

# Capture The Flag (CTF)

CTF kao uvod u računarsku bezbednost

Andrija Urošević

Univerzitet u Beogradu  
Matematički fakultet

April, 2022.

# Pregled

---

1. CTF takmičenja
2. Znanja i veštine koje se stiču kroz CTF
3. Problemi u CTF modelu
4. CTF na univerzitetskim kursevima
5. Zaključak

# CTF takmičenje

---

## Capture The Flag (CTF)

*Capture The Flag* (CTF) je takmičenje u oblasti računarske bezbednosti. Cilj takmičenja je pronaći *flag*-ove u nekom okruženju.

## Flag

*Flag* je tipično neki string karaktera, čiju specifikaciju daju organizatori takmičenja. *Flag* obično ima neki prefiks.

## Primer Flag-a

Prefiks: FLAG

*Flag*: FLAG{K73BSSxY3nFc1oAs9WwG}

# Vrste CTF takmičenja

---

## Jeopardy

U *Jeopardy* CTF-u, takmičari dobiju unapred zadate zadatke, koji su statični.

## Attack-Defence

*Attack-Defence* stil podrazumeva borbu između timova. Svaki tim ima sopstvenu mrežu koja ima ranjive servise. Cilj je “zakrpiti” ranjive servise, i u isto vreme eksploatisati druge timove.

## Mixed

*Mixed* CTF može biti različitih formata, ali kao što ime sugerije predstavlja mešavinu prethodna dva stila.

# Popularna CTF takmičenja

## CTF takmičenja

DEFCON CTF, UCSB iCTF, Mozilla CTF, Facebook CTF, Google CTF, PHD CTF, RuCTFe, Hack.lu CTF, SECUINSIDE CTF, rwth CTF, CSAW CTF, PICO CTF,..., DESCON CTF [CTFTime.org] [DESCON.me]

```
DEFCON CTF finals 2021 (whole game)

service milestones
time in play : 1 days, 23 hrs, 36 min, 17 sec
from firstblood : 2 days, 2 hrs, 13 min, 29 sec
firstblood team : StarBugs
last flag steal : 0 days, 0 hrs, 40 min, 57 sec

round progress
old round : 329
round began at : 21:32:46 UTC

service progress
ooo now : spawning containers
patch rule : 000 policy
pcaps : (service by service)
indicator : awesome!

round pwns / global score
DiceGang : 658 / 194
HITCONwBalsn : 939 / 398
Katzebln : 2703 / 869
rhackeroni : 612 / 183
NorseCode : 778 / 193
Null : 1134 / 269
ooorganizers : 834 / 286
pasten : 297 / 118
PPP : 2288 / 824
PTB_MTL : 1146 / 260
r3kapi0 : 386 / 145
Shellphish : 599 / 175
StarBugs : 2707 / 539
PerfctxGuesr : 1092 / 323
Teabellvrs : 1573 / 551
Samurai : 824 / 260

attack stats
rounds played : 328
flags stolen : 18570
teams pwning : 16
teams pwned : 16

patch stats
attempted : 510 patching attempts
functional: 274 patches deployed
what is this thing?!!

A real, live attack/defense CTF game
Olympics of Hacking, since 1996!

brought to you by
Order of the Overflow
want to play?
archive.ooo
keep being awesome!

every team both pwned and was pwned [rtc0: RETIRED]
```

Slika: DEFCON CTF finale 2021

# CSEC2017 oblasti znanja

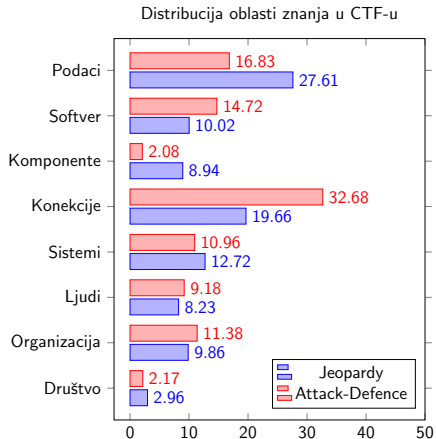
---

## CyberSecurity Curricula 2017

[CSEC2017] definiše osam oblasti znanja u računarskoj bezbednosti:

1. Bezbednost podataka
2. Bezbednost softvera
3. Bezbednost komponenti
4. Bezbednost konekcije
5. Bezbednost sistema
6. Bezbednost ljudi
7. Organizaciona bezbednost
8. Društvena bezbednost

# Distribucija oblasti znanja u CTF zadacima



Slika: Distribucija oblasti znanja u 15879 *jeopardy* i 86 *attack-defense writeup*-ova.[Švabenski i dr. 2021.]

# Problemi u CTF modelu

---

[Čang i Koen, 2021.] pronalaze sledeće probleme u CTF modelu:

1. Težina igre
2. Relacija između dizajna zadataka i njegove uspešnosti pri rešavanju
3. Dokaz o kvalitetu
4. Poeni i njihov obrnuti efekat na takmičare i organizatore
5. Infrastruktura zadataka
6. Dvosmisleni zadaci



# CTF na univerzitetским kursevima

---

Osobina	CTF	CCTF
Pripremanje	nekoliko meseci	nekoliko nedelja
Trajanje	1-2 dana	2 časa
Uloge timova	crveni ili plavi	crveni i plavi
Uparivanje timova	svi na sve	parovi
Učestalost	jednom godišnje	2-3 puta po semestru
Analiza	retko	uvek
Težina	stručni	početni do srednji

Tabela: Upoređivanje CTF-a i CCTF-a.[Mirković i Piterson, 2014.]

# Poboljšanje edukacija kroz CTF

---

[Leune i Petrilli, 2017.] u svom radu pokazuju sledeće hipoteze:

1. Samopouzdanje studenata će se povećati učestvovanjem u CTF-u.
2. Studenti će uživati u CTF-u.
3. Studenti će steći praktične veštine učestvovanjem u CTF-u.
4. Učestvovanje u CTF potkrepljuje teorijske koncepte.

# Prednosti i mane CTF-a na kursevima

---

[Vikopa i dr, 2020.]:

- Performanse studenata
- Korisno navođenje
- Deljenje CTF *flag*-ova
- CTF igre sa studentske strane

# Zaključak

---

## Gejmifikacija kroz CTF

Gejmifikacija u obliku CTF-a se pokazuje kao veoma dobar alat za učenje o računarskoj bezbednosti, uz savladive probleme koje donosi.

# Reference

---



## CTFTime

All about CTF (Capture The Flag)

[ctftime.org](https://ctftime.org)



## DESCON CTF

DESCON IoT Hackathon

[descon.me](https://descon.me)




## Over The Wire


We're hackers, and we are good-looking. We are 1%.

[overthewire.org](https://overthewire.org)

# Reference

---

 CyberSecurity Curricula 2017  
Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity  
*Joint Task Force*

 Švábenský, Valdemar i Celeda, Pavel i Vykopal, Jan i Brisakova, Silvia  
Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges  
*Elsevier Computers & Security*, 2021.

 Kevin Chung i Julian Cohen  
Learning Obstacles in the Capture The Flag Model  
*USENIX Summit on Gaming, Games, and Gamification in Security Education*, 2014.

# Reference

---



Jelena Mirković i Peter A. H. Peterson.

Class Capture-the-Flag Exercises

*USENIX Summit on Gaming, Games, and Gamification in Security Education*, 2014.



Kees Leune i Salvatore J. Petrilli

Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education

*Proceeding of the 18th Annual Conference on Information Technology Education*, str. 47-52, 2017.



Jan Vykopal, Valdemar Švábenský i Ee-Chien Chang

Benefits and Pitfalls of Using Capture the Flag Games in University Courses

2020.

# Pitanja?