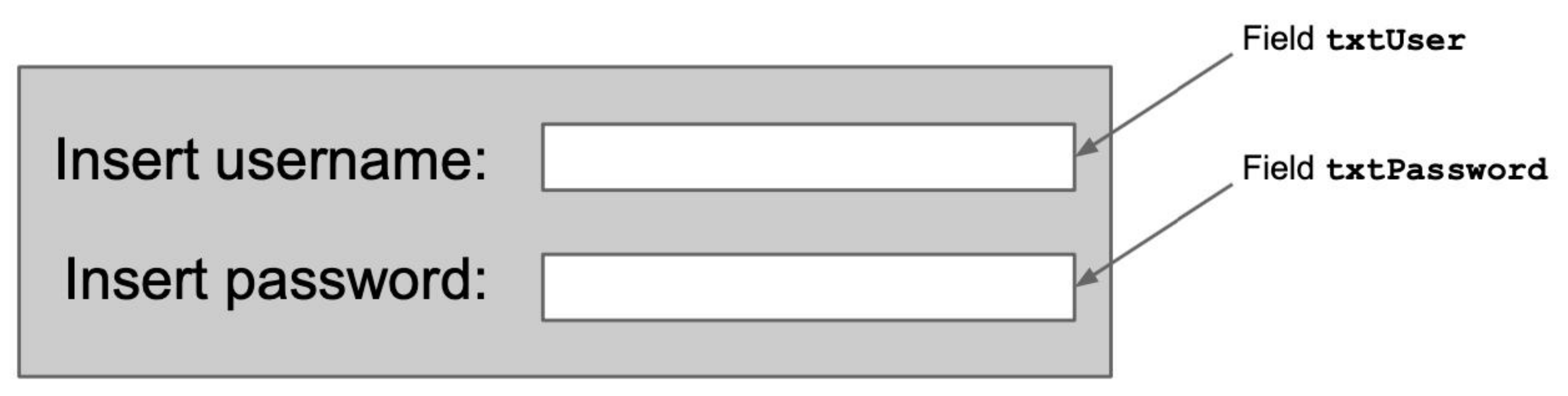
- The golden rule of web application security is that the client is never trustworthy
- We need to filter and check carefully anything that is sent to us (server)

- Examples:
  - We cannot validate inputs on the client side e.g., through JavaScript
  - Variables, such as REFERRER or USER-AGENT, that the client is sending us, can lie…

THREE-TIER WEB APPLICATION ARCHITECTURE



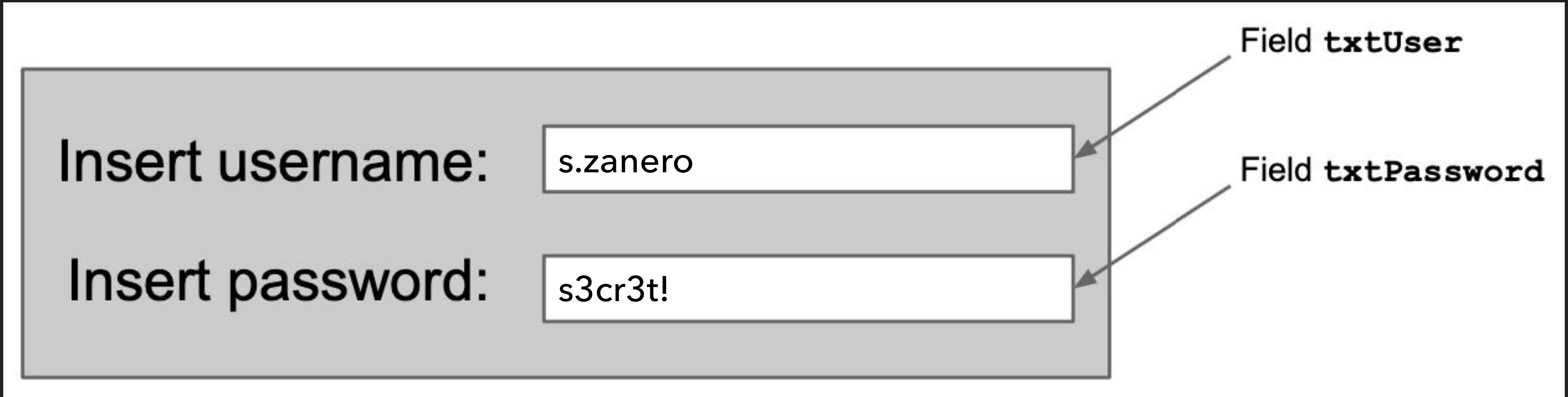
A SIMPLE LOGIN EXAMPLE…



LET'S LOOK AT THE SERVER-SIDE CODE

```
public void onLogon(Field txtUser, Field txtPassword) {
  SqlCommand cmd = new SqlCommand(String.Format(
    "SELECT * FROM Users
    WHERE username='{0}'
     AND password='{1}';",
     txtUser.Text, txtPassword.Text));

   SqlDataReader reader = cmd.ExecuteReader();



   if(reader.HasRows())
     IssueAuthenticationTicket();
   else
     RedirectToErrorPage();

}
```

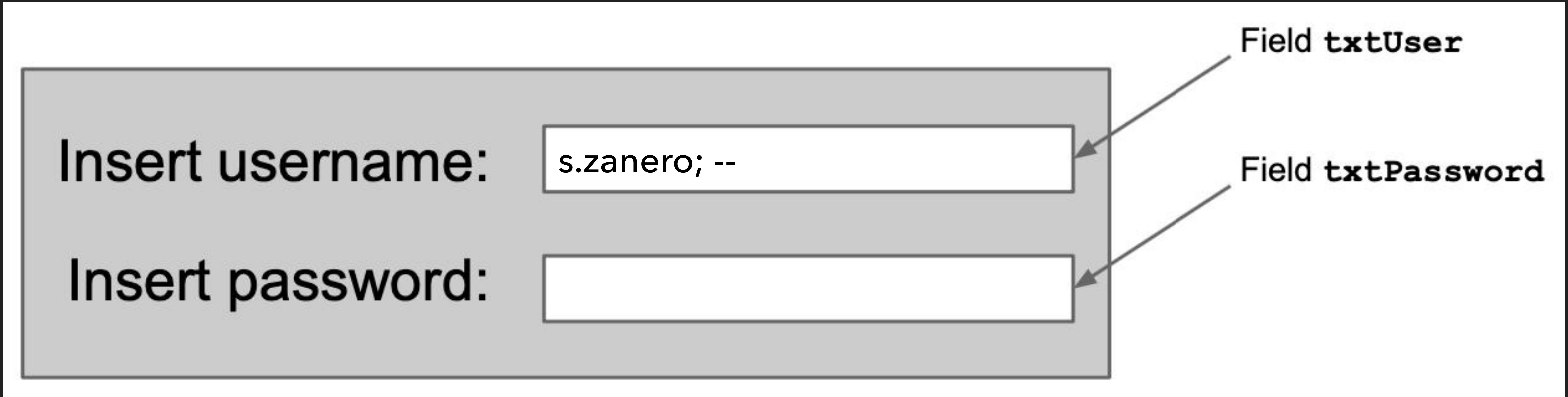
WHAT THE PROGRAMMER THOUGHT



SELECT * FROM Users WHERE username=‘s.zanero' AND password=‘s3cr3t!'

This query gets executed and if it returns at least one row the user is granted access

WHAT THE HACKER SEES



Insert username: s.zanero; --

Insert password:

Field txtUser

Field txtPassword

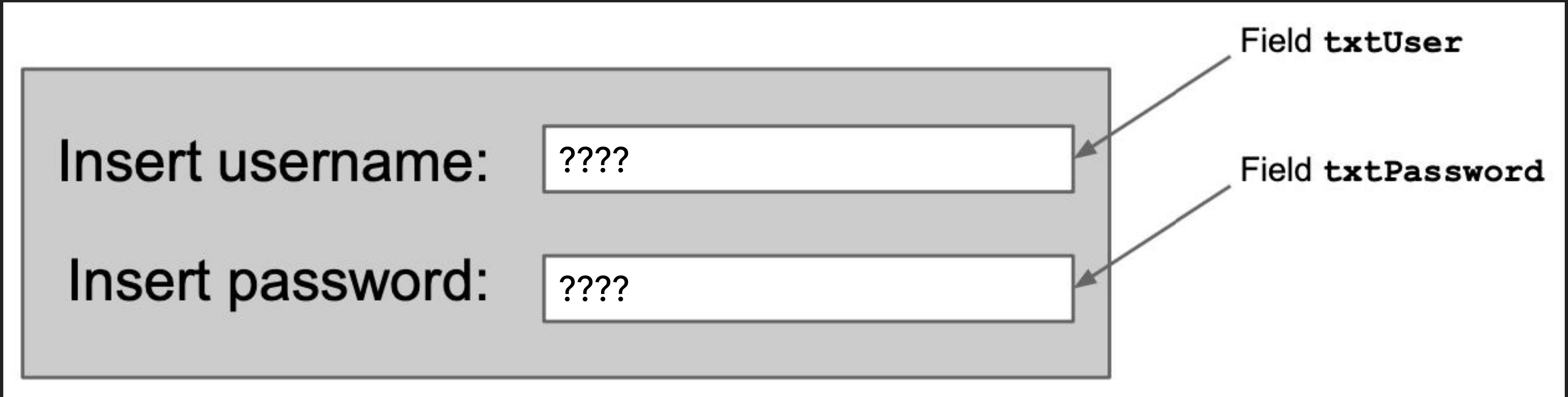
SELECT * FROM Users WHERE username=’s.zanero’; -- ’ AND password=’’

-- means “comment”

This query gets executed and if the users exists, it returns at least one row regardless of the password. Our attacker is granted access.

Beware: some DBMS, e.g., MySQL, have a slightly different comment syntax

WHAT IF YOU DON'T KNOW A VALID USER?

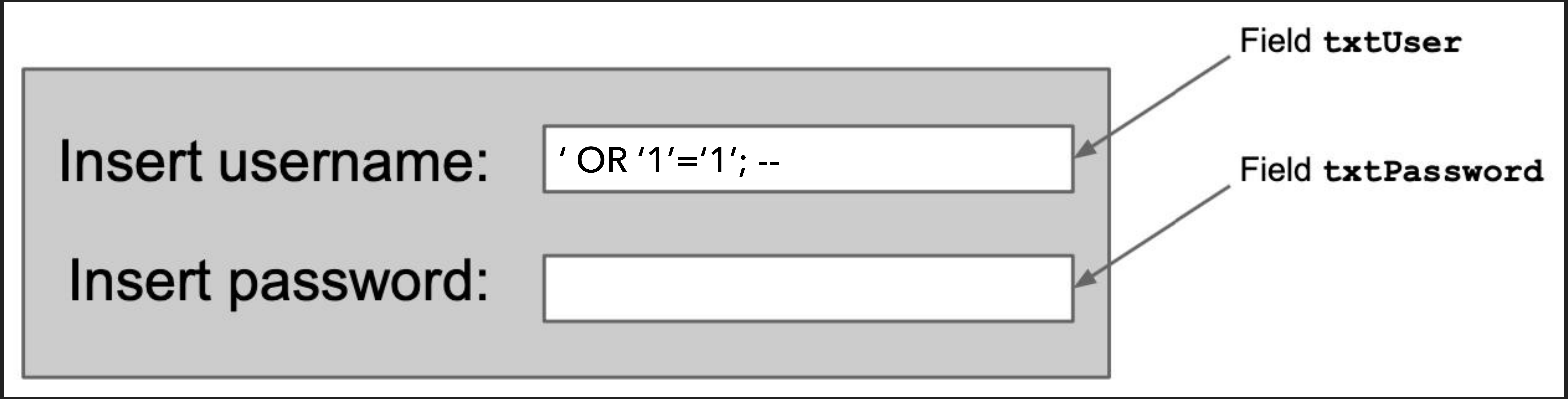


Insert username: ????

Insert password: ????

SELECT * FROM Users WHERE username='?' AND password='?'

WHAT IF YOU DON’T KNOW A VALID USER?



Insert username: ’ OR ‘1’=‘1’; --

Insert password:

SELECT * FROM Users WHERE username=’’ OR ‘1’=‘1’; -- ’ AND password=’’

This query gets executed and the second part of the OR is always true; returns all rows, which is more tha one, and our attacker is granted access

HANDS ON

https://web1.chall.necst.it/bobby.php

Let's log in as Bobby :)

HANDS ON – YOUR TURN!

https://hackinglab.necst.it

ARMANDO BELLANTE
@IKIGA1
@ARMANDO_BELLANTE

You can login as:

- usr: hackinglab@necst.it
- psw: hackinglab

HTTPS://TOH.NECST.IT
@TOWEROFHANOI
TOH@NECST.IT

Choose a username and remember the code to recover your game!