Natjecanja u informacijskoj sigurnosti

Žad Deljkić

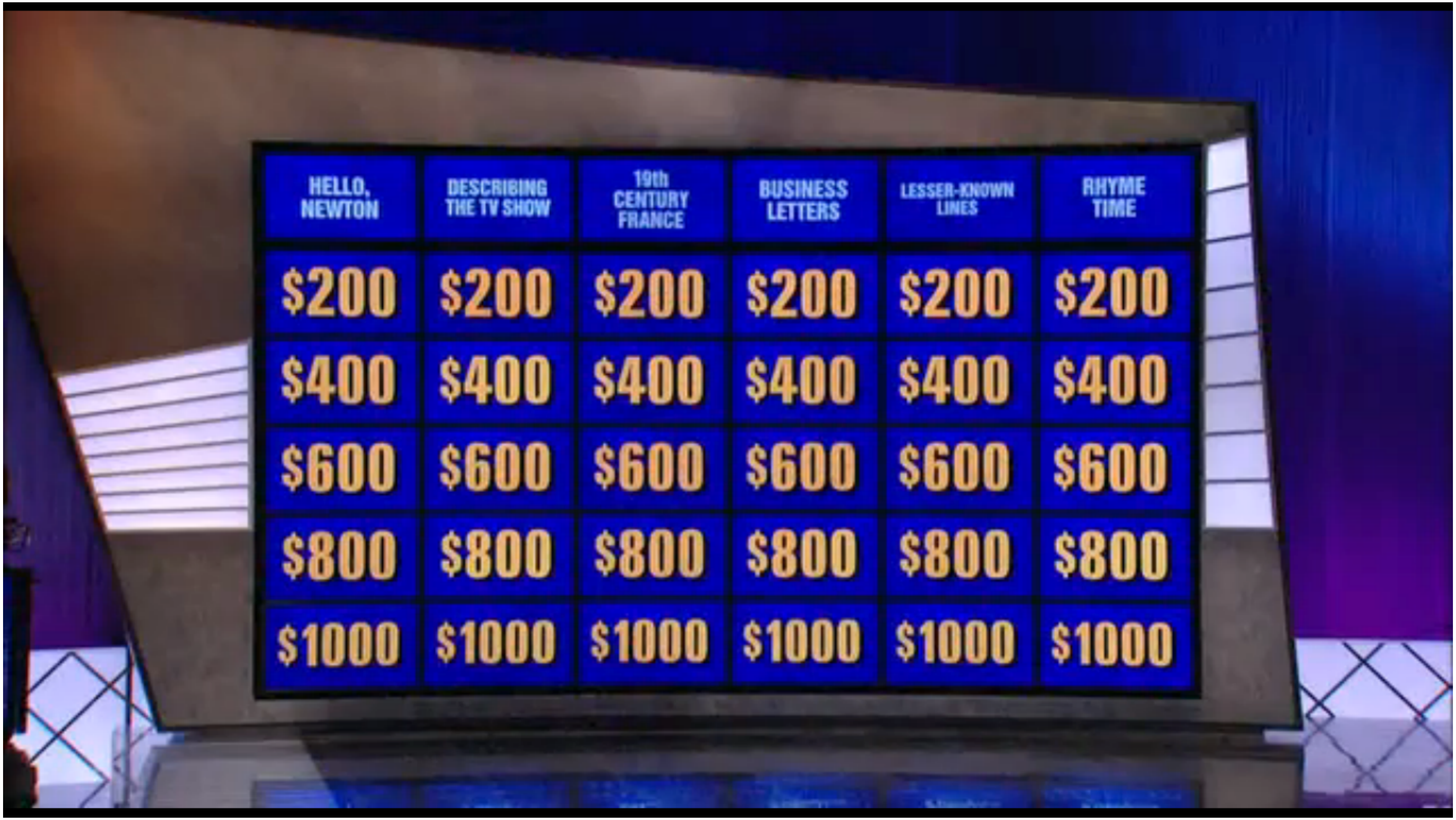
Informacijska sigurnost?

- **"Cyber" sigurnost, računalna sigurnost, mrežna sigurnost ...**
  - Ali i ne samo vezano uz računala!
- **Fizička sigurnost**
  - Npr. brava na vratima, sef
- **Ljudska komponenta sigurnosti**
- **...**
- **Nije samo tajnost!**
  - Integritet, dostupnost ...

Natjecanja

- **Razni formati natjecanja**
- **"CTF" natjecanja**
  - CTF = *Capture The Flag*
- **Flag – informacija koju želimo**
- **Razni formati CTF natjecanja**

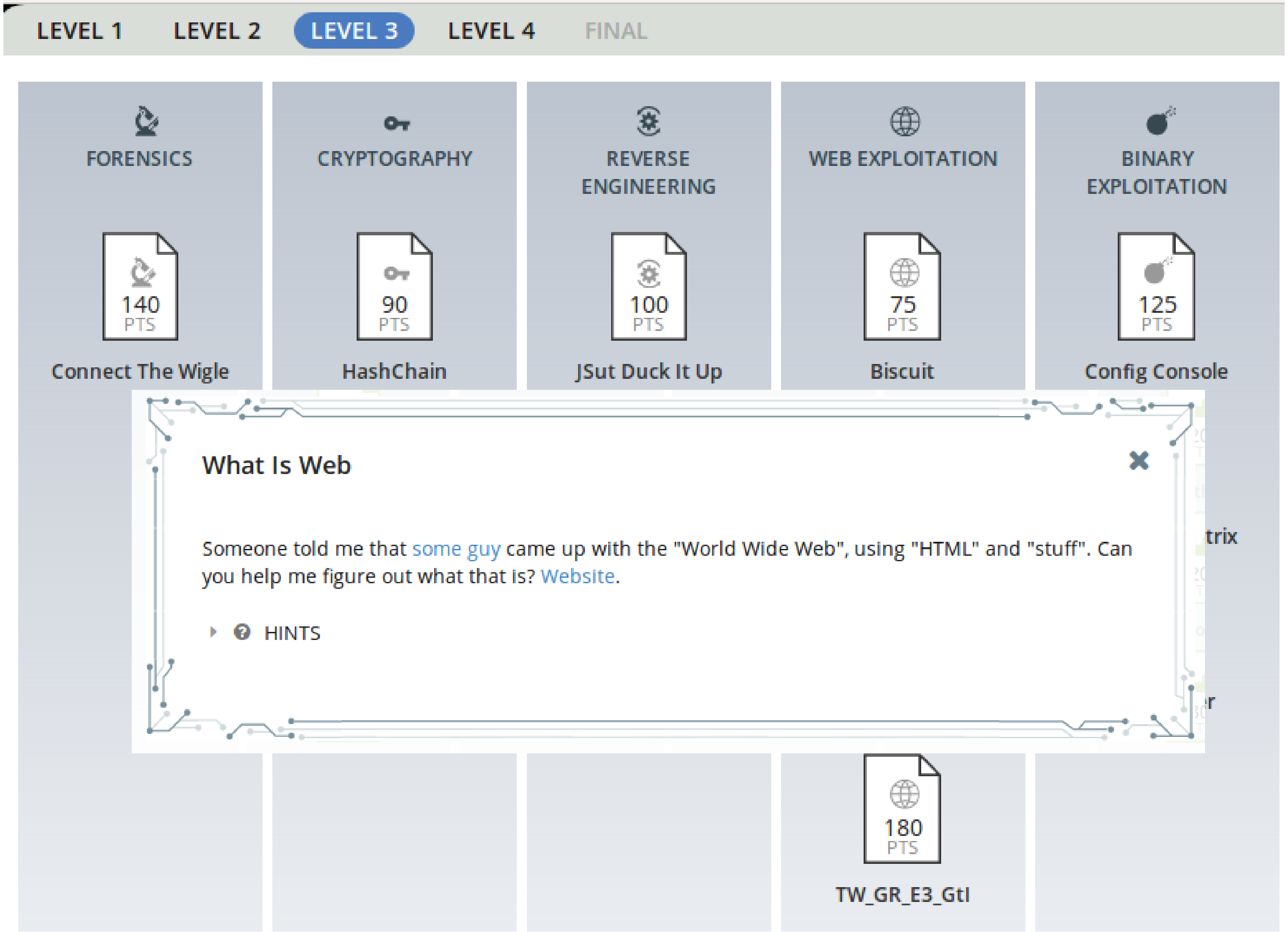
Jeopardy!



HELLO, NEWTON	DESCRIBING THE TV SHOW	19th CENTURY FRANCE	BUSINESS LETTERS	LESSER-KNOWN LINES	RHYME TIME
$200	$200	$200	$200	$200	$200
$400	$400	$400	$400	$400	$400
$600	$600	$600	$600	$600	$600
$800	$800	$800	$800	$800	$800
$1000	$1000	$1000	$1000	$1000	$1000

http://gameshows.wikia.com/wiki/File:Jeopardy_Wallpaper_7.png

Jeopardy natjecanje (picoCTF 2017)



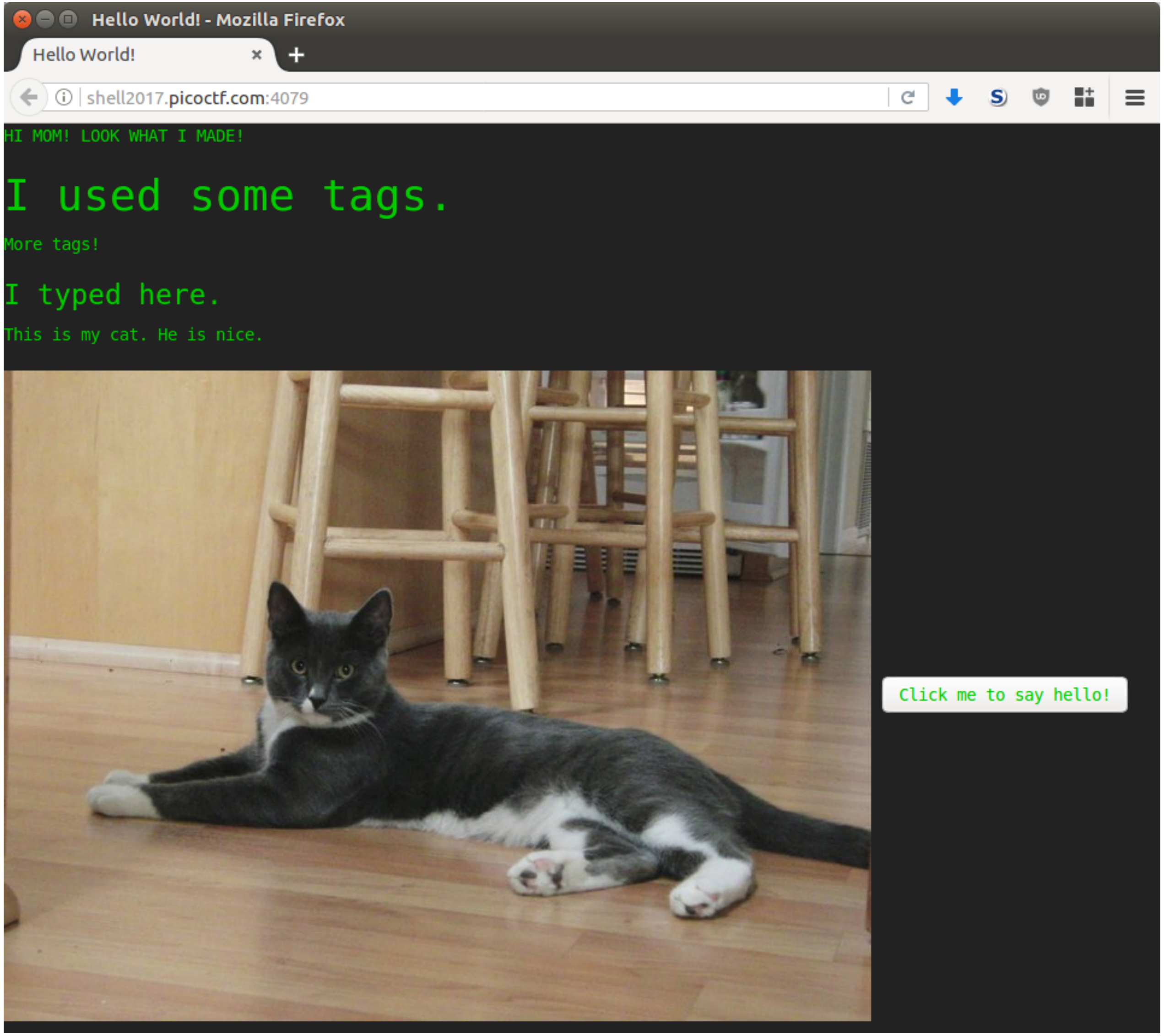
What Is Web

✖

Someone told me that some guy came up with the "World Wide Web", using "HTML" and "stuff". Can you help me figure out what that is? Website.

HINTS

Primjer zadatka (web sigurnost)



HI MOM! LOOK WHAT I MADE!

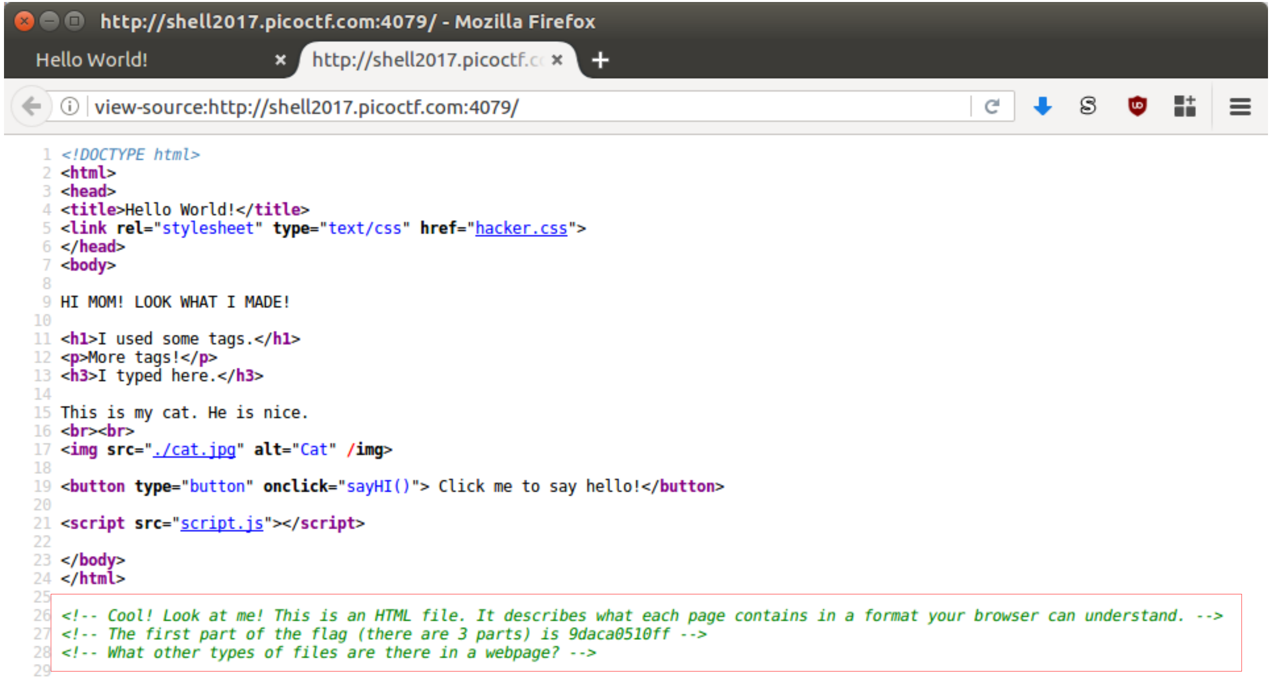
I used some tags.

More tags!

I typed here.

This is my cat. He is nice.

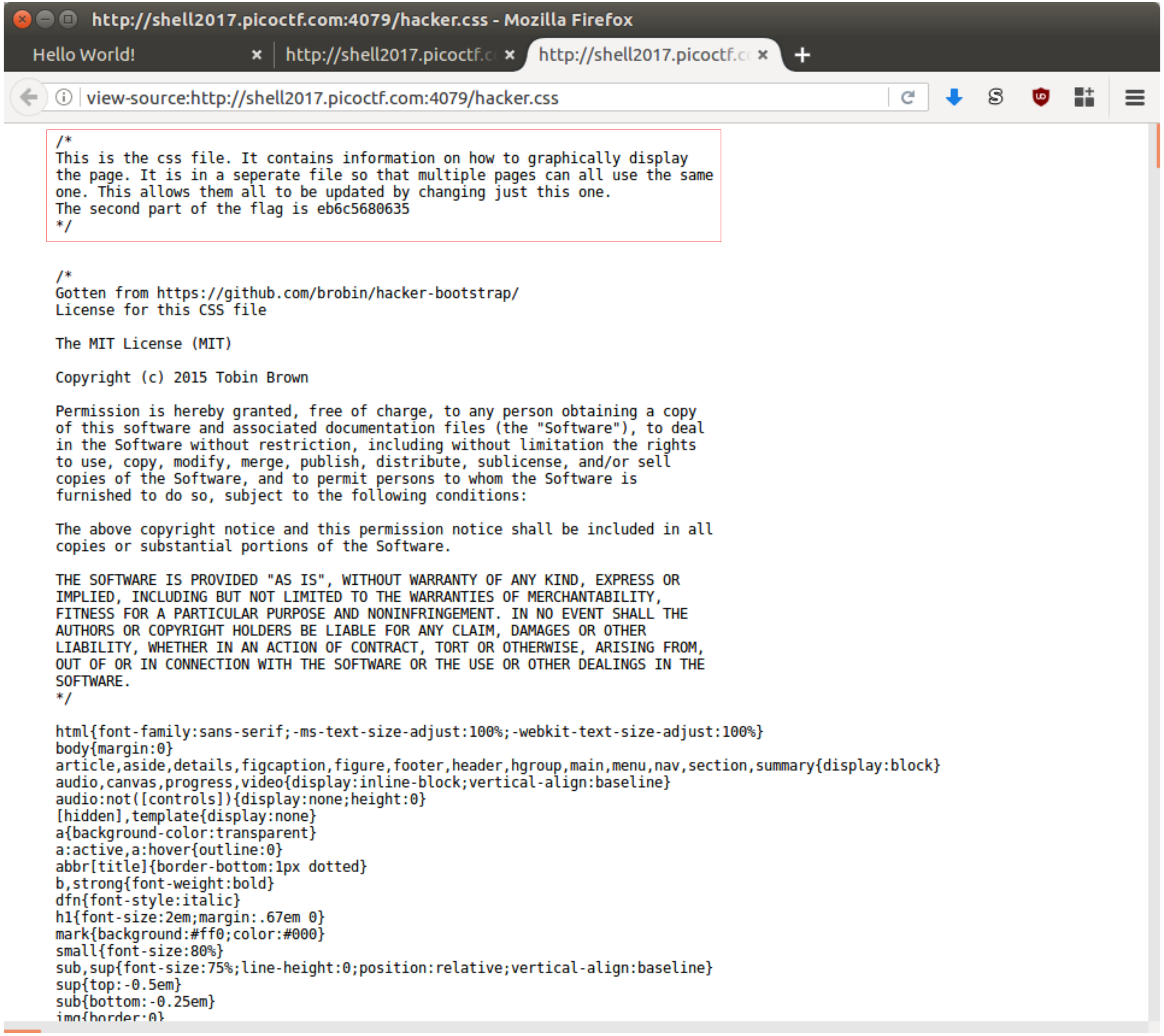
Primjer zadatka (web sigurnost)



http://shell2017.picoctf.com:4079/ - Mozilla Firefox
Hello World!
http://shell2017.picoctf.c
view-source:http://shell2017.picoctf.com:4079/

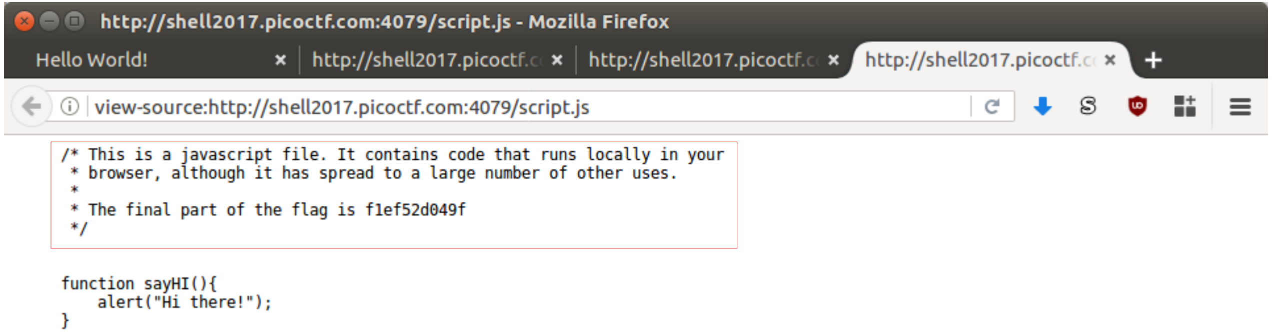
```html
<!DOCTYPE html>
<html>
<head>
<title>Hello World!</title>
<link rel="stylesheet" type="text/css" href="hacker.css">
</head>
<body>

HI MOM! LOOK WHAT I MADE!

<h1>I used some tags.</h1>
<p>More tags!</p>
<h3>I typed here.</h3>

This is my cat. He is nice.
<br><br>
<img src="./cat.jpg" alt="Cat" /img>

<button type="button" onclick="sayHI()"> Click me to say hello!</button>

<script src="script.js"></script>

</body>
</html>

<!-- Cool! Look at me! This is an HTML file. It describes what each page contains in a format your browser can understand. -->
<!-- The first part of the flag (there are 3 parts) is 9daca0510ff -->
<!-- What other types of files are there in a webpage? -->

```

Primjer zadatka (web sigurnost)


http://shell2017.picoctf.com:4079/hacker.css - Mozilla Firefox
Hello World!
http://shell2017.picoctf.c
http://shell2017.picoctf.c
view-source:http://shell2017.picoctf.com:4079/hacker.css

```
/*
This is the css file. It contains information on how to graphically display
the page. It is in a seperate file so that multiple pages can all use the same
one. This allows them all to be updated by changing just this one.
The second part of the flag is eb6c5680635
*/


/*
Gotten from https://github.com/brobin/hacker-bootstrap/
License for this CSS file

The MIT License (MIT)

Copyright (c) 2015 Tobin Brown

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.
*/

html{font-family:sans-serif;-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%}
body{margin:0}
article,aside,details,figcaption,figure,footer,header,hgroup,main,menu,nav,section,summary{display:block}
audio,canvas,progress,video{display:inline-block;vertical-align:baseline}
audio:not([controls]){display:none;height:0}
[hidden],template{display:none}
a{background-color:transparent}
a:active,a:hover{outline:0}
abbr[title]{border-bottom:1px dotted}
b,strong{font-weight:bold}
dfn{font-style:italic}
h1{font-size:2em;margin:.67em 0}
mark{background:#ff0;color:#000}
small{font-size:80%}
sub,sup{font-size:75%;line-height:0;position:relative;vertical-align:baseline}
sup{top:-0.5em}
sub{bottom:-0.25em}
img{border:0}
```

Primjer zadatka (web sigurnost)

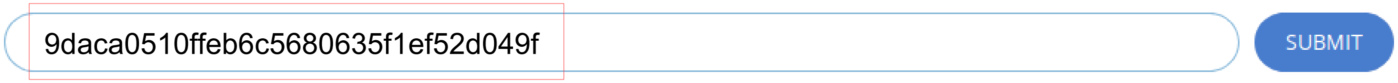


http://shell2017.picoctf.com:4079/script.js - Mozilla Firefox
Hello World!
http://shell2017.picoctf.c
http://shell2017.picoctf.c
http://shell2017.picoctf.c
view-source:http://shell2017.picoctf.com:4079/script.js

```
/* This is a javascript file. It contains code that runs locally in your
 * browser, although it has spread to a large number of other uses.
 *
 * The final part of the flag is f1ef52d049f
 */


function sayHI(){
    alert("Hi there!");
}
```

Primjer zadatka (web sigurnost)

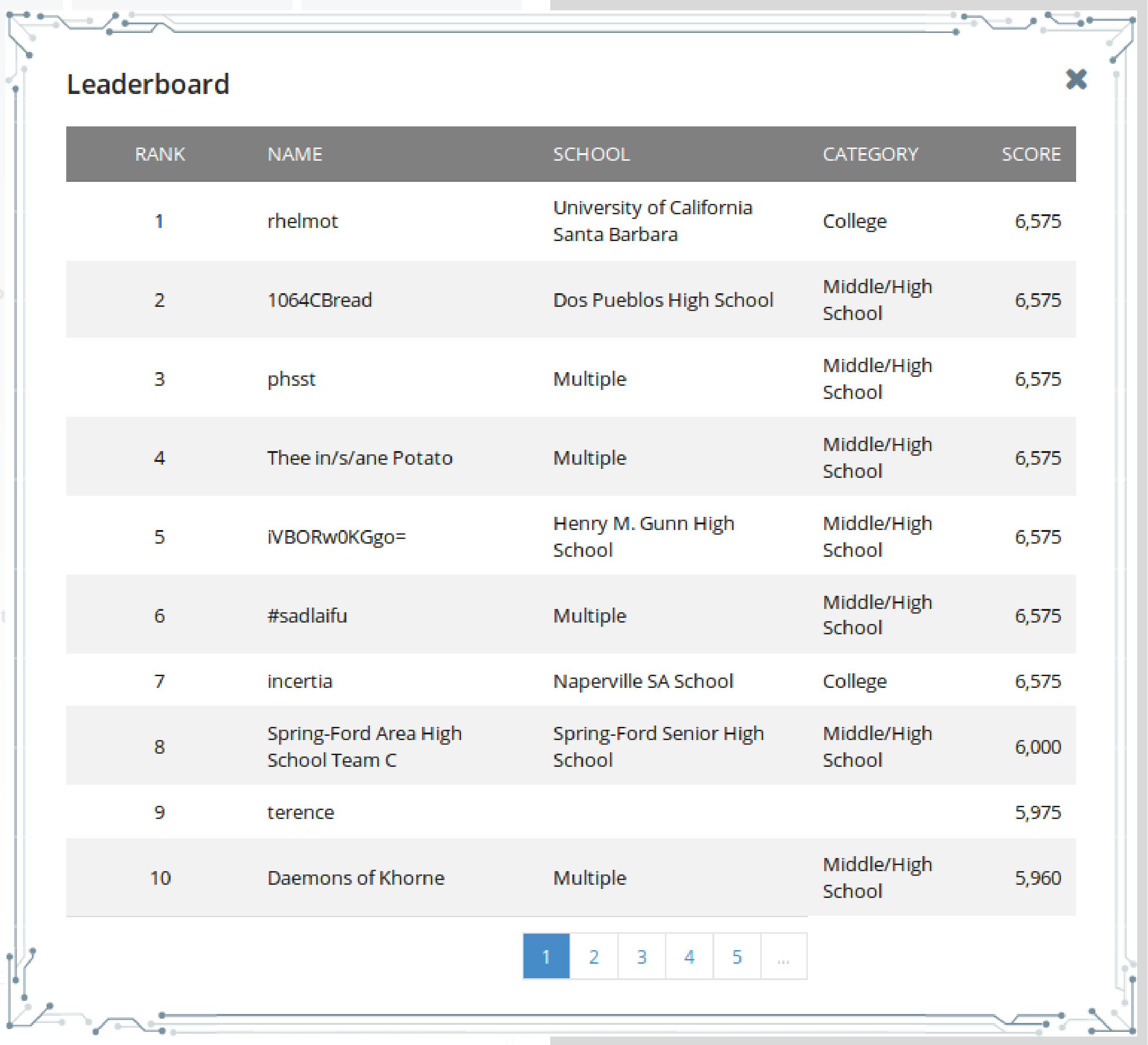
Correct!
+20 Points!



9daca0510ffeb6c5680635f1ef52d049f

Rješenje = *flag*
(zato *Capture The Flag*)

Primjer zadatka (web sigurnost)



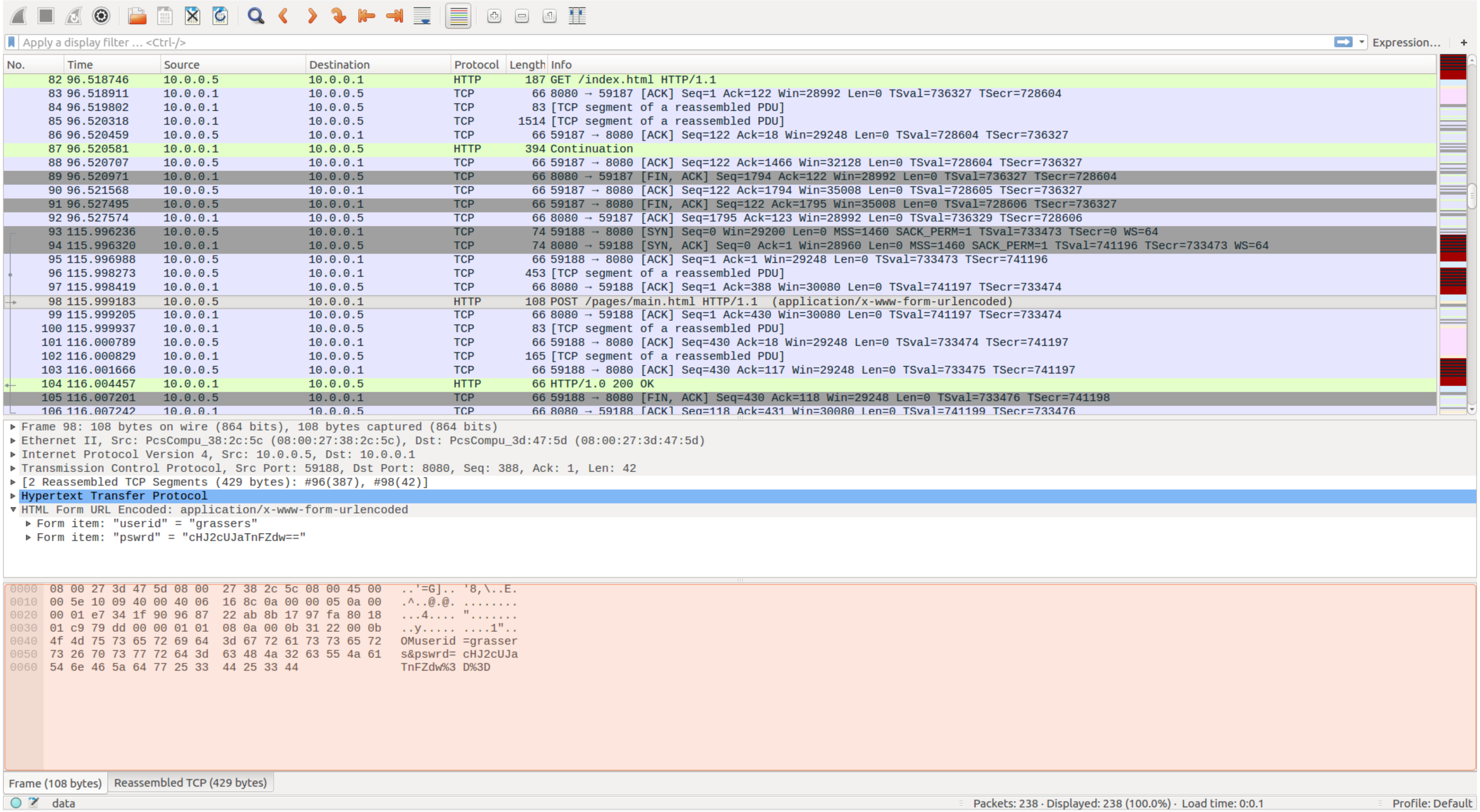
Leaderboard

RANK	NAME	SCHOOL	CATEGORY	SCORE
1	rhelmot	University of California Santa Barbara	College	6,575
2	1064CBread	Dos Pueblos High School	Middle/High School	6,575
3	phsst	Multiple	Middle/High School	6,575
4	Thee in/s/ane Potato	Multiple	Middle/High School	6,575
5	iVBORw0KGgo=	Henry M. Gunn High School	Middle/High School	6,575
6	#sadlaifu	Multiple	Middle/High School	6,575
7	incertia	Naperville SA School	College	6,575
8	Spring-Ford Area High School Team C	Spring-Ford Senior High School	Middle/High School	6,000
9	terence			5,975
10	Daemons of Khorne	Multiple	Middle/High School	5,960

Kategorije

- Web sigurnost
- Kriptografija
- Forenzika
- *Reverse Engineering*
- Razvoj *exploita*
- Steganografija
- Mobilna sigurnost
- Zakrpavanje rupa
- Programiranje ...

Forenzika



```
No.  Time        Source    Destination Protocol Length Info
 82 96.518746   10.0.0.5  10.0.0.1    HTTP      187 GET /index.html HTTP/1.1
 83 96.518911   10.0.0.1  10.0.0.5    TCP        66 8080 → 59187 [ACK] Seq=1 Ack=122 Win=28992 Len=0 TSval=736327 TSecr=728604
 84 96.519802   10.0.0.1  10.0.0.5    TCP        83 [TCP segment of a reassembled PDU]
 85 96.520318   10.0.0.1  10.0.0.5    TCP      1514 [TCP segment of a reassembled PDU]
 86 96.520459   10.0.0.5  10.0.0.1    TCP        66 59187 → 8080 [ACK] Seq=122 Ack=18 Win=29248 Len=0 TSval=728604 TSecr=736327
 87 96.520581   10.0.0.1  10.0.0.5    HTTP      394 Continuation
 88 96.520707   10.0.0.5  10.0.0.1    TCP        66 59187 → 8080 [ACK] Seq=122 Ack=1466 Win=32128 Len=0 TSval=728604 TSecr=736327
 89 96.520971   10.0.0.1  10.0.0.5    TCP        66 8080 → 59187 [FIN, ACK] Seq=1794 Ack=122 Win=28992 Len=0 TSval=736327 TSecr=728604
 90 96.521568   10.0.0.5  10.0.0.1    TCP        66 59187 → 8080 [ACK] Seq=122 Ack=1794 Win=35008 Len=0 TSval=728605 TSecr=736327
 91 96.527495   10.0.0.5  10.0.0.1    TCP        66 59187 → 8080 [FIN, ACK] Seq=122 Ack=1795 Win=35008 Len=0 TSval=728606 TSecr=736327
 92 96.527574   10.0.0.1  10.0.0.5    TCP        66 8080 → 59187 [ACK] Seq=1795 Ack=123 Win=28992 Len=0 TSval=736329 TSecr=728606
 93 115.996236  10.0.0.5  10.0.0.1    TCP        74 59188 → 8080 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=733473 TSecr=0 WS=64
 94 115.996320  10.0.0.1  10.0.0.5    TCP        74 8080 → 59188 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=741196 TSecr=733473 WS=64
 95 115.996988  10.0.0.5  10.0.0.1    TCP        66 59188 → 8080 [ACK] Seq=1 Ack=1 Win=29248 Len=0 TSval=733473 TSecr=741196
 96 115.998273  10.0.0.5  10.0.0.1    TCP       453 [TCP segment of a reassembled PDU]
 97 115.998419  10.0.0.1  10.0.0.5    TCP        66 8080 → 59188 [ACK] Seq=1 Ack=388 Win=30080 Len=0 TSval=741197 TSecr=733474
 98 115.999183  10.0.0.5  10.0.0.1    HTTP      108 POST /pages/main.html HTTP/1.1  (application/x-www-form-urlencoded)
 99 115.999205  10.0.0.1  10.0.0.5    TCP        66 8080 → 59188 [ACK] Seq=1 Ack=430 Win=30080 Len=0 TSval=741197 TSecr=733474
100 115.999937  10.0.0.1  10.0.0.5    TCP        83 [TCP segment of a reassembled PDU]
101 116.000789  10.0.0.5  10.0.0.1    TCP        66 59188 → 8080 [ACK] Seq=430 Ack=18 Win=29248 Len=0 TSval=733474 TSecr=741197
102 116.000829  10.0.0.1  10.0.0.5    TCP       165 [TCP segment of a reassembled PDU]
103 116.001666  10.0.0.5  10.0.0.1    TCP        66 59188 → 8080 [ACK] Seq=430 Ack=117 Win=29248 Len=0 TSval=733475 TSecr=741197
104 116.004457  10.0.0.1  10.0.0.5    HTTP       66 HTTP/1.0 200 OK
105 116.007201  10.0.0.5  10.0.0.1    TCP        66 59188 → 8080 [FIN, ACK] Seq=430 Ack=118 Win=29248 Len=0 TSval=733476 TSecr=741198
106 116.007242  10.0.0.1  10.0.0.5    TCP        66 8080 → 59188 [ACK] Seq=118 Ack=431 Win=30080 Len=0 TSval=741199 TSecr=733476
```

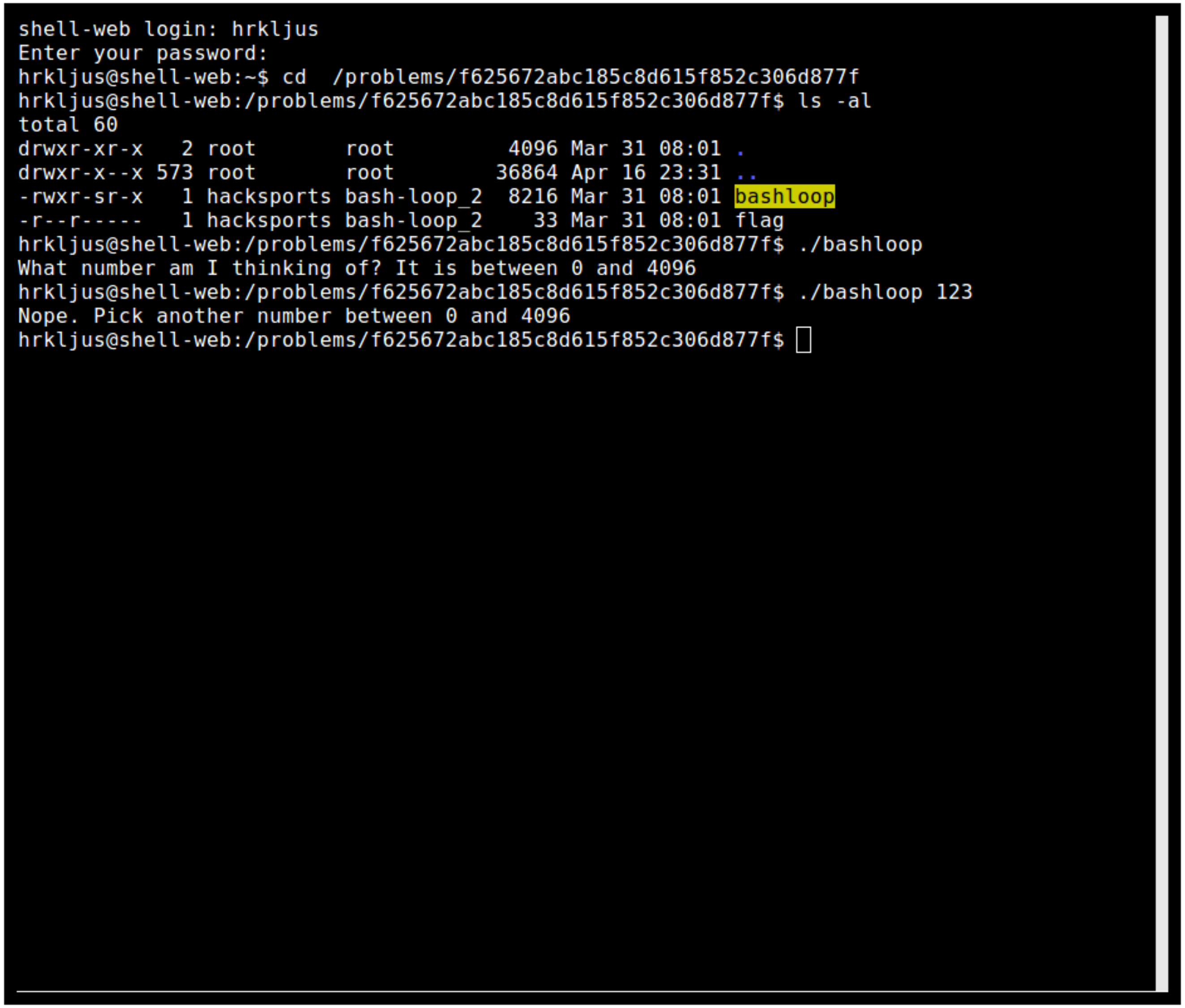
```
▸ Frame 98: 108 bytes on wire (864 bits), 108 bytes captured (864 bits)
▸ Ethernet II, Src: PcsCompu_38:2c:5c (08:00:27:38:2c:5c), Dst: PcsCompu_3d:47:5d (08:00:27:3d:47:5d)
▸ Internet Protocol Version 4, Src: 10.0.0.5, Dst: 10.0.0.1
▸ Transmission Control Protocol, Src Port: 59188, Dst Port: 8080, Seq: 388, Ack: 1, Len: 42
▸ [2 Reassembled TCP Segments (429 bytes): #96(387), #98(42)]
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
   ▸ Form item: "userid" = "grassers"
   ▸ Form item: "pswrd" = "cHJ2cUJaTnFZdw=="
```

```
0000  08 00 27 3d 47 5d 08 00  27 38 2c 5c 08 00 45 00   ..'=G].. '8,\..E.
0010  00 5e 10 09 40 00 40 06  16 8c 0a 00 00 05 0a 00   .^..@.@. ........
0020  00 01 e7 34 1f 90 96 87  22 ab 8b 17 97 fa 80 18   ...4.... ".......
0030  01 c9 79 dd 00 00 01 01  08 0a 00 0b 31 22 00 0b   ..y..... ....1"..
0040  4f 4d 75 73 65 72 69 64  3d 67 72 61 73 73 65 72   OMuserid =grasser
0050  73 26 70 73 77 72 64 3d  63 48 4a 32 63 55 4a 61   s&pswrd= cHJ2cUJa
0060  54 6e 46 5a 64 77 25 33  44 25 33 44               TnFZdw%3 D%3D
```

Frame (108 bytes) | Reassembled TCP (429 bytes)

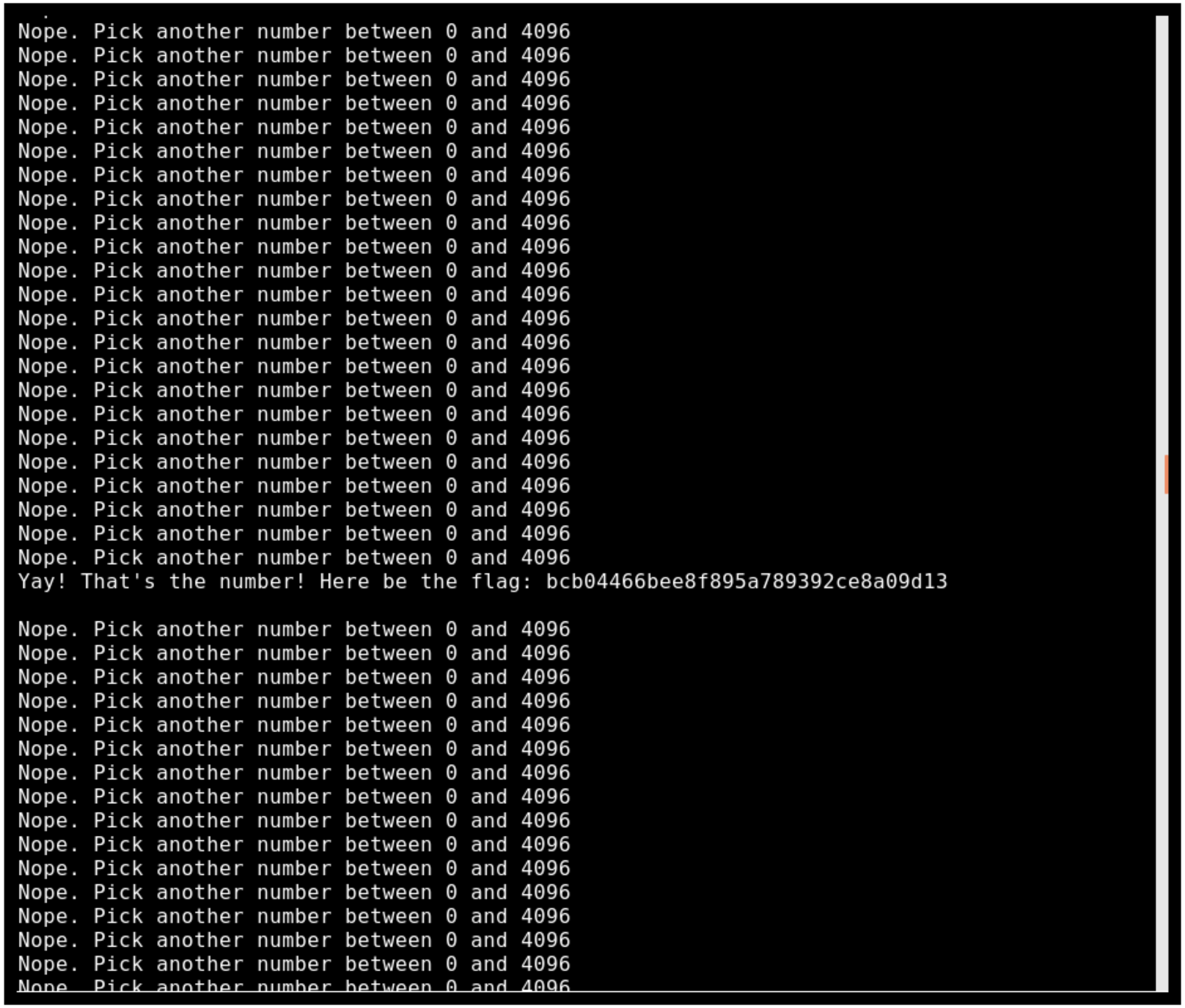
data · Packets: 238 · Displayed: 238 (100.0%) · Load time: 0:0.1 · Profile: Default

Bash vještine



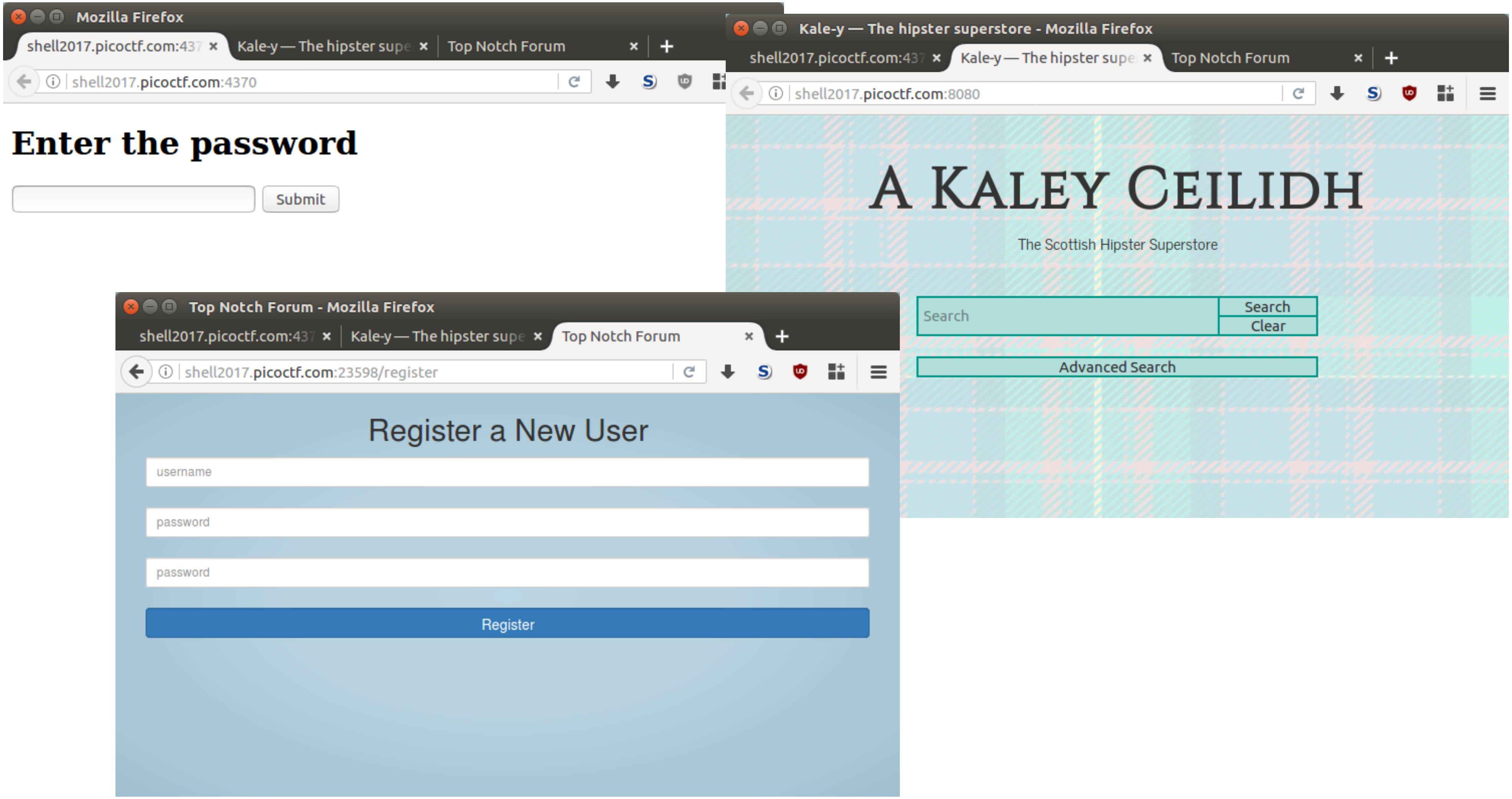
```
shell-web login: hrkljus
Enter your password:
hrkljus@shell-web:~$ cd  /problems/f625672abc185c8d615f852c306d877f
hrkljus@shell-web:/problems/f625672abc185c8d615f852c306d877f$ ls -al
total 60
drwxr-xr-x   2 root       root         4096 Mar 31 08:01 .
drwxr-x--x 573 root       root        36864 Apr 16 23:31 ..
-rwxr-sr-x   1 hacksports bash-loop_2  8216 Mar 31 08:01 bashloop
-r--r-----   1 hacksports bash-loop_2    33 Mar 31 08:01 flag
hrkljus@shell-web:/problems/f625672abc185c8d615f852c306d877f$ ./bashloop
What number am I thinking of? It is between 0 and 4096
hrkljus@shell-web:/problems/f625672abc185c8d615f852c306d877f$ ./bashloop 123
Nope. Pick another number between 0 and 4096
hrkljus@shell-web:/problems/f625672abc185c8d615f852c306d877f$ 
```

Bash vještine



```
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Yay! That's the number! Here be the flag: bcb04466bee8f895a789392ce8a09d13

Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
Nope. Pick another number between 0 and 4096
```

Web sigurnost



Mozilla Firefox

shell2017.picoctf.com:437 | Kale-y — The hipster supe | Top Notch Forum

shell2017.picoctf.com:4370

Enter the password

Submit

Kale-y — The hipster superstore - Mozilla Firefox

shell2017.picoctf.com:437 | Kale-y — The hipster supe | Top Notch Forum

shell2017.picoctf.com:8080

A KALEY CEILIDH

The Scottish Hipster Superstore

Search | Search | Clear

Advanced Search

Top Notch Forum - Mozilla Firefox

shell2017.picoctf.com:437 | Kale-y — The hipster supe | Top Notch Forum

shell2017.picoctf.com:23598/register

Register a New User

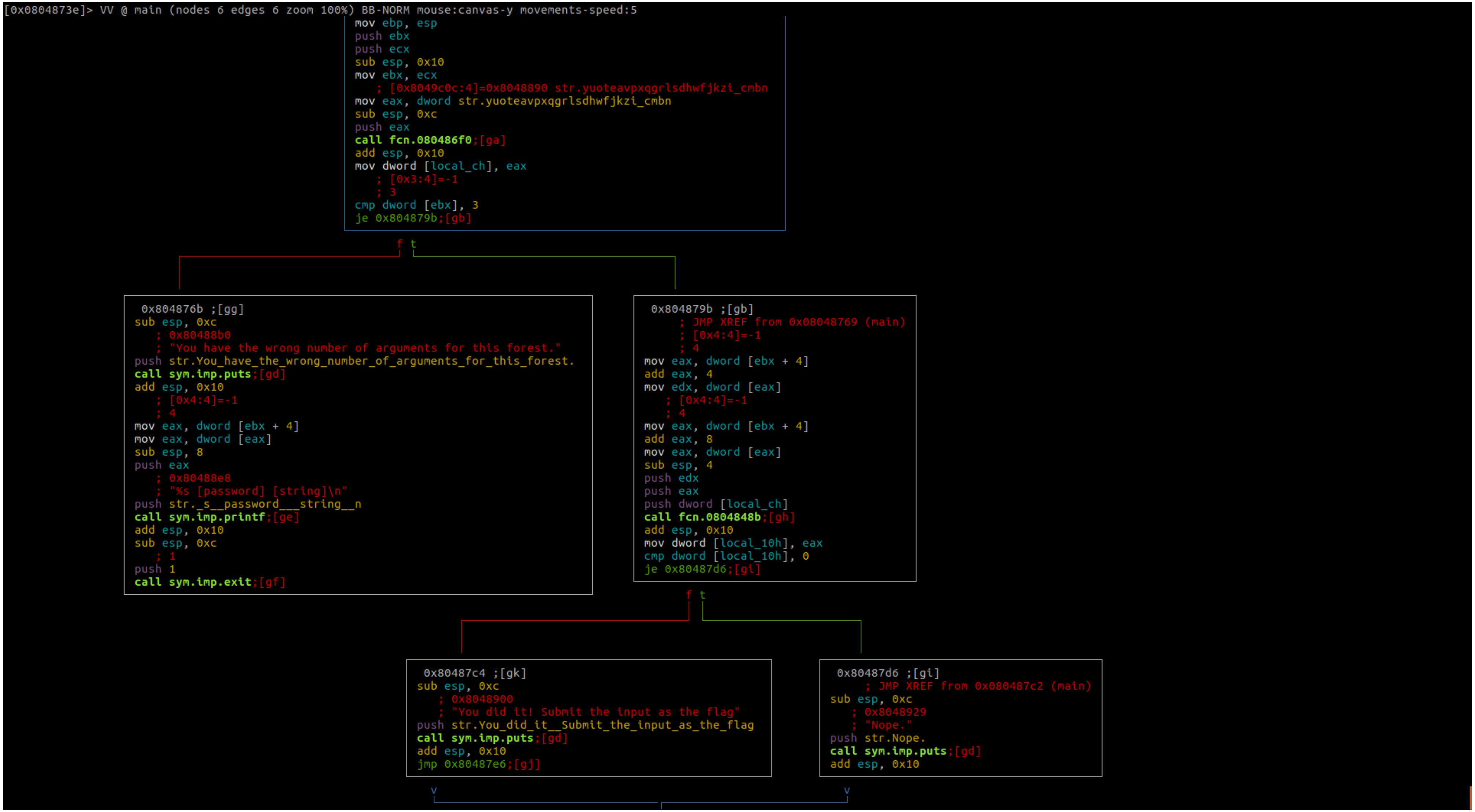
username

password

password

Register

Reverse engineering



```
[0x0804873e]> VV @ main (nodes 6 edges 6 zoom 100%) BB-NORM mouse:canvas-y movements-speed:5
```

```
mov ebp, esp
push ebx
push ecx
sub esp, 0x10
mov ebx, ecx
   ; [0x8049c0c:4]=0x8048890 str.yuoteavpxqgrlsdhwfjkzi_cmbn
mov eax, dword str.yuoteavpxqgrlsdhwfjkzi_cmbn
sub esp, 0xc
push eax
call fcn.080486f0;[ga]
add esp, 0x10
mov dword [local_ch], eax
   ; [0x3:4]=-1
   ; 3
cmp dword [ebx], 3
je 0x804879b;[gb]
```

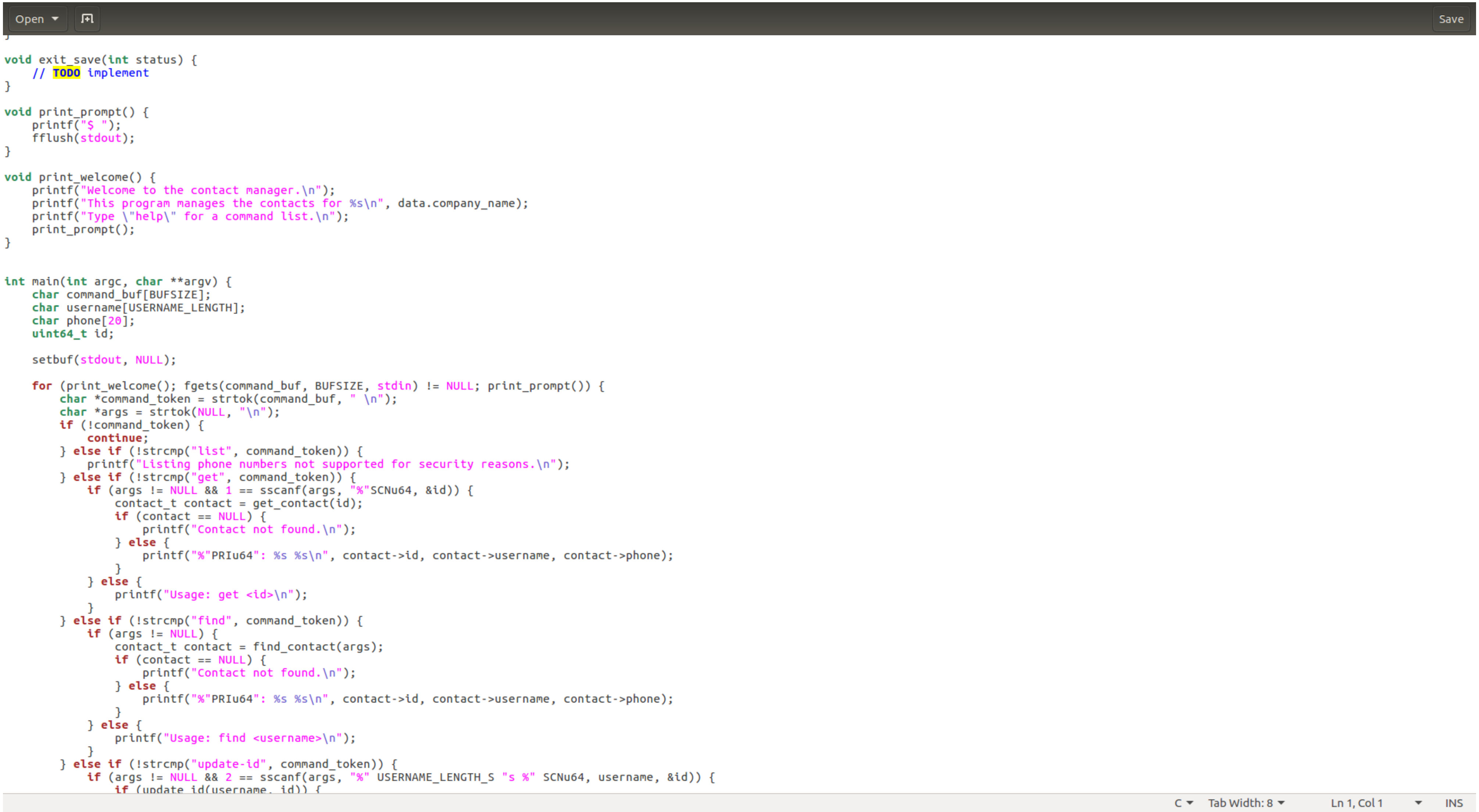
```
 0x804876b ;[gg]
sub esp, 0xc
   ; 0x80488b0
   ; "You have the wrong number of arguments for this forest."
push str.You_have_the_wrong_number_of_arguments_for_this_forest.
call sym.imp.puts;[gd]
add esp, 0x10
   ; [0x4:4]=-1
   ; 4
mov eax, dword [ebx + 4]
mov eax, dword [eax]
sub esp, 8
push eax
   ; 0x80488e8
   ; "%s [password] [string]\n"
push str._s__password___string__n
call sym.imp.printf;[ge]
add esp, 0x10
sub esp, 0xc
   ; 1
push 1
call sym.imp.exit;[gf]
```

```
 0x804879b ;[gb]
      ; JMP XREF from 0x08048769 (main)
      ; [0x4:4]=-1
      ; 4
mov eax, dword [ebx + 4]
add eax, 4
mov edx, dword [eax]
   ; [0x4:4]=-1
   ; 4
mov eax, dword [ebx + 4]
add eax, 8
mov eax, dword [eax]
sub esp, 4
push edx
push eax
push dword [local_ch]
call fcn.0804848b;[gh]
add esp, 0x10
mov dword [local_10h], eax
cmp dword [local_10h], 0
je 0x80487d6;[gi]
```

```
 0x80487c4 ;[gk]
sub esp, 0xc
   ; 0x8048900
   ; "You did it! Submit the input as the flag"
push str.You_did_it__Submit_the_input_as_the_flag
call sym.imp.puts;[gd]
add esp, 0x10
jmp 0x80487e6;[gj]
```

```
 0x80487d6 ;[gi]
      ; JMP XREF from 0x080487c2 (main)
sub esp, 0xc
   ; 0x8048929
   ; "Nope."
push str.Nope.
call sym.imp.puts;[gd]
add esp, 0x10
```

Razvoj *exploita*



```c
}

void exit_save(int status) {
    // TODO implement
}

void print_prompt() {
    printf("$ ");
    fflush(stdout);
}

void print_welcome() {
    printf("Welcome to the contact manager.\n");
    printf("This program manages the contacts for %s\n", data.company_name);
    printf("Type \"help\" for a command list.\n");
    print_prompt();
}


int main(int argc, char **argv) {
    char command_buf[BUFSIZE];
    char username[USERNAME_LENGTH];
    char phone[20];
    uint64_t id;

    setbuf(stdout, NULL);

    for (print_welcome(); fgets(command_buf, BUFSIZE, stdin) != NULL; print_prompt()) {
        char *command_token = strtok(command_buf, " \n");
        char *args = strtok(NULL, "\n");
        if (!command_token) {
            continue;
        } else if (!strcmp("list", command_token)) {
            printf("Listing phone numbers not supported for security reasons.\n");
        } else if (!strcmp("get", command_token)) {
            if (args != NULL && 1 == sscanf(args, "%"SCNu64, &id)) {
                contact_t contact = get_contact(id);
                if (contact == NULL) {
                    printf("Contact not found.\n");
                } else {
                    printf("%"PRIu64": %s %s\n", contact->id, contact->username, contact->phone);
                }
            } else {
                printf("Usage: get <id>\n");
            }
        } else if (!strcmp("find", command_token)) {
            if (args != NULL) {
                contact_t contact = find_contact(args);
                if (contact == NULL) {
                    printf("Contact not found.\n");
                } else {
                    printf("%"PRIu64": %s %s\n", contact->id, contact->username, contact->phone);
                }
            } else {
                printf("Usage: find <username>\n");
            }
        } else if (!strcmp("update-id", command_token)) {
            if (args != NULL && 2 == sscanf(args, "%" USERNAME_LENGTH_S "s %" SCNu64, username, &id)) {
                if (update_id(username, id)) {
```

Detalji

- **Najčešće svi mogu sudjelovati**
  - Učenici, studenti, ljudi iz struke...
  - Kada su nagrade u pitanju, znaju postojati neki uvjeti
- **Obično *online***
  - Moguće sudjelovati od bilo kuda
- **Oprema**
  - Računalo
  - Pristup Internetu

Detalji

- **Najčešće timska natjecanja**
  - Timovi od jedne osobe do desetaka ljudi
  - Postoje i individualna
- **Trajanje**
  - Obično 24 ili 48h
  - Ponekad i do par tjedana

Potrebno znanje

- **Osnovne informatičke vještine**
  - Dovoljne za započeti na lakšim natjecanjima
- **Sigurnost nije neko "zasebno" područje!**
  - Znanje se temelji na razumijevanju računalnih sustava
- **Npr. kako funkcioniraju web stranice?**
  - HTML, JavaScript...
  - Što ako se lozinka provjerava u JavaScriptu?
  - Cookie: admin = false
    - Sigurno?

Attack-defense CTF

- **Svaki tim dobije pristup jednom serveru**
- **Na serveru se vrte razni servisi**
  - Web stranica, baza podataka, nešto posebno...
- **Cilj**
  - Traženje ranjivosti u servisima i ...
- **Napad**
  - Krađa *flagova* iz tuđih servera
- **Obrana**
  - Zaštita i zakrpavanje vlastitih servisa

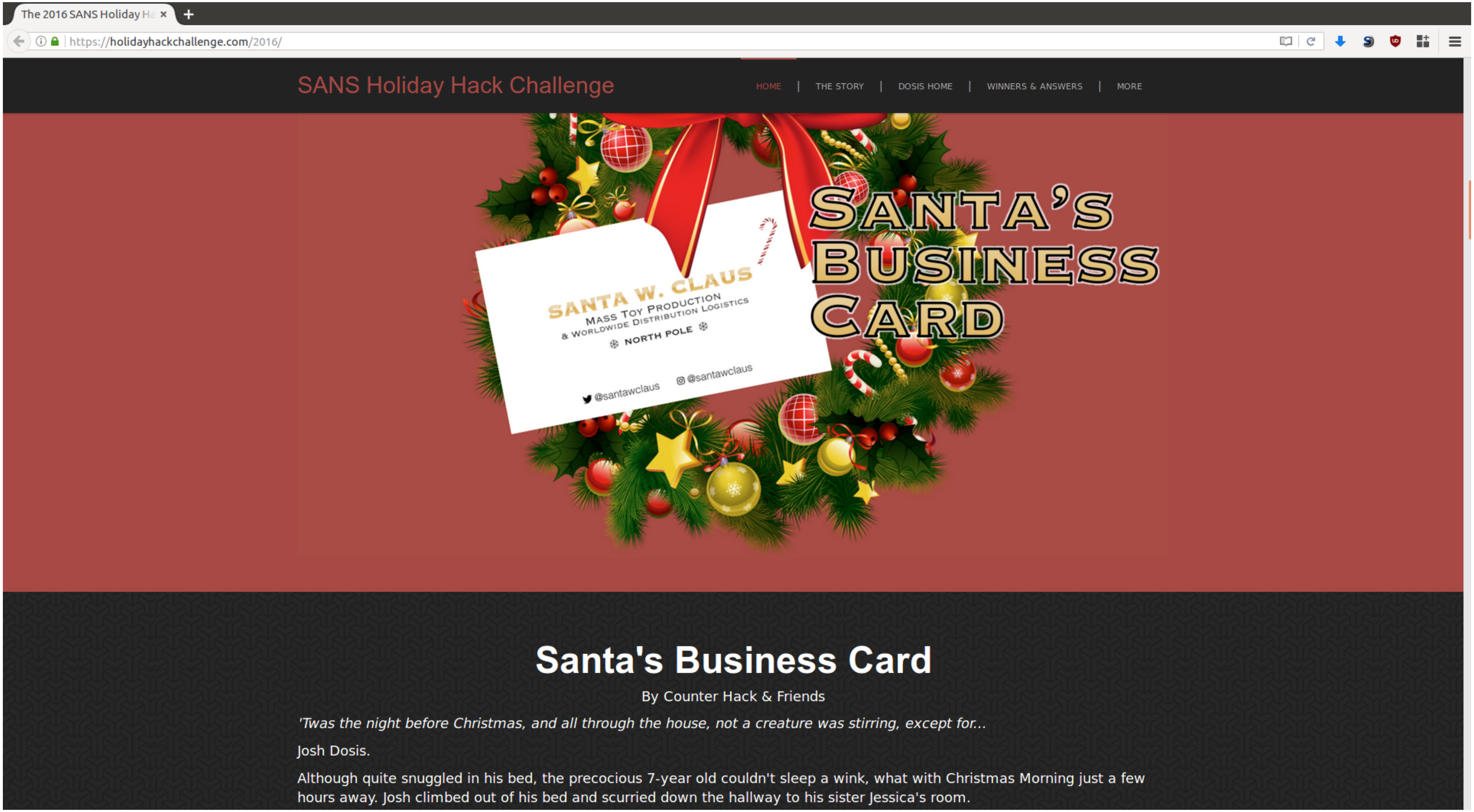
DEF CON 17 CTF

https://en.wikipedia.org/wiki/File:DEF_CON_17_CTF_competition.jpg

Ostali oblici natjecanja

- **Wargame/challenge stranice**
  - Slično *Jeopardy* CTF-u, ali stalno otvoreno
  - https://overthewire.org/
  - http://smashthestack.org/
  - https://www.hackthissite.org/
  - https://www.wechall.net/
- **Ostalo**
  - https://holidayhackchallenge.com/
  - Obijanje brava
  - *Social engineering*

Holiday Hack Challenge (SANS)



The 2016 SANS Holiday Ha
https://holidayhackchallenge.com/2016/
SANS Holiday Hack Challenge
HOME | THE STORY | DOSIS HOME | WINNERS & ANSWERS | MORE
SANTA W. CLAUS
MASS TOY PRODUCTION
& WORLDWIDE DISTRIBUTION LOGISTICS
NORTH POLE
@santawclaus
@santawclaus
SANTA'S BUSINESS CARD

Santa's Business Card

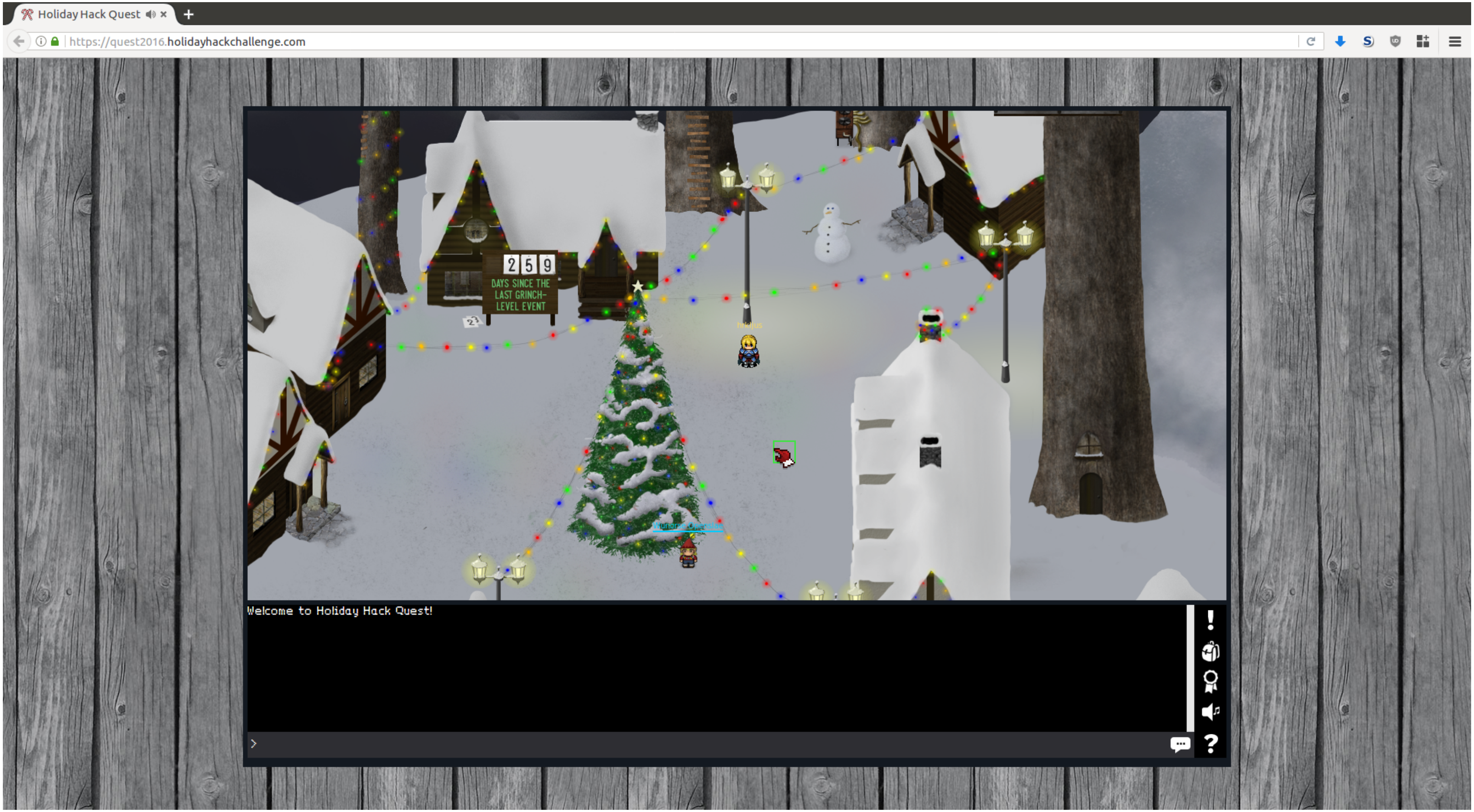
By Counter Hack & Friends

'Twas the night before Christmas, and all through the house, not a creature was stirring, except for...

Josh Dosis.

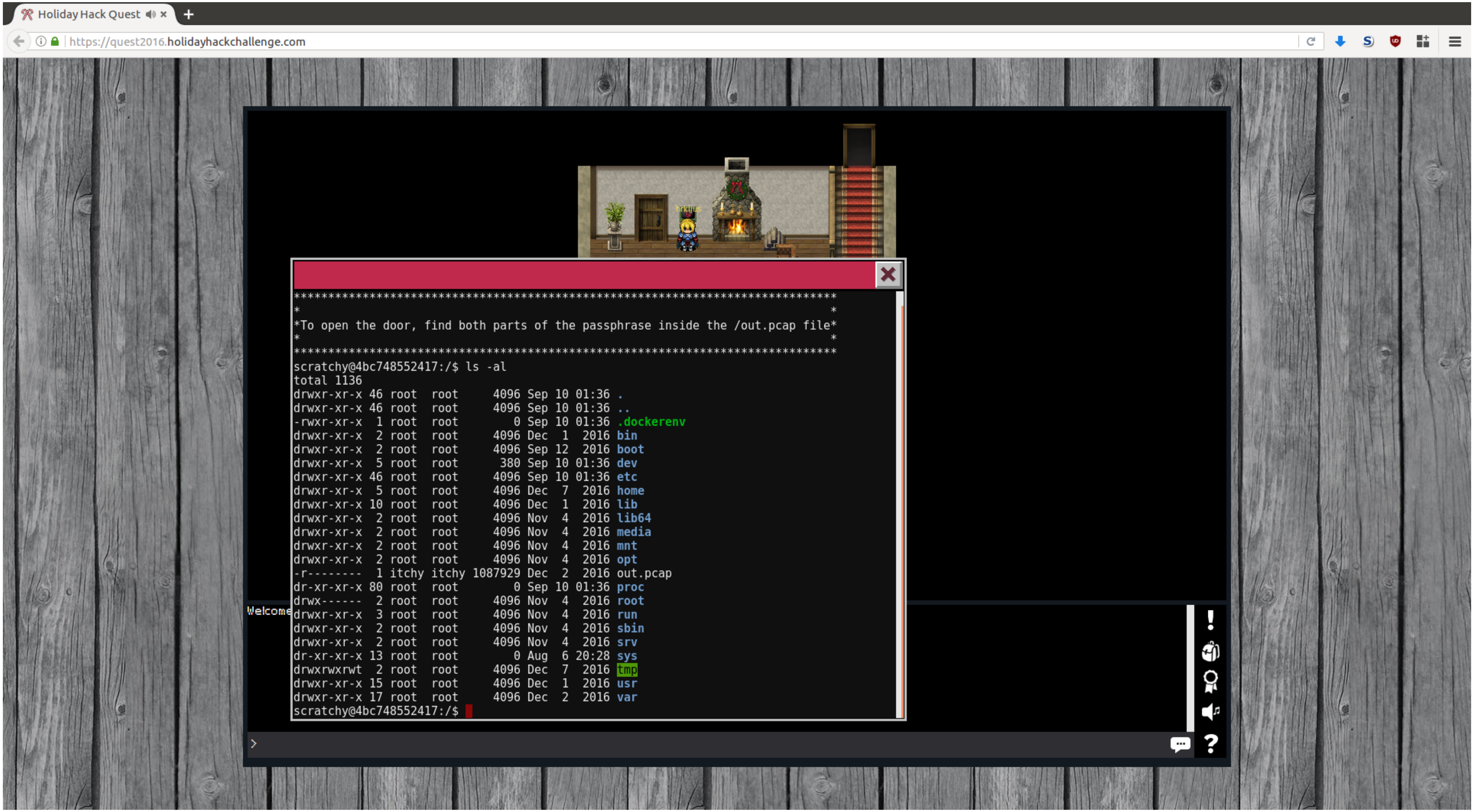
Although quite snuggled in his bed, the precocious 7-year old couldn't sleep a wink, what with Christmas Morning just a few hours away. Josh climbed out of his bed and scurried down the hallway to his sister Jessica's room.

Holiday Hack Challenge (SANS)



Welcome to Holiday Hack Quest!

Holiday Hack Challenge (SANS)



```
*******************************************************************************
*                                                                             *
*To open the door, find both parts of the passphrase inside the /out.pcap file*
*                                                                             *
*******************************************************************************
scratchy@4bc748552417:/$ ls -al
total 1136
drwxr-xr-x 46 root  root     4096 Sep 10 01:36 .
drwxr-xr-x 46 root  root     4096 Sep 10 01:36 ..
-rwxr-xr-x  1 root  root        0 Sep 10 01:36 .dockerenv
drwxr-xr-x  2 root  root     4096 Dec  1  2016 bin
drwxr-xr-x  2 root  root     4096 Sep 12  2016 boot
drwxr-xr-x  5 root  root      380 Sep 10 01:36 dev
drwxr-xr-x 46 root  root     4096 Sep 10 01:36 etc
drwxr-xr-x  5 root  root     4096 Dec  7  2016 home
drwxr-xr-x 10 root  root     4096 Dec  1  2016 lib
drwxr-xr-x  2 root  root     4096 Nov  4  2016 lib64
drwxr-xr-x  2 root  root     4096 Nov  4  2016 media
drwxr-xr-x  2 root  root     4096 Nov  4  2016 mnt
drwxr-xr-x  2 root  root     4096 Nov  4  2016 opt
-r--------  1 itchy itchy 1087929 Dec  2  2016 out.pcap
dr-xr-xr-x 80 root  root        0 Sep 10 01:36 proc
drwx------  2 root  root     4096 Nov  4  2016 root
drwxr-xr-x  3 root  root     4096 Nov  4  2016 run
drwxr-xr-x  2 root  root     4096 Nov  4  2016 sbin
drwxr-xr-x  2 root  root     4096 Nov  4  2016 srv
dr-xr-xr-x 13 root  root        0 Aug  6 20:28 sys
drwxrwxrwt  2 root  root     4096 Dec  7  2016 tmp
drwxr-xr-x 15 root  root     4096 Dec  1  2016 usr
drwxr-xr-x 17 root  root     4096 Dec  2  2016 var
scratchy@4bc748552417:/$
```

Lockpicking Village (DEF CON)

https://www.wired.com/2010/08/gallery-defcon-18/

Social Engineering CTF (DEF CON)

PHOTO: STACY COWLEY/CNNMONEY

http://money.cnn.com/2012/08/07/technology/walmart-hack-defcon/index.htm

Zašto?

- **Zabavno i korisno**
- **Razvija korisne vještine**
  - Ne samo za karijere u informacijskoj sigurnosti!
  - Software developer, system administrator...
- **Znanje korisno i u svakodnevnom životu**
  - Sve je digitalizirano (ako nije, biti će)
  - Kako ostati siguran?
- **Prednost pri zapošljavanju**

Zašto?

- **Zabavno i korisno**
- **Razvija korisne vještine**
  - Ne samo za karijere u informacijskoj sigurnosti!
  - Software developer, system administrator...
- **Znanje korisno i u svakodnevnom životu**
  - Sve je digitalizirano (ako nije, biti će)
  - Kako ostati siguran?
- **Prednost pri zapošljavanju**

Ako ste zainteresirani

- **picoctf.com (2017)**
  - i 2013, 2014, ali ne rade trenutno
- **ctftime.org**
  - Popis gotovo svih CTF-ova, rang lista
- **wechall.net**
  - Popis wargame/challenge stranica, rang lista
- **Write-up**
  - "Tutorial" kako riješiti zadatak
  - https://github.com/ctfs/write-ups-2017

Negativne strane?

- **Poticanje na kaznena djela?**
  - Stvaranje "loših hakera"?
- **House Resolution 459**
  - "Whereas **competitions that promote ethical hacking skills, such as the picoCTF** competition which was developed collaboratively by a leading university, the private sector, and Federal agencies, have proven to be **instrumental in developing technical experience and promoting interest in exploring cybersecurity careers**"
  - https://www.congress.gov/bill/115th-congress/house-resolution/459/text

CTF u Hrvatskoj

- **FSec (FOI)**
  - https://fsec.foi.hr/
- **FERSEC Challenge**
  - http://eestec-zg.hr/fersec/
  - https://www.facebook.com/ferseczg/
- **Još?**

Organizacija (Jeopardy) CTF-a

- **Tehnički dio – lakši nego što se čini**
- **CTFd**
  - Capture The Flag in a can
  - https://github.com/CTFd/CTFd
- **Hardware – VPS-ovi**
  - Iznajmiti unaprijed
- **Najteži dio – smisliti zadatke**
  - Lakše za lagani CTF gdje je očekivano imati "tipične" zadatke
- **http://eestec-zg.hr/**