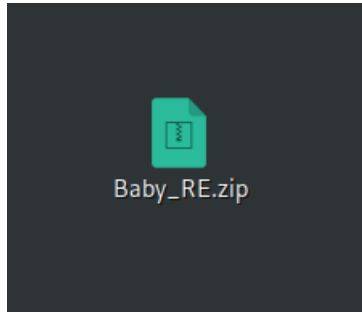


# BabyRE

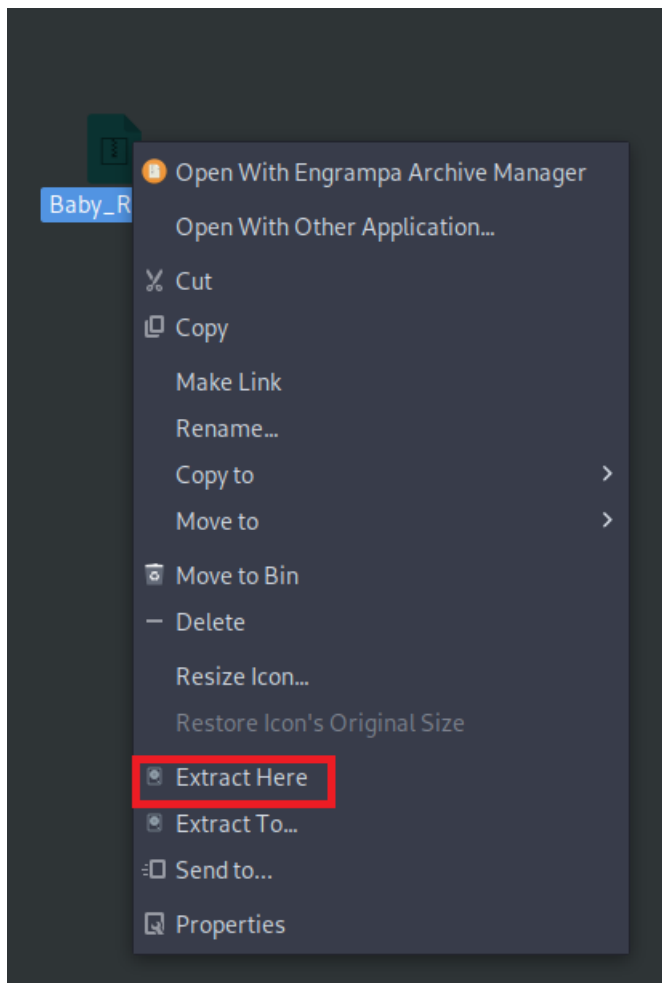


*Reported by kaiUb (<https://github.com/kaiUb777>)*

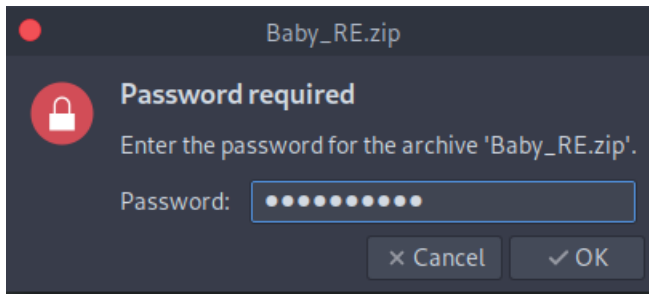
## ***1. Folder to decompress***



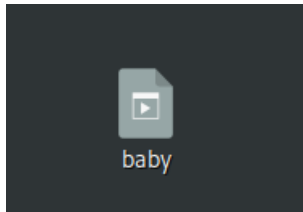
## ***2. Unzipped file***



### 3. Insert the password for extract the file content (pw: hackthebox)



### 4. Decompressed file



### 5. Use radar2 to see file content (reversing)

```
[root@parrot]-[/home/kaiub/Desktop]
#r2 -A baby
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze function calls (aac)
[x] Analyze len bytes of instructions for references (aar)
[x] Check for objc references
[x] Check for vtables
[x] Type matching analysis for all functions (aaft)
[x] Propagate noreturn information
[x] Use -AA or aaaa to perform additional experimental analysis.
[0x00001070]> pdf@main
```

## 6. Found the flag!

```
0x000011a3 48b84854427b. movabs rax, 0x594234427b425448 ; 'HTB
0x000011ad 48ba5f523356. movabs rdx, 0x3448545f5633525f ; '
0x000011b7 488945c0      mov qword [s], rax
0x000011bb 488955c8      mov qword [var_38h], rdx
0x000011bf c745d054535f. mov dword [var_30h], 0x455f5354 ; '
0x000011c6 66c745d45a7d mov word [var_2ch], 0x7d5a ; '}'
0x000011cc 488d45c0      lea rax, qword [s]
0x000011d0 4889c7        mov rdi, rax ; const c
char *s
0x000011d3 e858feffff    call sym.imp.puts ; int put
s(const char *s)
0x000011d8 eb0c          jmp 0x11e6
; CODE XREF from main @ 0x11a1
0x000011da 488d3d7f0e00. lea rdi, qword str.Try_again_later. ;
0x2060 ; "Try again later." ; const char *s
0x000011e1 e84afeffff    call sym.imp.puts ; int put
```