

Front matter

lang: ru-RU title: Ind Project Stage №2 author: | Anna D. Zaytseva\inst{1,3} institute: |\inst{1}RUDN University, Moscow, Russian Federation date: NEC--2024, 21 September, Moscow

Formatting

toc: false slide_level: 2 theme: metropolis header-includes:

- \metroset{progressbar=frametitle,sectionpage=progressbar,numbering=fraction}
- \makeatletter'
- \beamer@ignorenonframefalse'
- \makeatother' aspectratio: 43 section-titles: true

Цель работы

Цель работы --- Установка DVWA.

Задание

- Установить DVWA в гостевую систему к Kali Linux из репозитория: <https://github.com/digininja/DVWA>.

Теоретические выкладки

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 (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 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.

Выполнение этапа индивидуального проекта

Steps 1-6

В установленной при выполнении предыдущего этапа индивидуального проекта операционной системе настроим DVWA.

```
kali@kali: /var/www/html
File Actions Edit View Help
(kali@kali)-[~]
$ cd /var/www/html

(kali@kali)-[/var/www/html]
$ sudo git clone https://github.com/digininja/DVWA
[sudo] password for kali:
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 185), reused 266 (delta 139), pack-reused 4450 (from 1)
Receiving objects: 100% (4784/4784), 2.36 MiB | 4.70 MiB/s, done.
Resolving deltas: 100% (2296/2296), done.

(kali@kali)-[/var/www/html]
$ { #fig:001 width=70% }
```

```
(kali@kali)-[/var/www/html]
$ ls
DVWA  index.html  index.nginx-debian.html

(kali@kali)-[/var/www/html]
$ sudo chmod -R 777 DVWA { #fig:002 width=70% }
```

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

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

{ #fig:003 width=70% }
```

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

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

{ #fig:004 width=70% }
```

```
(kali@kali)-[/var/www/html/DVWA/config]
$ sudo nano config.inc.php

{ #fig:005 width=70% }
```

```
File Actions Edit View Help

GNU nano 8.1 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 @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 during setup.
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated 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' ] = 'dvwa';
$DVWA[ 'db_user' ] = 'userDVWA';
$DVWA[ 'db_password' ] = 'dvwa';
$DVWA[ 'db_port' ] = '3306';

{ #fig:006 width=70% }
```

Steps 7-9

Настроила базу данных:

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

(kali@kali)-[~]
$ sudo systemctl start mysql
[sudo] password for kali:

(kali@kali)-[~]
$ systemctl status mysql
● mariadb.service - MariaDB 11.4.2 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-09-21 07:07:40 EDT; 22s ago
     Invocation: 5cb206cf53ff459badaa75f0e6df8d64
       Docs: man:mariadb(8)
             https://mariadb.com/kb/en/library/systemd/
   Process: 45426 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
   Process: 45427 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 45430 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR=/cd /usr/bin/.. /usr/bin/galera_recovery; [ $? -eq 0 ] || exit 1
   Process: 45529 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
   Process: 45531 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
  Main PID: 45490 (mariabdd)
    Status: "Taking your SQL requests now..."
     Tasks: 15 (limit: 30405)
    Memory: 241.2M (peak: 245.4M)
       CPU: 4.354s
    CGroup: /system.slice/mariadb.service
           └─45490 /usr/sbin/mariabdd

Sep 21 07:07:37 kali mariabdd[45490]: 2024-09-21 7:07:37 0 [Note] InnoDB: Loading buffer pool(s) from /var/lib/mysql/ib_buffer_pool
Sep 21 07:07:37 kali mariabdd[45490]: 2024-09-21 7:07:37 0 [Note] Plugin 'FEEDBACK' is disabled.
Sep 21 07:07:37 kali mariabdd[45490]: 2024-09-21 7:07:37 0 [Note] Plugin 'wsrep-provider' is disabled.
Sep 21 07:07:37 kali mariabdd[45490]: 2024-09-21 7:07:37 0 [Note] InnoDB: Buffer pool(s) load completed at 240921 7:07:37
Sep 21 07:07:39 kali mariabdd[45490]: 2024-09-21 7:07:39 0 [Note] Server socket created on IP: '127.0.0.1'.
Sep 21 07:07:39 kali mariabdd[45490]: 2024-09-21 7:07:39 0 [Note] mariabdd: Event Scheduler: Loaded 0 events
Sep 21 07:07:39 kali mariabdd[45490]: 2024-09-21 7:07:39 0 [Note] /usr/sbin/mariabdd: ready for connections.
Sep 21 07:07:39 kali mariabdd[45490]: Version: '11.4.2-MariaDB-4' socket: '/run/mysqld/mysqld.sock' port: 3306 Debian n/a
Sep 21 07:07:40 kali systemd[1]: Started mariadb.service - MariaDB 11.4.2 database server.
Sep 21 07:07:40 kali /etc/mysql/debian-start[45546]: Checking for insecure root accounts.

lines 1-29/29 (END)

{ #fig:007 width=70% }
```

Для выхода из режима проверки в консоли нажимаю q.

```
(kali@kali)~$ sudo mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
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)]> userDVWA
→ dvwa
→ ^C
MariaDB [(none)]> create user 'userDVWA '@'127.0.0.1' identified by "dvwa";
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that co
MariaDB [(none)]> create user 'userDVWA '@'127.0.0.1' identified by "dvwa"
→
→ \c
MariaDB [(none)]> create user 'userDVWA '@'127.0.0.1' identified by "dvwa";
Query OK, 0 rows affected (0.036 sec)
```

{ #fig:008 width=70% }

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA '@'127.0.0.1' identified by 'dvwa';
Query OK, 0 rows affected (0.003 sec)

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

{ #fig:009 width=70% }

Steps 10-12

Настроила сервер apache2:

```
(kali@kali)-[/var/www/html/DVWA/config]
$ cd /etc/php/8.2/apache2

(kali@kali)-[/etc/php/8.2/apache2]
$ sudo nano php.ini
[sudo] password for kali:
```

{ #fig:010 width=70% }

```
File Actions Edit View Help
GNU nano 8.1 php.ini *
;cgi.check_shebang_line=1

; Уровень безопасности, они меняют уровень безопасности каждого веб приложения в DVWA:
; - этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода
; File Uploads ; - это расширение среднего уровня сложности, со смесью более сложных или альтернативных плохих практик в попытке об
; - этот уровень безопасности предназначен главным образом для того, чтобы дать пользователю пример плохих практик и
; Whether to allow HTTP file uploads. Он совершенно уязвим и совсем не имеет защиты. Его предназначение быть примером среди уязв
; https://php.net/file-uploads
file_uploads = On

; Temporary directory for HTTP uploaded files (will use system default if not
; specified).
; https://php.net/upload-tmp-dir
upload_tmp_dir =

; Maximum allowed size for uploaded files.
; https://php.net/upload-max-filesize
upload_max_filesize = 2M

; Maximum number of files that can be uploaded via a single request
max_file_uploads = 20

; В DVWA, нужно перейти в каталог /var/www/html/. Проверим содержимое каталога (Рис. [ #fig:001 ]):
; Fopen wrappers ;
; https://php.net/allow-url-fopen
allow_url_fopen = On

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

{ #fig:011 width=70% }

```
(kali㉿kali)-[/etc/php/8.2/apache2]
$ sudo systemctl start apache2

(kali㉿kali)-[/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; preset: disabled)
   Active: active (running) since Sat 2024-09-21 07:45:21 EDT; 53s ago
 Invocation: 3c524baca5bd4d0da90225c3dab00893
    Docs: https://httpd.apache.org/docs/2.4/
   Process: 64417 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 64441 (apache2)
    Tasks: 6 (limit: 4606)
  Memory: 19.3M (peak: 19.6M)
     CPU: 163ms
    CGroup: /system.slice/apache2.service
            └─64441 /usr/sbin/apache2 -k start
            └─64444 /usr/sbin/apache2 -k start
            └─64445 /usr/sbin/apache2 -k start
            └─64446 /usr/sbin/apache2 -k start
            └─64447 /usr/sbin/apache2 -k start
            └─64448 /usr/sbin/apache2 -k start

Sep 21 07:45:21 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Sep 21 07:45:21 kali apachectl[64432]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. See
Sep 21 07:45:21 kali systemd[1]: Started apache2.service - The Apache HTTP Server.

(kali㉿kali)-[/etc/php/8.2/apache2]
$
```

Steps 13-14

DVWA, Apache и база данных настроены, поэтому теперь остаётся открыть браузер и запустить веб-приложение, введя в адресной строке 127.0.0.1/DVWA (Рис. [-@fig:013]):

127.0.0.1/DVWA/setup.php

Kali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

Setup DVWA

Instructions

About

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: /var/www/html/DVWA/config/config.inc.php

If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.

Setup Check

Web Server SERVER_NAME: 127.0.0.1

Operating system: *nix

PHP version: 8.2.21
PHP function display_errors: Disabled
PHP function display_startup_errors: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP module gd: Missing - Only an issue if you want to play with captchas
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: MySQL/MariaDB
Database username: userDVWA
Database password: *****
Database database: dvwa
Database host: 127.0.0.1
Database port: 3306

reCAPTCHA key: Missing

Writable folder /var/www/html/DVWA/hackable/uploads/: Yes
Writable folder /var/www/html/DVWA/config: Yes

Status in red, indicate there will be an issue when trying to complete some modules.

If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.

allow_url_fopen = On
allow_url_include = On

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

{ #fig:014 width=70% }

Но необходимо было авторизоваться с помощью предложенных по умолчанию данных ("admin // password") и оказаться на домашней странице веб-приложения. На этом установка окончена.

Выводы

Приобрела практические навыки по установке уязвимого веб-приложения DVWA.

Библиография

1. Методические материалы курса

{.standout}

Спасибо за внимание!