

Индивидуальный проект

Этап 2

Прокопьева Марина Евгеньевна

Содержание

1	2 Этап	5
2	Выполнение этапы	6
3	Выводы	13

Список иллюстраций

Список таблиц

1 2 Этап

Этап 2. Установка DVWA

Установите DVWA в гостевую систему к Kali Linux.

Репозиторий: <https://github.com/digininja/DVWA>.

Некоторые из уязвимостей веб приложений, который содержит DVWA:

Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструмен

Исполнение (внедрение) команд: Выполнение команд уровня операционной системы.

Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» изменить пароль администратора.

Внедрение (инклюд) файлов: Позволяет «атакующему» присоединить удалённые/локальные файлы.

SQL внедрение: Позволяет «атакующему» внедрить SQL выражения в HTTP из поля ввода, DVWA

Небезопасная выгрузка файлов: Позволяет «атакующему» выгрузить вредоносные файлы на веб-сервер.

Межсайтовый скриптинг (XSS): «Атакующий» может внедрить свои скрипты в веб приложение.

Пасхальные яйца: раскрытие полных путей, обход аутентификации и некоторые другие.

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

Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для тестирования.

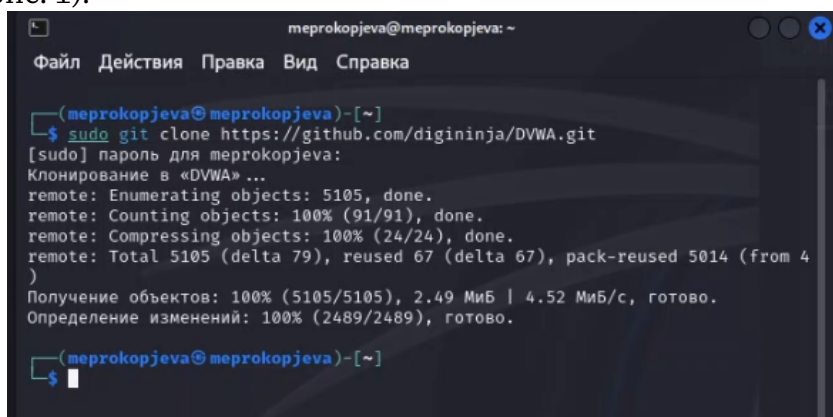
Высокий — это расширение среднего уровня сложности, со смесью более сложных или альтернативных уязвимостей.

Средний — этот уровень безопасности предназначен главным образом для того, чтобы дать новичкам.

Низкий — этот уровень безопасности совершенно уязвим и совсем не имеет защиты. Его пр

2 Выполнение этапы

Настройка DVWA происходит на нашем локальном хосте, поэтому нужно перейти в директорию `/var/www/html`. Затем клонирую нужный репозиторий GitHub (рис. 1).

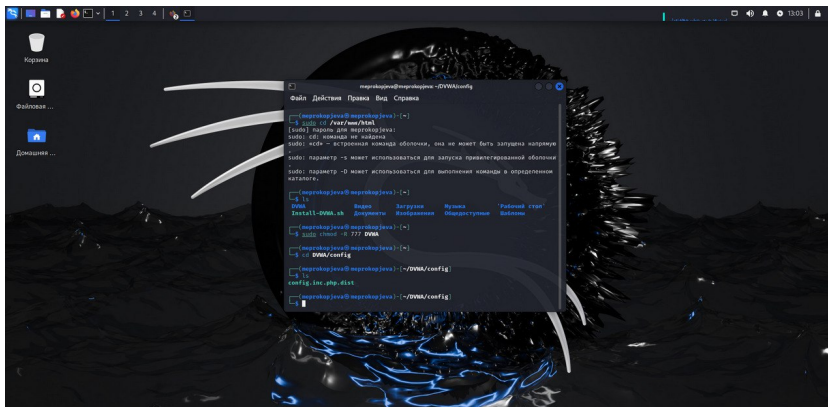


```
mepronkopjeva@mepronkopjeva: ~  
Файл Действия Правка Вид Справка  
$ sudo git clone https://github.com/digininja/DVWA.git  
[sudo] пароль для mepronkopjeva:  
Клонирование в «DVWA» ...  
remote: Enumerating objects: 5105, done.  
remote: Counting objects: 100% (91/91), done.  
remote: Compressing objects: 100% (24/24), done.  
remote: Total 5105 (delta 79), reused 67 (delta 67), pack-reused 5014 (from 4)  
Получение объектов: 100% (5105/5105), 2.49 МиБ | 4.52 МиБ/с, готово.  
Определение изменений: 100% (2489/2489), готово.  
$
```

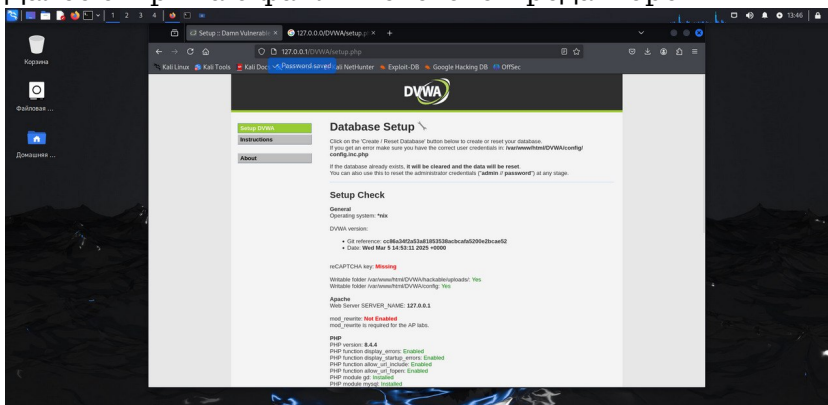
Проверяю, что файлы скопировались правильно, далее повышаю права доступа к этой папке до 777

Чтобы настроить DVWA, нужно перейти в каталог `/dvwa/config`, затем проверяю содержимое каталога

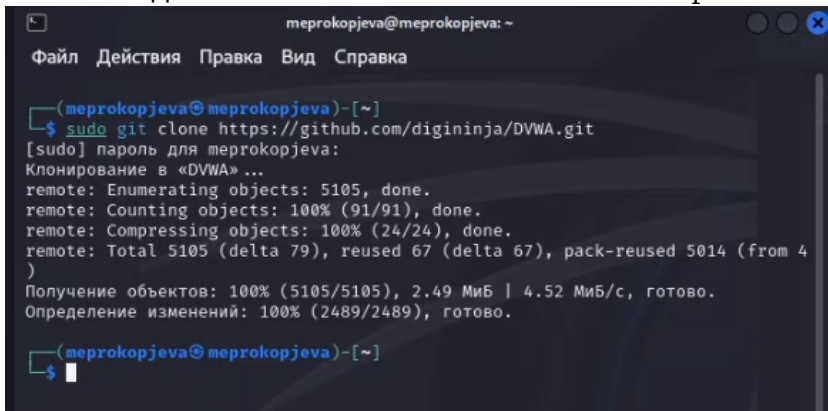
Создаем копию файла, используемого для настройки DVWA `config.inc.php.dist` с именем `config.inc.php`. Копируем файл, а не изменяем его, чтобы у нас был запасной вариант, если что-то пойдет не так



Далее открываю файл в текстовом редакторе



Изменяю данные об имени пользователя и пароле



По умолчанию в Kali Linux установлен mysql, поэтому можно его запустить без предварительного скачивания, далее выполняю проверку, запущен ли процесс

```
meprokojjeva@meprokojjeva: ~  
Файл Действия Правка Вид Справка  
Получение объектов: 100% (5105/5105), 2.49 МиБ | 4.52 МиБ/с, готово.  
Определение изменений: 100% (2489/2489), готово.  
  
(meprokojjeva@meprokojjeva)-[~]  
$ sudo bash -c "$(curl --fail --show-error --silent --location https://githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh)"  
dquote>  
dquote>  
  
(meprokojjeva@meprokojjeva)-[~]  
$ wget https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh  
--2025-03-13 10:11:15-- https://raw.githubusercontent.com/IamCarron/DVWA-Script/main/Install-DVWA.sh  
Распознаётся raw.githubusercontent.com (raw.githubusercontent.com)... 185.10.133, 185.199.108.133, 185.199.111.133, ...  
Подключение к raw.githubusercontent.com (raw.githubusercontent.com)|185.10.133|:443 ... соединение установлено.  
HTTP-запрос отправлен. Ожидание ответа... 200 OK  
Длина: 16902 (17K) [text/plain]  
Сохранение в: «Install-DVWA.sh»  
  
Install-DVWA.sh 100%[=====>] 16,51K --.-KB/s за 0,00  
2025-03-13 10:11:15 (2,69 MB/s) - «Install-DVWA.sh» сохранён [16902/16902]  
  
(meprokojjeva@meprokojjeva)-[~]  
$
```

Авторизируюсь в базе данных от имени пользователя root. Появляется командная строка с приглашением “MariaDB”, далее создаем в ней нового пользователя, используя учетные данные из файла config.inc.php

```
meprokojjeva@meprokojjeva: ~  
Файл Действия Правка Вид Справка  
  
Creating config file /etc/php/8.4/apache2/php.ini with new version  
apache2_invoke: Enable module php8.4  
Настраивается пакет libapache2-mod-php (2:8.4+96) ...  
Настраивается пакет php8.4 (8.4.4-1) ...  
Настраивается пакет php (2:8.4+96) ...  
Обрабатываются триггеры для man-db (2.13.0-1) ...  
Обрабатываются триггеры для kali-menu (2024.4.0) ...  
Обрабатываются триггеры для php8.4-cli (8.4.4-1) ...  
Обрабатываются триггеры для libapache2-mod-php8.4 (8.4.4-1) ...  
libapache2-mod-php is installed!  
git is installed!  
Downloading DVWA from GitHub ...  
Клонирование в «/var/www/html/DVWA» ...  
remote: Enumerating objects: 5105, done.  
remote: Counting objects: 100% (91/91), done.  
remote: Compressing objects: 100% (24/24), done.  
remote: Total 5105 (delta 79), reused 67 (delta 67), pack-reused 5014 (from 4)  
Получение объектов: 100% (5105/5105), 2.49 МиБ | 7.15 МиБ/с, готово.  
Определение изменений: 100% (2489/2489), готово.  
Enabling MariaDB ...  
Starting MariaDB ...  
  
Default credentials:  
Username: root  
  
Password: [No password just hit Enter]  
Enter SQL user: 
```



```
File Действия Правка Вид Справка
)
Получение объектов: 100% (5105/5105), 2.49 МиБ | 7.15 МиБ/с, готово.
Определение изменений: 100% (2489/2489), готово.
... Enabling MariaDB...
Starting MariaDB...

Default credentials:
Username: root

.. Password: [No password just hit Enter]
Enter SQL user: root
Enter SQL password (press Enter for no password):
Enter password:
SQL commands executed successfully.
Configuring DVWA...
Configuring permissions...
Configuring PHP...
Enabling Apache...
Restarting Apache...
DVWA has been installed successfully. Access http://localhost/DVWA to get started.
Credentials:
Username: admin
Password: password

With by IamCarron

(meprokopjeva@meprokopjeva)-[~]
$

File Действия Правка Вид Справка
Enter SQL user: root
Enter SQL password (press Enter for no password):
... Enter password:
SQL commands executed successfully.
Configuring DVWA...
Configuring permissions...
Configuring PHP...
Enabling Apache...
Restarting Apache...
.. DVWA has been installed successfully. Access http://localhost/DVWA to get started.
Credentials:
Username: admin
Password: password

With by IamCarron

(meprokopjeva@meprokopjeva)-[~]
$ docker version
Команда «docker» не найдена, но может быть установлена с помощью:
sudo apt install docker-cli
sudo apt install podman-docker

(meprokopjeva@meprokopjeva)-[~]
$ cd /etc/php/7.4/apache2
cd: Нет такого файла или каталога: /etc/php/7.4/apache2

(meprokopjeva@meprokopjeva)-[~]
$ docker compose logs
```

Теперь нужно пользователю предоставить привилегии для работы с этой базой данных

Необходимо настроить сервер apache2, перехожу в соответствующую директорию

В файле php.ini нужно будет изменить один параметр, поэтому открываю файл

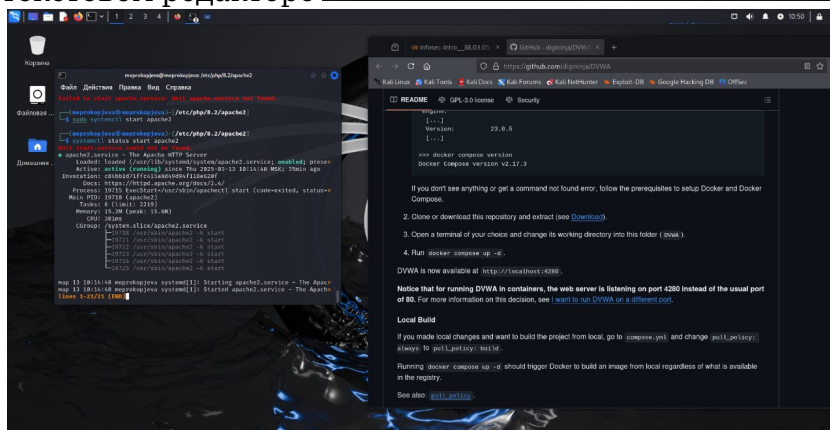
```
терговкоржева@терговкоржева: /etc/php/8.2/apache2
Файл Действия Правка Вид Справка
GNU nano 8.2 php.ini
;;;;;;;;;;;;;;;;;;;;;;;;
; PHP's initialization file, generally called php.ini, is responsible for
; configuring many of the aspects of PHP's behavior.

; PHP attempts to find and load this configuration from a number of locations
; The following is a summary of its search order:
; 1. SAPI module specific location.
; 2. The PHPRC environment variable.
; 3. A number of predefined registry keys on Windows
; 4. Current working directory (except CLI)
; 5. The web server's directory (for SAPI modules), or directory of PHP
; (otherwise in Windows)
; 6. The directory from the --with-config-file-path compile time option, or
; Windows directory (usually C:\windows)
; See the PHP docs for more specific information.
; https://php.net/configuration.file

; The syntax of the file is extremely simple. Whitespace and lines
; beginning with a semicolon are silently ignored (as you probably guessed).
; Section headers (e.g. [Foo]) are also silently ignored, even though
; they might mean something in the future.

; Directives following the section heading [PATH=/www/mysite] only
; apply to PHP files in the /www/mysite directory. Directives
; following the section heading [HOST=www.example.com] only apply to
```

в текстовом редакторе



В файле параметры allow_url_fopen и allow_url_include должны быть поставлены как On

```
File Actions Edit View Help
$ sudo systemctl start apache2

(meprokopjeva@meprokopjeva)~[/etc/php/8.2/apache2]
$ systemctl status start apache2
Unit start.service could not be found.
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; prese>
   Active: active (running) since Thu 2025-03-13 10:14:48 MSK; 35min ago
   Invocation: c84bb1d71ffc415a8d49d94f118e620f
   Docs: https://httpd.apache.org/docs/2.4/
   Process: 19715 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
   Main PID: 19718 (apache2)
   Tasks: 6 (limit: 2219)
   Memory: 15.2M (peak: 15.6M)
   CPU: 301ms
   CGroup: /system.slice/apache2.service
           └─19718 /usr/sbin/apache2 -k start
             └─19721 /usr/sbin/apache2 -k start
               └─19722 /usr/sbin/apache2 -k start
                 └─19723 /usr/sbin/apache2 -k start
                   └─19724 /usr/sbin/apache2 -k start
                     └─19725 /usr/sbin/apache2 -k start

mar 13 10:14:48 meprokopjeva systemd[1]: Starting apache2.service - The Apac>
mar 13 10:14:48 meprokopjeva systemd[1]: Started apache2.service - The Apach>

(meprokopjeva@meprokopjeva)~[/etc/php/8.2/apache2]
$
```

```
Оболочка № 1
File Actions Edit View Help
# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETE
# D during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a de
# dicated DVWA user.
# See README.md for more information on this.
$ DVWA = array();
$ DVWA[ 'db_server' ] = getenv('DB_SERVER') ? : '127.0.0.1';
$ DVWA[ 'db_database' ] = getenv('DB_DATABASE') ? : 'dvwa';
$ DVWA[ 'db_user' ] = getenv('DB_USER') ? : 'dvwa';
$ DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ? : 'p@ssw0rd';
$ DVWA[ 'db_port' ] = getenv('DB_PORT') ? : '3306';

# ReCAPTCHA settings

# Used for the 'Insecure CAPTCHA' module
# You'll need to generate your own keys at: https://www.google.com/recaptch
a/admin
$ DVWA[ 'recaptcha_public_key' ] = getenv('RECAPTCHA_PUBLIC_KEY') ? : '';
$ DVWA[ 'recaptcha_private_key' ] = getenv('RECAPTCHA_PRIVATE_KEY') ? : '';

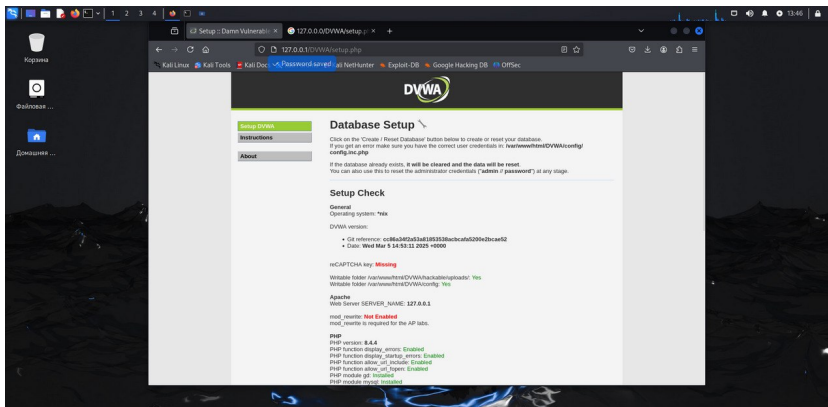
# Default security level
# Default value for the security level with each session.
12,1 19 %
```

Запускаем службу веб-сервера apache и проверяем, запущена ли служба

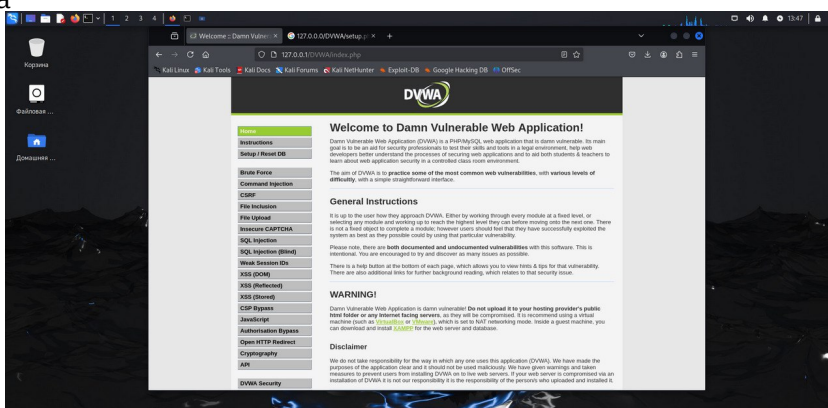
Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0/DVWA

Прокручиваем страницу вниз и нажмем на кнопку create\reset database

Авторизуюсь с помощью предложенных по умолчанию данных



Оказываюсь на домашней странице веб-приложения, на этом установка окончена



3 Выводы

Приобрела практические навыки по установке уязвимого веб-приложения DVWA.