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

```
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)
| 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

```
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)
                                              http://100.10.10.134
                                              GET
150
      Method:
     Threads:
                                            /usr/share/seclists/Discovery/Web-Content/common.txt
404
      Wordlist:
      Negative Status codes:
                                              gobuster/3.1.0
html,php,txt,bak
      User Agent:
[+] Extensions:
[+] Timeout:
                                              10s
2022/05/08 17:40:05 Starting gobuster in directory enumeration mode
                                  (Status: 403) [Size: 278]
/.hta.html
/.htpasswd.txt
 htaccess.
 '.htpasswd.bak
/.htpasswd
/.htaccess.html
 /.htpasswd.html
/.htpasswd.php
/.htaccess.php
/antibot_image
/ hta_php
                                                                            [--> http://100.10.10.134/antibot_image/]
```

← → C ▲ 不安全 | 100.10.10.134/antibot_image/antibots/

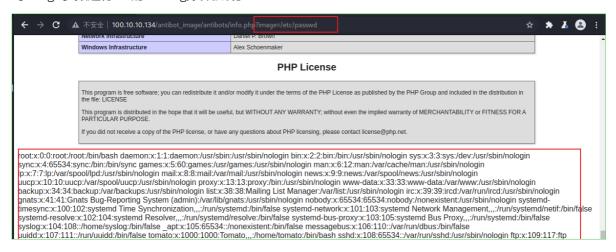
Index of /antibot_image/antibots

Parent Directory - antibot.php 2020-07-10 06:37 6.7K assets/ 2020-08-12 10:23 - dashboard/ 2020-08-12 10:23 - functions/ 2020-08-12 10:23 - guide/ 2020-08-12 10:23 - info.php 2020-09-07 02:23 286 language/ 2020-08-12 10:23 - license.txt 2020-03-18 16:56 18K readme.txt 2020-08-12 10:23 2.4K screenshot-1.jpg 2020-03-18 16:56 60K screenshot-2.jpg 2020-03-18 16:56 60K screenshot-3.jpg 2020-03-18 16:56 35K settings/ 2020-03-18 16:56 -	<u>Name</u>	<u>Last modified</u>	Size Description
assets/ 2020-08-12 10:23 - dashboard/ 2020-08-12 10:23 - functions/ 2020-08-12 10:23 - guide/ 2020-08-12 10:23 - info.php 2020-09-07 02:23 286 language/ 2020-08-12 10:23 - license.txt 2020-03-18 16:56 18K readme.txt 2020-08-12 10:23 2.4K screenshot-1.jpg 2020-03-18 16:56 70K screenshot-2.jpg 2020-03-18 16:56 60K screenshot-3.jpg 2020-03-18 16:56 35K	Parent Directory		-
dashboard/ 2020-08-12 10:23 - functions/ 2020-08-12 10:23 - guide/ 2020-09-07 02:23 286 language/ 2020-08-12 10:23 - license.txt 2020-03-18 16:56 18K readme.txt 2020-08-12 10:23 2.4K screenshot-1.jpg 2020-03-18 16:56 70K screenshot-2.jpg 2020-03-18 16:56 60K screenshot-3.jpg 2020-03-18 16:56 35K	antibot.php	2020-07-10 06:37	6.7K
functions/ 2020-08-12 10:23 - guide/ 2020-08-12 10:23 - info.php 2020-09-07 02:23 286 language/ 2020-08-12 10:23 - license.txt 2020-03-18 16:56 18K readme.txt 2020-08-12 10:23 2.4K screenshot-1.jpg 2020-03-18 16:56 70K screenshot-2.jpg 2020-03-18 16:56 60K screenshot-3.jpg 2020-03-18 16:56 35K	assets/	2020-08-12 10:23	-
info.php 2020-08-12 10:23 - info.php 2020-09-07 02:23 286 language/ 2020-08-12 10:23 - license.txt 2020-03-18 16:56 18K readme.txt 2020-08-12 10:23 2.4K screenshot-1.jpg 2020-03-18 16:56 70K screenshot-2.jpg 2020-03-18 16:56 60K screenshot-3.jpg 2020-03-18 16:56 35K	ashboard/	2020-08-12 10:23	-
info.php 2020-09-07 02:23 286 language/ 2020-08-12 10:23 - license.txt 2020-03-18 16:56 18K readme.txt 2020-08-12 10:23 2.4K screenshot-1.jpg 2020-03-18 16:56 70K screenshot-2.jpg 2020-03-18 16:56 60K screenshot-3.jpg 2020-03-18 16:56 35K	functions/	2020-08-12 10:23	-
language/ 2020-08-12 10:23 - license.txt 2020-03-18 16:56 18K readme.txt 2020-08-12 10:23 2.4K screenshot-1.jpg 2020-03-18 16:56 70K screenshot-2.jpg 2020-03-18 16:56 60K screenshot-3.jpg 2020-03-18 16:56 35K	guide/	2020-08-12 10:23	-
license.txt 2020-03-18 16:56 18K readme.txt 2020-08-12 10:23 2.4K screenshot-1.jpg 2020-03-18 16:56 70K screenshot-2.jpg 2020-03-18 16:56 60K screenshot-3.jpg 2020-03-18 16:56 35K	info.php	2020-09-07 02:23	286
readme.txt 2020-08-12 10:23 2.4K screenshot-1.jpg 2020-03-18 16:56 70K screenshot-2.jpg 2020-03-18 16:56 60K screenshot-3.jpg 2020-03-18 16:56 35K	<u>language/</u>	2020-08-12 10:23	-
screenshot-1.jpg 2020-03-18 16:56 70K screenshot-2.jpg 2020-03-18 16:56 60K screenshot-3.jpg 2020-03-18 16:56 35K	license.txt	2020-03-18 16:56	18K
screenshot-2.jpg 2020-03-18 16:56 60K screenshot-3.jpg 2020-03-18 16:56 35K	readme.txt	2020-08-12 10:23	2.4K
screenshot-3.jpg 2020-03-18 16:56 35K	screenshot-1.jpg	2020-03-18 16:56	70K
_	screenshot-2.jpg	2020-03-18 16:56	60K
<u>settings/</u> 2020-03-18 16:56 -	screenshot-3.jpg	2020-03-18 16:56	35K
	<u>settings/</u>	2020-03-18 16:56	-
<u>table/</u> 2020-08-12 10:23 -	table/	2020-08-12 10:23	-
uninstall.php 2020-03-18 16:56 1.1K	uninstall.php	2020-03-18 16:56	1.1K

web信息搜集

对image参数进行LFI的fuzzing,发现成功

<!-- </?php include \$_GET['image']; -->



漏洞发现

业务重构

8

9

.0

<body>

1 </body>

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