Индивидуальный проект 2

Информационная безопасность

Волчок Кристина Александровна НПМбд-02-21

19 сентября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Волчок Кристина Александровна, студентка кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов
- [1032215007@rudn.ru]

Вводная часть

Вводная часть

Damn Vulnerable Web Application (DVWA) — это специально разработанное уязвимое веб-приложение, предназначенное для обучения и практики в области веб-безопасности. Его установка на систему Kali Linux позволяет специалистам по безопасности и разработчикам тестировать методы обнаружения и устранения уязвимостей в веб-приложениях.

Актуальность

С ростом киберугроз и развитием технологий, навыки обнаружения уязвимостей и защиты веб-приложений становятся важной частью работы специалистов по информационной безопасности. DVWA предоставляет удобную и безопасную платформу для отработки методов защиты, повышения квалификации и тестирования инструментов на уязвимости, такие как SQL-инъекции, XSS, CSRF, и другие.

Объект и предмет исследования

- **Объект исследования:** Уязвимые веб-приложения.
- **Предмет исследования:** Методы обнаружения и эксплуатации уязвимостей, которые могут быть использованы в веб-приложениях для улучшения защиты.

Цели и задачи

-Установить DVWA на гостевую систему Kali Linux для тестирования и практики на базе преднамеренных уязвимостей.

Для выполнения задания были использованы следующие материалы и инструменты: - **Операционная система:** Kali Linux. - **Программное обеспечение:** Apache, MariaDB, PHP. - **Репозиторий:** DVWA GitHub. - **Методика установки и настройки:** 1. Обновление системы с помощью команды: `(sudo apt update && sudo apt upgrade -y)` 2. Установка необходимых пакетов: `(sudo apt install apache2 mariadb-server php php-mysqli php-gd libapache2-mod-php git -y)` 3. Настройка баз данных: `(sudo mysql_secure_installation)` `(sudo mysql -u root -p)` В MySQL были выполнены следующие команды для создания базы данных и пользователя: `sql CREATE DATABASE dvwa; CREATE USER 'dvwauser'@'localhost' IDENTIFIED BY 'password'; GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwauser'@'localhost'; FLUSH PRIVILEGES; EXIT;` 4. Клонирование репозитория DVWA: `(cd /var/www/html/)` `(sudo git clone https://github.com/digininja/DVWA.git)` 5. Настройка прав доступа: `(sudo chown -R www-data:www-data /var/www/html/DVWA/)` `(sudo chmod -R 755`

Рекомендации

Рекомендации

Для успешной работы с DVWA и дальнейшего изучения веб-безопасности рекомендуется: 1. **Работа с уровнями безопасности:** Начать с низкого уровня безопасности, чтобы понять базовые методы эксплуатации уязвимостей, затем постепенно увеличивать уровень безопасности и анализировать, как изменения влияют на работу приложения. 2. **Изучение документации:** Ознакомьтесь с дополнительной документацией по DVWA и основам веб-безопасности для более глубокого понимания каждой уязвимости. 3. **Использование изолированной среды:** Поскольку DVWA содержит преднамеренные уязвимости, рекомендуется использовать виртуальные машины или песочницы для работы с приложением.

Выводы

Установка и использование DVWA в гостевой системе Kali Linux предоставляет мощный инструмент для изучения и практики методов безопасности веб-приложений. Это позволяет на практике освоить такие виды уязвимостей, как SQL-инъекции, XSS, CSRF и брутфорс. Приложение позволяет изучать поведение системы на разных уровнях безопасности, что способствует лучшему пониманию механизмов защиты веб-приложений. Таким образом, DVWA является важным инструментом для тех, кто стремится углубить свои знания в области кибербезопасности.