信息收集

主机发现

端口扫描

```
Not shown: 65531 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
2211/tcp open  emwin
8888/tcp open  sun-answerbook
```

服务识别

```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Tomato
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
2211/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d2:53:0a:91:8c:f1:a6:10:11:0d:9e:0f:22:f8:49:8e (RSA)
|   256 b3:12:60:32:48:28:eb:ac:80:de:17:d7:96:77:6e:2f (ECDSA)
|_  256 36:6f:52:ad:fe:f7:92:3e:a2:51:0f:73:06:8d:80:13 (ED25519)
8888/tcp open  http    nginx 1.10.3 (Ubuntu)
|_http-title: 401 Authorization Required
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Private Property
|_http-server-header: nginx/1.10.3 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

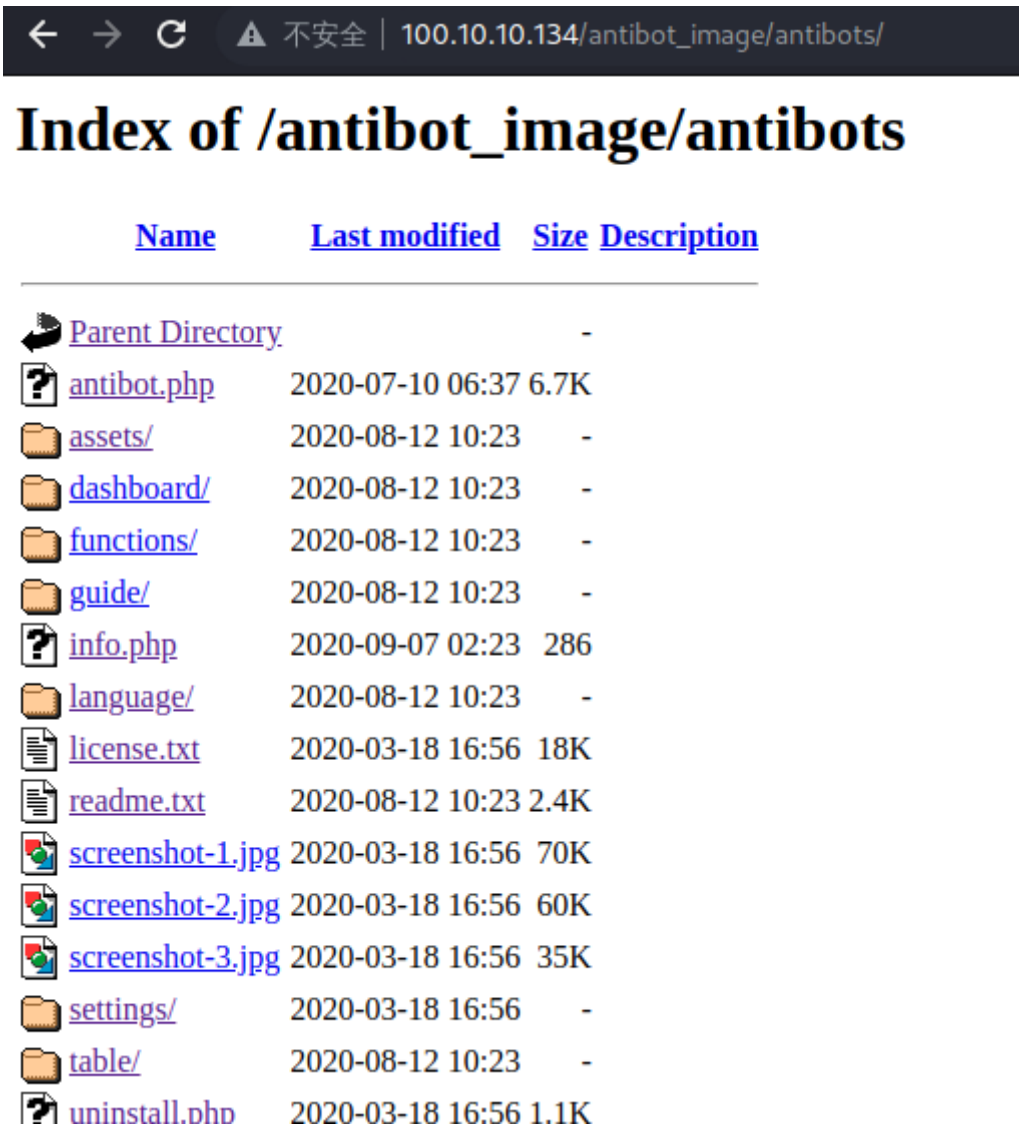
子域名发现

敏感目录遍历

用seclist的common字典

挖到一个目录

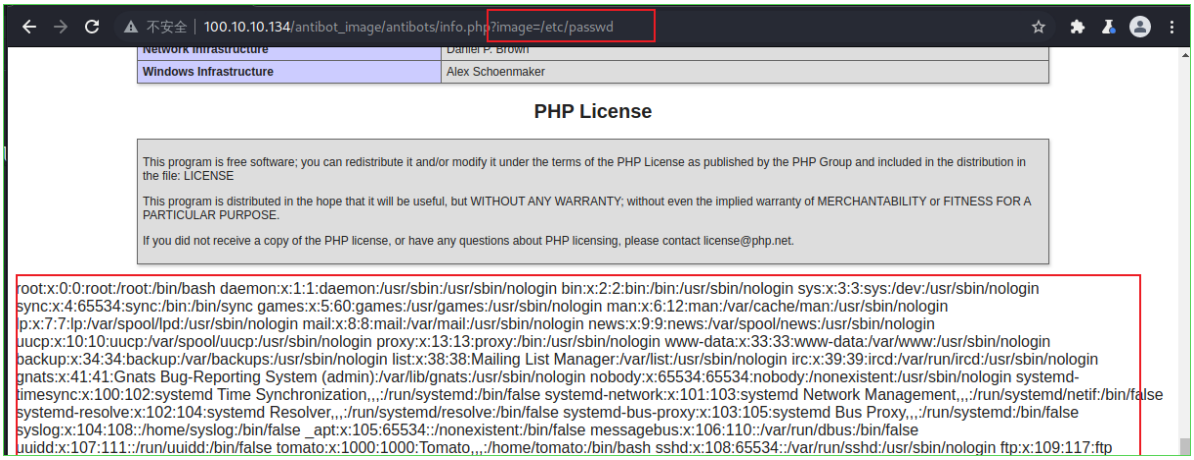
```
┌──(pinginglab㉿pinginglab)-[~]
└─$ gobuster dir -t 150 -u http://100.10.10.134 -w /usr/share/seclists/Discovery/Web-Content/common.txt -x html,php,txt,
bak
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://100.10.10.134
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              html,php,txt,bak
[+] Timeout:                 10s
===============================================================
2022/05/08 17:40:05 Starting gobuster in directory enumeration mode
===============================================================
/.hta.html            (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd.bak        (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/antibot_image        (Status: 301) [Size: 322] [--> http://100.10.10.134/antibot_image/]
/.hta.php             (Status: 403) [Size: 278]
```



web信息搜集

查看对应文件夹下的info.php发现隐藏参数

对image参数进行LFI的fuzzing,发现成功



漏洞发现

业务重构

威胁建模

21:密码爆破

2211:密码爆破

8888:密码爆破

80:LFI

漏洞利用

边界突破

权限提升

总结