

Индивидуальный проект. Этап 2

Установка DVWA на Kali Linux

Хамдамова А. А.

15 марта 2024

Российский университет дружбы народов, Москва, Россия

Информация

- Хамдамова Айжана Абдукаримовна
- студент Факультета Физико-математических и естественных наук
- Российский университет дружбы народов
- 1032225989@pfur.ru
- https://github.com/AizhanaKhamdamova/study_2023-2024_infosec

Вводная часть

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 три уровня безопасности, они меняют уровень безопасности каждого веб приложения в DVWA: Невозможный — этот уровень должен быть безопасным от

- Установить DVWA в гостевую систему к Kali Linux.

- Установили DVWA в гостевую систему к Kali Linux.
- Настроили

Настраиваем права доступа

```
—(akhamdamova@akhamdamova)-[/var/www/html]
—$ cd DVWA

—(akhamdamova@akhamdamova)-[/var/www/html/DVWA]
—$ ls
CHANGELOG.md  README.id.md  compose.yml  hackable  robots.txt
COPYING.txt   README.md     config       index.php  security.
Dockerfile    README.pt.md  database     instructions.php  security.
README.ar.md  README.tr.md  docs        login.php  setup.php
README.es.md  README.zh.md  dvwa        logout.php tests
README.fa.md  SECURITY.md   external    php.ini   vulnerabi
README.fr.md  about.php    favicon.ico  phpinfo.php

—(akhamdamova@akhamdamova)-[/var/www/html/DVWA]
—$ cd config

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


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

—(akhamdamova@akhamdamova)-[/var/www/html/DVWA/config]
—$ sudo mousepad config.inc.php
```


Welcome :: Damn Vulnerable Web Application

127.0.0.1/DVWA/index.php

Kali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec



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

JavaScript

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

Logout

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 vulnerability** 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 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.

Disclaimer

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 person/s who uploaded and installed it.

More Training Resources