### Задание 23.5.2 (HW-03)

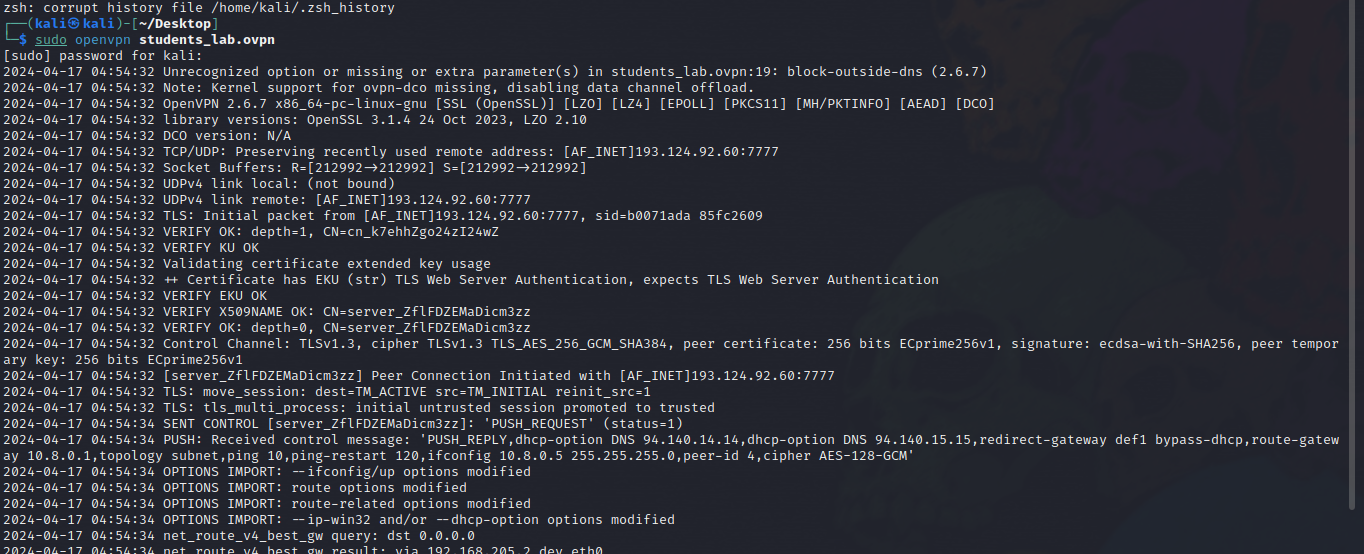
**Персонализация:** Михайлов Юрий Никитич (uramihajlov481@gmail.com)

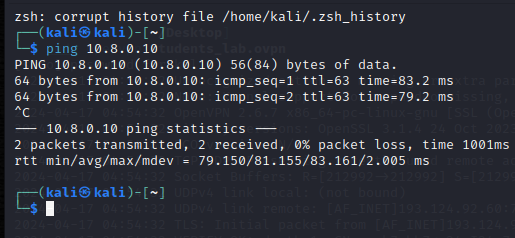
**Лабораторная работа:** Задание**№**23.5.2 (HW-03)**:**

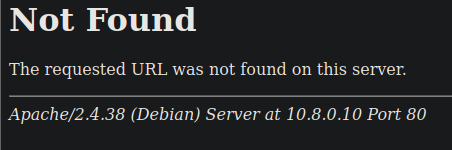
**Общая информация:**

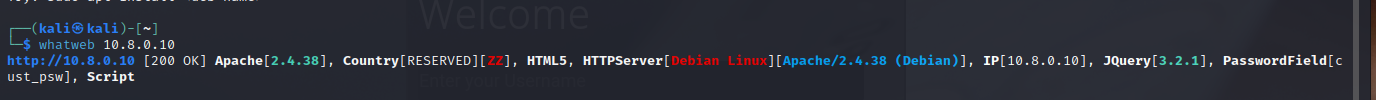
* Период тестирования: 17.04.2024
* Задание: Лабораторные работы. (root)

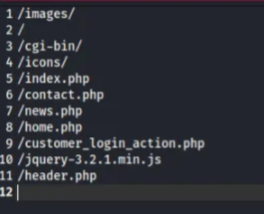
**Описание действий:  
  
1) Включаем openvpn**

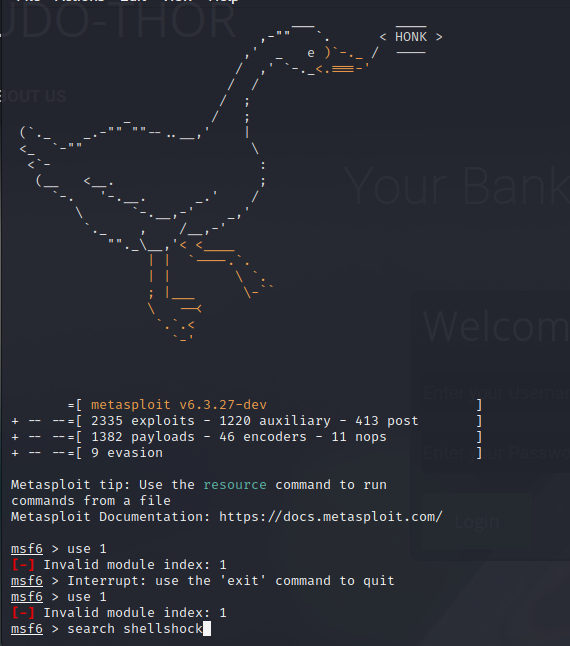
****

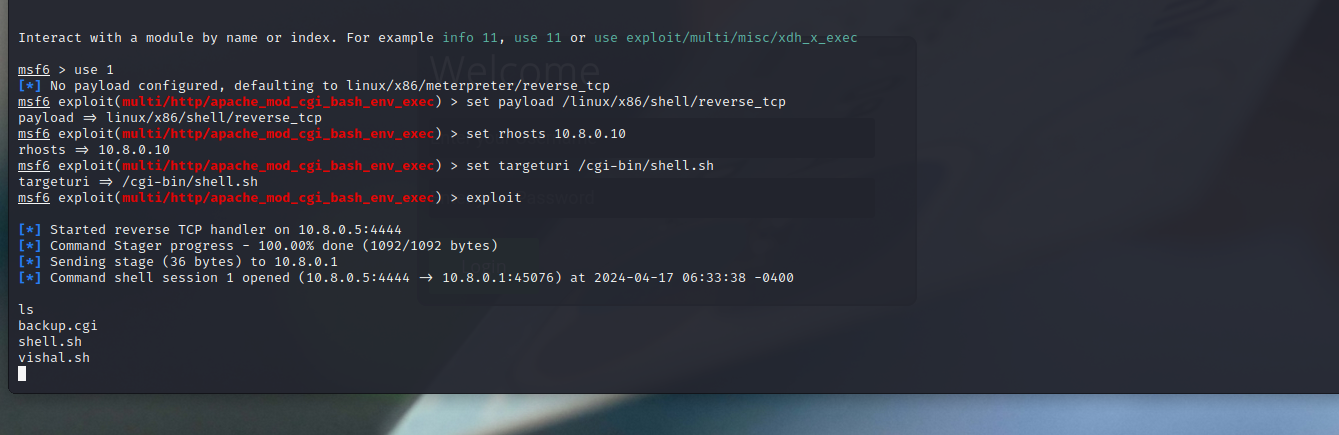
**2) Проверяем ip пингуя его  
**

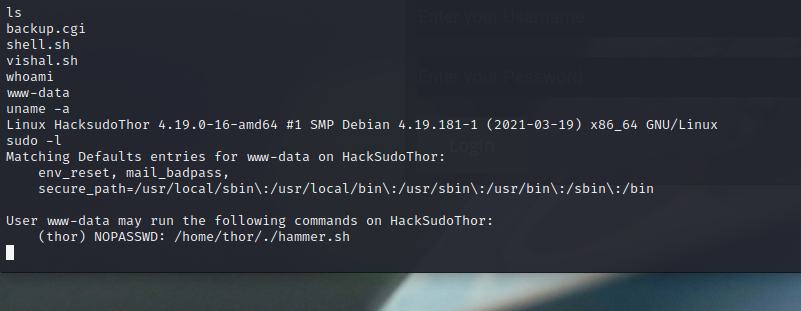
**3) находим версию базы данных что позволяет найм найти нужный эксплойт и использовать его  
  
**

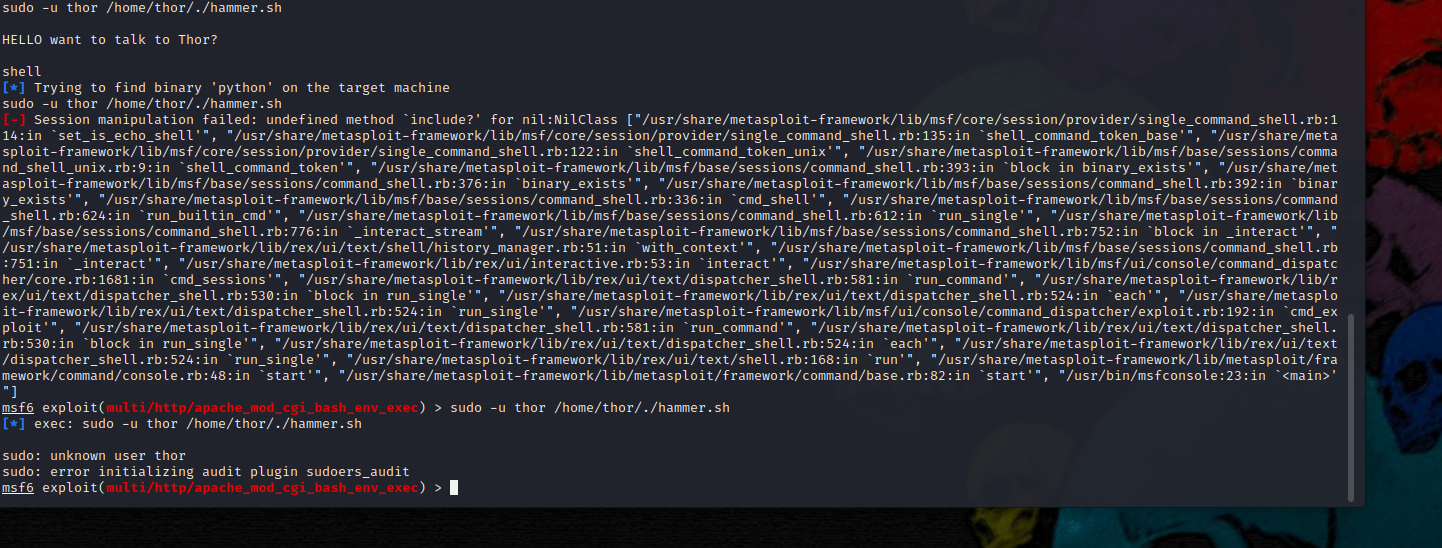
**4) так же решил поискать директории через dirbuster ну и узнал что используется на сайте с помощью whatweb**

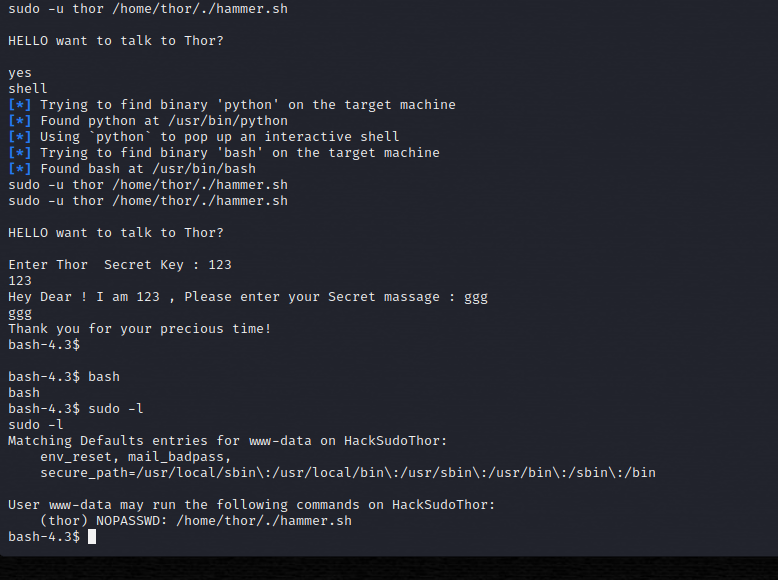
****

**5) Из интересного отметим /cgi-bin/   
**

**6) Эксплуатируем  
**

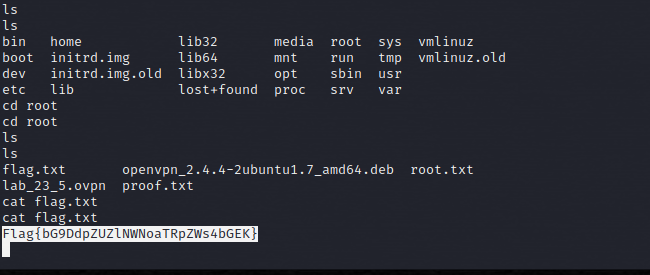
**7)** 

**8) Пробуем sudo -u thor /home/thor/./hammer.sh не выходит добавляем Shell и пробуем ещё раз**

**9) sudo service ../../bin/bash**

**10) Спустя пару попыток я понял что надо открыть файл паролем bash и тогда мы можешь использовать sudo service ../../bin/bash**



**11) **

**Finally…**