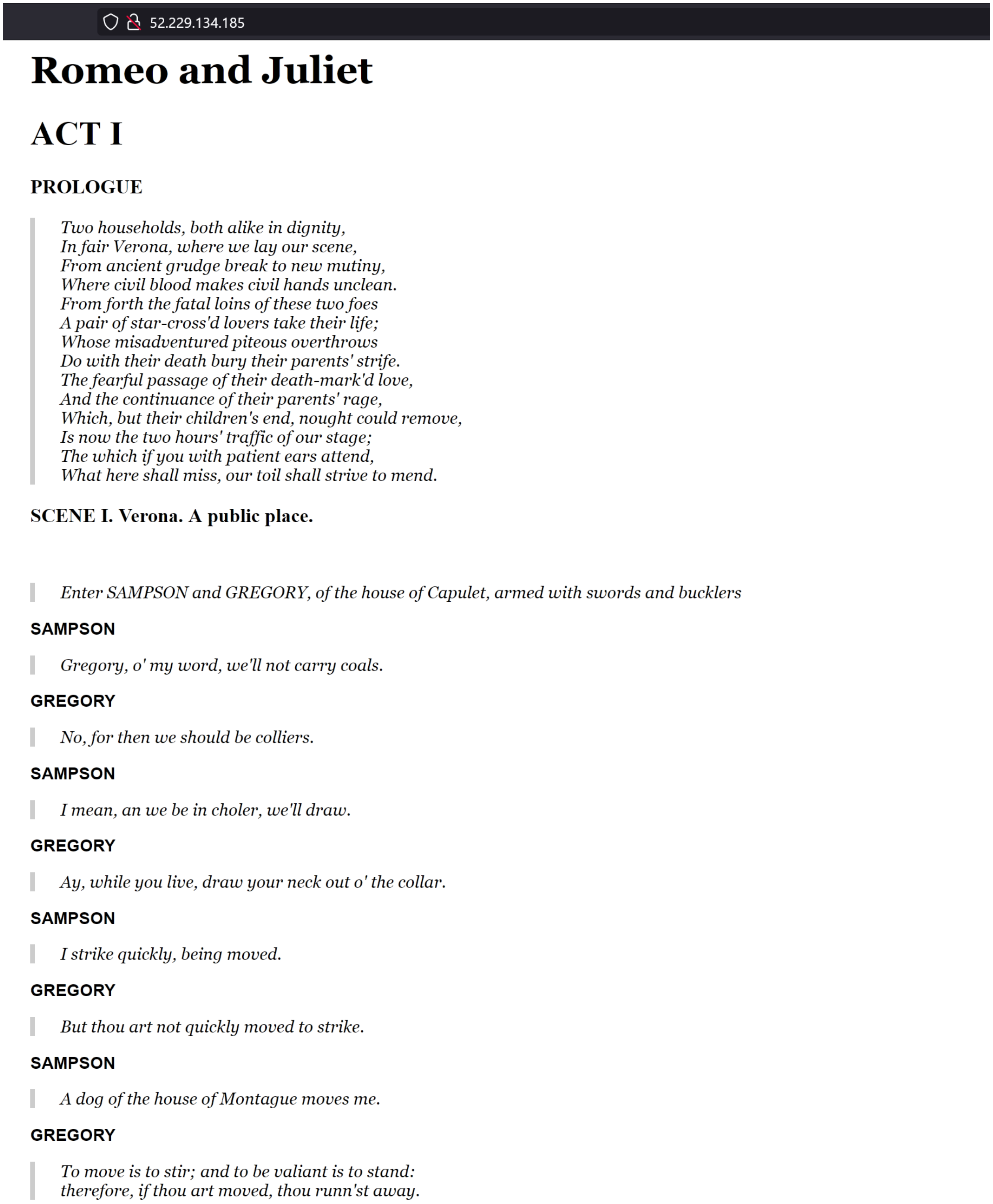
Oh Romeo – Writeup

http://52.229.134.185/



Romeo and Juliet

ACT I

PROLOGUE

> *Two households, both alike in dignity,*
> *In fair Verona, where we lay our scene,*
> *From ancient grudge break to new mutiny,*
> *Where civil blood makes civil hands unclean.*
> *From forth the fatal loins of these two foes*
> *A pair of star-cross'd lovers take their life;*
> *Whose misadventured piteous overthrows*
> *Do with their death bury their parents' strife.*
> *The fearful passage of their death-mark'd love,*
> *And the continuance of their parents' rage,*
> *Which, but their children's end, nought could remove,*
> *Is now the two hours' traffic of our stage;*
> *The which if you with patient ears attend,*
> *What here shall miss, our toil shall strive to mend.*

SCENE I. Verona. A public place.

> *Enter SAMPSON and GREGORY, of the house of Capulet, armed with swords and bucklers*

SAMPSON

> *Gregory, o' my word, we'll not carry coals.*

GREGORY

> *No, for then we should be colliers.*

SAMPSON

> *I mean, an we be in choler, we'll draw.*

GREGORY

> *Ay, while you live, draw your neck out o' the collar.*

SAMPSON

> *I strike quickly, being moved.*

GREGORY

> *But thou art not quickly moved to strike.*

SAMPSON

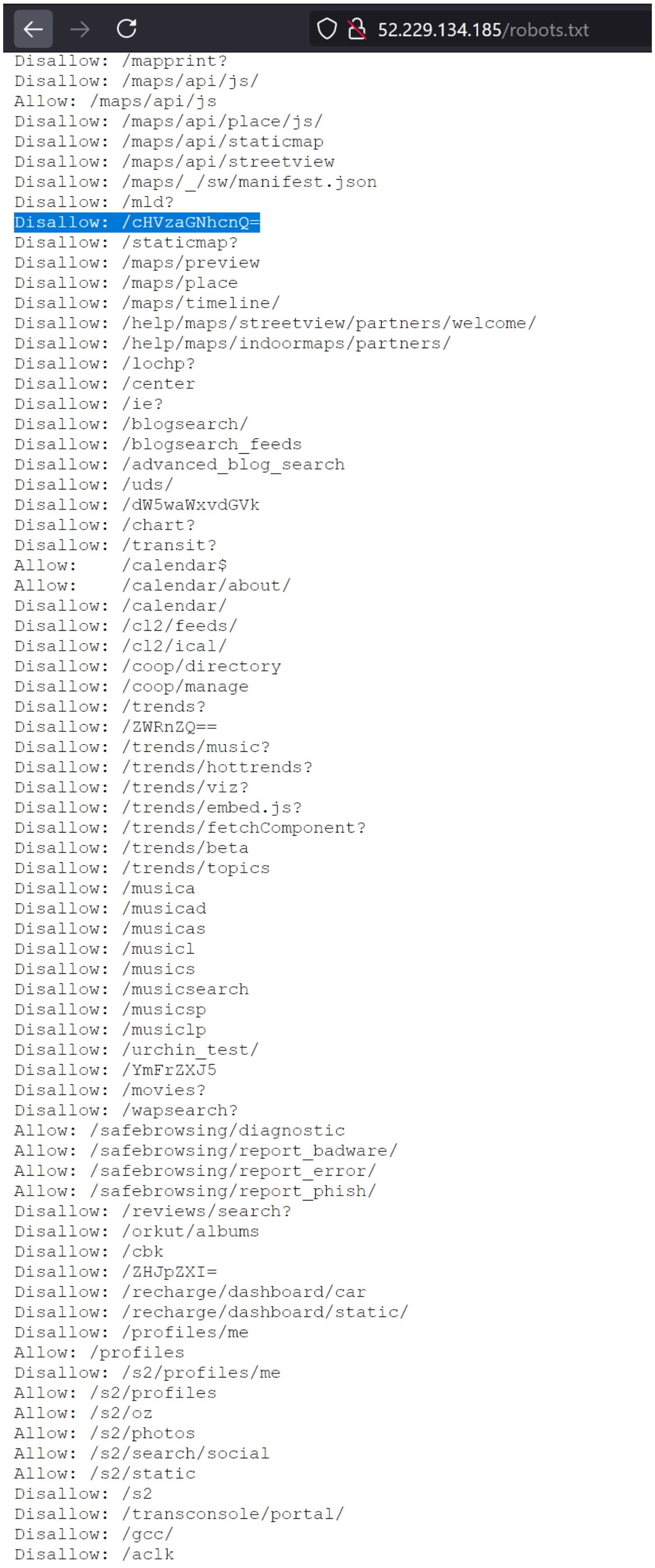
> *A dog of the house of Montague moves me.*

GREGORY

> *To move is to stir; and to be valiant is to stand:*
> *therefore, if thou art moved, thou runn'st away.*

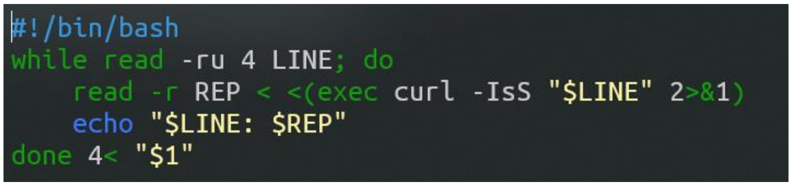
Hmm a static page, nothing interesting in the source either, lets look around for more interesting files and directories

A robots.txt, with some weird base64 looking strings:



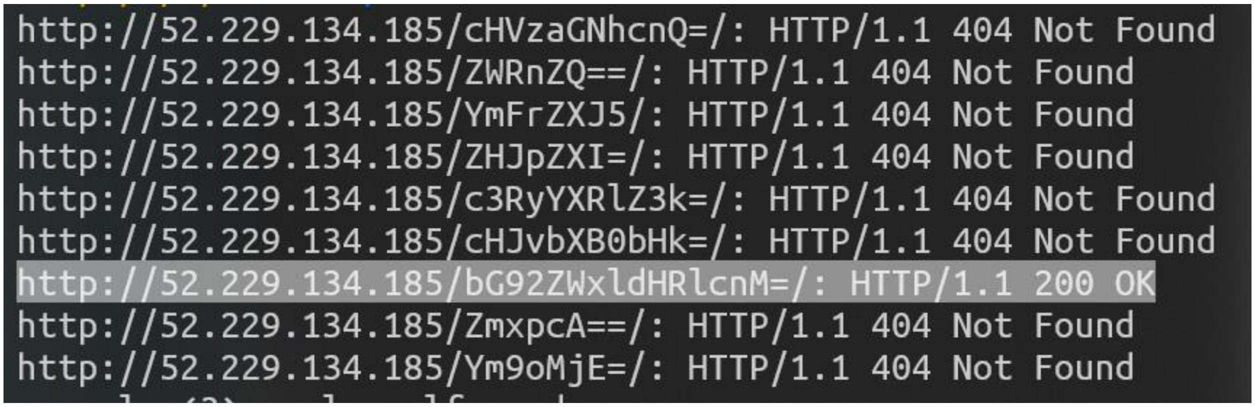
```
Disallow: /mapprint?
Disallow: /maps/api/js/
Allow: /maps/api/js
Disallow: /maps/api/place/js/
Disallow: /maps/api/staticmap
Disallow: /maps/api/streetview
Disallow: /maps/_/sw/manifest.json
Disallow: /mld?
Disallow: /cHVzaGNhcnQ=
Disallow: /staticmap?
Disallow: /maps/preview
Disallow: /maps/place
Disallow: /maps/timeline/
Disallow: /help/maps/streetview/partners/welcome/
Disallow: /help/maps/indoormaps/partners/
Disallow: /lochp?
Disallow: /center
Disallow: /ie?
Disallow: /blogsearch/
Disallow: /blogsearch_feeds
Disallow: /advanced_blog_search
Disallow: /uds/
Disallow: /dW5waWxvdGVk
Disallow: /chart?
Disallow: /transit?
Allow:    /calendar$
Allow:    /calendar/about/
Disallow: /calendar/
Disallow: /cl2/feeds/
Disallow: /cl2/ical/
Disallow: /coop/directory
Disallow: /coop/manage
Disallow: /trends?
Disallow: /ZWRnZQ==
Disallow: /trends/music?
Disallow: /trends/hottrends?
Disallow: /trends/viz?
Disallow: /trends/embed.js?
Disallow: /trends/fetchComponent?
Disallow: /trends/beta
Disallow: /trends/topics
Disallow: /musica
Disallow: /musicad
Disallow: /musicas
Disallow: /musicl
Disallow: /musics
Disallow: /musicsearch
Disallow: /musicsp
Disallow: /musiclp
Disallow: /urchin_test/
Disallow: /YmFrZXJ5
Disallow: /movies?
Disallow: /wapsearch?
Allow: /safebrowsing/diagnostic
Allow: /safebrowsing/report_badware/
Allow: /safebrowsing/report_error/
Allow: /safebrowsing/report_phish/
Disallow: /reviews/search?
Disallow: /orkut/albums
Disallow: /cbk
Disallow: /ZHJpZXI=
Disallow: /recharge/dashboard/car
Disallow: /recharge/dashboard/static/
Disallow: /profiles/me
Allow: /profiles
Disallow: /s2/profiles/me
Allow: /s2/profiles
Allow: /s2/oz
Allow: /s2/photos
Allow: /s2/search/social
Allow: /s2/static
Disallow: /s2
Disallow: /transconsole/portal/
Disallow: /gcc/
Disallow: /aclk
```

Hmm lets check these out:

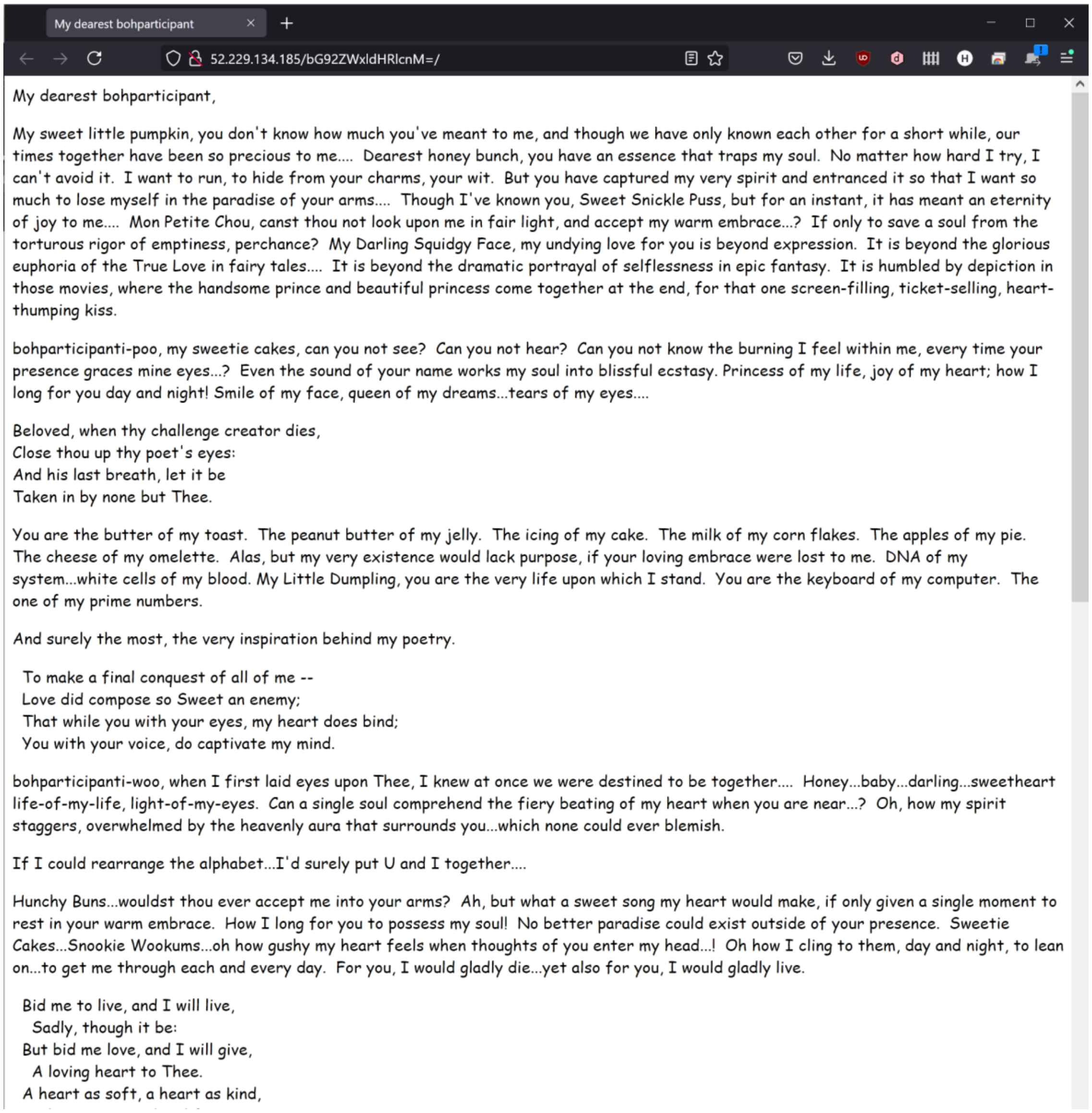


```
#!/bin/bash
while read -ru 4 LINE; do
    read -r REP < <(exec curl -IsS "$LINE" 2>&1)
    echo "$LINE: $REP"
done 4< "$1"
```

A quick script and url list parse later, a hit!:



```
http://52.229.134.185/cHVzaGNhcnQ=/: HTTP/1.1 404 Not Found
http://52.229.134.185/ZWRnZQ==/: HTTP/1.1 404 Not Found
http://52.229.134.185/YmFrZXJ5/: HTTP/1.1 404 Not Found
http://52.229.134.185/ZHJpZXI=/: HTTP/1.1 404 Not Found
http://52.229.134.185/c3RyYXRlZ3k=/: HTTP/1.1 404 Not Found
http://52.229.134.185/cHJvbXB0bHk=/: HTTP/1.1 404 Not Found
http://52.229.134.185/bG92ZWxldHRlcnM=/: HTTP/1.1 200 OK
http://52.229.134.185/ZmxpcA==/: HTTP/1.1 404 Not Found
http://52.229.134.185/Ym9oMjE=/: HTTP/1.1 404 Not Found
```



My dearest bohparticipant,

My sweet little pumpkin, you don't know how much you've meant to me, and though we have only known each other for a short while, our times together have been so precious to me.... Dearest honey bunch, you have an essence that traps my soul. No matter how hard I try, I can't avoid it. I want to run, to hide from your charms, your wit. But you have captured my very spirit and entranced it so that I want so much to lose myself in the paradise of your arms.... Though I've known you, Sweet Snickle Puss, but for an instant, it has meant an eternity of joy to me.... Mon Petite Chou, canst thou not look upon me in fair light, and accept my warm embrace...? If only to save a soul from the torturous rigor of emptiness, perchance? My Darling Squidgy Face, my undying love for you is beyond expression. It is beyond the glorious euphoria of the True Love in fairy tales.... It is beyond the dramatic portrayal of selflessness in epic fantasy. It is humbled by depiction in those movies, where the handsome prince and beautiful princess come together at the end, for that one screen-filling, ticket-selling, heart-thumping kiss.

bohparticipanti-poo, my sweetie cakes, can you not see? Can you not hear? Can you not know the burning I feel within me, every time your presence graces mine eyes...? Even the sound of your name works my soul into blissful ecstasy. Princess of my life, joy of my heart; how I long for you day and night! Smile of my face, queen of my dreams...tears of my eyes....

Beloved, when thy challenge creator dies,
Close thou up thy poet's eyes:
And his last breath, let it be
Taken in by none but Thee.

You are the butter of my toast. The peanut butter of my jelly. The icing of my cake. The milk of my corn flakes. The apples of my pie. The cheese of my omelette. Alas, but my very existence would lack purpose, if your loving embrace were lost to me. DNA of my system...white cells of my blood. My Little Dumpling, you are the very life upon which I stand. You are the keyboard of my computer. The one of my prime numbers.

And surely the most, the very inspiration behind my poetry.

To make a final conquest of all of me --
Love did compose so Sweet an enemy;
That while you with your eyes, my heart does bind;
You with your voice, do captivate my mind.

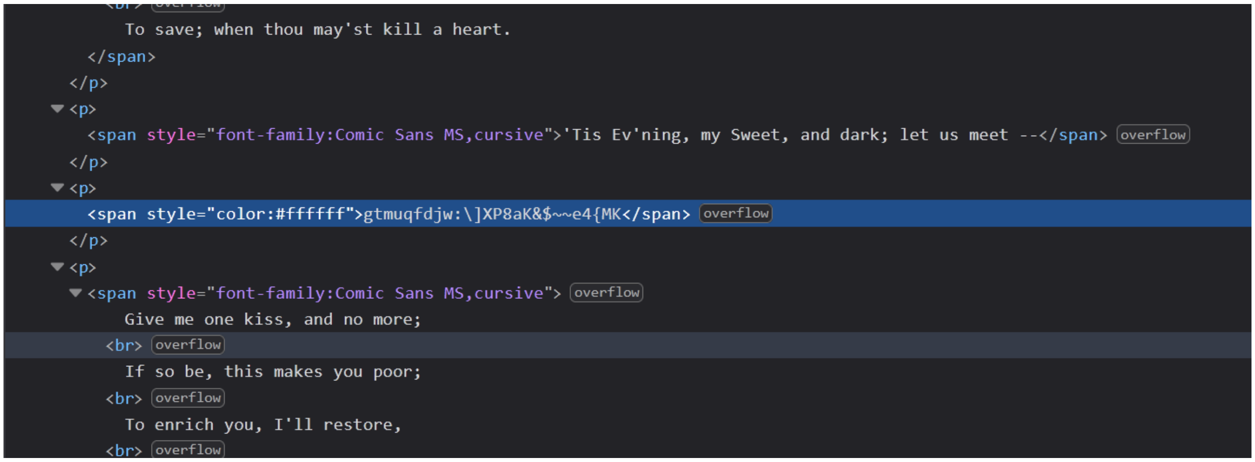
bohparticipanti-woo, when I first laid eyes upon Thee, I knew at once we were destined to be together.... Honey...baby...darling...sweetheart life-of-my-life, light-of-my-eyes. Can a single soul comprehend the fiery beating of my heart when you are near...? Oh, how my spirit staggers, overwhelmed by the heavenly aura that surrounds you...which none could ever blemish.

If I could rearrange the alphabet...I'd surely put U and I together....

Hunchy Buns...wouldst thou ever accept me into your arms? Ah, but what a sweet song my heart would make, if only given a single moment to rest in your warm embrace. How I long for you to possess my soul! No better paradise could exist outside of your presence. Sweetie Cakes...Snookie Wookums...oh how gushy my heart feels when thoughts of you enter my head...! Oh how I cling to them, day and night, to lean on...to get me through each and every day. For you, I would gladly die...yet also for you, I would gladly live.

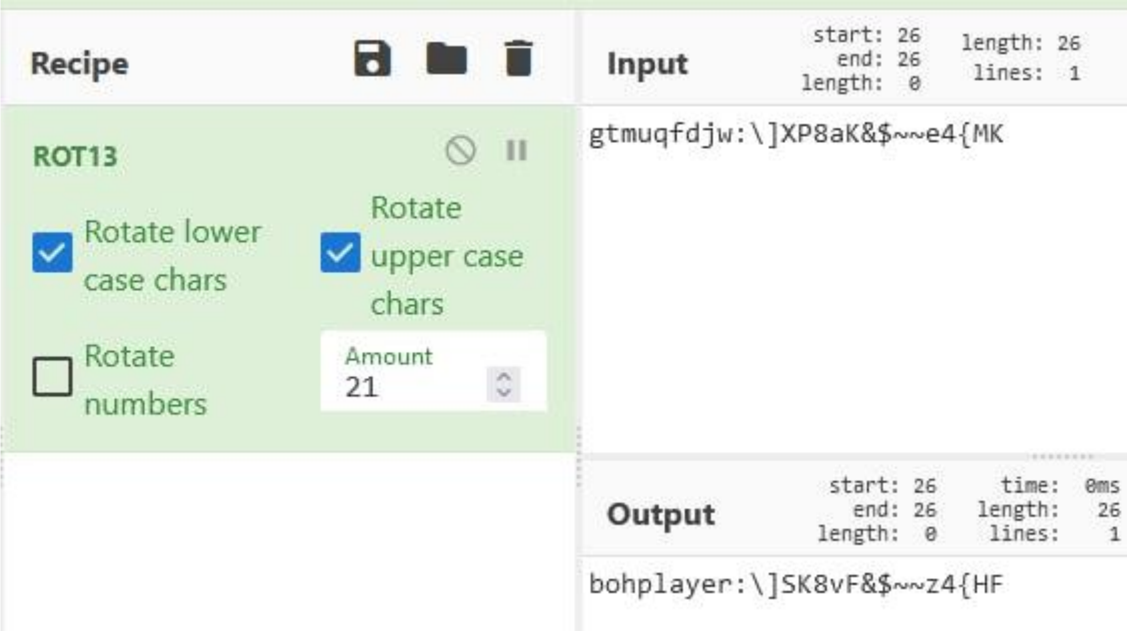
Bid me to live, and I will live,
  Sadly, though it be:
But bid me love, and I will give,
  A loving heart to Thee.
A heart as soft, a heart as kind,

Inspecting the source we see a funny looking string:



```
      To save; when thou may'st kill a heart.
    </span>
  </p>
▼ <p>
    <span style="font-family:Comic Sans MS,cursive">'Tis Ev'ning, my Sweet, and dark; let us meet --</span> overflow
  </p>
▼ <p>
    <span style="color:#ffffff">gtmuqfdjw:\]XP8aK&$~~e4{MK</span> overflow
  </p>
▼ <p>
  ▼ <span style="font-family:Comic Sans MS,cursive"> overflow
      Give me one kiss, and no more;
      <br> overflow
      If so be, this makes you poor;
      <br> overflow
      To enrich you, I'll restore,
      <br> overflow
```

Playing around with the string in cyber chef, it looks like the usual format for credentials:



ROT13

☑ Rotate lower case chars ☑ Rotate upper case chars

□ Rotate numbers Amount 21

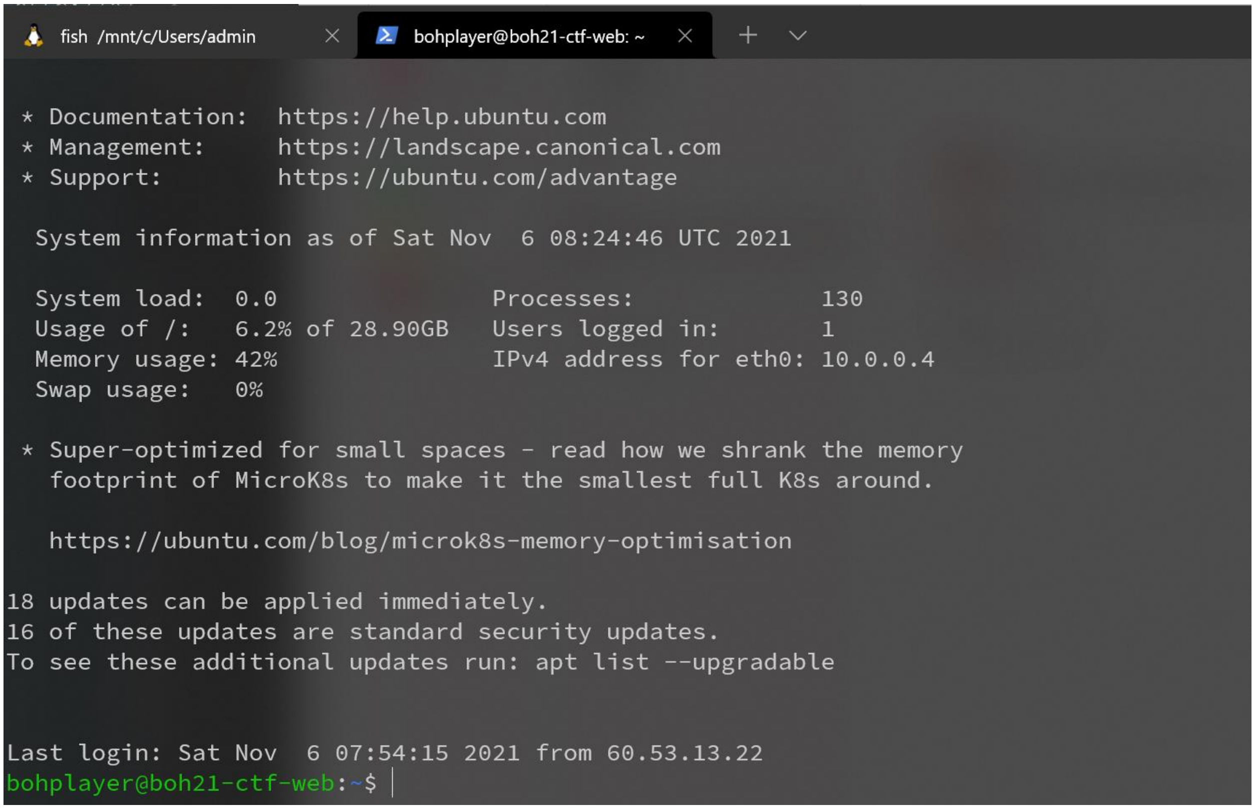
Input: start: 26 end: 26 length: 0 length: 26 lines: 1

```
gtmuqfdjw:\]XP8aK&$~~e4{MK
```

Output: start: 26 end: 26 length: 0 time: 0ms length: 26 lines: 1

```
bohplayer:\]SK8vF&$~~z4{HF
```

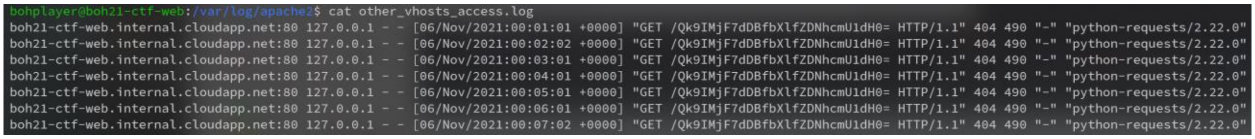
Which lets us ssh into the machine:



```
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Nov  6 08:24:46 UTC 2021

  System load:  0.0               Processes:             130
  Usage of /:   6.2% of 28.90GB   Users logged in:       1
  Memory usage: 42%               IPv4 address for eth0: 10.0.0.4
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

18 updates can be applied immediately.
16 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


Last login: Sat Nov  6 07:54:15 2021 from 60.53.13.22
bohplayer@boh21-ctf-web:~$
```

The challenge mentioned something about receiving love letters every minute

After much searching we see that the http server logs are accessible with the user we got:



```
bohplayer@boh21-ctf-web:/var/log/apache2$ cat other_vhosts_access.log
boh21-ctf-web.internal.cloudapp.net:80 127.0.0.1 - - [06/Nov/2021:00:01:01 +0000] "GET /Qk9IMjF7dDBfbXlfZDNhcmU1dH0= HTTP/1.1" 404 490 "-" "python-requests/2.22.0"
boh21-ctf-web.internal.cloudapp.net:80 127.0.0.1 - - [06/Nov/2021:00:02:02 +0000] "GET /Qk9IMjF7dDBfbXlfZDNhcmU1dH0= HTTP/1.1" 404 490 "-" "python-requests/2.22.0"
boh21-ctf-web.internal.cloudapp.net:80 127.0.0.1 - - [06/Nov/2021:00:03:01 +0000] "GET /Qk9IMjF7dDBfbXlfZDNhcmU1dH0= HTTP/1.1" 404 490 "-" "python-requests/2.22.0"
boh21-ctf-web.internal.cloudapp.net:80 127.0.0.1 - - [06/Nov/2021:00:04:01 +0000] "GET /Qk9IMjF7dDBfbXlfZDNhcmU1dH0= HTTP/1.1" 404 490 "-" "python-requests/2.22.0"
boh21-ctf-web.internal.cloudapp.net:80 127.0.0.1 - - [06/Nov/2021:00:05:01 +0000] "GET /Qk9IMjF7dDBfbXlfZDNhcmU1dH0= HTTP/1.1" 404 490 "-" "python-requests/2.22.0"
boh21-ctf-web.internal.cloudapp.net:80 127.0.0.1 - - [06/Nov/2021:00:06:01 +0000] "GET /Qk9IMjF7dDBfbXlfZDNhcmU1dH0= HTTP/1.1" 404 490 "-" "python-requests/2.22.0"
boh21-ctf-web.internal.cloudapp.net:80 127.0.0.1 - - [06/Nov/2021:00:07:02 +0000] "GET /Qk9IMjF7dDBfbXlfZDNhcmU1dH0= HTTP/1.1" 404 490 "-" "python-requests/2.22.0"
```

Decoding that base64 portion gives us the flag: BOH21{t0_my_d3are5t}