Шаблон отчёта по проект 2

Установка DVWA

Туем Гислен

Содержание

# 1 Цель работы

Установить DVWA в гостевую систему к Kali Linux.

# 2 Задание

1. Скачать DVWA
2. Настройка DVWA
3. Настройка База данных
4. Настройка сервера Apache
5. Откройте DVWA в своем веб-браузере

# 3 Теоретическое введение

1. Установите DVWA в гостевую систему к Kali Linux.
2. Репозиторий: https://github.com/digininja/DVWA.
3. 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.  
    
   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.

# 4 Выполнение лабораторной работы

1. клонировать репозиторий DVWA GitHub(рис. [??]).
2. назначьте разрешения на чтение, запись и выполнение (777) для папки DVWA[??]).
3. посмотреть содержимое каталога конфигурации и создать копию файла с именем config.inc.php(рис. [??]).
4. Теперь откройте файл config.inc.php в редакторе nano, чтобы выполнить необходимые настройки(рис. [??]).
5. запустить службу MySQL и проверьте, запущена ли служба(рис. [??]).
6. войти в базу данных(рис. [??]).
7. создайте нового пользователя и предоставьте этому пользователю полные права доступа к базе данных dvwa(рис. [??]).
8. запустите терминал и выполните мониторинг в каталоге /etc/php/8.2/apache2, а затем выполните команду sudo nano php.ini, найдите строкиallow\_url\_fopen иallow\_url\_include и убедитесь, что для обоих установлено значение «ON»(рис. [??]).
9. запустите и посмотрите статус apache2(рис. [??]).
10. Запустите веб-браузер и введите URL-адрес: 127.0.0.1/DVWA(рис. [??]).
11. Нажмите кнопку «Создать/сбросить базу данных» в конце страницы(рис. [??]).
12. После успешного входа в систему вас встретит домашняя страница DVWA.(рис. [??]).

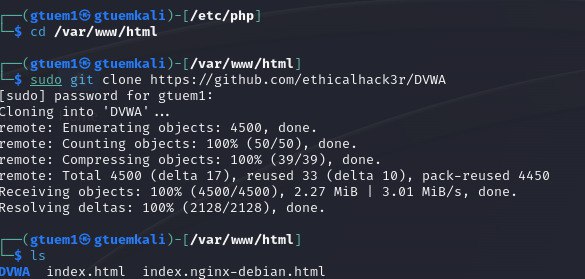


рис 1

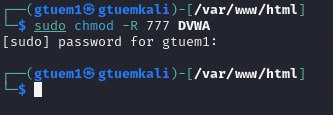


рис 2

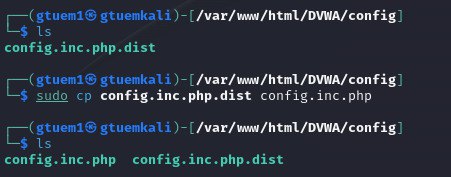


рис 3

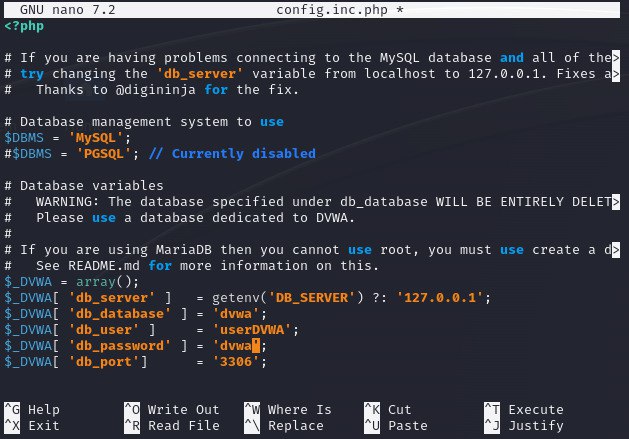


рис 4

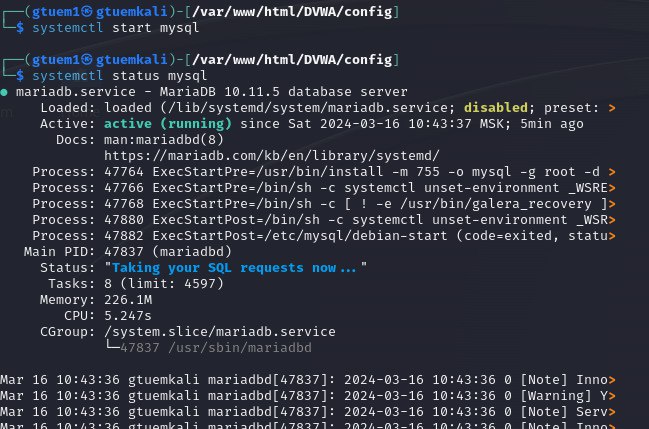


рис 5

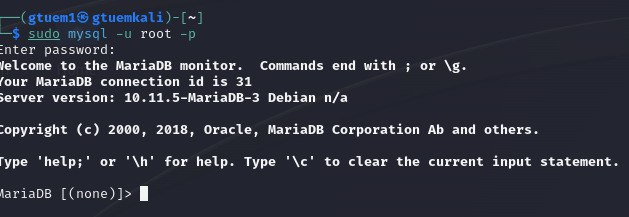


рис 6

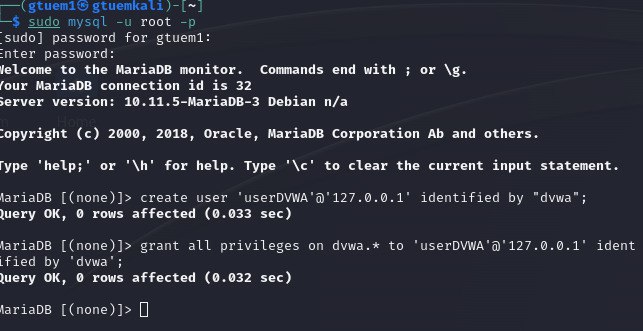


рис 7

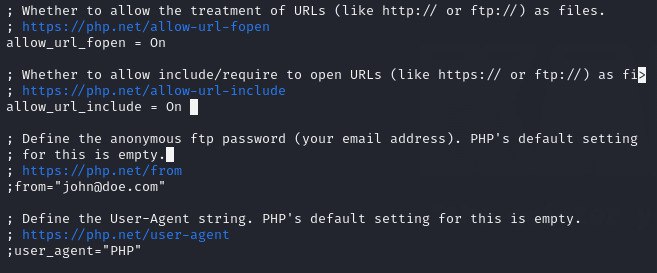


рис 8

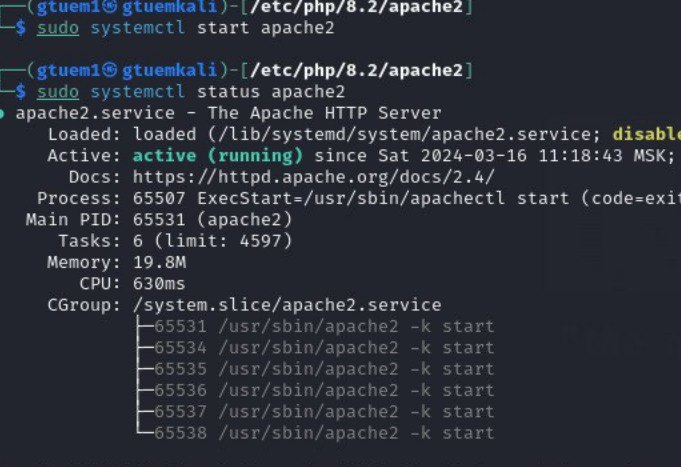


рис 9

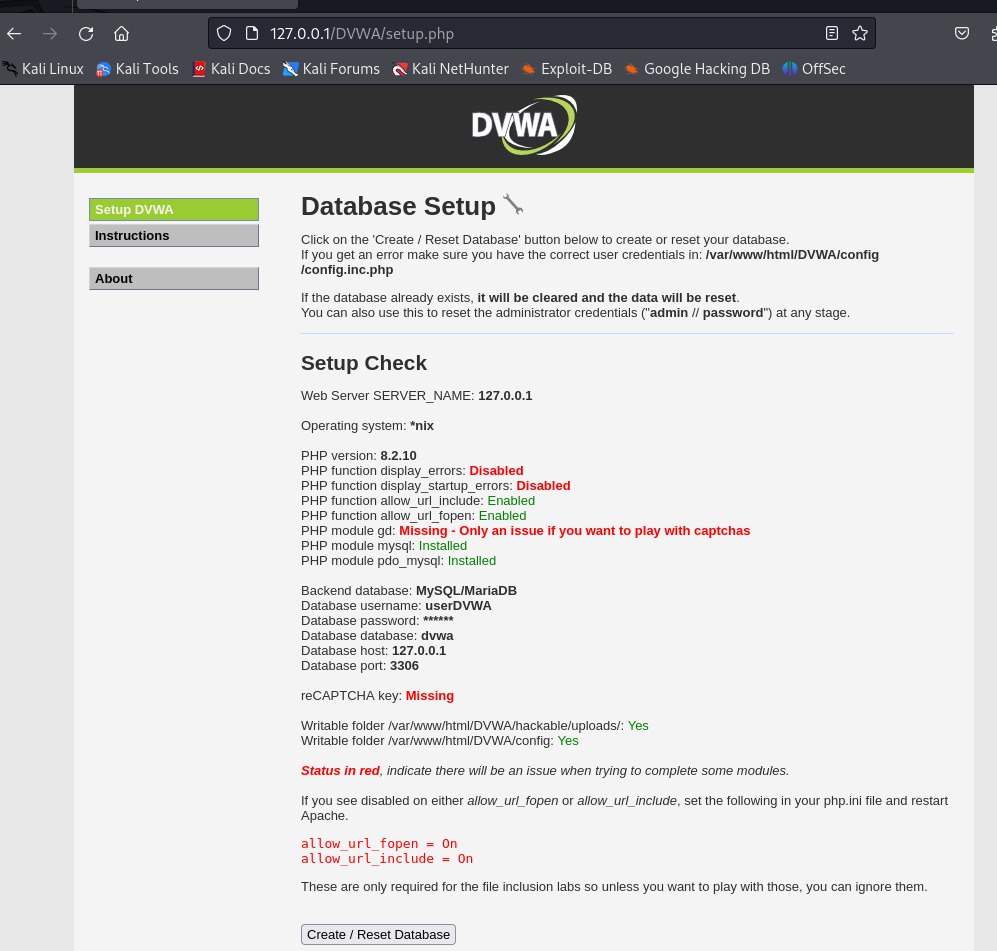


рис 10

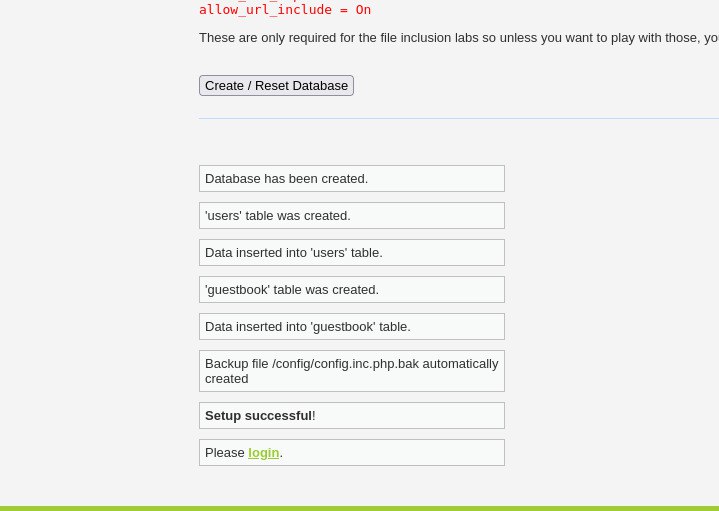


рис 11

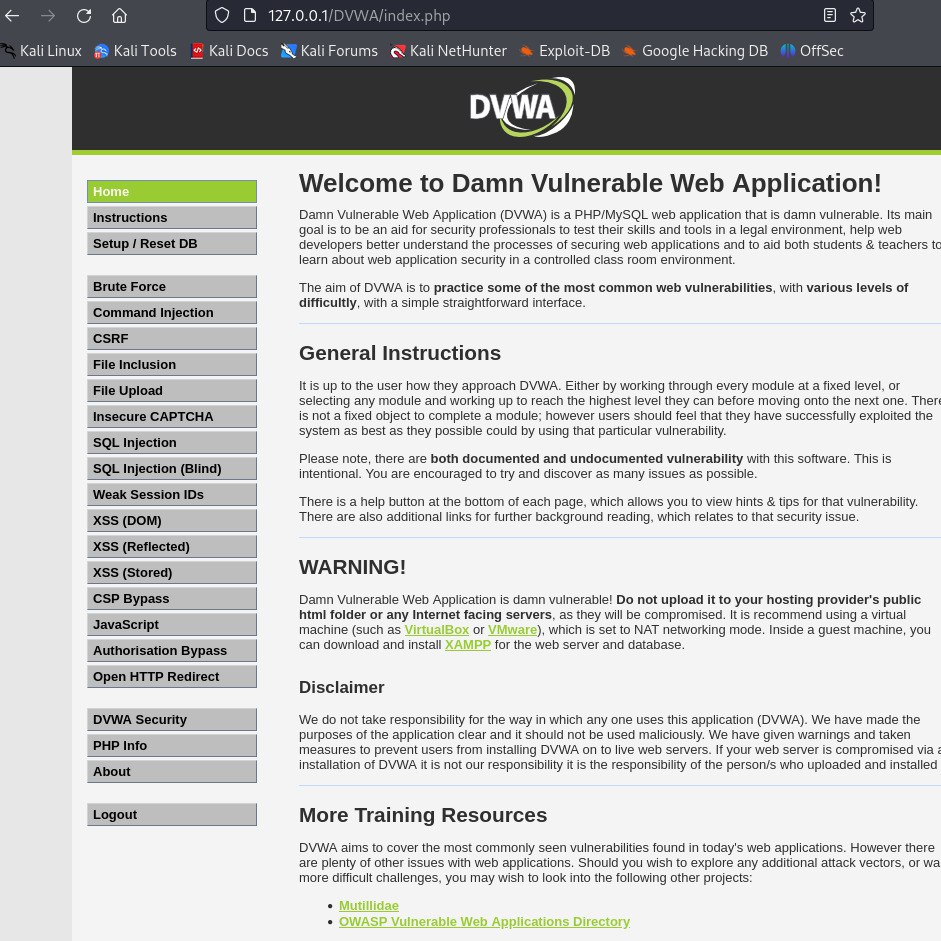


рис 12

# 5 Выводы

DVWA — отличная платформа как для начинающих, так и для опытных пользователей благодаря многоуровневой поддержке безопасности. Я считаю, что этот пост дал вам подробное руководство по настройке DVWA в вашей системе Kali Linux.