

# **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

The screenshot shows a search results page for "monkey statue" on a dark-themed search engine. The interface includes a search bar with the query "monkey statue", a navigation bar with "All", "Images" (which is selected), "Videos", "News", "Maps", and "Settings", and various filters for location ("Germany"), safe search ("moderate"), time, size, color, type, layout, and license. The results are displayed in two rows of five items each, showing different types of monkey statues.

Image	Description	Source
	Monkey Statue   The Gar...	gardenandpatiohomeguide...
	Vintage Monkey Statue Fl...	modrendition.com
	12" Black Baby Monkey Sit...	walmart.com
	Vintage Monkey Statue Fl...	modrendition.com
	6" Hand Carved W...	world-bazaar.com
	Vintage Brass Monkey Chimp Seate...	modrendition.com
	Wooden African Monkey Fl...	globebids.com
	Design Toscano Anisetta Liq...	hayneedle.com
	CINOVATION - Flying...	propstoreauction.com
	Realistic Chimpan...	ebay.com

# Ein Beispiel: DaVinciCTF 2022

monkey balls statue

All Images Videos News Maps Settings

Germany Safe search: moderate Any time All sizes All colors All types All layouts All Licenses

I know nothing of this mo...  
pinterest.com

Bronze Statue of a ...  
nifao.com

#prague #npara#памятн...  
pinterest.com

Bronze Statue of a ...  
nifao.com

Gold Golden monkey with Ball, sculpture, f...  
ebay.com

golden monkey | gold sitting monk...  
artisanti.com

Resin Gold Animal Sculptu...  
alibaba.com

Kudy z nudy - Socha modré opice Kling Ko...  
kudyznudy.cz

Bronze Statue of a...  
nifao.com

Ape Gorilla Me...  
etsy.com

# 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)
- ...





## picoGym Practice Challenges

picoGym Score: 0

&gt; Web:

### Progress Tracker



#### Filters

 Hide Solved Show Bookmarked

#### Search by Name



« < 1 2 3 4 5 6 7 > »

General Skills	👤   5 points	Cryptography	👤   10 points	General Skills	👤   10 points
Obedient Cat		Mod 26		Python Wrangling	
133,769 solves	89% ↗	112,863 solves	91% ↗	70,033 solves	64% ↗
General Skills	👤   10 points	Forensics	👤   10 points	General Skills	👤   15 points
Wave a flag		information		Nice netcat...	
80,629 solves	90% ↗	52,772 solves	42% ↗	65,643 solves	90% ↗

#### Category Filter

[All Categories \(271\)](#)[Web Exploitation \(45\)](#)[Cryptography \(50\)](#)[Reverse Engineering \(55\)](#)

The screenshot shows the TryHackMe platform interface. At the top, there's a navigation bar with links for Dashboard, Learn, Compete, and Other, along with a red 'Access Machines' button, a green '0' icon, a bell icon, and a 'Go Premium' button. Below the navigation is a banner for the 'OWASP Top 10' challenge, featuring the OWASP logo and a bee icon. The banner also includes a thumbs up count of 5753, a thumbs down icon, and buttons for 'Start AttackBox', 'Awards', 'Help', and 'Settings'. A progress bar at the top indicates 100%. Below the banner, a specific task titled 'Task 1 ✓ Introduction' is displayed, showing the OWASP logo and the text: '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.' It lists four topics: Injection, Broken Authentication, Sensitive Data Exposure, and XML External Entity.

The screenshot shows the HackTheBox platform interface. At the top, there's a navigation bar with a search bar for 'Search Hack The Box', an 'UPGRADE TO VIP' button, and an 'ACTIVE' status indicator. Below the navigation is a sidebar with links for Home, My Profile, My Team, and Labs (selected). The main area shows a 'Starting Point' section with a 'NEW' badge, followed by a 'Tracks' section with categories like Challenges, Fortresses, Endgames, Pro Labs, Rankings, Battlegrounds, Enterprise, and Customer Support. The 'Machines' section is the active tab, showing a list of active machines. The list includes 'Awkward' (Medium, RELEASE AREA), 'Forest' (Easy, STAFF PICK), and other machines like 'RainyDay' (Hard) and 'Photobomb' (Easy). Each machine entry provides details such as user rating, number of users who own it, and system ownership counts. There are also buttons for 'RELEASE AREA' and 'SCHEDULED BOX RELEASES'.

# **Wie wird gespielt?**

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

# Jeopardy



# Jeopardy

DownUnderCTF 2022   Prizes   Users   Teams   Scoreboard   Challenges   Notifications   Team   Profile   Settings

14 solves   10 solves   7 solves   5 solves  
498   499   500   500  
easy   medium   easy   medium

## DFIR

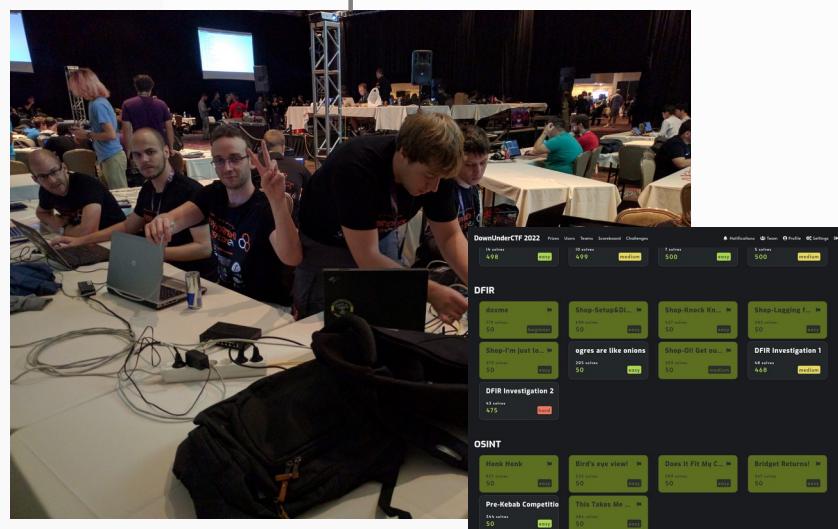
doxme   779 solves   50   beginner  
Shop-Setup&Di...   698 solves   50   easy  
Shop-Knock Kn...   427 solves   50   easy  
Shop-Logging f...   282 solves   50   easy  
Shop-I'm just lo...   279 solves   50   easy  
ogres are like onions   205 solves   50   easy  
Shop-Oi! Get ou...   203 solves   50   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



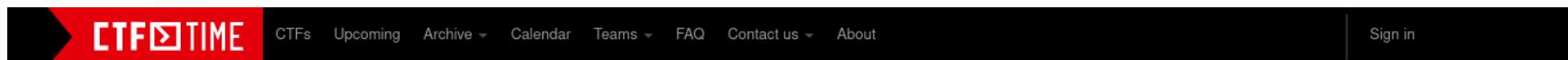
# Attack-Defense



# **Wer richtet aus?**

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

# CTF TIME



## Team rating

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)	Mon, Sept. 26, 13:00 — Tue, Sept. 27, 13:00 UTC	1d 0h
🌐	On-line		17 teams
██	DefCamp Capture the Flag (D-CTF) 2022 Quals	Fri, Sept. 30, 09:00 — Sat, Oct. 01, 15:00 UTC	1d 6h
🌐	On-line		10 teams

## Now running ⚡

### ██ WPICTF 2022 ⚡

🌐 On-line  
Fri, Sept. 23, 2022 21:00 — Sun, Sept. 25, 21:00 UTC

52 teams  
(0d 8h more)

### ██ LakeCTF Qualifications ⚡

🌐 On-line  
Sat, Sept. 24, 2022 18:00 — Sun, Sept. 25, 18:00 UTC

41 teams  
(0d 5h more)

## Past events ⚡

[With scoreboard](#)

All

### ██ DownUnderCTF 2022 (Online) ⚡

Sep. 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 ⚡

Sep. 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 ⚡

Sep. 22, 2022 13:00 UTC | Samara, Russian Federation | [Weight voting in progress](#)

# **Wer spielt?**

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

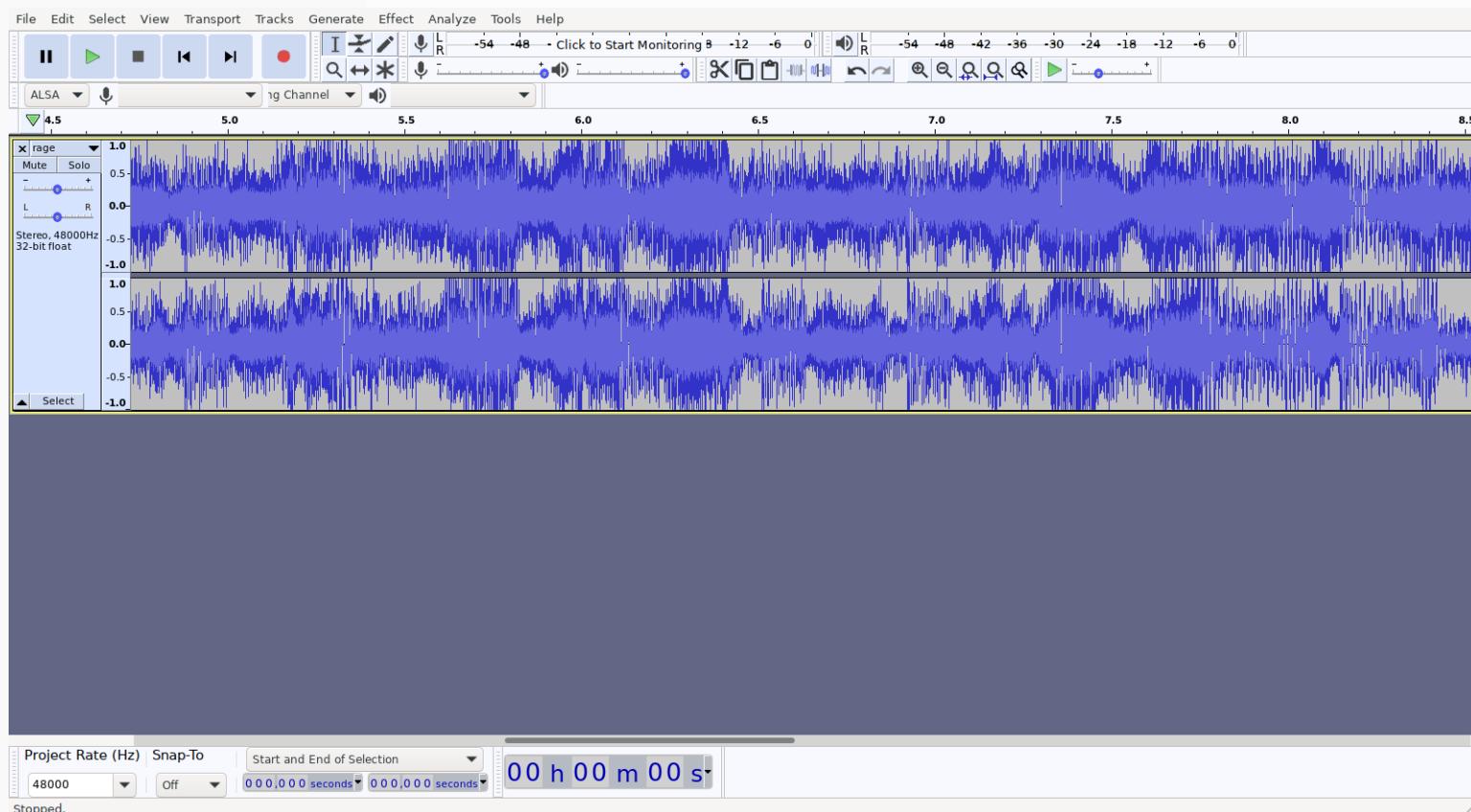
# **Warum wird gespielt?**

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

# Ein Beispiel:

*DownUnderCTF 2022*

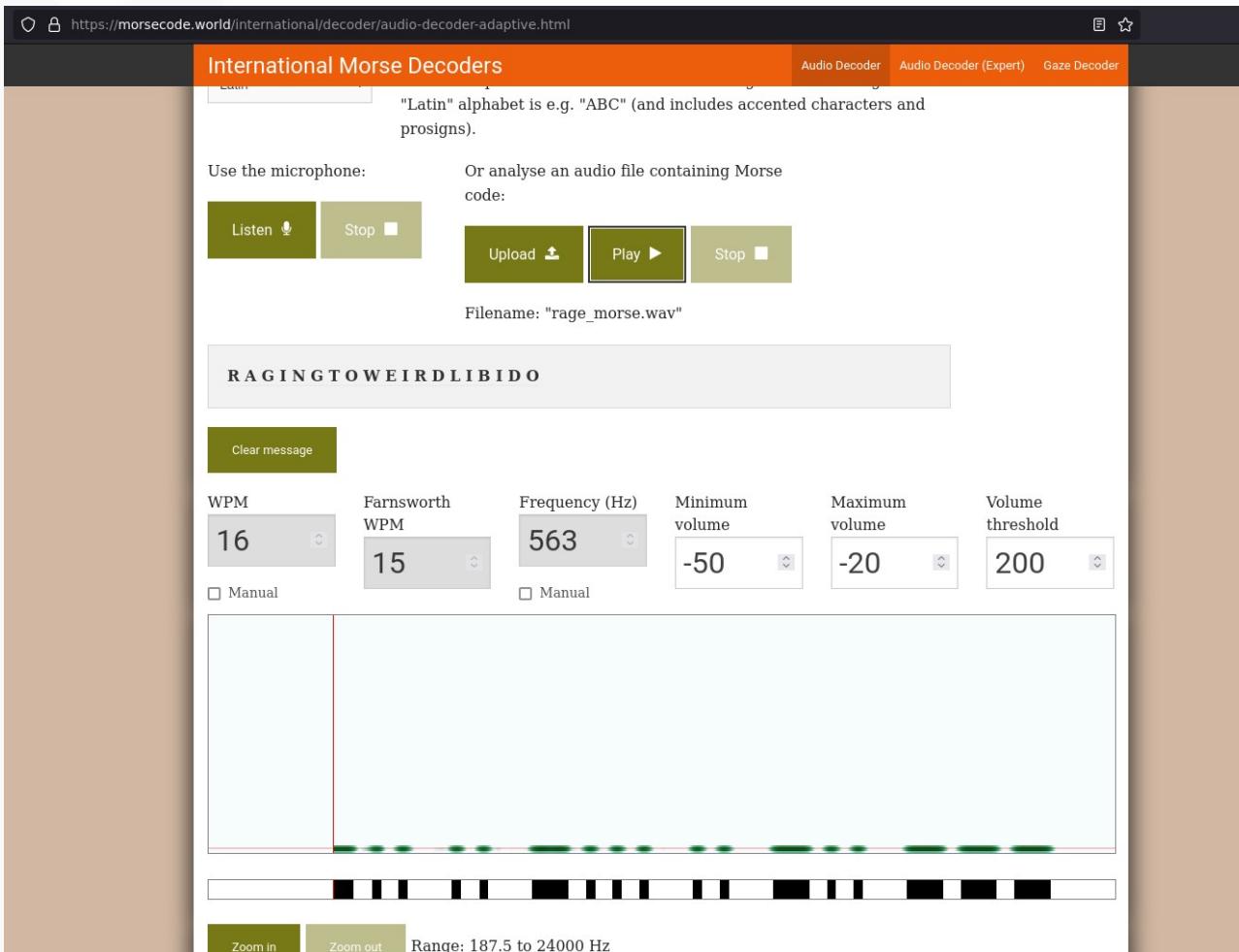
Rage:



# Ein Beispiel:

*DownUnderCTF 2022*

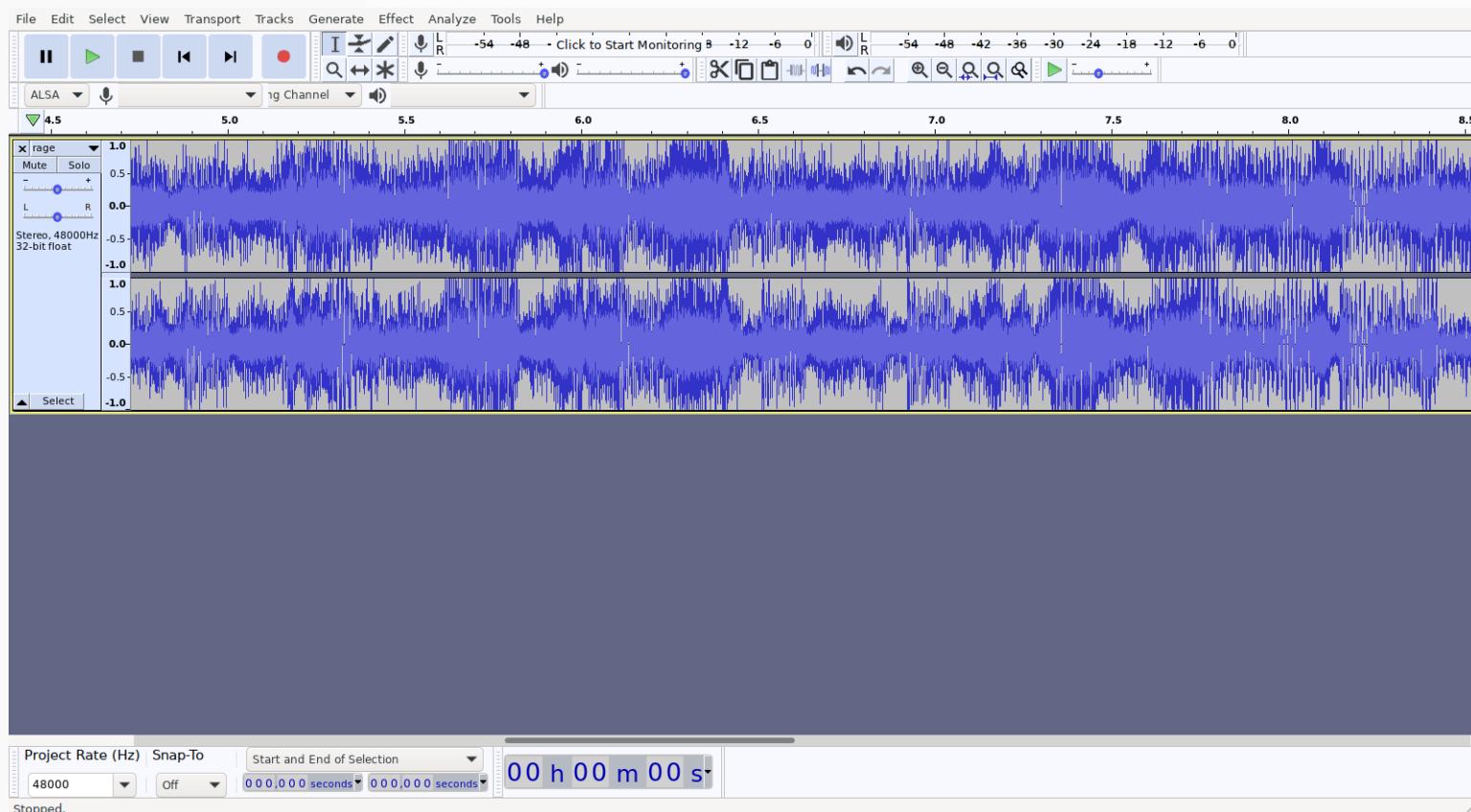
Rage:



# 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 'RGFuua2UhCg==' | base64 -d
```

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