Индивидуальный проект. Третий этап

Королёв Иван Андреевич

Содержание

1 Цель работы **5**

2 Задание **6**

3 Теоретическое введение **7**

4 Выполнение лабораторной работы **8**
4.1 Проверка веб-сайта 8
4.2 Проверка вкладки Сеть 8
4.3 Получение параметров POST 9
4.4 Запустите Hydra 10

5 Выводы **11**

Список литературы **12**

Список иллюстраций

4.1 hydra 8
4.2 hydra 9
4.3 hydra 9
4.4 hydra 10
4.5 hydra 10

Список таблиц

1 Цель работы

Использовать hydra

2 Задание

Подобрать логин и пароль к сайту

3 Теоретическое введение

Hydra – это программное обеспечение с открытым исходным кодом для перебора паролей в реальном времени от различных онлайн сервисов, веб-приложений, FTP, SSH и других протоколов. Это распараллеленный взломщик для входа в систему, он поддерживает множество протоколов для осуществления атак.

4 Выполнение лабораторной работы

4.1 Проверка веб-сайта

1. Дополнительные инструменты > Инструменты разработчика. (рис. 4.1).

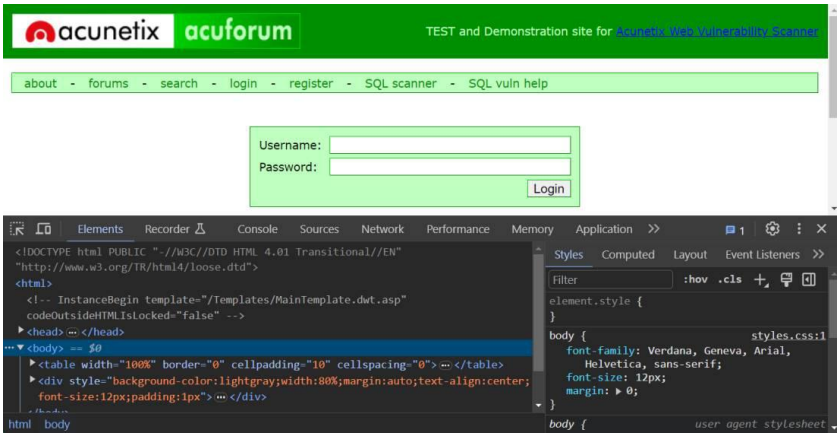

Рис. 4.1: hydra

4.2 Проверка вкладки Сеть

2. Перейдите на вкладку Сеть, чтобы просмотреть входящие файлы и информацию. Если на вкладке ничего не отображается, это означает, что мы еще не РАЗМЕСТИЛИ какие-либо данные. (рис. 4.2).

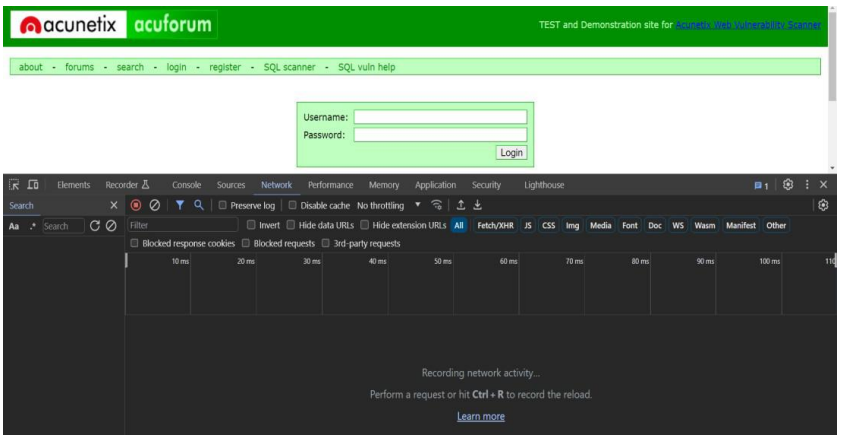

Рис. 4.2: hydra

4.3 Получение параметров POST

3. Чтобы получить параметры post-формы, введите имя пользователя и / или пароль в форме входа, какие вам нравятся, а затем нажмите “Войти”. Вы заметите новый метод публикации на вкладке сеть в консоли разработчика. (рис. 4.3).

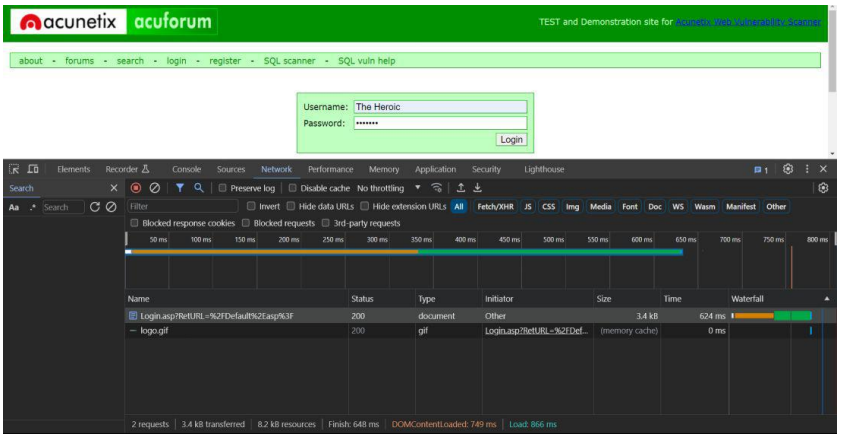

Рис. 4.3: hydra

4.4 Запустите Hydra

3. Введите приведенную выше команду, нажмите Enter, и пусть Hydra попытается взломать пароль для нас. Поскольку это атака на основе словаря, это займет время. Когда он найдет правильную комбинацию имени пользователя и пароля, он остановит все последующие попытки входа в систему и отобразит обнаруженные им правильные учетные данные. (рис. 4.4), (рис. 4.5)

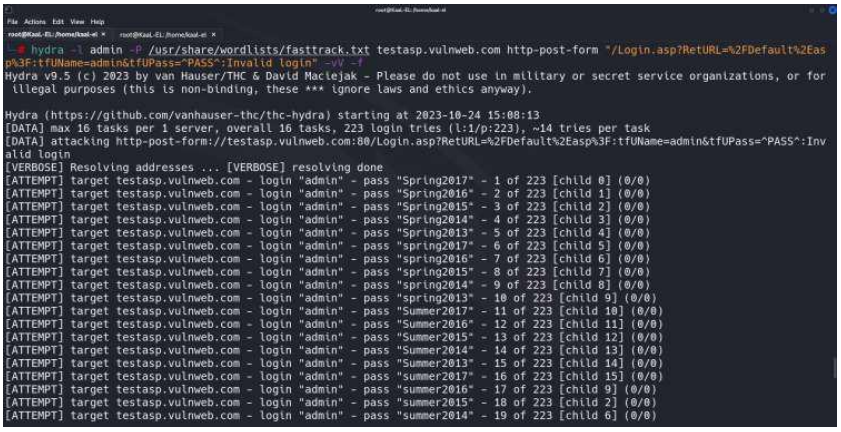

Рис. 4.4: hydra

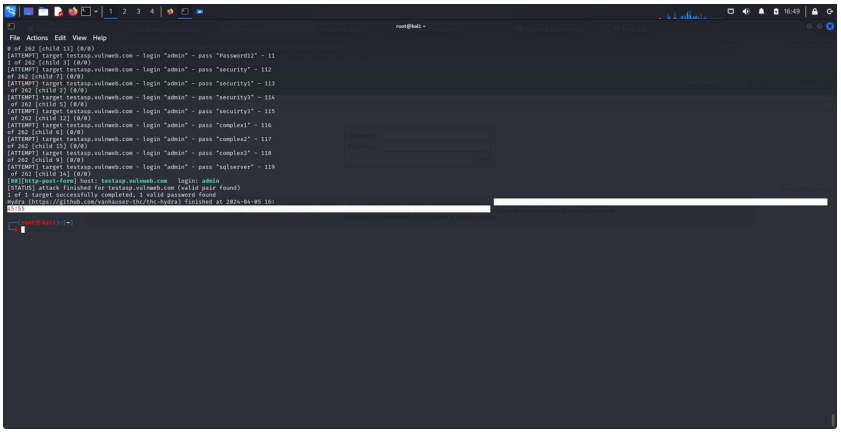

Рис. 4.5: hydra

5 Выводы

Неэтично и незаконно использовать Hydra для попытки взлома веб-системы входа или любой другой системы без надлежащей авторизации. Это нарушение конфиденциальности и компьютерной безопасности, и это может привести к серьезным последствиям, таким как судебный иск и уголовные обвинения. Важно предупредить соответствующие органы или владельца системы, если у вас есть какие-либо опасения или подозрения по поводу безопасности страницы входа или системы. Безопасность может быть повышена за счет этичного и ответственного раскрытия информации без нарушения закона или моральных обязательств.

Список литературы

:::