

Отчет по индивидуальному проекту

Этап 2. Установка DVWA

Лебедева Ольга Андреевна

Содержание

Цель работы	4
Теоретическое введение	5
Выполнение лабораторной работы	6
Заключение	11
Библиографическая справка	12

Список иллюстраций

1	Клонирование репозитория	6
2	Предоставление прав доступа	6
3	Создание копии файла	7
4	Открытый файл в редакторе nano	7
5	Изменение имени пользователя и пароля	7
6	Авторизация	8
7	Изменение прав	8
8	Редактирование файла	8
9	Запуск apache	9
10	Запуск веб-приложения	9
11	Авторизация	10
12	Домашняя страницы DVWA	10

Цель работы

Приобретение практических навыков по установке DVWA.

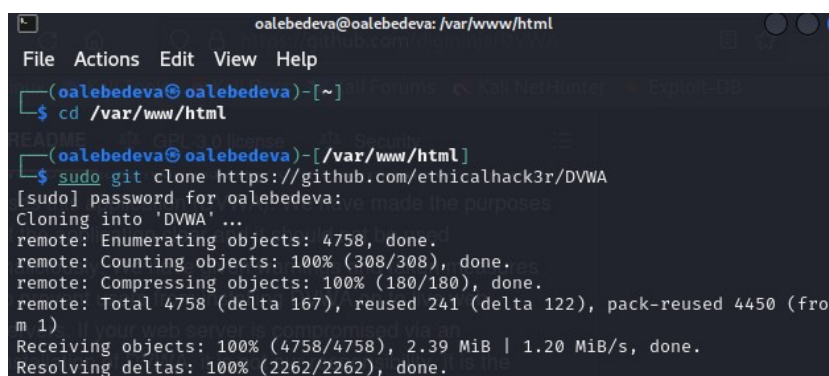
Теоретическое введение

Damn Vulnerable Web Application (DVWA) – это веб-приложение PHP / MySQL, которое чертовски уязвимо.

Его основная цель – помочь специалистам по безопасности проверить свои навыки и инструменты в правовой среде, помочь веб-разработчикам лучше понять процессы обеспечения безопасности веб-приложений и помочь студентам и преподавателям узнать о безопасности веб-приложений в контролируемой среде[1].

Выполнение лабораторной работы

Начнём выполнение лабораторной работы с клонирования репозитория по предоставленной ссылке: См. рис. 1



```
oalebedeva@oalebedeva: /var/www/html
File Actions Edit View Help
(oalebedeva@oalebedeva)-[~]
$ cd /var/www/html
(oalebedeva@oalebedeva)-[/var/www/html]
$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] password for oalebedeva:
Cloning into 'DVWA' ...
remote: Enumerating objects: 4758, done.
remote: Counting objects: 100% (308/308), done.
remote: Compressing objects: 100% (180/180), done.
remote: Total 4758 (delta 167), reused 241 (delta 122), pack-reused 4450 (from 1)
Receiving objects: 100% (4758/4758), 2.39 MiB | 1.20 MiB/s, done.
Resolving deltas: 100% (2262/2262), done.
```

Рис. 1: Клонирование репозитория

Предоставляем все права доступа к папке DVWA: См. рис. 2



```
(oalebedeva@oalebedeva)-[/var/www/html]
$ sudo chmod -R 777 DVWA
```

Рис. 2: Предоставление прав доступа

Создаём копию файла, если вдруг возникнут ошибки в ходе выполнения работы: См. рис. 3

```
(oalebedeva@oalebedeva)-[/var/www/html]
$ cd DVWA/config

(oalebedeva@oalebedeva)-[/var/www/html/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php

(oalebedeva@oalebedeva)-[/var/www/html/DVWA/config]
$ ls
config.inc.php  config.inc.php.dist
```

Рис. 3: Создание копии файла

Открываем файл в текстовом редакторе nano: См. рис. 4.

```
# If you are having problems connecting to the MySQL database and all of the
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a
# Thanks to @diginiinja 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 DELETED
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must create a database
# See README.md for more information on this.
$_DVWA = array();
$_DVWA['db_server'] = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA['db_database'] = 'dvwa';
$_DVWA['db_user'] = 'userDVWA';
$_DVWA['db_password'] = '1111';
$_DVWA['db_port'] = '3306';
```

Рис. 4: Открытый файл в редакторе nano

Меняем данные об имени пользователя и пароле: См. рис. 5.

```
(oalebedeva@oalebedeva)-[~]
$ sudo systemctl start mysql

(oalebedeva@oalebedeva)-[~]
$ systemctl status mysql
● mariadb.service - MariaDB 11.4.2 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>
   Active: active (running) since Fri 2024-09-20 14:24:05 MSK; 31s ago
   Invocation: 124cc8eda1e4e88b63470a800d6f878
   Docs: man:mariadb(8)
         https://mariadb.com/kb/en/library/systemd/
   Process: 16147 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d >
   Process: 16149 ExecStartPre=/bin/sh -c systemctl unset-environment _WSRE>
   Process: 16151 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ]>
```

Рис. 5: Изменение имени пользователя и пароля

Проходим авторизацию в базе данных от имени пользователя root. Создаём нового пользователя, при этом пользуемся учетными данными из файла config.inc.php: См. рис. 6.

```
(oalebedeva@oalebedeva)-[~]
$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 32
Server version: 11.4.2-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
.

MariaDB [(none)]> create user 'userDVWA'@'127.0.0.1' identified by "1111";
Query OK, 0 rows affected (0.009 sec)
```

Рис. 6: Авторизация

Предоставляем все привилегии для работы с базой данных: См. рис. 7.

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1' id
entified by '1111';
Query OK, 0 rows affected (0.007 sec)

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

Рис. 7: Изменение прав

В файле параметры allow_url_fopen и allow_url_include должны быть проставлены как On: См. рис. 8.

```
GNU nano 8.1      php.ini *
;;;;;;;;;;;;;;;;;;;;;;;;;
; 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
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default sett
; for this is empty.
; https://php.net/from
;from="john@doe.com"
```

Рис. 8: Редактирование файла

Запускаем службу веб-сервера apache и проверяем, была ли служба запущена: См. рис.

9.

```
(oalebedeva@oalebedeva)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2

(oalebedeva@oalebedeva)-[/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; disabled; pres>
   Active: active (running) since Fri 2024-09-20 14:38:52 MSK; 21s ago
 Invocation: 5b78338469da4dbdb0c028ed251f739c
    Docs: https://httpd.apache.org/docs/2.4/
  Process: 23670 ExecStart=/usr/sbin/apachectl start (code=exited, status=>
 Main PID: 23686 (apache2)
    Tasks: 6 (limit: 4607)
  Memory: 19.7M (peak: 19.9M)
     CPU: 48ms
   CGroup: /system.slice/apache2.service
           └─23686 /usr/sbin/apache2 -k start
             └─23689 /usr/sbin/apache2 -k start
               └─23690 /usr/sbin/apache2 -k start
                 └─23691 /usr/sbin/apache2 -k start
                   └─23692 /usr/sbin/apache2 -k start
                     └─23693 /usr/sbin/apache2 -k start
```

Рис. 9: Запуск apache

Теперь можем открыть браузер и запустить веб-приложение: См. рис. 10.

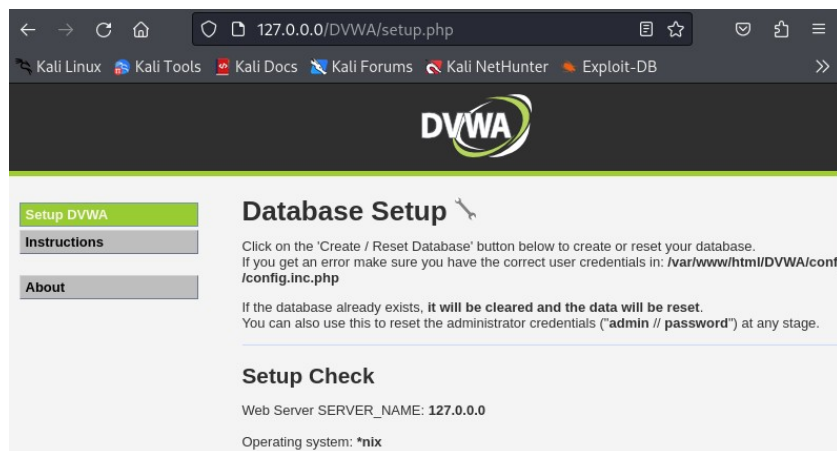


Рис. 10: Запуск веб-приложения

Проходим авторизацию при помощи предложенных по умолчанию данных: См. рис.

11.



Username

Password

[Damn Vulnerable Web Application \(DVWA\)](#)

Рис. 11: Авторизация

Оказываемся на домашней странице веб-приложения: См. рис. 12.

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual

Рис. 12: Домашняя страницы DVWA

Заключение

Получили практические навыки по установке DVWA.

Библиографическая справка

[1] DVWA: <https://itsecforu.ru/2018/02/14/5071/>