



CTF Competitions

Ali Ghaffarian

May 4, 2025

About Me

- FlagMotori member
- CTF categories
 - Traffic analysis
 - Reverse engineering
 - pwn
- Interested in
 - operating systems
 - computer networks
- Github: github.com/AliGhaffarian

FlagMotori

- 2024 Ranking: 2nd in Iran, 73rd worldwide
- Organized the Nowruz 1404 CTF


 Iran, Islamic Republic of				
Worldwide position	Country position	Name	Points	Events
24	👑1	ASIS	570.393	11
73	2	FlagMotori	376.368	73
908	3	Disqualified	53.987	16
952	4	Execut3	51.611	15

Table of content

- What is CTF?
- Types of CTF
 - Attack and Defense
 - Jeopardy
- Types of CTF Challenges
- How to Get Started
- CTFtime Walk through

What is CTF?

Jeopardy

Filters

- ☐ Hide Solved
- ☐ Show Bookmarked
- ☐ Show Assigned

Search by Name

Difficulty

All Difficulties

Easy

Medium

Hard

Category

All Categories

Web Exploitation

Cryptography

« < 1 2 3 4 5 6 7 > »

Web Exploitation

Easy

SSTI1

5,930 solves

96%

Binary Exploitation

Easy

PIE TIME

3,212 solves

95%

Web Exploitation

Easy

n0s4n1ty 1

4,361 solves

98%

Web Exploitation

Easy

head-dump

5,657 solves

73%

Cryptography

Easy

hashcrack

7,243 solves

95%

Reverse Engineering

Easy

Flag Hunters

3,717 solves

90%

General Skills

Easy

FANTASY CTF

10,003 solves

87%

Cryptography

Easy

EVEN RSA CAN BE BROKEN???

3,950 solves

96%

Web Exploitation

Easy

Cookie Monster Secret Recipe

8,179 solves

94%

General Skills

Easy

General Skills

Easy

General Skills

6
Easy

Attack and Defense

- Secure your server, attack other's
- Not as common as jeopardy
- More complex and expensive

Types of CTF Challenges

- Web Exploitation
- Binary Exploitation (pwn)
- Reverse Engineering
- Cryptography
- Misc

Web Exploitation

picoCTF-SQLiLite (2/10)

Binary Exploitation (pwn)

- Nowruz 1404-Seen shopping (2/10)

Seens and quantities

Seen	Cost	quantity
Sabzeh	30000	0
Senjed	20000	1
Seer	20000	2
Seeb	10000	3
Samanu	35000	4
Serkeh	40000	0
Sekkeh	80000000	6

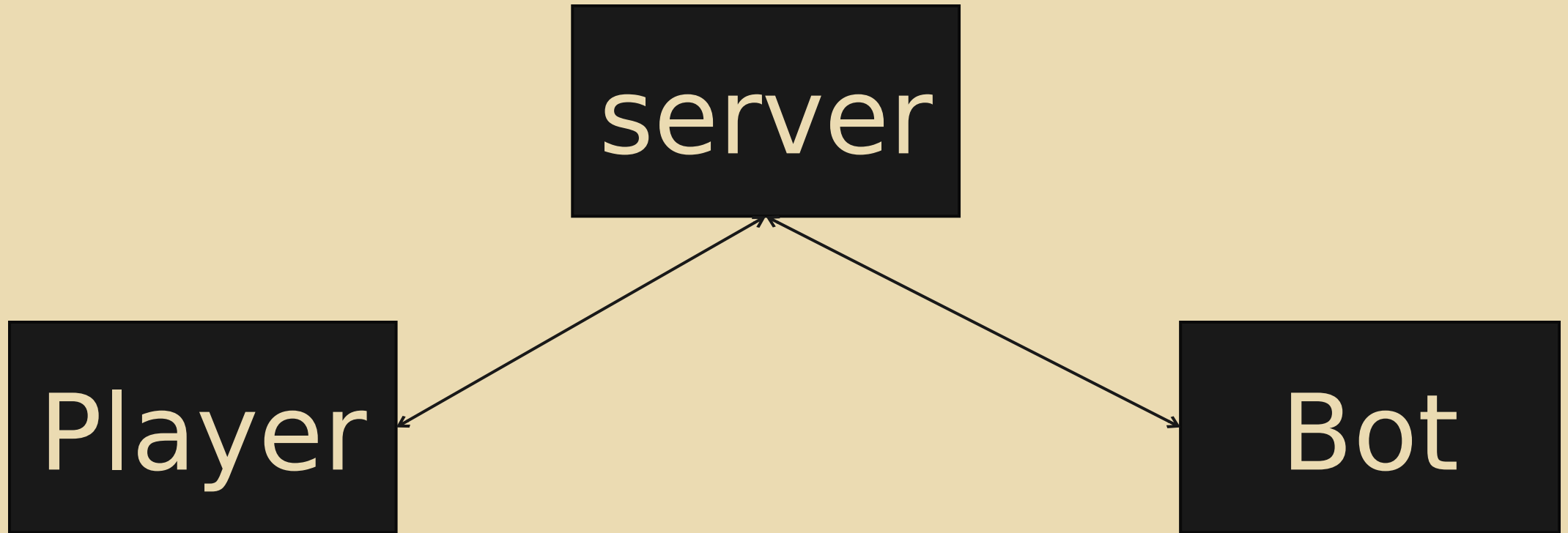
Reverse Engineering

- picoCTF- Transformation (1/10)

Misc

- TFCCTF-bad-invaders (3/10)

TFCCTF-bad_invaders



Player

```
struct Player {  
    int Id,  
    string Name,  
    int Position,  
    tcp_socket Connection  
}
```

Generate playerId

```
int GenerateId() {  
    return rand.Intn(100)  
}
```

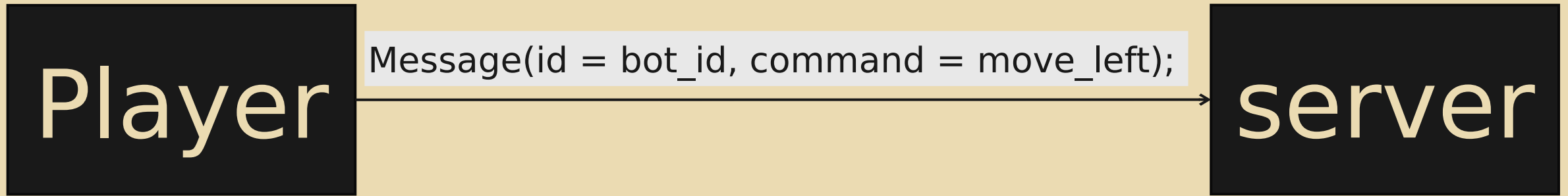

playerExists logic

```
playerExists = false
for _, player in range game.Players {
    if player.Connection == connection {
        playerExists = true
        break
    }
}
```

Server's logic

1. Read until ';'
2. If player is not registered, allow only register command
3. Get playerId from received message
4. Execute the command on playerId

Our Approach?



- Player is registered (allowed to request commands)
- Message contains id of bot
- Server accepts message and executes the command

How to Get Started

writeups.fmc.tf

Some Tips

- CTF is HARD!
- Lookout for bad challenges

Thank You