Этап 4. Использование nikto

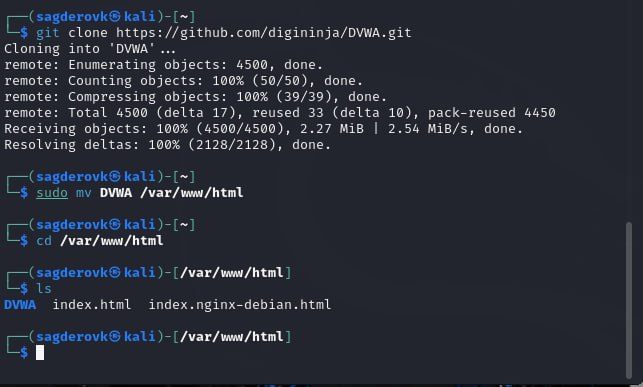
Использование nikto

Сагдеров Камал

Содержание

# 1 Выполнение лабораторной работы

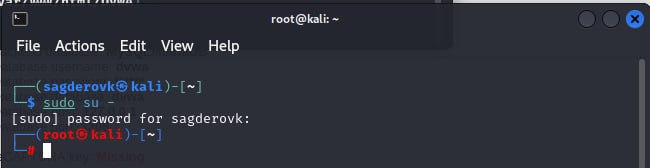
nikto — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями.



1

Исходные данные:

IP сервера 178.72.90.181;  
Сервис http на стандартном 80 порту;  
Для авторизации используется html форма, которая отправляет по адресу http://178.72.90.181/cgi-bin/luci методом POST запрос вида username=root&password=test\_password;  
В случае не удачной аутентификации пользователь наблюдает сообщение Invalid username and/or password! Please try again.



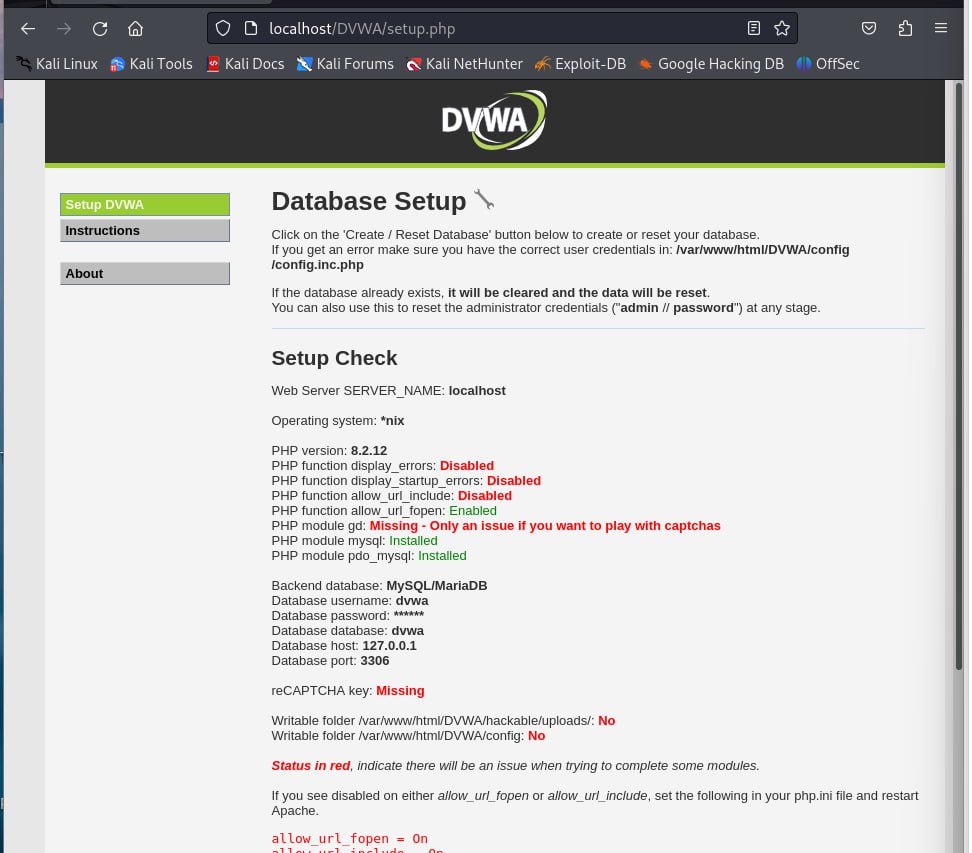
2

Запрос к Hydra будет выглядеть примерно так:

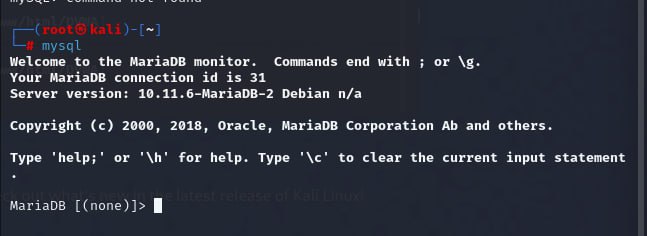


3

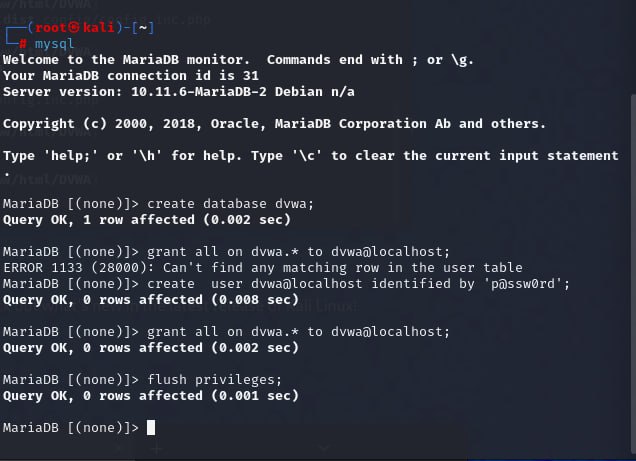
Используется http-post-form потому, что авторизация происходит по http методом post. Пасхальные яйца: раскрытие полных путей, обход аутентификации и некоторые другие.



4



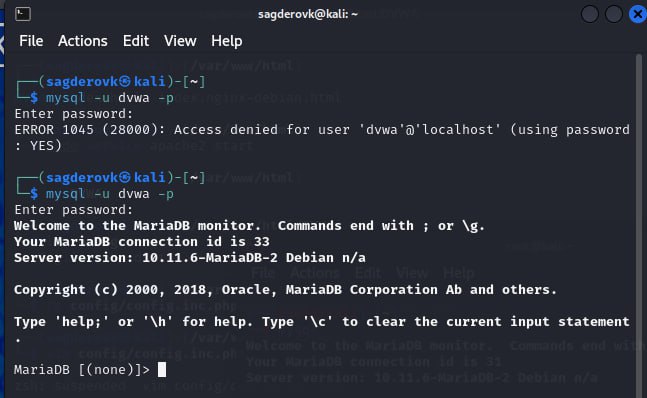
5



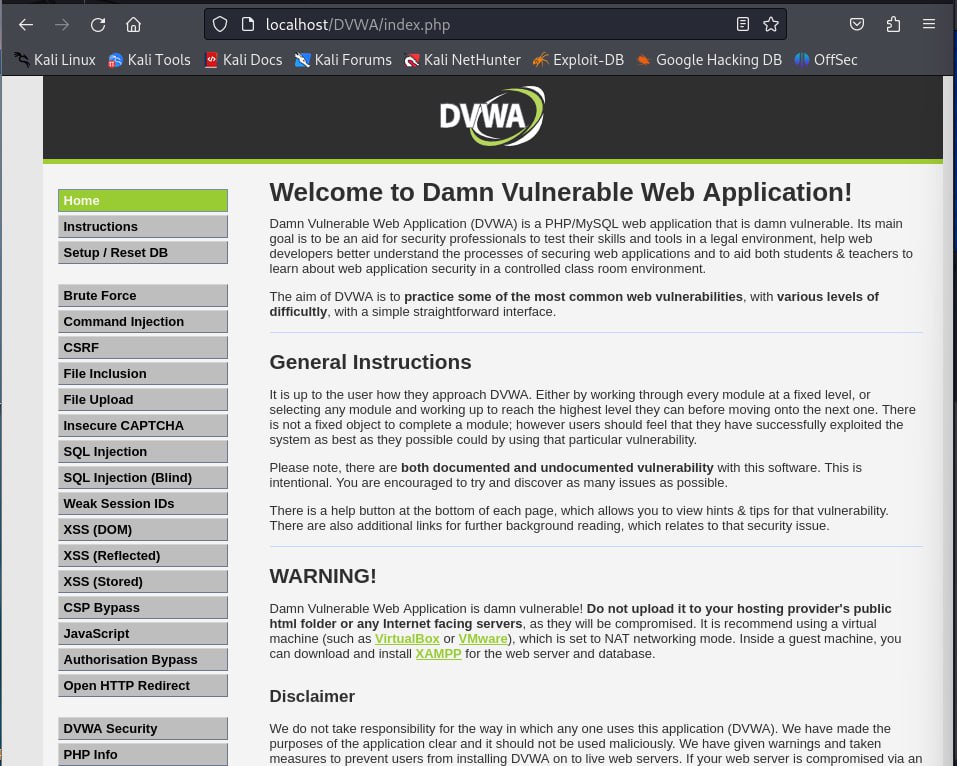
6

После указания этого модуля идёт строка /cgi-bin/luci:username=USER&password=PASS:Invalid username, у которой через двоеточие (:) указывается:

путь до скрипта, который обрабатывает процесс аутентификации (/cgi-bin/luci);

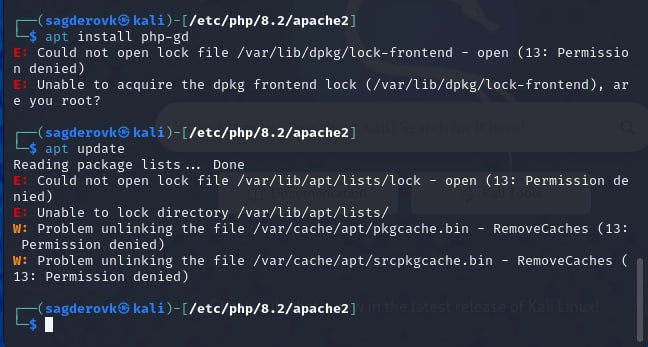


7

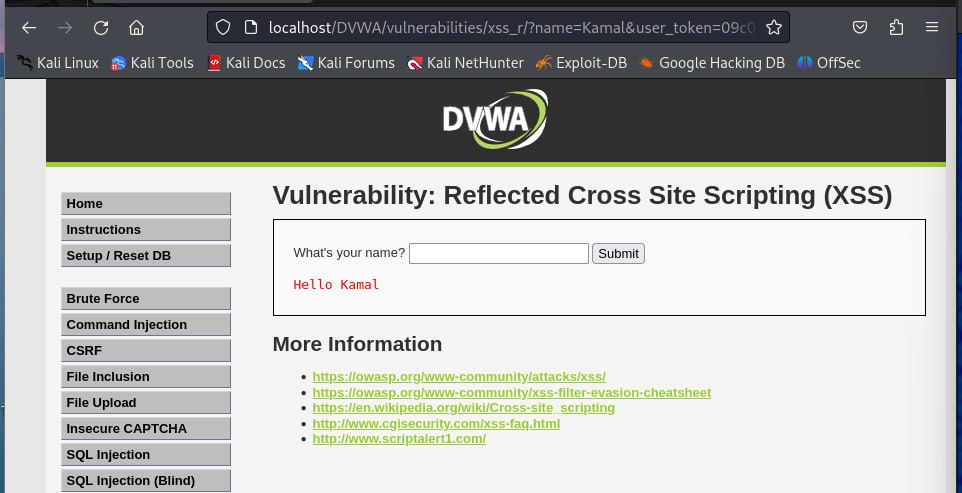


8

строка, которая передаётся методом POST, в которой логин и пароль заменены на USER и PASS соответственно (username=USER&password=PASS); строка, которая присутствует на странице при неудачной аутентификации; при её отсутствии Hydra поймёт, что мы успешно вошли (Invalid username



9



10

# 2 Выводы

Я научился использовать Hydra