babypass

by sunset

端口扫描

无 fa 可说

```
➜  Test nmap -p- -min-rate 10000 -n -Pn -sCV 192.168.56.142
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-11 22:31 CST
Nmap scan report for 192.168.56.142
Host is up (0.00020s latency).
Not shown: 65533 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)
MAC Address: 08:00:27:F7:A9:32 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.57 seconds
```

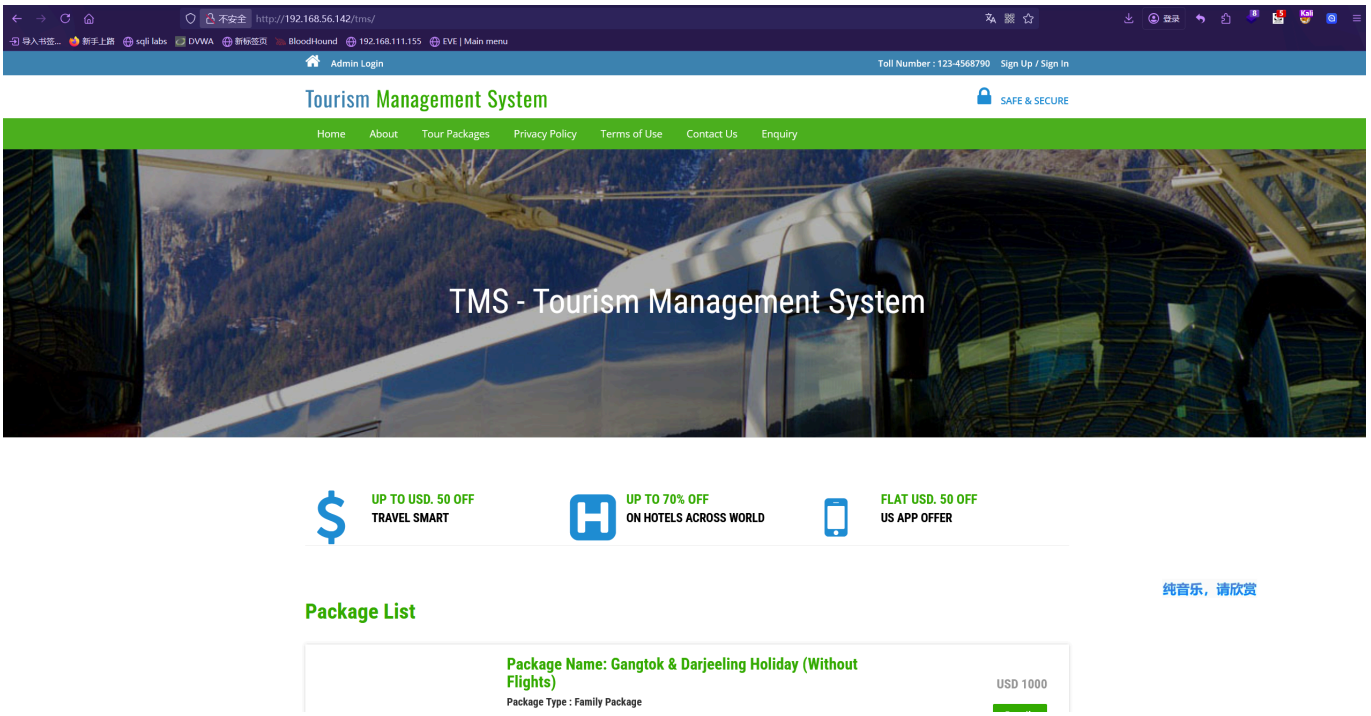
枚举

80 端口，F12 源代码中能找到如下内容

开发大哥不仅留下了 `tms` 这个神秘暗号，还特地嘱咐我们“不要在不同账户用同一个密码”

```
hello world
<!-- tms -->
<!-- Do not use same password in different account.  -->
```

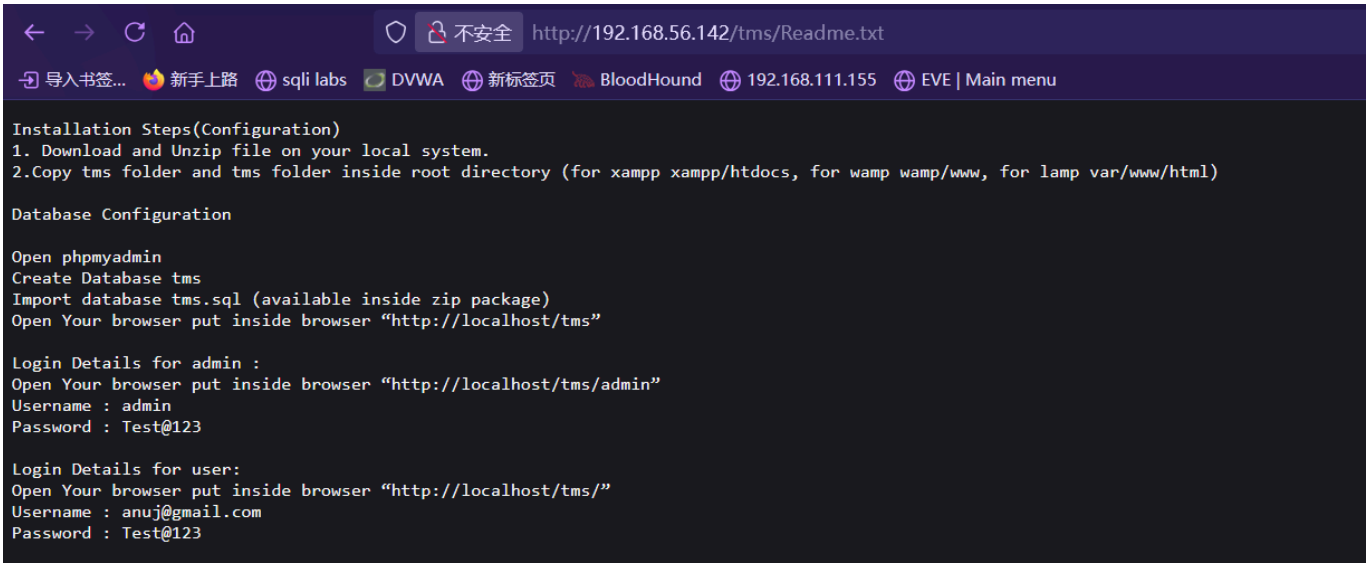
尝试给出的 `tms` 作为路径 `http://192.168.56.142/tms/` ，跳转到一个xx管理系统



目录扫描（结果略，窗口关掉了）

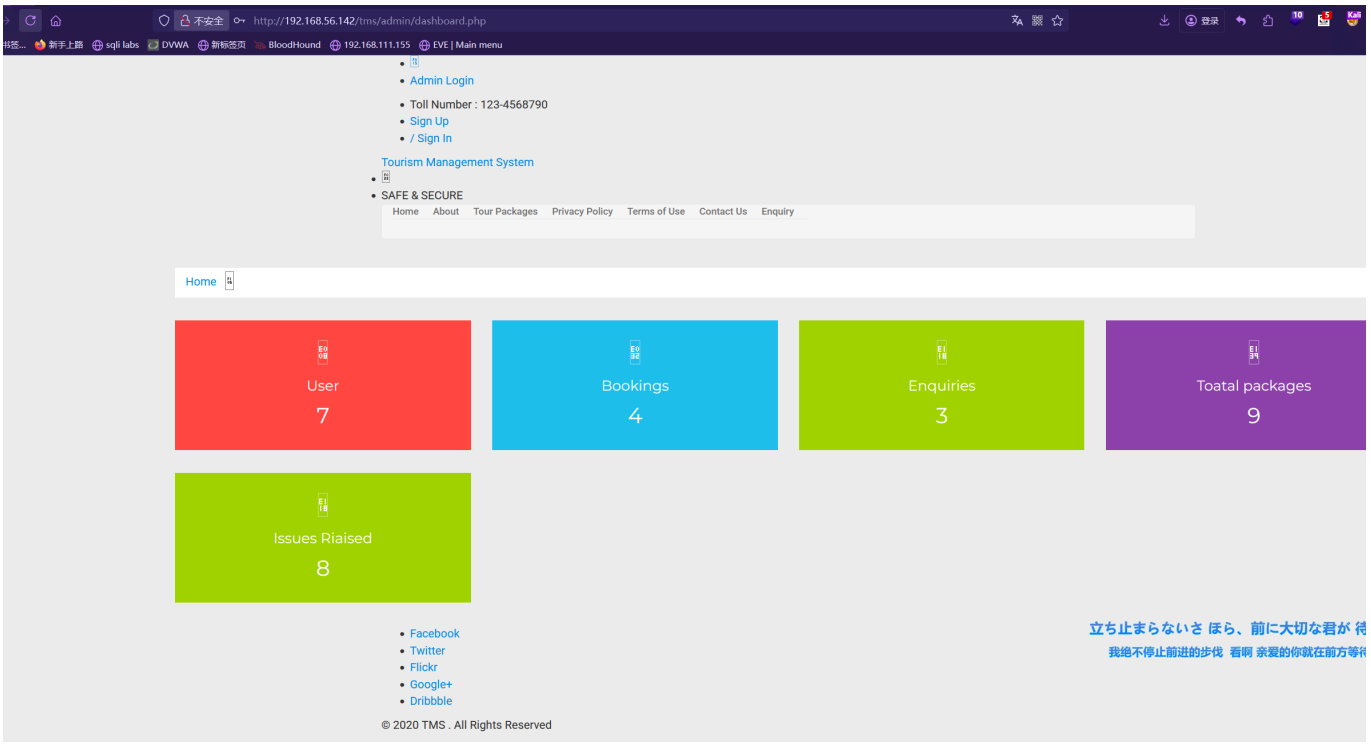
```
feroxbuster --url http://192.168.56.142/tms -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt --filter-status 404,503,400 -x php,txt
```

扫到的 `Readme.txt` 信息，能拿到两个凭据



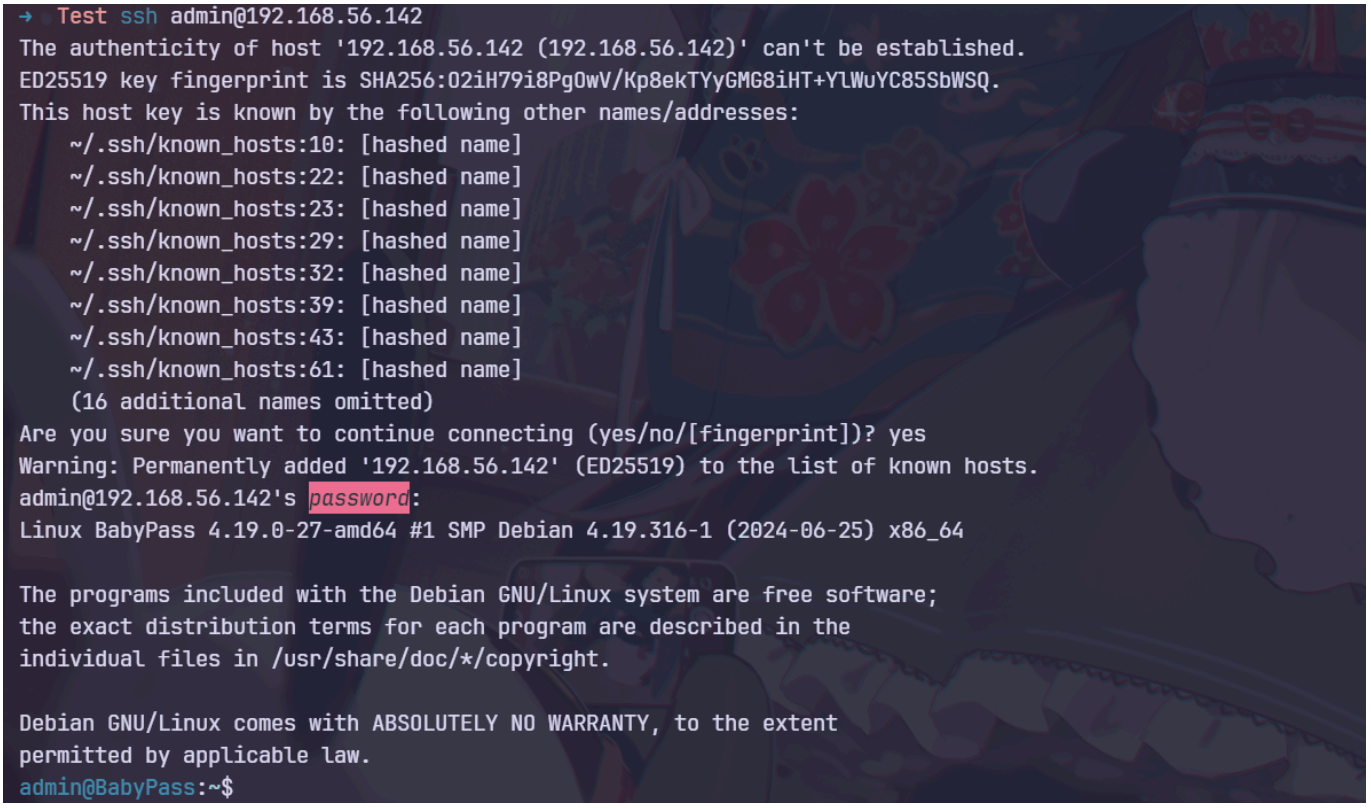
> 管理员登录: 用户名: `admin` 密码: `Test@123`
>
> 用户登录: 用户名: `anuj@gmail.com` 密码: `Test@123`

`anuj@gmail.com` 和`admin` 均可登录进入后台，但是后台没有可以利用的点



调转枪头，对准了那个 22 端口。使用上面的得到凭据进行登录

成功登录上去了，并且 `admin` 和 `anuj` 的用户密码是同一个



`admin` 用户能读 `user.txt`

```
drwxr-xr-x  2 welcome welcome 4096 Nov  4 05:40 w
admin@BabyPass:/home$ cd welcome
admin@BabyPass:/home/welcome$ ls
user.txt
admin@BabyPass:/home/welcome$ cat user.txt
flag{user-0bb3c30dc72e63881db5005f1aa19ac3}
admin@BabyPass:/home/welcome$
```

提权

找到网站的配置文件 `config.php`

```
anuj@BabyPass:/var/www/html/tms/includes$ cat config.php
<?php
// DB credentials.
define('DB_HOST','localhost');
define('DB_USER','tms_user');
define('DB_PASS','secure_password');
define('DB_NAME','tms');
// Establish database connection.
try
{
```

扒拉数据库（一开始没看到 `root` 研究别的去了）

```
MariaDB [tms]> select * from admin;
+----+----------+----------------------------------+---------------------+
| id | UserName | Password                         | updationDate        |
+----+----------+----------------------------------+---------------------+
|  1 | admin    | f925916e2754e5e03f75dd58a5733251 | 2020-05-11 07:18:49 |
+----+----------+----------------------------------+---------------------+
1 row in set (0.000 sec)

MariaDB [tms]> select * from tblusers;
+----+---------------+-------------+-----------------+--------------------------
---------+---------------------+---------------------+
| id | FullName      | MobileNumber | EmailId         | Password
| RegDate             | UpdationDate        |
+----+---------------+-------------+-----------------+--------------------------
---------+---------------------+---------------------+
|  1 | Manju Srivatav | 4456464654   | manju@gmail.com  |
202cb962ac59075b964b07152d234b70 | 2020-07-08 02:33:20 | NULL                |
|  2 | Kishan         | 9871987979   | kishan@gmail.com |
202cb962ac59075b964b07152d234b70 | 2020-07-08 02:33:56 | NULL                |
|  3 | Salvi Chandra  | 1398756416   | salvi@gmail.com  |
```

```
202cb962ac59075b964b07152d234b70 | 2020-07-08 02:34:20 | NULL                |
|  4 | Abir           | 4789756456   | abir@gmail.com    |
202cb962ac59075b964b07152d234b70 | 2020-07-08 02:34:38 | NULL                |
|  5 | Test'"         | 1987894654   | anuj@gmail.com    |
f925916e2754e5e03f75dd58a5733251 | 2020-07-08 02:35:06 | 2025-11-11 09:51:27 |
|  6 | root           | 123456789    | root@gmail.com    |
fd50619cd7026f0f32272f77f4da6e92 | 2020-07-08 02:35:06 | 2021-05-11 00:37:41 |
|  8 | sunset         | 1980207743   | 1@q.com           |
30f80affc3322427a482878e75e4cdfc | 2025-11-11 09:53:54 | NULL                |
+----+----------------+--------------+-------------------+-------------------------
---------+----------------------+----------------------+
7 rows in set (0.001 sec)
```

`opt` 下有个名为 `pass` 的可执行文件

```
anuj@BabyPass:/opt$ ./pass
06cfVLhwofgYpPZKHtpo
```

拉出去分析一下 pass

结果就是一个单纯的密码生成器

```
_BYTE *__fastcall generatePassword(_BYTE *a1, int a2)
{
  _BYTE *result; // rax
  char s[69]; // [rsp+10h] [rbp-B0h] BYREF
  char v4[43]; // [rsp+55h] [rbp-6Bh] BYREF
  char v5[32]; // [rsp+80h] [rbp-40h] BYREF
  int v6; // [rsp+A0h] [rbp-20h]
  int v7; // [rsp+A4h] [rbp-1Ch]
  int j; // [rsp+A8h] [rbp-18h]
  int i; // [rsp+ACh] [rbp-14h]

  strcpy(v5, "ABCDEFGHIJKLMNOPQRSTUVWXYZ");
  strcpy(&v4[11], "abcdefghijklmnopqrstuvwxyz");
  strcpy(v4, "0123456789");
  *a1 = v5[rand() % 26];
  a1[1] = v4[rand() % 26 + 11];
  a1[2] = v4[rand() % 10];
  strcpy(s, "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789");
  v7 = strlen(s);
  for ( i = 3; i < a2; ++i )
    a1[i] = s[rand() % v7];
  for ( j = a2 - 1; j > 0; --j )
  {
    v6 = rand() % (j + 1);
    v5[31] = a1[j];
    a1[j] = a1[v6];
    a1[v6] = v5[31];
  }
```

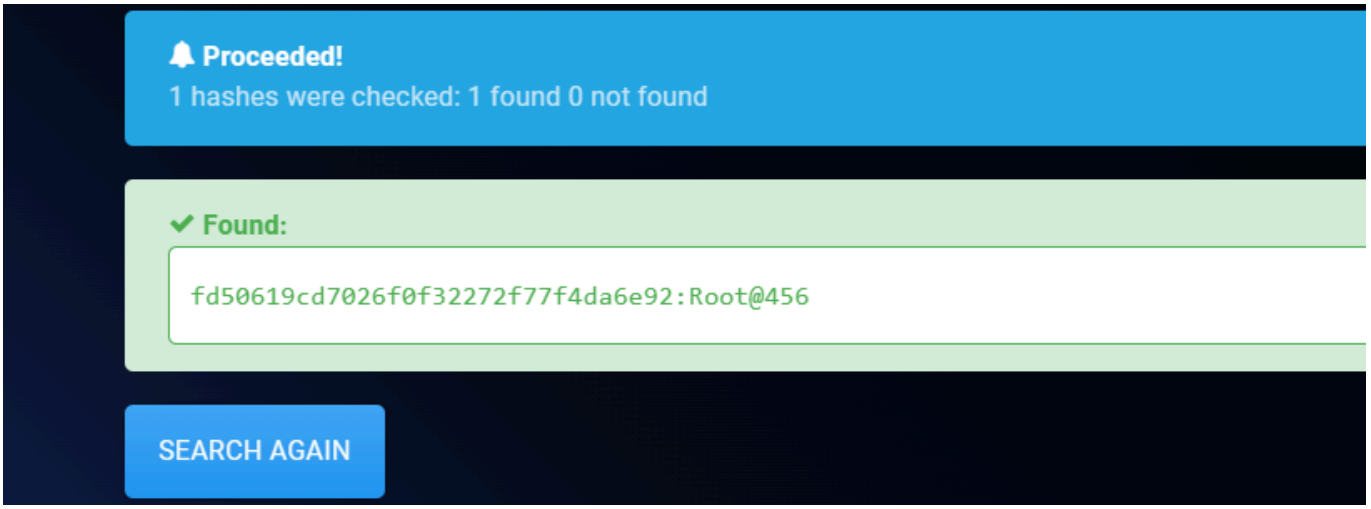
```
  result = &a1[a2];
  *result = 0;
  return result;
}
```

随后跑了 linpeas 和很多的手工枚举，无功而返，开始怀疑自己。

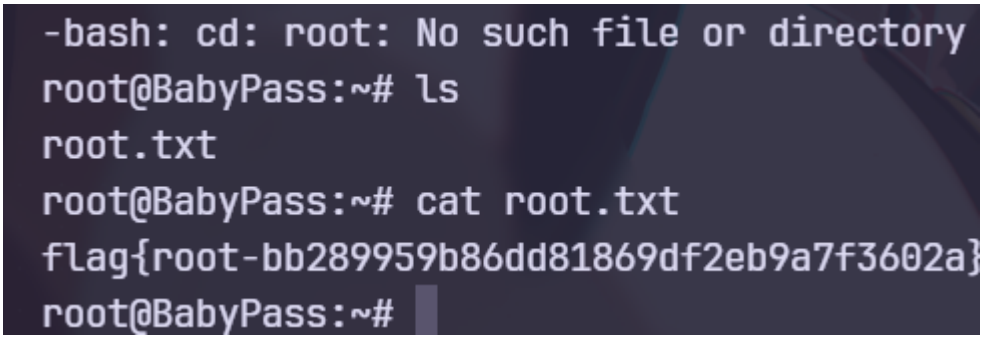
回顾内容，发现数据库中藏着 root@gmail.com

```
|  6 | root           | 123456789     | root@gmail.com    |
fd50619cd7026f0f32272f77f4da6e92 | 2020-07-08 02:35:06 | 2021-05-11 00:37:41 |
```

破解密码并尝试进行登录



成功登录



https://www.sunsetaction.top