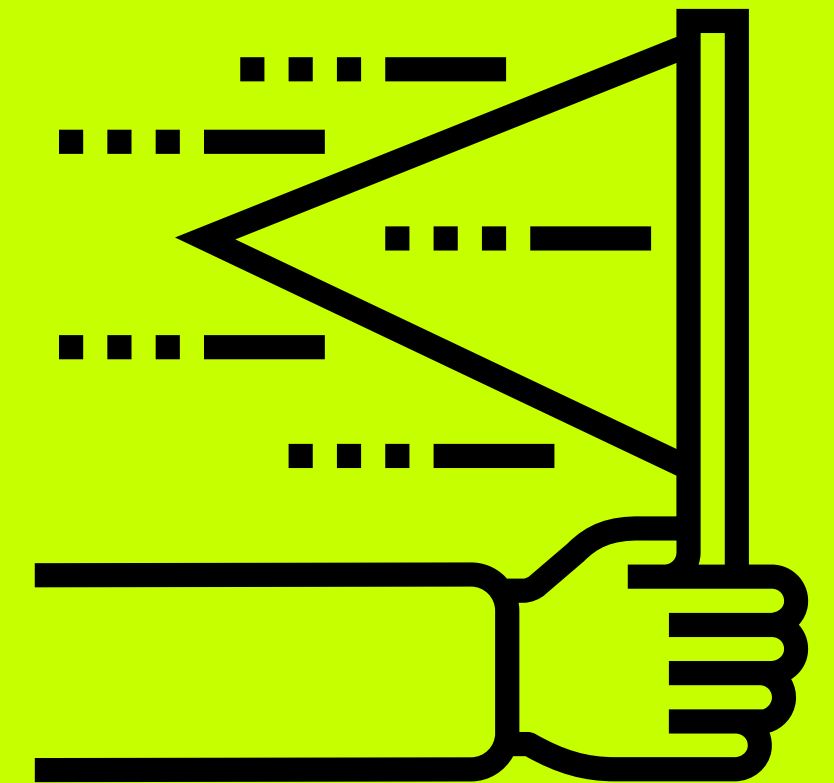


OD ZERA DO CTF PLAYERA.



Od zera do CTF Playera.

Poznań Security Meetup 2023

Agenda

✓ Czym właściwie są te "CTFy"?

✓ Jak i gdzie zacząć zabawę?

✓ Polska na tle światowej sceny CTF.

✓ Garść tipów od CTF playera.

Od zera do CTF Playera.

~#whoami

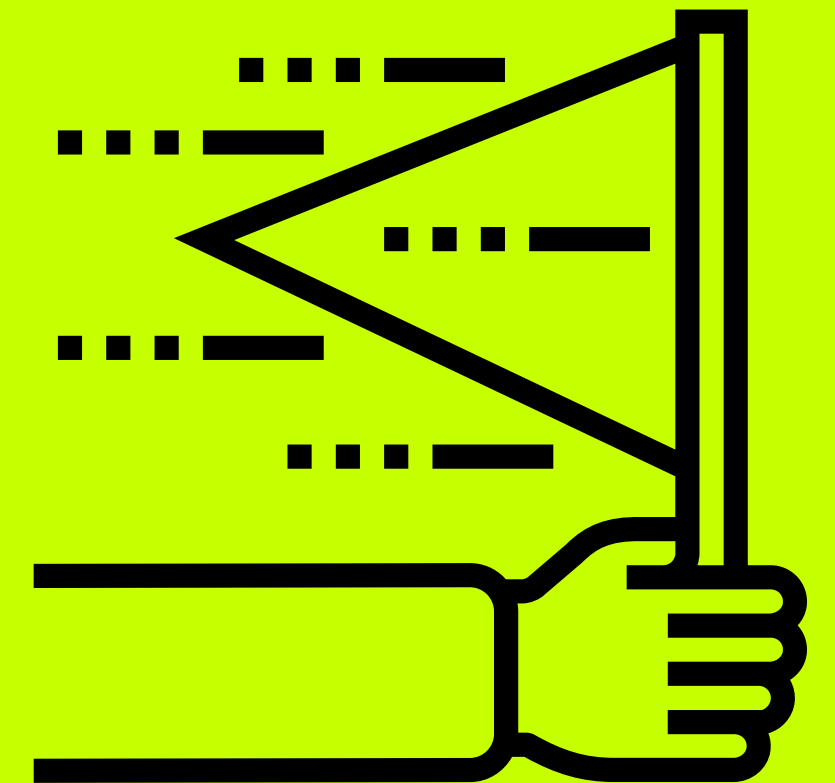
- ✓ Michał “miblak” Błaszczak
- ✓ W dzień: Security Manager w Vercom S.A
- ✓ W nocy: CTF Player, Pentester, Red Teamer
- ✓ Hobby: Malware Dev, Elektronika, Gotowanie :)

Poznan Security Meetup 2023

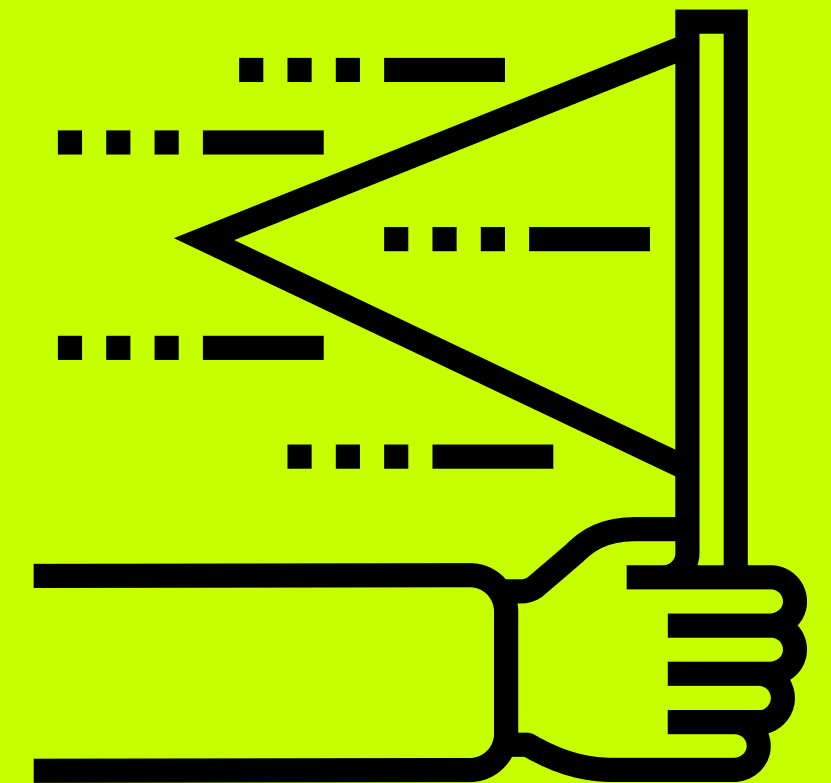


Michał Błaszczak
Security Manager, Vercom

CTF CO TO JEST?



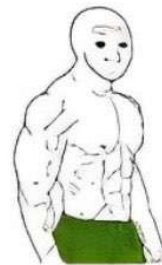
CAPTURE THE FLAG



CTF Player



I flew 7000 miles to attend an on-site event and didn't sleep for 3 days straight



I was lazy getting XSS and CSP bypass instead I used my Chrome 0-day



People like sex but have you got a firstblood in hard Pwn 500?



The challenge is unsolvable, hacked authors pc and didn't found any solution

Bug Bounty Hunter



My custom Nuclei template returned 23 exposed robots.txt file



I have OSCP, CEH, OSWE, OSGAY, eCCPT and I use VIM like a real hacker



Yay, I was awarded a \$50 bounty for world record holder (any updates?) in one day



CTF is easy I don't play it why wasting your time for free instead I will hunt on Redbull program to get some drinks and stick it in my as

“
**JAK WYGLĄDA POLSKA
NA TLE
CAPTURE THE FLAG?**

Od zera do CTF Playera.

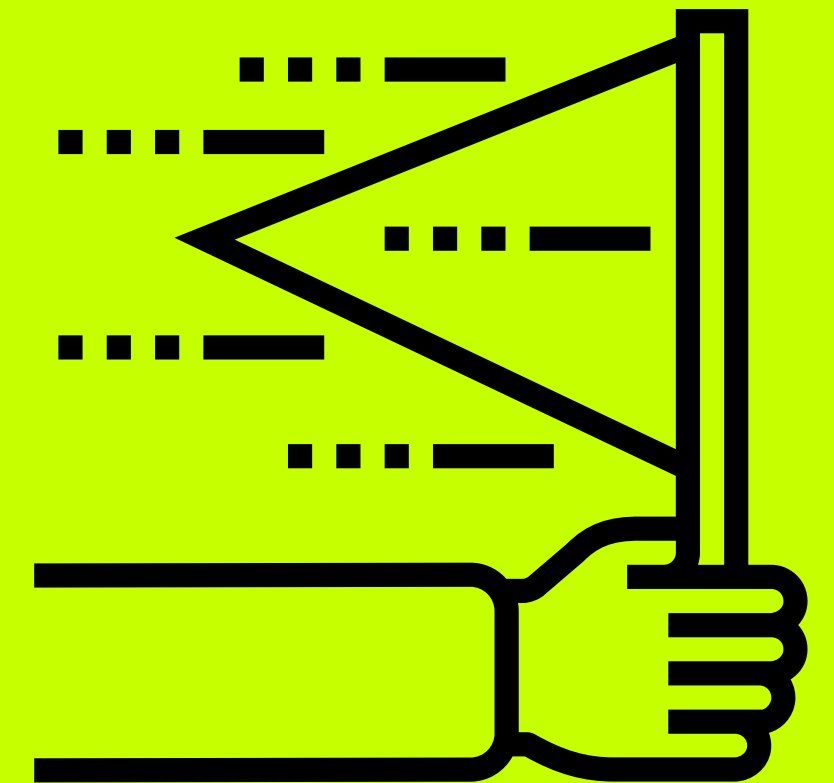
Poznań Security Meetup 2023



Od zera do CTF Playera.

Poznań Security Meetup 2023

PLATFORMY DO CTF





CTF TIME

CTFsUpcomingArchiveCalendarTeamsFAQContact usAbout

Sign in

Team rating

2023202220212020201920182017201620152014201320122011

Place	Team	Country	Rating
1	Blue Water		1314.245
2	kalmarunionen		1122.218
3	C4T BuT S4D		1119.509
4	justCatTheFish		1103.182
5	r3kapig		891.056
6	Never Stop Exploiting		785.161
7	SKSD		764.609
8	organizers		740.629
9	WreckTheLine		712.763
10	thehackerscrew		703.325

Full rating | Rating formula

Now running

HITCON CTF 2023 Final

Taiwan, Taipei

Tue, Nov. 14, 2023 00:00 — Wed, Nov. 15, 08:00 UTC

21 teams

(0d 23h more)

BlackHat MEA CTF Final 2023

In-site - Riyadh

Tue, Nov. 14, 2023 07:00 — Thu, Nov. 16, 14:30 UTC

0 teams

(2d 5h more)

Past events

With scoreboardAll

Cybercoliseum II

Nov. 13, 2023 07:00 UTC | On-line | Weight voting in progress

Place	Team	Country	Points *
1	Cyber Mushrooms		0.000
2	ne-pin-guem		0.000
3	MHC		0.000

468 teams total | Tasks and writeups



CRYPTOHACK

COURSES

CHALLENGES

SCOREBOARD

BLOG

CHAT

CAREERS

FAQ

REGISTER

LOGIN



CRYPTOHACK

A fun, free platform for learning modern cryptography

LEARN BY DOING

Learn about modern cryptography by solving a series of interactive puzzles and challenges. Get to know the ciphers and protocols that secure the digital world by breaking them.



RECENT SOLVES


Manyprime	FengShan2000	07:47
Greatest Common Divisor	gkerschb	09:46
Base64	pgu	09:44
Extended GCD	Cl4r1ty	09:43
Scalar Multiplication	Mazino246	09:41

View more →

RECENT SOLUTIONS

Micro Transmissions	Phaazhhasse	👍 0
Backpack Cryptography	rust_chan	👍 0
Backpack Cryptography	ConnorM	👍 0
Encoding Challenge	aidaner_	👍 0
Extended GCD	thisismo	👍 0





Learn

Compete

For Education

For Business

Pricing

Search

Login

Join for FREE

Anyone can learn cyber security with TryHackMe


Hands-on cyber security training through real-world scenarios




Email

Join for FREE

✓ Beginner Friendly

✓ Guides and Challenges






Byte-sized gamified lessons

Learning cyber security on TryHackMe is fun and addictive. Earn points by answering questions, taking on challenges and maintain your hacking streak through short lessons.



HACKTHEBOX


Home

Profile

Groups

Ruby

RANK - 29



Starting Point

Open Beta Season III

Machines

Challenges

Tracks

Sherlocks

Rankings

Academy


Advanced Labs

Job Board

Universities


HTB for Business

Search Hack The Box

LIVE

Red Trails

MEDIUM

STAFF PICK

Prison Escape

MEDIUM

Submit a Challenge

Upgrade to VIP+

ACTIVE CHALLENGES 1

RETIRED CHALLENGES 1

CHALLENGES TO-DO LIST











Search active challenges...

STATUS • BOTH

SORT BY


DIFFICULTY

ALL CHALLENGES

 Pwn	24 Pwn challenges
 Hardware	17 Hardware challenges
 Crypto	27 Crypto challenges
 Reversing	23 Reversing challenges
 GamePwn	9 GamePwn challenges
 Blockchain	8 Blockchain challenges
 Forensics	13 Forensics challenges
 Misc	14 Misc challenges
 Mobile	11 Mobile challenges
 Web	16 Web challenges

Web Security Academy





[Products](#) [Solutions](#) [Research](#) [Academy](#) [Support](#) [Login](#)

[Dashboard](#) [Learning paths](#) [Latest topics](#) [All content](#) [Hall of Fame](#) [Get started](#) [Get certified](#)

Ne

Ex

Pr


Ap

Web Security Academy

Free, online web security training from the creators of Burp Suite


Sign up

Login




Boost your career

The Web Security Academy is a strong step toward a career in cybersecurity.




Flexible learning

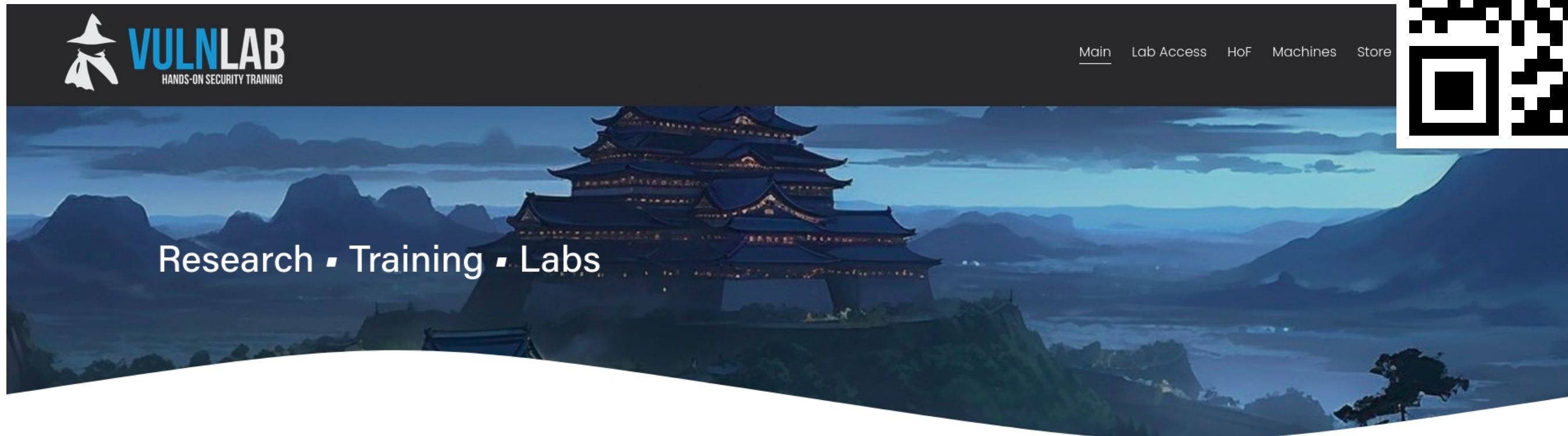
Learn anywhere, anytime, with free interactive labs and progress-tracking.



Learn from experts

Produced by a world-class team - led by the author of The Web Application Hacker's Handbook.






Training & Labs

Vulnlab features a **pentesting & red teaming** lab environment by [xct](#) with **60+** vulnerable machines, ranging from standalone machines to big **active directory environments** with multiple forests that require **bypassing modern defenses**. The labs have various difficulties from easy to advanced and come with guidance in the form of notes, hints & walkthroughs. New content gets added on a regular basis.

Once subscribed, you get access to the lab area on the vulnlab discord server from which you can interact with a bot that allows you to get your VPN packs, control the machines and submit flags. You are welcome to create public walkthroughs or stream machine solutions. To get an idea what the content is like you can check out the walkthrough videos for a part of the red team labs on [YouTube](#).





Capture The Flag

Challenges


Community


Information


298 visitors now


Newest members :
johnsmith1 kultiv Raph67500
klekktic Xavier Ultron sdnho

Offers


 CDI Penetration tester

 CDI Incident response


 CDI Cybersecurity consultant

 AUT R&D engineer

Chatbox


 **The_Corruptor**
14 November 2023 at 00:20

how to i even ping a host here? all of them seem offline no matter what i do.






brankata03

12 November 2023 at 17:47

sdfasd


 **Andrushka104**
9 November 2023 at 18:43

Solidaren, zdes vse umom



Search


HOME / CHALLENGES



Challenges

Over five hundred challenges available to learn hacking.


You may only access remote challenges after having authenticated to this portal. You need to be authenticated on this website with the same IP address you use to solve challenges.



App - Script

31 challenges


Exploit environment weaknesses, configuration mistakes and vulnerability patterns in scripts and (...)



App - System

88 challenges


These challenges will help you understand applicative vulnerabilities.



Cracking

64 challenges


Reverse binaries and crack executables.



Forensic

42 challenges


Train digital investigation skills by analyzing memory dumps, log files, network captures...



Programming

21 challenges


Automate tasks and build shellcodes.



Network

27 challenges

Investigate captured traffic, network services and perform packet analysis

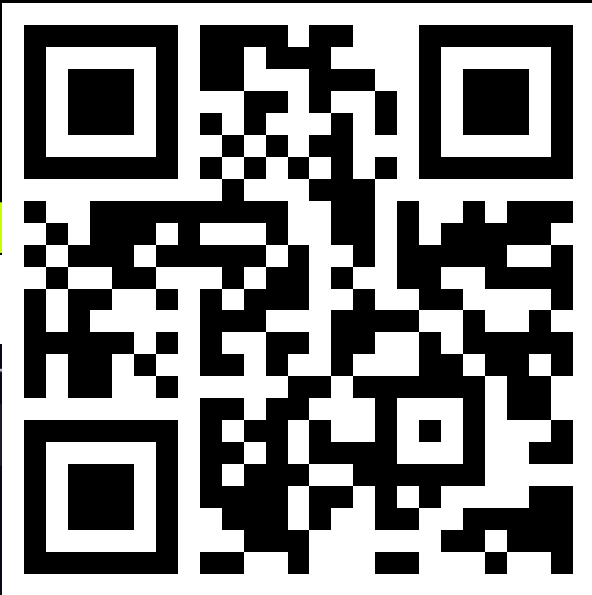



Realist

56 challenges

Realistic challenges.

Lets Defend



 LETSDEFEND

Learn

Practice

Challenge

Filter Menu

Reset All

Challenge Type

DFIR (26)

Malware Analysis (17)

Cloud Security (3)

Categories

Cloud Security (4)

Code Analysis (3)

Forensics (14)

Linux (5)

Malware (32)

Memory Analysis (23)

Network (23)

PDF Analysis (1)

Phishing (2)

Ransomware (9)

Reverse Engineering (4)

Windows (18)

Role

Security Analyst (35)

Incident Responder (11)

Detection Engineer (0)

Skill Level


Beginner (1)

Easy (14)

Medium (15)

Hard (16)

Google Cloud Incident




Hard

Enterprise

Google Cloud Incident

A developer accidentally committed a Google Cloud identity's key to a public repository.

HTTP/2 Rapid Reset




Hard

Enterprise

HTTP/2 Rapid Reset

We were able to capture the traffic from the web server, can you help us to figure out what

cl0p Ransom




Hard

Enterprise

cl0p Ransomware

Our friend fell victim to a ransomware attack and reached out to seek your expertise in analyzing

Royal Ransom




Medium

Enterprise

Royal Ransomware

Analyze the Royal ransomware malware

Python Stealer




Hard

Enterprise

Python Stealer

You are a security analyst tasked with analyzing a Python script that is suspected to be a malicious

Powershell Script



Easy

Powershell Script

You have a suspicious Powershell command and need to understand the purpose of this

Cyber Defenders



LabsTrain & CertifyFor EnterprisesTestimonialsMore

Sign InSign Up

CyberDefenders

A blue team training platform for
Threat Hunters.

CyberDefenders is a blue team training platform focused on the defensive side of cybersecurity to learn, validate, and advance CyberDefense skills.

Become a CyberDefender

Defenders everywhere use CyberDefenders

Google

IBM

Microsoft

CISCO

Meta

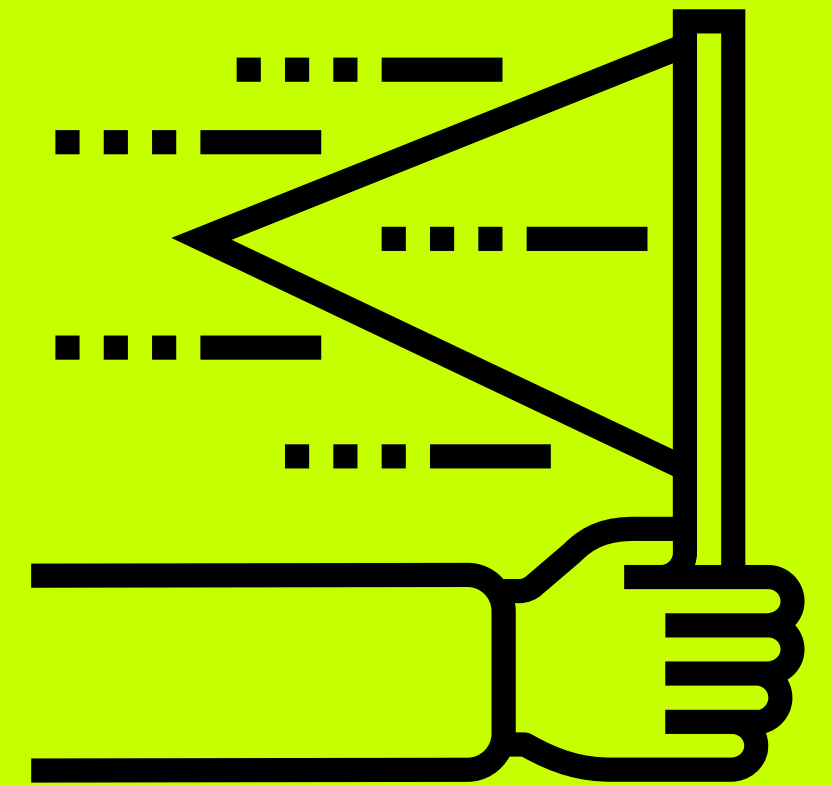
“

A CO Z WRITEUP'AMI?

Od zera do CTF Playera.

Poznań Security Meetup 2023

GARŚĆ DOBRYCH PORAD



1.

**Zdobądź podstawy
dotyczące m.in podatności
w aplikacjach webowych,
kryptografii itp.**

2.

Korzystaj z writeupów (zwłaszcza na początku)

3.

**Naucz się np. pythona,
bash, golanga czy innego
języka który pomoże Ci
zautomatyzować pewne
działania, napisać
customowego exploita.**

4.

Naucz się nieszablonowego myślenia - w CTF'ach bardzo często jest to "wymagane".

5.

**Jeśli nie możesz zrobić
jakiegoś zadania, warto się
przejsć, przespać i wrócić ze
świeżym spojrzeniem.**

6.

BAW SIĘ DOBRZE :)

Od zera do CTF Playera.

THE END

Od zera do CTF Playera.

Poznań Security Meetup 2023

**ZOSTAŃMY
W KONTAKCIE!**

