Индивидуальный проект

Этап 3. Использование Hydra

Артамонов Т. Е.

27 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Артамонов Тимофей Евгеньевич
- студент группы НКНбд-01-21
- Российский университет дружбы народов
- https://github.com/teartamonov

Цель работы

Применить метод bruteforce с помощью Hydra для подбора логина и пароля для слабозащищенных учетных записей.

DVWA (Damn Vulnerable Web Application) - это веб-приложение на PHP/MySQL, которое “чертовски” уязвимо. Его основная цель — помочь специалистам по безопасности протестировать свои навыки и инструменты в легальной среде, помочь веб-разработчикам лучше понять процессы обеспечения безопасности веб-приложений, а также помочь студентам и преподавателям изучить вопросы безопасности веб-приложений в контролируемой учебной среде.

Цель DVWA — отработать некоторые из наиболее распространенных веб-уязвимостей с различными уровнями сложности, используя простой и понятный интерфейс. Пожалуйста, обратите внимание, что в этом программном обеспечении есть как задокументированные, так и незадокументированные уязвимости. Это сделано намеренно. Вам предлагается попытаться обнаружить как можно больше проблем.

Некоторые из уязвимостей веб приложений, который содержит DVWA

Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей. Исполнение (внедрение) команд: Выполнение команд уровня операционной системы. Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» изменить пароль администратора приложений. Внедрение (инклуд) файлов: Позволяет «атакующему» присоединить удалённые/локальные файлы в веб приложение.

Некоторые из уязвимостей веб приложений, который содержит DVWA

SQL внедрение: Позволяет «атакующему» внедрить SQL выражения в HTTP из поля ввода, DVWA включает слепое и основанное на ошибке SQL внедрение. Небезопасная выгрузка файлов: Позволяет «атакующему» выгрузить вредоносные файлы на веб сервер. Межсайтовый скриптинг (XSS): «Атакующий» может внедрить свои скрипты в веб приложение/базу данных. DVWA включает отражённую и хранимую XSS. Пасхальные яйца: раскрытие полных путей, обход аутентификации и некоторые другие.

DVWA имеет три уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA

Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом. Высокий — это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости не позволяют такой простор эксплуатации как на других уровнях. Средний — этот уровень безопасности предназначен главным образом для того, чтобы дать пользователю пример плохих практик безопасности, где разработчик попытался сделать приложение безопасным, но потерпел неудачу. Низкий — этот уровень безопасности совершенно уязвим и совсем не имеет защиты. Его предназначение быть примером среди уязвимых веб приложений, примером плохих практик программирования и служить платформой обучения базовым техникам эксплуатации.

Выполнение лабораторной работы

Сменили уровень безопасности на Low. (рис. 1)

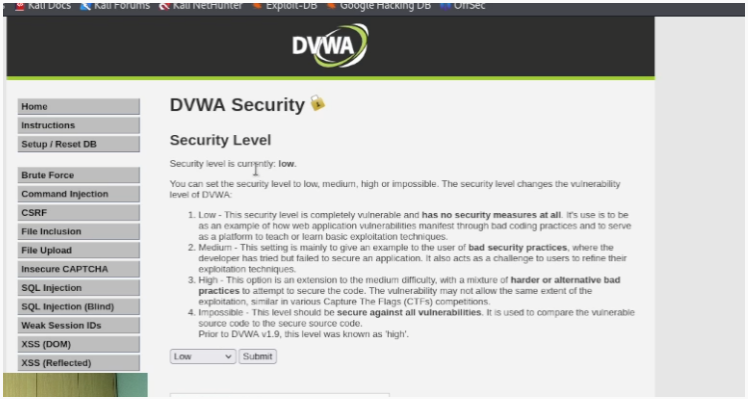
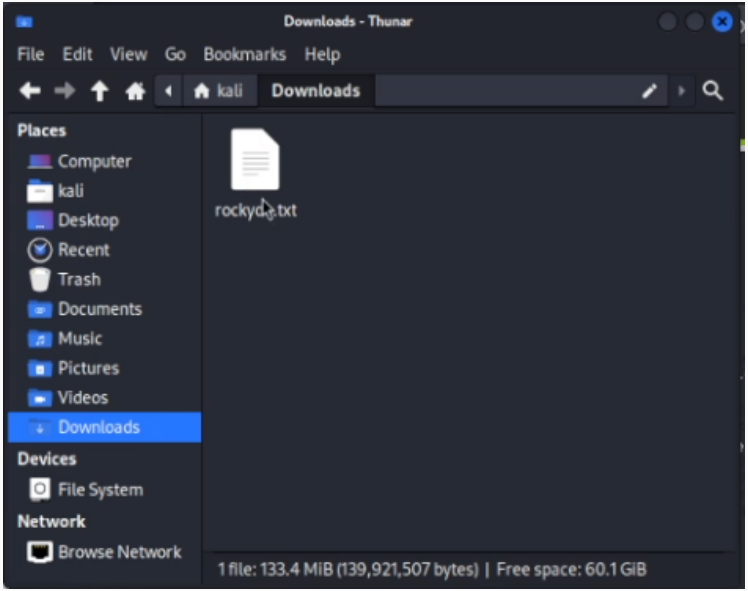


Figure 1: Security level Low

Распаковали архив с файлом с наиболее распространенными паролями. (рис. 2)



Зашли в раздел brute force. (рис. 3)

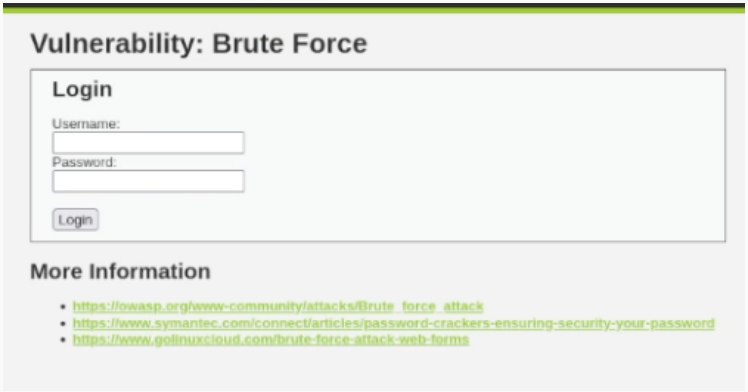


Figure 3: Окно с логином и паролем

Посмотрим код этой страницы. (рис. 4)

Figure 4: Запрос GET

Посмотрим содержимое файла. (рис. 5)

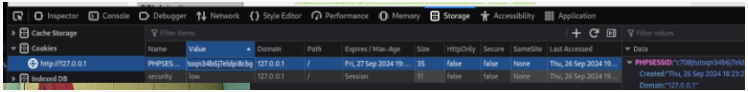


Figure 5: Содержимое файла config.inc.php.dist

Найдем в куки PHPSESSID. (рис. 6)

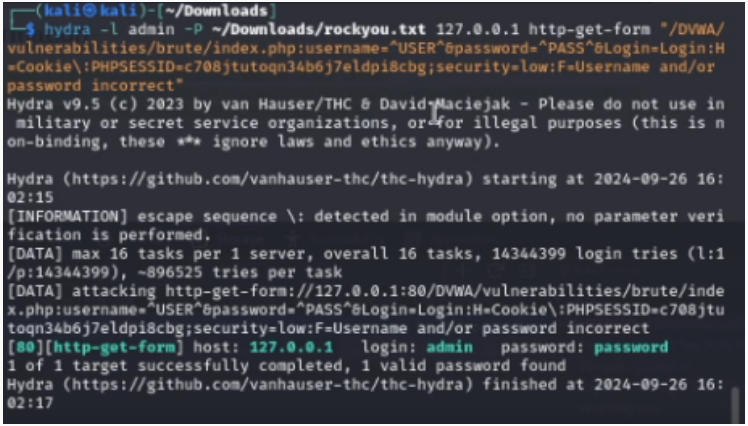


Figure 6: PHPSESSID домена 127.0.0.1

Запустим командой подбор паролей. (рис. 7)

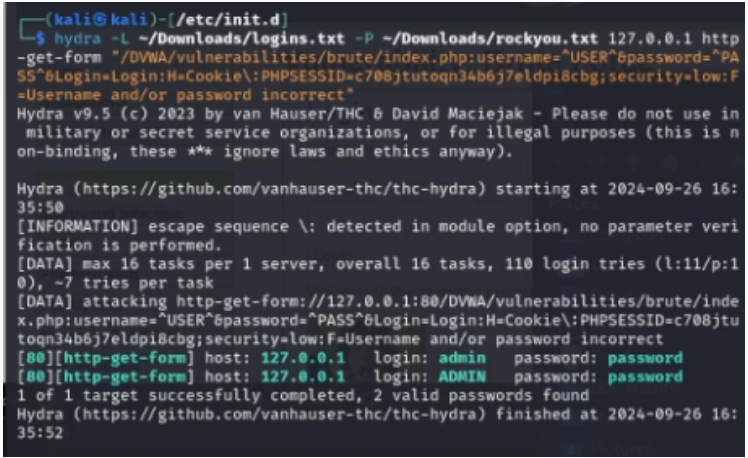


Figure 7: Получили пароль password для логина admin, все получилось

Теперь создадим файл с частыми логинами и будем подбирать и логин и пароль. (рис. 8)

Получили две пары логинов и паролей, потому что для логина регистр не учитывается, а в файле это разные строки

Figure 8: Получили две пары логинов и паролей, потому что для логина регистр не учитывается, а в файле это разные строки

Выводы

Использовали Hydra и подобрали логин и пароль для слабозащищенной учетной записи.

Список литературы

1. DVWA [Электронный ресурс]. Github, Inc., 2024. URL: https://github.com/digininja/DVWA.
2. Этап 2. Установка DVWA [Электронный ресурс]. RUDN. 2024. URL: https://esystem.rudn.ru/mod/page/view.php?id=1140704