# How to: Capture the Flag

## Einführung in die Welt des kompetetiven Findes von Sicherheitslücken

# WTF is CTF?

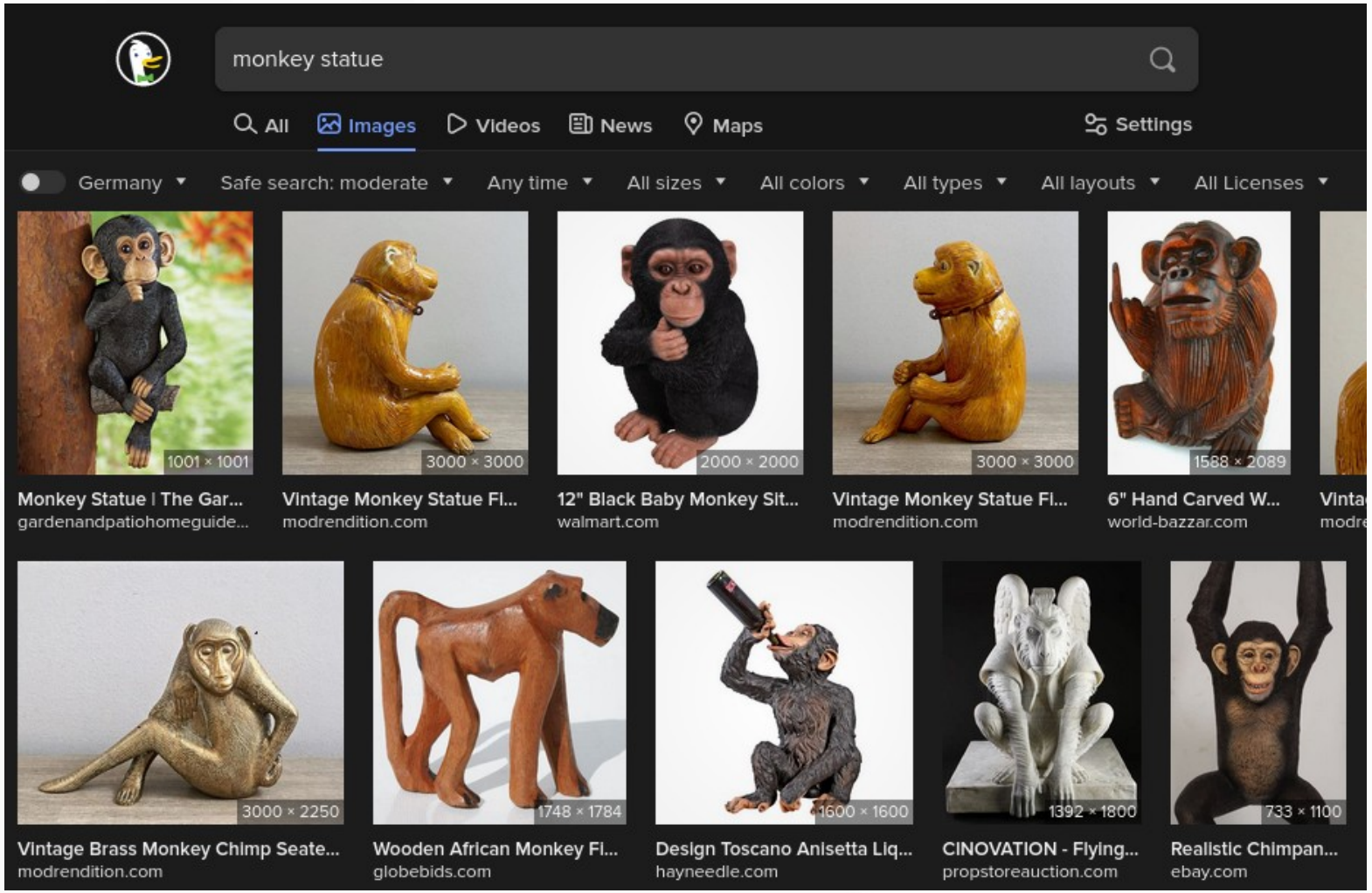
- **Wettkampf**
- **Lernplattform**
- **Übung**
- **Spiel**

# Ein Beispiel: *DaVinciCTF 2022*

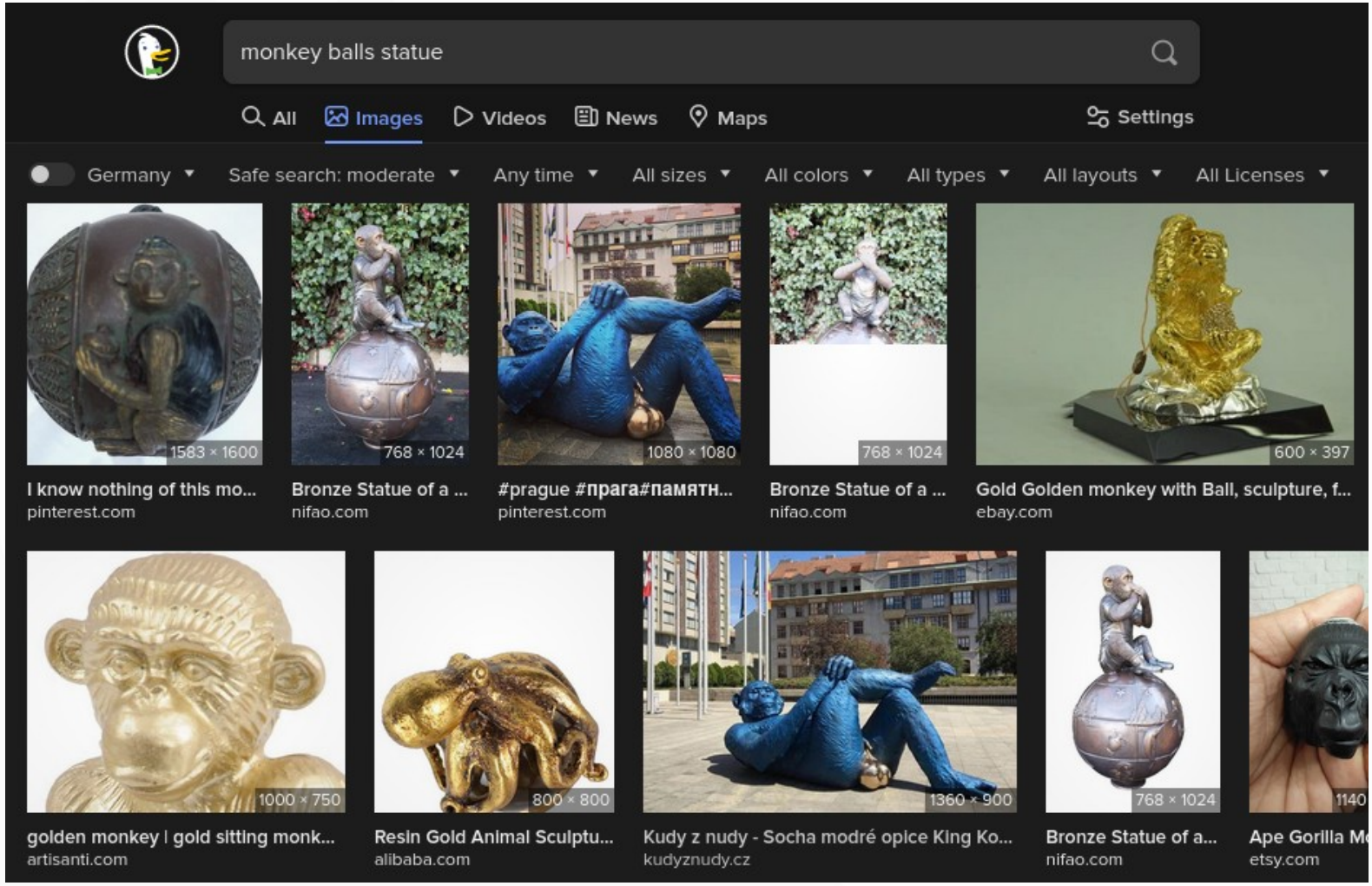
## Monkeey

> *"In what city is the statue of this monkey found? Wrap it around with the wrapper:* `dvCTF{city_in_lowercase}` *"*

# Ein Beispiel: *DaVinciCTF 2022*



# Ein Beispiel: *DaVinciCTF 2022*



# Ein Beispiel: *DaVinciCTF 2022*

## Monkeey

> *"In what city is the statue of this monkey found? Wrap it around with the wrapper:*
> `dvCTF{city_in_lowercase}`*"*

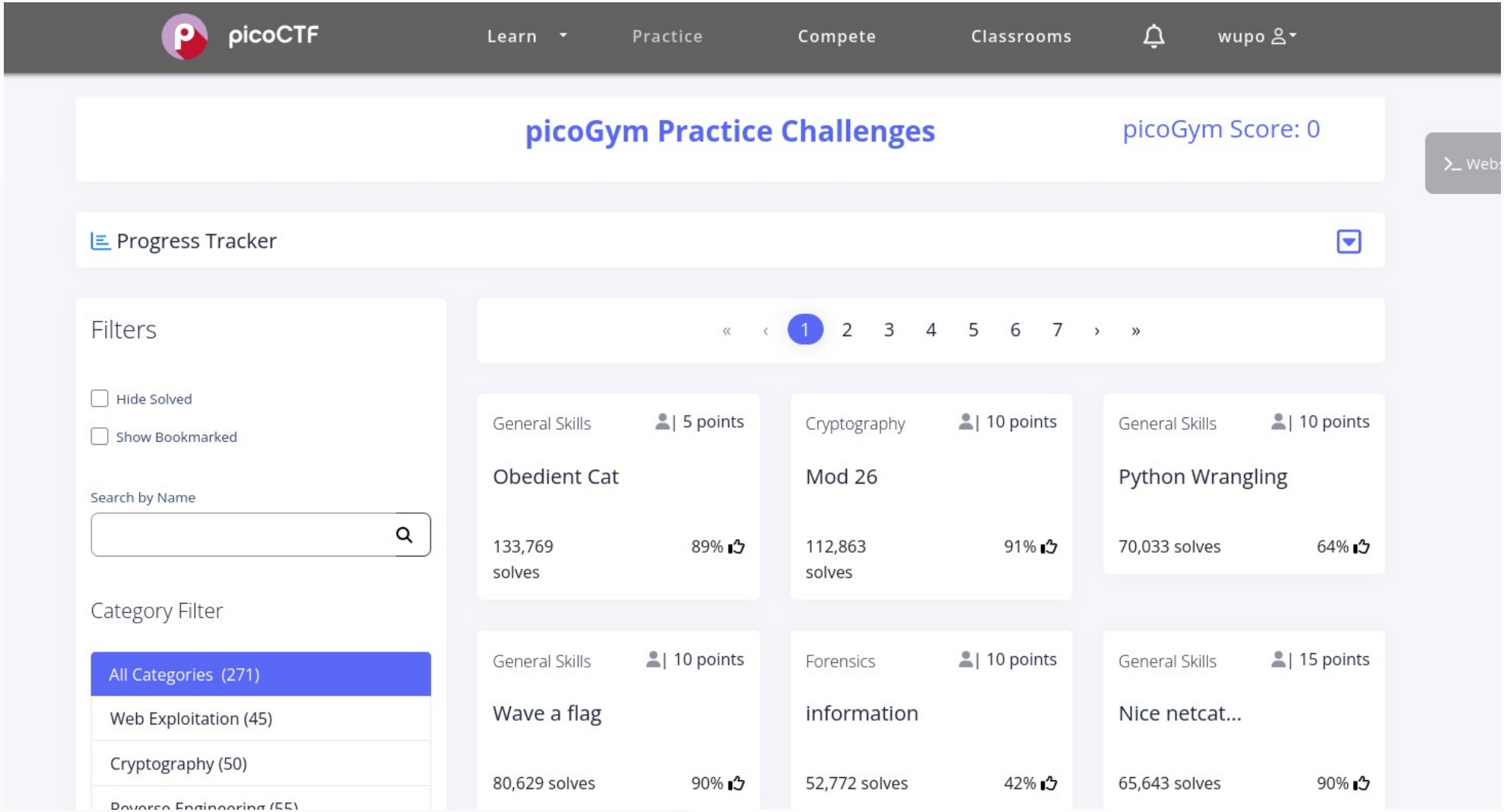
*dvCTF{prague}*

# Kategorien

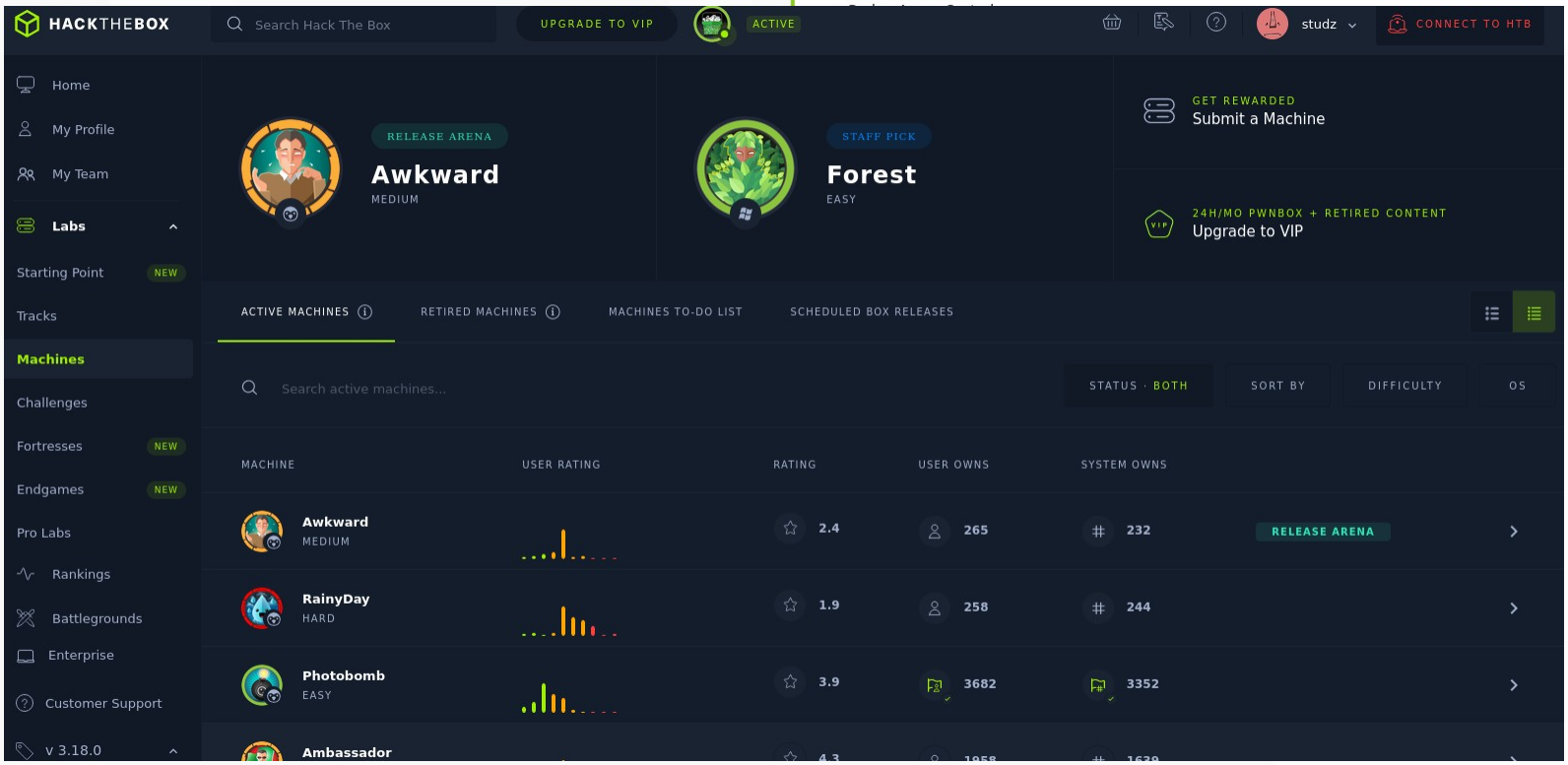
- **pwn/binary exploitation (‘illegal’ access)**
- **crypto (cryptography)**
- **osint (open source intelligence)**
- **rev (reverse engineering)**
- **web (web application exploitation)**
- **forensic (log/incident analysis)**
- **blockchain (bugs in smart contracts)**
- **…**


SIXGEN
SIXGEN


DEF CON


picoCTF
Learn
Practice
Compete
Classrooms
wupo
picoGym Practice Challenges
picoGym Score: 0
Progress Tracker
Filters
Hide Solved
Show Bookmarked
Search by Name
Category Filter
All Categories (271)
Web Exploitation (45)
Cryptography (50)
« ‹ 1 2 3 4 5 6 7 › »
General Skills | 5 points
Obedient Cat
133,769 solves
89%
Cryptography | 10 points
Mod 26
112,863 solves
91%
General Skills | 10 points
Python Wrangling
70,033 solves
64%
General Skills | 10 points
Wave a flag
80,629 solves
90%
Forensics | 10 points
information
52,772 solves
42%
General Skills | 15 points
Nice netcat...
65,643 solves
90%


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
0
Go Premium
OWASP Top 10
5753
Learn about and exploit each of the OWASP Top 10 vulnerabilities; the 10 most critical web security risks.
Start AttackBox
Awards
Help
100%
Task 1 Introduction
OWASP
Open Web Application Security Project
This room breaks each OWASP topic down and includes details on what the vulnerability is, how it occurs and how you can exploit it. You will put the theory into practise by completing supporting challenges.
Injection
Broken Authentication
Sensitive Data Exposure
XML External Entity


HACKTHEBOX
Search Hack The Box
UPGRADE TO VIP
ACTIVE
studz
CONNECT TO HTB
Home
My Profile
My Team
Labs
Starting Point
Tracks
Machines
Challenges
Fortresses
Endgames
Pro Labs
Rankings
Battlegrounds
Enterprise
Customer Support
v 3.18.0
RELEASE ARENA
Awkward
MEDIUM
STAFF PICK
Forest
EASY
GET REWARDED
Submit a Machine
24H/MO PWNBOX + RETIRED CONTENT
Upgrade to VIP
ACTIVE MACHINES
RETIRED MACHINES
MACHINES TO-DO LIST
SCHEDULED BOX RELEASES
Search active machines...
STATUS · BOTH
SORT BY
DIFFICULTY
OS
MACHINE
USER RATING
RATING
USER OWNS
SYSTEM OWNS
Awkward
MEDIUM
2.4
265
232
RELEASE ARENA
RainyDay
HARD
1.9
258
244
Photobomb
EASY
3.9
3682
3352
Ambassador

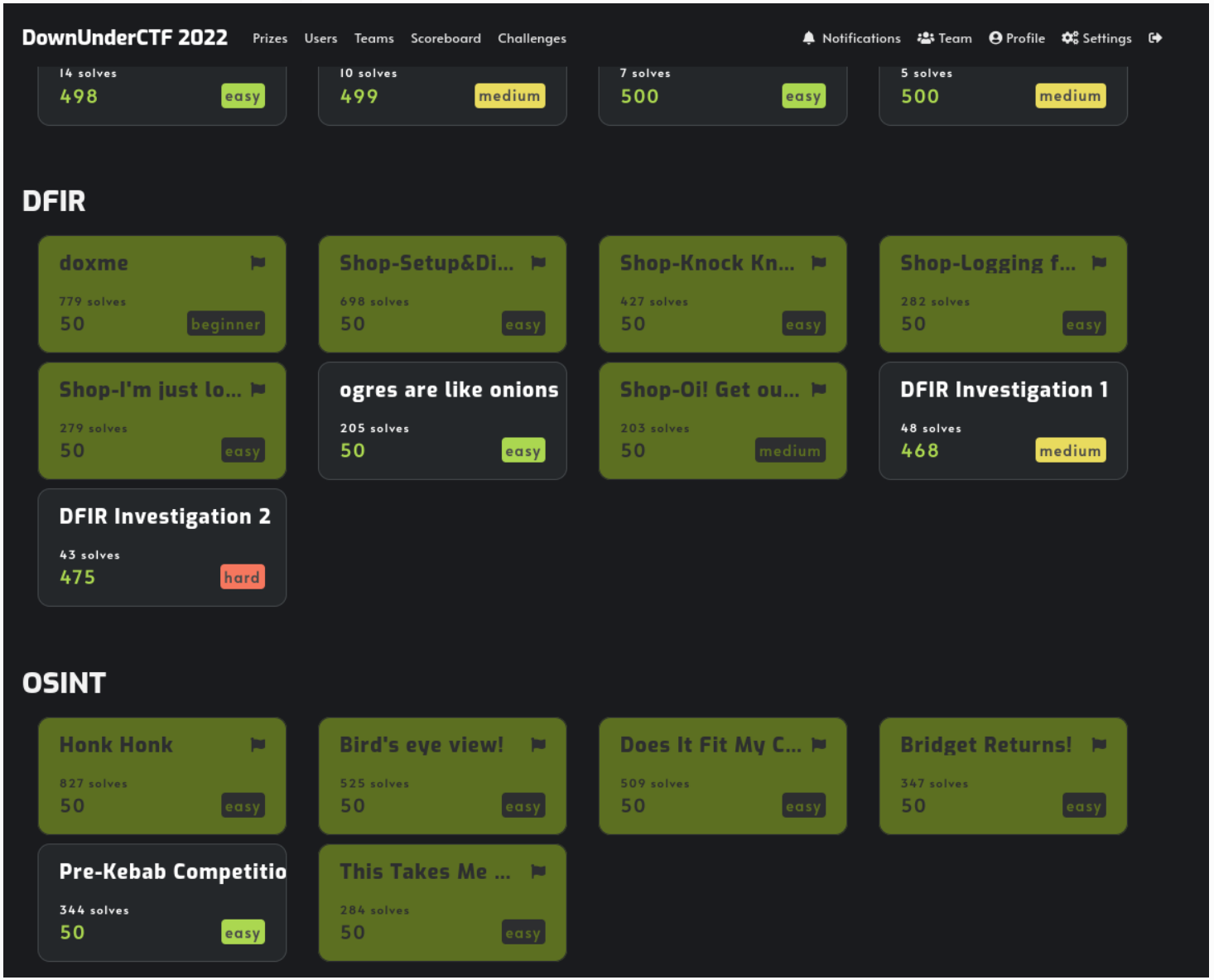
# Wie wird gespielt?

- **Jeopardy (On-Demand, Live)**
- **Attack-Defense**

# Jeopardy

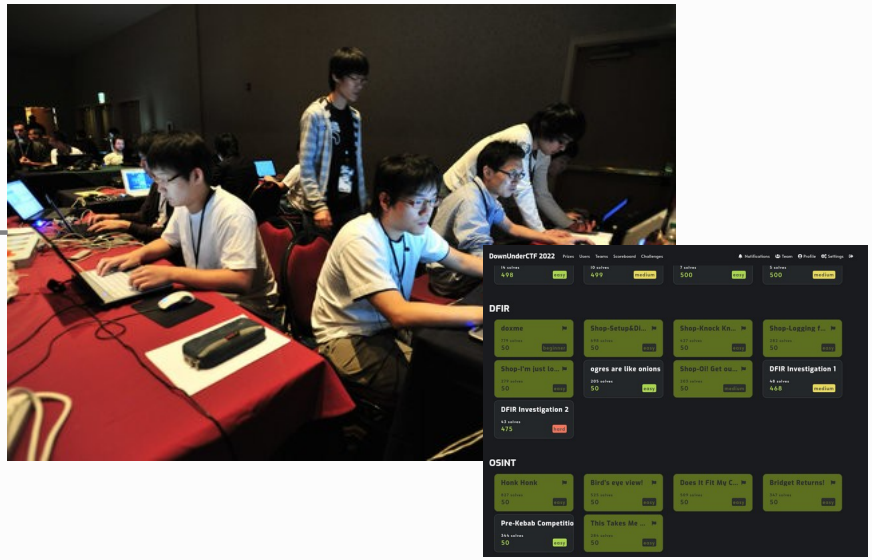

JEOPARDY!
$200 $200 $200 $200 $200 $200
$400 $400 $400 $400 $400 $400
$600 $600 $600 $600 $600 $600
$800 $800 $800 $800 $800 $800
$1000 $1000 $1000 $1000 $1000 $1000

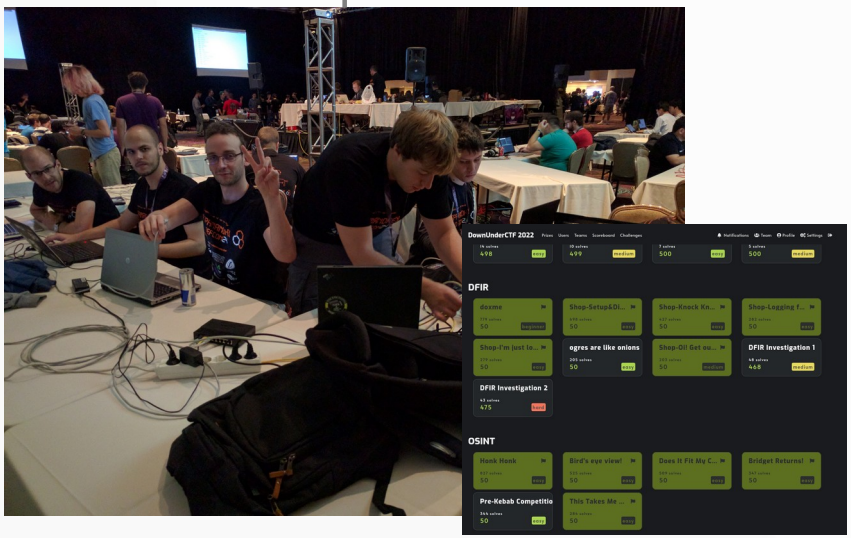
# Jeopardy


DownUnderCTF 2022
Prizes
Users
Teams
Scoreboard
Challenges
Notifications
Team
Profile
Settings
14 solves
498
easy
10 solves
499
medium
7 solves
500
easy
5 solves
500
medium
DFIR
doxme
779 solves
50
beginner
Shop-Setup&Di...
698 solves
50
easy
Shop-Knock Kn...
427 solves
50
easy
Shop-Logging f...
282 solves
50
easy
Shop-I'm just lo...
279 solves
50
easy
ogres are like onions
205 solves
50
easy
Shop-Oi! Get ou...
203 solves
50
medium
DFIR Investigation 1
48 solves
468
medium
DFIR Investigation 2
43 solves
475
hard
OSINT
Honk Honk
827 solves
50
easy
Bird's eye view!
525 solves
50
easy
Does It Fit My C...
509 solves
50
easy
Bridget Returns!
347 solves
50
easy
Pre-Kebab Competitio
344 solves
50
easy
This Takes Me ...
284 solves
50
easy

# Jeopardy


SIXGEN


DownUnderCTF 2022
DFIR
OSINT

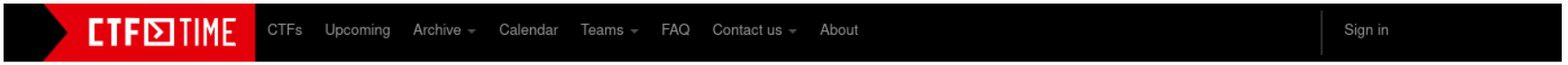

DownUnderCTF 2022
DFIR
OSINT

# Attack-Defense


# Wer richtet aus?

- **Universitäten**
- **Firmen**
- **CTF-Teams**
- **Konferenzen**

# CTF TIME




## Team rating

2022 | 2021 | 2020 | 2019 | 2018 | 2017 | 2016 | 2015 | 2014 | 2013 | 2012 | 2011

| Place | Team | Country | Rating |
|---|---|---|---|
| 1 | perfect r00t | | 953.339 |
| 2 | C4T BuT S4D | | 931.343 |
| 3 | organizers | | 894.599 |
| 4 | Water Paddler | | 826.718 |
| 5 | Bushwhackers | | 789.082 |
| 6 | Never Stop Exploiting | | 755.532 |
| 7 | Nu1L | | 661.713 |
| 8 | DiceGang | | 639.590 |
| 9 | idek | | 605.378 |
| 10 | r3kapig | | 596.731 |

Full rating | Rating formula

## Upcoming events

Open

| Format | Name | Date | Duration |
|---|---|---|---|
| | 1st stage MetaRed CTF Argentina 2022 (10:00 GMT-3)<br>On-line | Mon, Sept. 26, 13:00 — Tue, Sept. 27, 13:00 UTC<br>17 teams | 1d 0h |
| | DefCamp Capture the Flag (D-CTF) 2022 Quals<br>On-line | Fri, Sept. 30, 09:00 — Sat, Oct. 01, 15:00 UTC<br>10 teams | 1d 6h |

## Now running

### WPICTF 2022

On-line — 52 teams
Fri, Sept. 23, 2022 21:00 — Sun, Sept. 25, 21:00 UTC — (0d 8h more)

### LakeCTF Qualifications

On-line — 41 teams
Sat, Sept. 24, 2022 18:00 — Sun, Sept. 25, 18:00 UTC — (0d 5h more)

## Past events

With scoreboard | All

### DownUnderCTF 2022 (Online)

Sept. 25, 2022 09:30 UTC | On-line | Weight voting in progress

| Place | Team | Country | Points |
|---|---|---|---|
| 1 | idek | | 64.480 |
| 2 | thehackerscrew | | 46.447 |
| 3 | PwN3v3rY7h1nG | | 37.240 |

1405 teams total | Tasks and writeups

### RomHack 2022 CTF

Sept. 24, 2022 08:00 UTC | On-line

| Place | Team | Country | Points |
|---|---|---|---|
| 1 | erated | | 49.800 |
| 2 | CrusadersOfRust | | 37.350 |
| 3 | bootplug | | 25.822 |

386 teams total | Tasks and writeups

### VolgaCTF 2022 Final

Sept. 22, 2022 13:00 UTC | Samara, Russian Federation | Weight voting in progress

# Wer spielt?

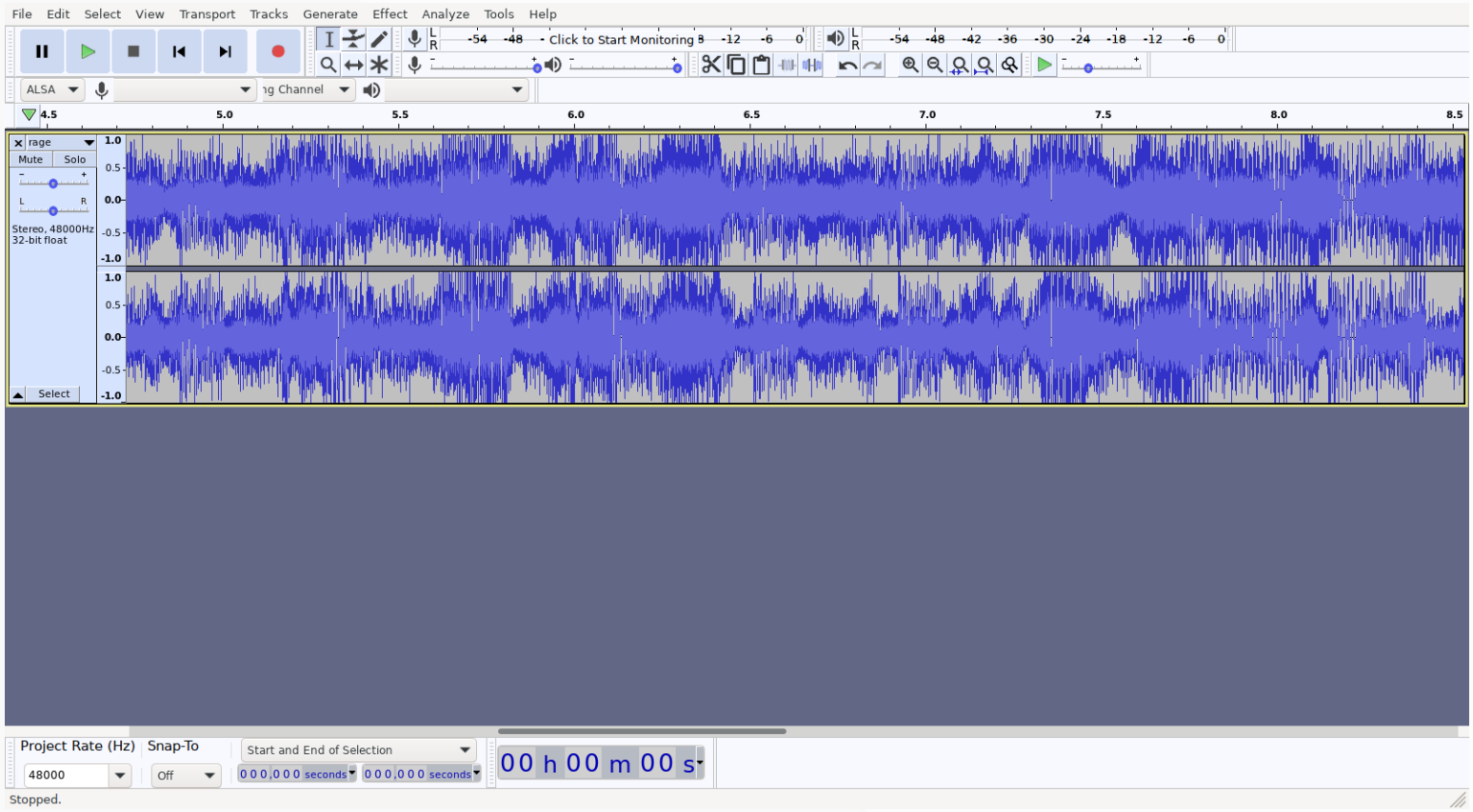
- **Schüler*innen/Studierende**
- **Angestellte**
- **Privatpersonen**

# Warum wird gespielt?

- **Spaß am Thema**
- **Lernen/Übung**
- **Bragging-Rights**
- **Preisgeld/Black Badge**

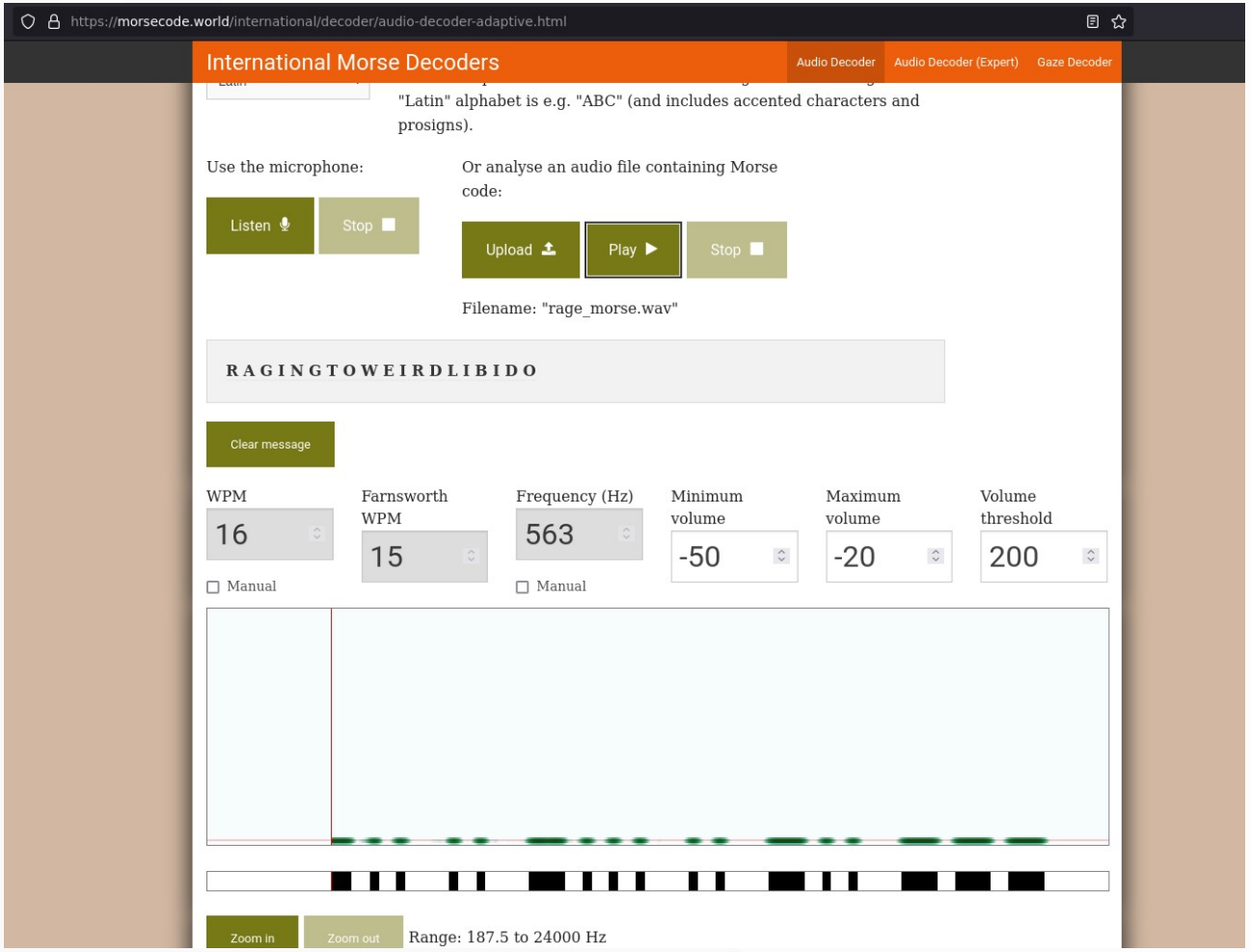
# Ein Beispiel: *DownUnderCTF 2022*

Rage:



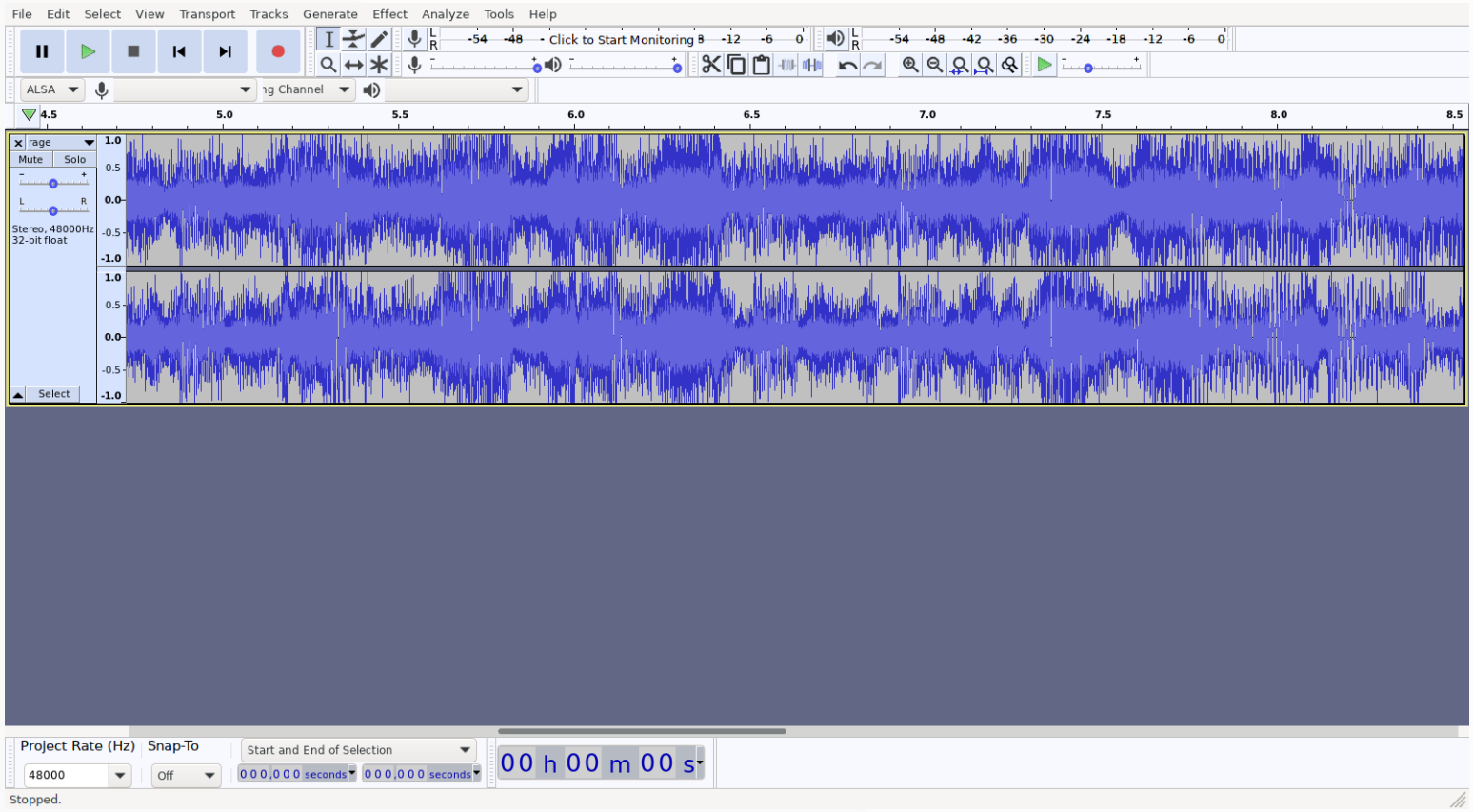
# Ein Beispiel: *DownUnderCTF 2022*

Rage:



# Ein Beispiel: *DownUnderCTF 2022*

Rage:




*DUCTF{raging_to_weird_libido}*

# Ein Beispiel: *DownUnderCTF 2022*

babypywn:

Python is memory safe, right?

`babypywn.py`

# Techniken vor/nach dem CTF

- **Writeups Lesen/Anschauen/Nachvollziehen**
- **Übungsplattformen nutzen**
- **Kommunikation**

# Ressourcen zum Lernen/Üben

- **hackthebox.com**
- **tryhackme.com**
- **overthewire.org**
- **picoctf.org**
- **ctf.sshuzl.de**
- **https://www.youtube.com/user/RootOfTheNull**

# Techniken während des CTF

- **Vergleichen mit Standard / Referenzimplementierung**
- **Timebox**
- **Suchmaschinen**
- **Kommunikation**

# Hilfsmittel

- **duckduckgo.com**
- **docs.pwntools.com**
- **book.hacktricks.xyz**
- **gchq.github.io/CyberChef**
- **...**

```
echo 'RGFua2UhCg==' | base64 -d
```

- **wiki.chaotikum.org/projekte:wargames**
- **wupo@chaotikum.org**
- **social.chaotikum.org/@wupo**