Front matter

title: "Отчет по второму этапу индивидуального проекта" subtitle: "Основы информационной безопасности" author: "Цоппа Ева, НКАбд-04-23"

Generic otions

lang: ru-RU toc-title: "Содержание"

Bibliography

bibliography: bib/cite.bib csl: pandoc/csl/gost-r-7-0-5-2008-numeric.csl

Pdf output format

toc: true # Table of contents toc-depth: 2 lof: true # List of figures lot: true # List of tables fontsize: 12pt linestretch: 1.5 papersize: a4 documentclass: scrreprt

I18n polyglossia

polyglossia-lang: name: russian options: - spelling=modern - babelshorthands=true polyglossia-otherlangs: name: english

I18n babel

babel-lang: russian babel-otherlangs: english

Fonts

mainfont: PT Serif romanfont: PT Serif sansfont: PT Sans monofont: PT Mono mainfontoptions: Ligatures=TeX romanfontoptions: Ligatures=TeX sansfontoptions: Ligatures=TeX,Scale=MatchLowercase monofontoptions: Scale=MatchLowercase,Scale=0.9

Biblatex

biblatex: true biblio-style: "gost-numeric" biblatexoptions:

- parentracker=true
- backend=biber
- hyperref=auto
- language=auto
- autolang=other*
- citestyle=gost-numeric

Pandoc-crossref LaTeX customization

figureTitle: "Рис." tableTitle: "Таблица" listingTitle: "Листинг" lofTitle: "Список иллюстраций" lotTitle: "Список таблиц" lolTitle: "Листинги"

Misc options

indent: true header-includes:

- \usepackage{indentfirst}
- \usepackage{float} # keep figures where there are in the text
- \floatplacement{figure}{H} # keep figures where there are in the text

Цель работы

Приобретение практических навыков по установке DVWA.

Задание

1. Установить DVWA на дистрибутив Kali Linux.

Теоретическое введение

DVWA - это уязвимое веб-приложение, разработанное на PHP и MYSQL.

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 четыре 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. [@guide, @parasram]

Выполнение лабораторной работы

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

```
┌──(evatsoppa㉿evatsoppa)-[~]
└─$ cd /var/www/html

┌──(evatsoppa㉿evatsoppa)-[/var/www/html]
└─$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] пароль для evatsoppa:
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 | 3.63 МиБ/с, готово.
Определение изменений: 100% (2489/2489), готово.

┌──(evatsoppa㉿evatsoppa)-[/var/www/html]
└─$
```

Проверяю, что файлы склонировались правильно, далее повышаю права доступа к этой папке до 777 (рис. 2.)

```
┌──(evatsoppa㉿evatsoppa)-[/var/www/html]
└─$ ls
DVWA  index.html  index.nginx-debian.html

┌──(evatsoppa㉿evatsoppa)-[/var/www/html]
└─$ sudo chmod -R 777 DVWA
```

Чтобы настроить DVWA, нужно перейти в каталог `/dvwa/config`, затем проверяю содержимое каталога (рис. 3)

```
┌──(evatsoppa㉿evatsoppa)-[/var/www/html]
└─$ cd DVWA/config

┌──(evatsoppa㉿evatsoppa)-[/var/www/html/DVWA/config]
└─$ ls
config.inc.php.dist
```

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 (рис. 4)

```
┌──(evatsoppa㉿evatsoppa)-[/var/www/html/DVWA/config]
└─$ sudo cp config.inc.php.dist config.inc.php

┌──(evatsoppa㉿evatsoppa)-[/var/www/html/DVWA/config]
└─$ ls
config.inc.php  config.inc.php.dist
```

Далее открываю файл в текстовом редакторе (рис. 5)

```
sudo nano config.inc.php
```

Изменяю данные об имени пользователя и пароле (рис. 6)

```
# If you are having problems connecting to the MySQL database and all of the variab>
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a proble>
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = getenv('DBMS') ?: 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED duri>
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicate>
#   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/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = getenv('RECAPTCHA_PUBLIC_KEY') ?: '';
$_DVWA[ 'recaptcha_private_key' ] = getenv('RECAPTCHA_PRIVATE_KEY') ?: '';

                [ Прочитано 56 строк (преобразовано из формата DOS) ]
^G Справка      ^O Записать     ^F Поиск        ^K Вырезать     ^T Выполнить    ^C Позиция
^X Выход        ^R ЧитФайл      ^\ Замена       ^U Вставить     ^J Выровнять    ^/ К строке
```

По умолчанию в Kali Linux установлен mysql, поэтому можно его запустить без предварительного скачивания, далее выполняю проверку, запущен ли процесс (рис. 7)

```
┌──(evatsoppa㉿evatsoppa)-[/var/www/html/DVWA/config]
└─$ sudo systemctl start mysql
[sudo] пароль для evatsoppa:

┌──(evatsoppa㉿evatsoppa)-[/var/www/html/DVWA/config]
└─$ systemctl status mysql
● mariadb.service - MariaDB 11.4.3 database server
     Loaded: loaded (/usr/lib/systemd/system/mariadb.service; dis
     Active: active (running) since Fri 2025-03-21 14:24:57 MSK;
 Invocation: ebccef7c83bf46699f976da731d01a37
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
```

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 (рис. 8)

```
┌──(evatsoppa㉿evatsoppa)-[/var/www/html/DVWA/config]
└─$ sudo mysql -u root -p
[sudo] пароль для evatsoppa:
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.4.3-MariaDB-1 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.

MariaDB [(none)]>
```

Теперь нужно пользователю предоставить привилегии для работы с этой базой данных (рис. 9)

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' identified by 'd
vwa';
Query OK, 0 rows affected (0.006 sec)

MariaDB [(none)]> exit
Bye
```

Необходимо настроить сервер apache2, перехожу в соответствующую директорию (рис. 10)

```
┌──(evatsoppa㉿evatsoppa)-[~]
└─$ cd /etc/php/8.2/apache2

┌──(evatsoppa㉿evatsoppa)-[/etc/php/8.2/apache2]
└─$
```

В файле `php.ini` нужно будет изменить один параметр, поэтому открываю файл в текстовом редакторе (рис. 11)

```
sudo nano php.ini
```

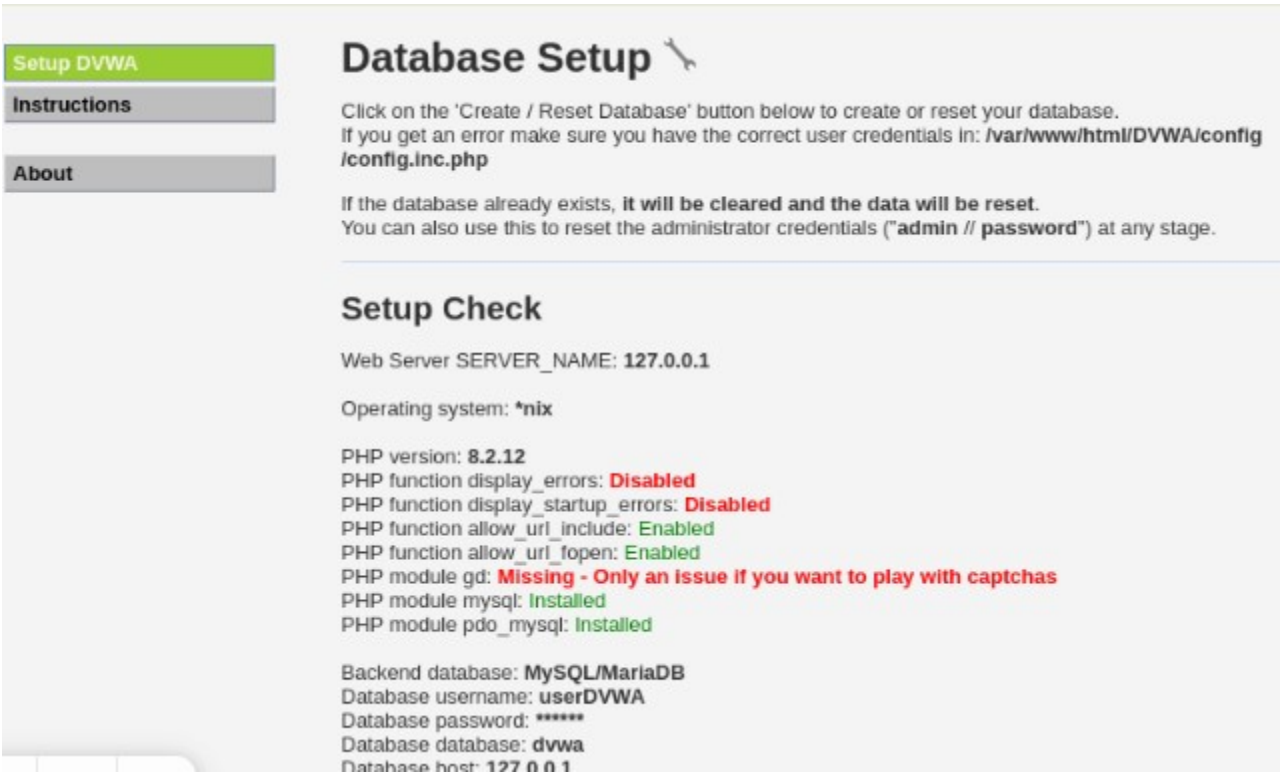
В файле параметры allow_url_fopen и allow_url_include должны быть поставлены как `On` (рис. 12)

```
max_file_uploads = 20

;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) as files.
; https://php.net/allow-url-include
allow_url_include = On
```

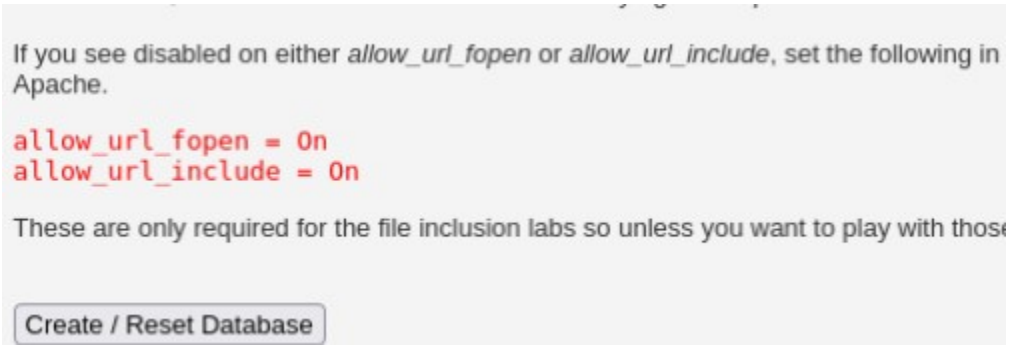
Запускаем службу веб-сервера apache и проверяем, запущена ли служба (рис. 13)

```
apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disa
     Active: active (running) since Sat 2024-03-16 00:31:47 MSK; 11s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 11911 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCES
   Main PID: 11927 (apache2)
      Tasks: 6 (limit: 4611)
     Memory: 23.8M (peak: 24.1M)
        CPU: 101ms
     CGroup: /system.slice/apache2.service
             ├─11927 /usr/sbin/apache2 -k start
             ├─11930 /usr/sbin/apache2 -k start
             ├─11931 /usr/sbin/apache2 -k start
             ├─11932 /usr/sbin/apache2 -k start
             ├─11933 /usr/sbin/apache2 -k start
```

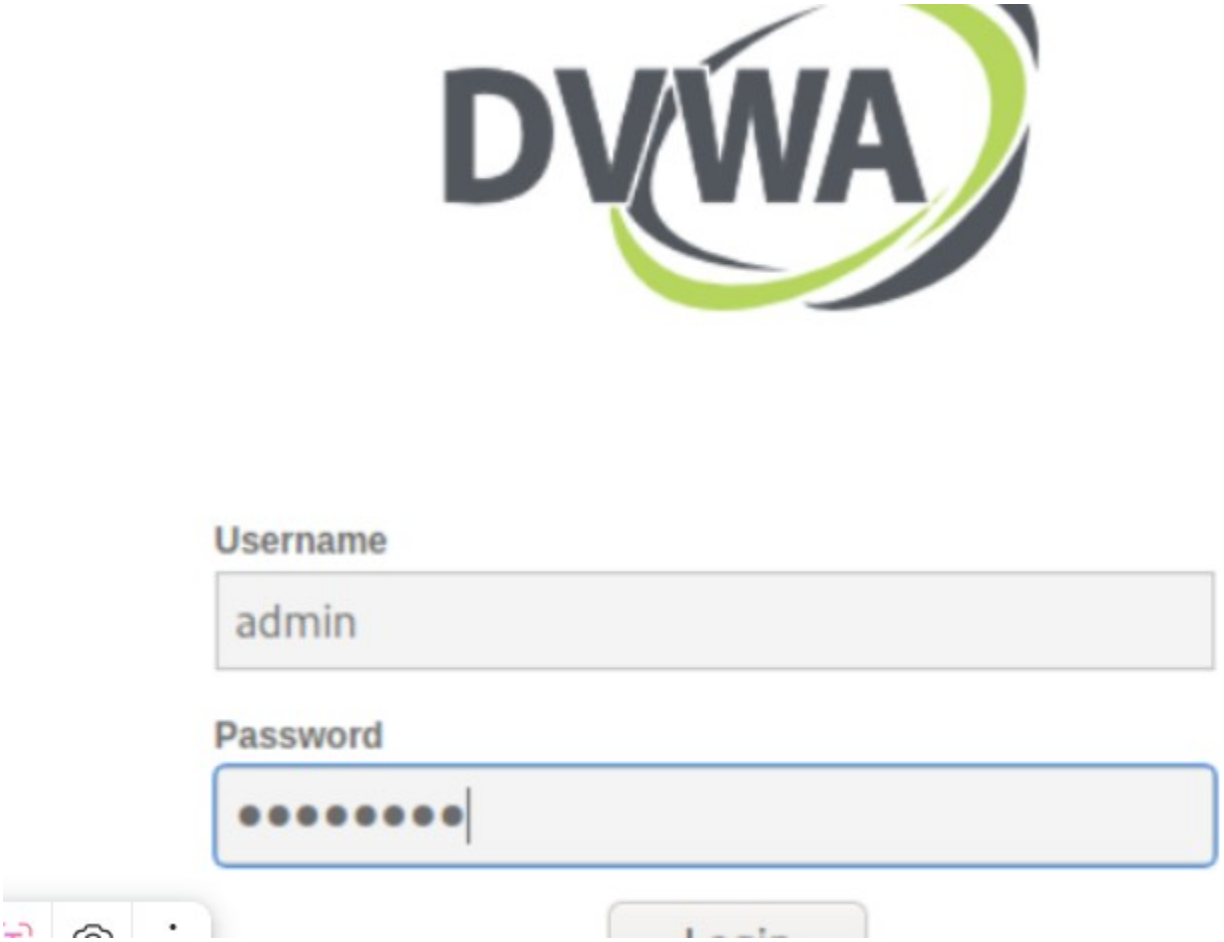
Мы настроили DVWA, Apache и базу данных, поэтому открываем браузер и запускаем веб-приложение, введя 127.0.0/DVWA (рис. 14)



Прокручиваем страницу вниз и нажимем на кнопку `create\reset database` (рис. 15)



Авторизуюсь с помощью предложенных по умолчанию данных (рис. 16)



Оказываюсь на домшней странице веб-приложения, на этом установка окончена (рис. 17)

Выводы

Приобрела практические навыки по установке уязвимого веб-приложения DVWA.

Список литературы{.unnumbered}

::: {#refs} :::