Основы информационной безопасности

Индивидуальный проект № 2. Установка DVWA

Смирнов-Мальцев Е. Д.

21 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Смирнов-Мальцев Егор Дмитриевич
- студент группы НКНбд-01-21
- Российский университет дружбы народов

Цель работы

Цель работы

Установить DVWA.

Теоретическое введение

Уязвимости веб приложений, которые содержит DVWA

1. Брутфорс: Брутфорс HTTP формы страницы входа - используется для тестирования инструментов по атаке на пароль методом грубой силы и показывает небезопасность слабых паролей.
2. Исполнение (внедрение) команд: Выполнение команд уровня операционной системы.
3. Межсайтовая подделка запроса (CSRF): Позволяет «атакующему» изменить пароль администратора приложений.
4. Внедрение (инклуд) файлов: Позволяет «атакующему» присоединить удалённые/локальные файлы в веб приложение.
5. SQL внедрение: Позволяет «атакующему» внедрить SQL выражения в HTTP из поля ввода, DVWA включает слепое и основанное на ошибке SQL внедрение.
6. Небезопасная выгрузка файлов: Позволяет «атакующему» выгрузить вредоносные файлы на веб сервер.
7. Межсайтовый скриптинг (XSS): «Атакующий» может внедрить свои скрипты в веб приложение/базу данных. DVWA включает отражённую и хранимую XSS.

Уровни безопасности DVWA

1. Невозможный — этот уровень должен быть безопасным от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом.
2. 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.
3. 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.
4. 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

Клонирование репозитория

```
┌──(edsmirnovmaljce㉿root)-[/var/www/html]
└─$ sudo git clone https://github.com/digininja/DVWA.git
[sudo] password for edsmirnovmaljce:
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 | 4.67 MiB/s, done.
Resolving deltas: 100% (2296/2296), done.

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

┌──(edsmirnovmaljce㉿root)-[/var/www/html]
└─$ sudo service apache2 start
```

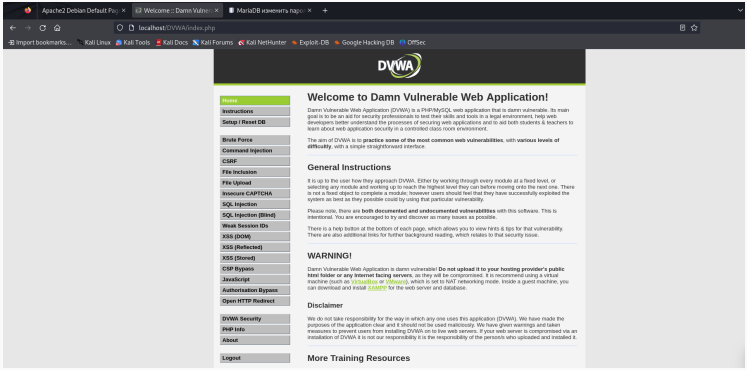
Копирование конфигурационного файла

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

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

Создание пользователя

```
┌──(edsmirnovmaljce㉿root)-[~]
└─$ sudo su -
[sudo] password for edsmirnovmaljce:
┌──(root㉿root)-[~]
└─# mysql
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 39
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 database dvwa
    -> ;
Query OK, 1 row affected (0.081 sec)

MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssword';
Query OK, 0 rows affected (0.386 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.175 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)
```

Стартовая страница DVWA



Выводы

Выводы

DVWA установлен.