

Основы информационной безопасности

Индивидуальный проект № 2. Установка DVWA

Смирнов-Мальцев Е. Д.

21 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

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

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 (инклюд) 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.

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
```

```
(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

The screenshot shows a web browser window with the address bar displaying 'localhost/DVWA/index.php'. The browser's bookmark bar includes links to 'Kali Linux', 'Kali Tools', 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. The DVWA homepage features a dark header with the DVWA logo. On the left, a sidebar menu lists various modules: Home (highlighted), 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, JavaScript, Authorization Bypass, Open HTTP Redirect, DVWA Security, PHP Info, About, and Logout. The main content area has a green header with the text 'Welcome to Damn Vulnerable Web Application!'. Below this, it states: '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.' It then explains the aim of DVWA: 'The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.' A 'General Instructions' section follows, stating: '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 possibly could by using that particular vulnerability.' It also includes a note about documented and undocumented vulnerabilities and a help button. A 'WARNING!' section states: '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 recommended using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.' A 'Disclaimer' section states: 'We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA, it is not our responsibility, it is the responsibility of the persons who uploaded and installed it.' Finally, a 'More Training Resources' section is listed at the bottom.

Выводы

DVWA установлен.