

Индивидуальный проект

Этап 2. Установка DVWA

Артамонов Т. Е.

21 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

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



Установить DVWA и сделать приготовления для последующей работы.

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.

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 (инклюд) 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

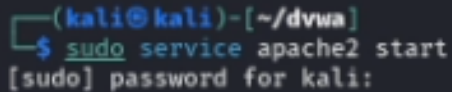
Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом. Высокий — это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке обезопасить код. Уязвимости 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.

Выполнение лабораторной работы

Загружаем репозиторий по ссылке. (рис. (fig:001?))

```
(kali@kali)-[~/dvwa]
$ git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA' ...
remote: Enumerating objects: 4784, done.
remote: Counting objects: 100% (334/334), done.
remote: Compressing objects: 100% (187/187), done.
remote: Total 4784 (delta 184), reused 267 (delta 139), pack-reused 4450 (from 1)
Receiving objects: 100% (4784/4784), 2.39 MiB | 262.00 KiB/s, done.
Resolving deltas: 100% (2279/2279), done.
```

Рис. 1: git clone



```
(kali@kali)-[~/dvwa]  
$ sudo service apache2 start  
[sudo] password for kali:
```

Рис. 2: Запуск apache2

Открываем веб-страницу Apache. (рис. (fig:003?))

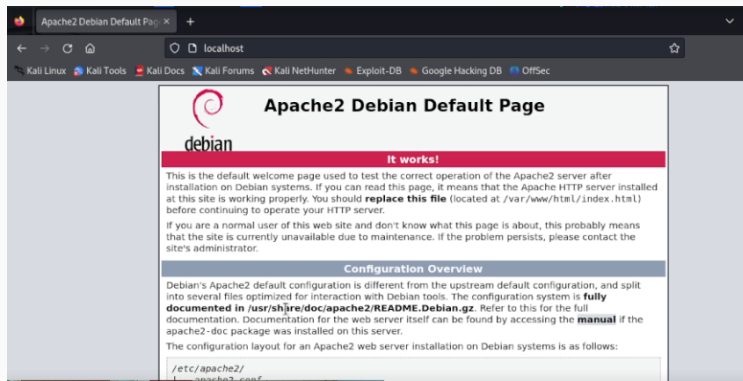


Рис. 3: Веб-страница Apache2 Debian Default Page

Копируем файл config.inc.php.dist в config.inc.php. (рис. (fig:004?))

```
└─$ sudo cp config.inc.php.dist config.inc.php
[sudo] password for kali:
(kali@kali)-[~/dvwa/DVWA/config]
└─$ ls ..
about.php      dvwa      phpinfo.php  README.md    security.txt
CHANGELOG.md   external  php.ini      README.pt.md setup.php
compose.yml     favicon.ico README.ar.md README.tr.md tests
config         hackable  README.es.md README.vi.md vulnerabilities
COPYING.txt    index.php README.fa.md README.zh.md
database       instructions.php README.fr.md robots.txt
Dockerfile     login.php README.id.md SECURITY.md
docs           logout.php README.ko.md security.php
```

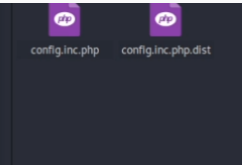


Рис. 4: Новый файл config.inc.php с содержимым config.inc.php.dist

Посмотрим содержимое файла. (рис. (fig:005?))

```
(kali@kali)-[~/dvwa/DVWA/config]
$ cat config.inc.php
<?php

# If you are having problems connecting to the MySQL database and all of the
variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a
problem due to sockets.
# Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETE
D during setup.
# Please use a database dedicated to DVWA.
#
```

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

Откроем стартовую страницу DVWA. (рис. (fig:006?))

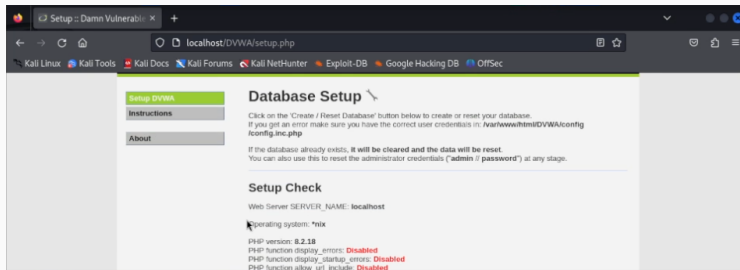
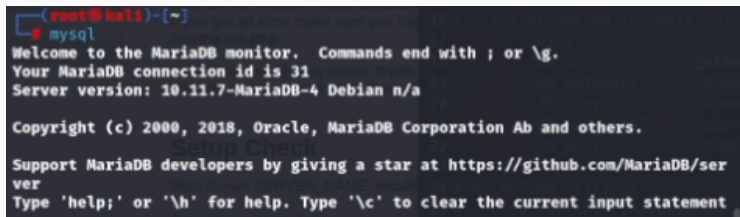


Рис. 6: Стартовую страница DVWA

Запустим mysql. (рис. (fig:007?))

A screenshot of a terminal window showing the MariaDB monitor interface. The prompt is '(root@kali)-[~]' and the user has entered 'mysql'. The output shows a welcome message, connection ID 31, server version 10.11.7-MariaDB-4 Debian n/a, copyright information, a GitHub link, and usage instructions.

```
(root@kali)-[~]  
• mysql  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 31  
Server version: 10.11.7-MariaDB-4 Debian n/a  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
Support MariaDB developers by giving a star at https://github.com/MariaDB/server  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
```

Рис. 7: MariaDB monitor

Создадим базу данных и пользователя, указав данные из файла. (рис. (fig:008?))

```
MariaDB [(none)]> create database dvwa;  
Query OK, 1 row affected (0.016 sec)  
  
MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';  
Query OK, 0 rows affected (0.097 sec)  
  
MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;  
Query OK, 0 rows affected (0.053 sec)  
  
MariaDB [(none)]> flush privileges;
```

Рис. 8: Создание базы данных и пользователя

Запустим MariaDB monitor с созданным пользователем и выберем нашу базу данных. (рис. (fig:009?))

```
(kali㉿kali)-[~]  
$ mysql -u dvwa -p  
Enter password:  
Welcome to the MariaDB monitor.  Commands end with ; or \g.  
Your MariaDB connection id is 31  
Server version: 10.11.7-MariaDB-4 Debian n/a  
  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
Support MariaDB developers by giving a star at https://github.com/MariaDB/server  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
```

Рис. 9: Запуск MariaDB monitor

Нажмем на странице DVWA create/reset database и попадем на страницу с логином. (рис. (fig:010?))

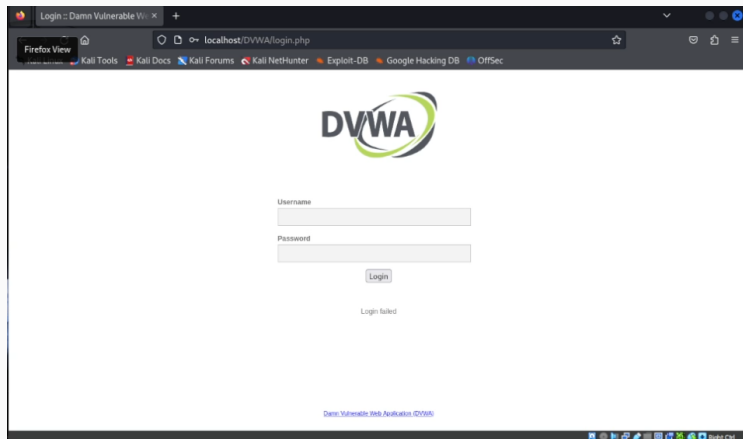


Рис. 10: Страница входа DVWA

После входа увидим рабочую область DVWA. (рис. (fig:011?))

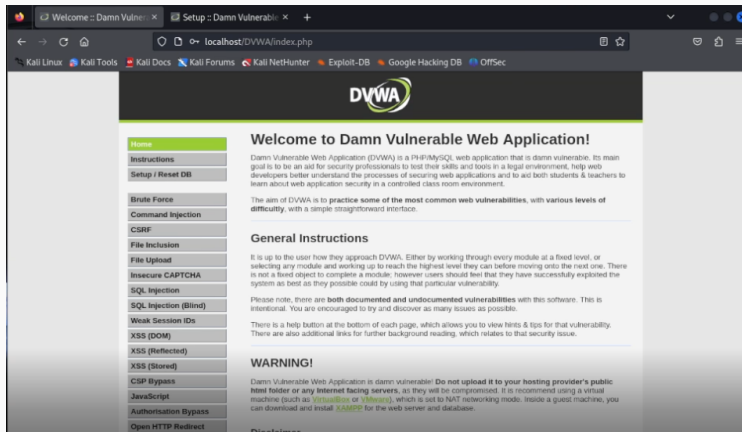


Рис. 11: Рабочая область DVWA

Установили DVWA и сделали приготовления для последующей работы.

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>