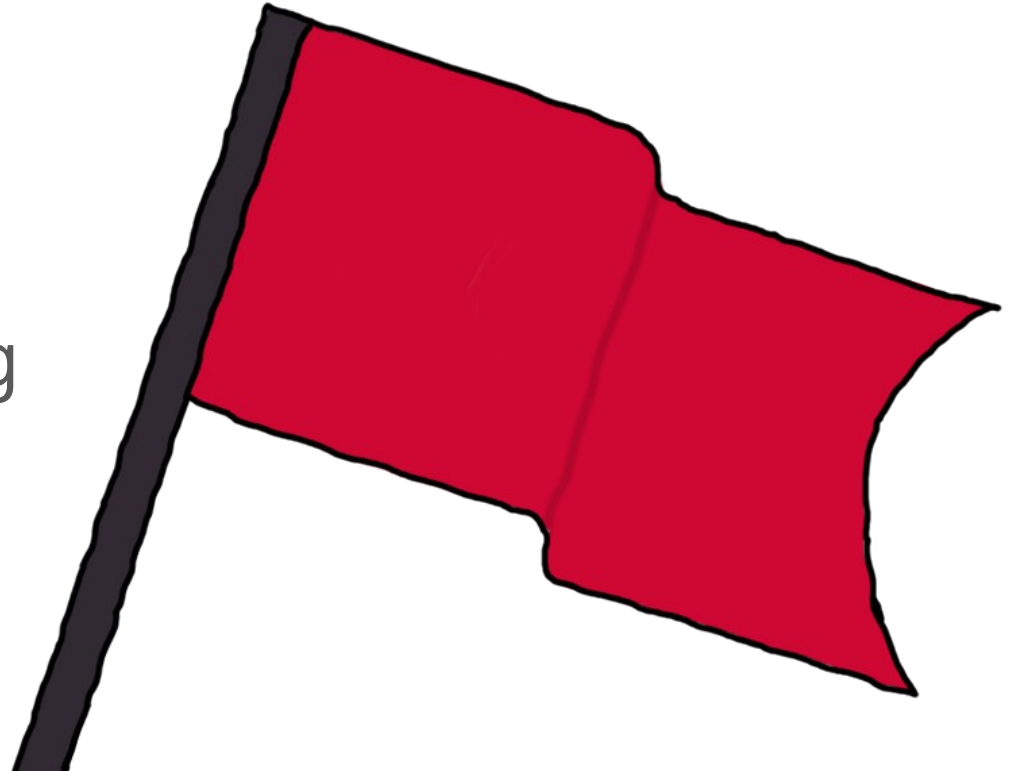
CTF

Capture The Flag



essembly

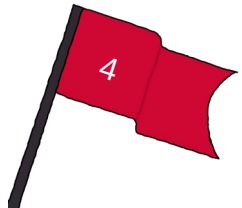
Agenda

1. Vorstellungsrunde
2. Was sind CTF-Wettbewerbe?
3. picoGym – Übungsplattform
4. CTF?

Bei Fragen/Anmerkungen einfach unterbrechen ;-)

Vorstellung

1. Wer bist du?
2. Welche Erfahrungen hast du mit CTFs?
3. Warum bist du hier?



Was ist CTF?

- IT-Security-Wettbewerbe
- Ziel: Flaggen durch das lösen von Aufgaben erbeuten
- eingereichte Flags geben Punkte
- Das Team mit den meisten Punkten gewinnt

Warum macht man das?

Fähigkeiten in Bereichen wie

- Binary Exploitation
- Reverse Engineering
- Kryptografie
- digitale Forensik
- WebApp-Security

testen und verbessern

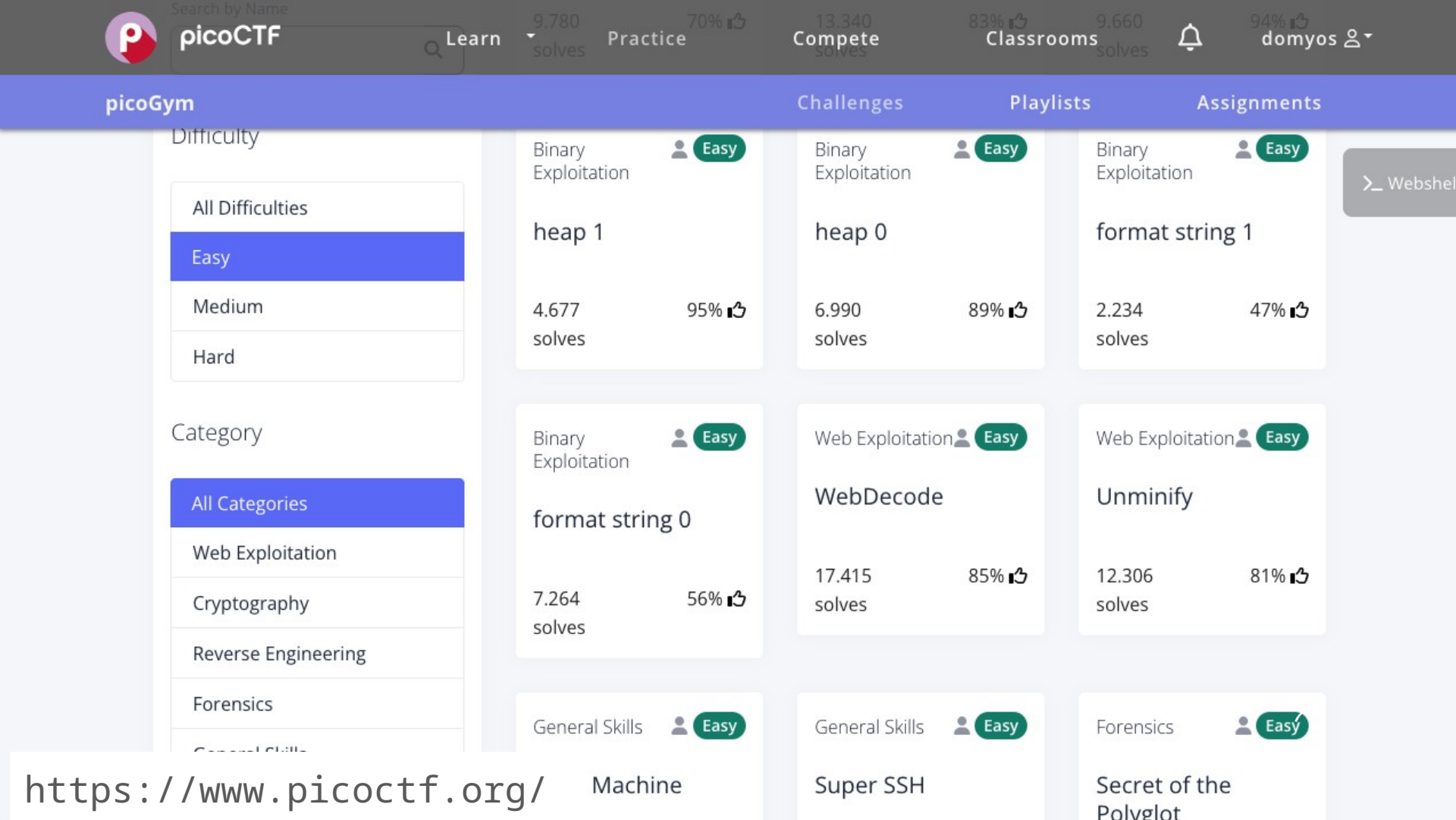
essembly

Jeopardy

- Aufgaben in unterschiedlichen Kategorien und mit unterschiedlichen Schwierigkeitsgraden
- Teams wählen und lösen die Aufgaben in beliebiger Reihenfolge
- Für jede erfolgreich eroberte Flagge gibt es Punkte

Attack-Defence

- jedes Team bekommt Zugriff auf ein Netzwerk an VMs
- Teams müssen die eigenen Systeme verteidigen (Sicherheitslücken schließen)
- und Systeme der anderen Teams angreifen (Sicherheitslücken ausnutzen)
- Punkte werden für erfolgreiche Angriffe und für die Aufrechterhaltung der Systemintegrität vergeben.



https://www.picoctf.org/

Unminify

Easy | Web Exploitation | picoCTF 2024 | obfuscation | browser_webshell_solvable | minification

AUTHOR: JEFFERY JOHN

Description

I don't like scrolling down to read the code of my website, so I've squished it. As a bonus, my pages load faster!

Additional details will be available after launching your challenge instance.

This challenge launches an instance on demand.

Its current status is: NOT_RUNNING

Launch Instance

Hints

1 2 3

12.308 users solved

81% Liked

picoCTF{FLAG}

Submit Flag

essembly

Wichtige Begriffe

- Flags
  - Lösungswort für eine Aufgabe
  - Beispiel: **vikeCTF{C0D3_8r34K3r5_637_Cr4CK1N6}**

- Writeups
  - https://ctftime.org/writeups
  - Im Discord nach dem event
  - Google: CTF-Name + Challenge-Name

Bock auf CTF?

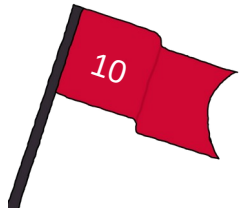
Einfach loslegen auf https://ctftime.org/

oder mit uns im Team Zwiebel zusammen spielen:

https://matrix.to/#/!RCDHiRbFTjbTLyHeSw:matrix.org?via=matrix.org

oder per E-Mail an kontakt@essembly.de

essembly



Jeopardy - Challengetypen (1)

- rev (reverse engineering)
  - Kompiliertes Programm, das auf Eingabe eines Lösungsworts wartet, gegeben.
  - Aufgabe: Prüfalgorithmus verstehen und Lösungswort finden
  - Lösungswort ist das Flag
- pwn (binary exploitation)
  - Kompiliertes Programm und IP + Port gegeben
  - Aufgabe:
    1. Lokal einen Exploit für das Programm finden (Code Execution)
    2. Dann mit Exploit das Flag auf dem Server auslesen
- crypto
  - Gegeben: verschlüsselter Text + Verschlüsselungscode
  - Aufgabe: Nachricht entschlüsseln
  - originaler Text ist das Flag

Jeopardy - Challengetypen (2)

- web
  - Webanwendung mit Sicherheitslücke gegeben
  - Aufgabe: Flag auf dem Server auslesen
  - bspw. mit SQLI, auth bypass, XSS, CSRF
- Forensic
  - verborgene Informationen in Digitalen Artefakten finden
  - bspw. Text in MP3 als Morse kodiert
  - oder Chatnachrichten aus PCAP extrahieren
- misc (prog)
  - alles andere
  - bspw: Minecraftbefehl erstellt QR-Code aus Wolle
  - diese QR-Code enthält das Flag

Übungen

https://ctftime.org/

https://www.picoctf.org/

https://overthewire.org/wargames/

https://cryptopals.com/

https://ctf.hackthebox.com

Lesematerial

https://www.reddit.com/r/securityCTF

https://www.reddit.com/r/ReverseEngineering/

https://www.reddit.com/r/crypto/

https://www.reddit.com/r/netsec/

Tools

https://dencode.com/

https://cyberchef.org/

https://www.kali.org/

https://portswigger.net/burp/communitydownload

https://www.usebruno.com/