Лабораторная работа №7

БАЗОВЫЕ МЕТОДЫ ИССЛЕДОВАНИЯ УЯЗВИМОСТИ БАЗ ДАННЫХ

1. Цель и задачи работы

Ознакомится с основными методами поиска уязвимостей присутствующих в базах данных WEB приложений, при помощи специализированных программных средств.

2. Теоретические положения

Как правило, базы данных современных WEB приложений, подвержены следующим видам уязвимостей.

1. Отсутствие физической защиты сервера СУБД, открытые порты, работа без защиты.
2. Некорректная настройка авторизации. Использование пользователей, или паролей по умолчанию, наличие возможности неавторизированного доступа, в том числе режима входа с привилегиями ОС и т.д.
3. Некорректная настройка мандатного доступа. Ошибки в настройке уровня доступа к данным СУБД.
4. Отсутствие валидации поступающих данных и контроля за исполнением команд, как частный случай ошибки разработки и работы с СУБД.

Ошибки первых 3 видов были ранее рассмотрены как в рамках данного курса, так и в рамках других курсов, преподаваемым в рамках модуля, поэтому исключаются из рассмотрения.

Наибольшего внимания заслуживают ошибки разработки и валидации входных и выходных данных. Данный ошибки в недавнем времени были крайне распространены и приводили к явлениям, получившим общее название SQL Injection(SQL инъекции).

Существует множество видов SQL инъекций, но вне зависимости от их вида, методы реализации заключаются в следующем.

1. Анализ запросов, поступающих на WEB приложения косвенно затрагивающих работу с СУБД.
2. Выявление передаваемых параметров и анализ получаемых значений.
3. Выполнение данных запросов при помощи сторонних средств.
4. Изменения параметров таким образом, чтобы получить иной результат выполнения SQL команд.
5. Оценка полученных результатов.

В качестве изменения параметров возможно использовать их модификации направленные на.

1. Прерывание выполнения SQL запроса.
2. Изменение текста запроса.
3. Изменение условий выполнения запроса.
4. Корректировку результата выдачи SQL запроса.

5. Выдача данных таблиц, изначально не предусмотренную разработчиком.
6. Выполнение хранимых процедур, в том числе, процедур, осуществляющих доступ к файловой системе ОС.
7. Другие действия, анализирующие возможные атаки, такие как получение списка пользователей и их паролей, удаление таблиц БД и данных из них, модификация структуры СУБД, аппаратное сжатие БД с потерей некоторых данных и др.

Не смотря на относительную массовость подобных атак и наличие типовых способов борьбы с SQL инъекциями, например, в виде внедрения прослойки между выполнением кода ПО и командами СУБД, получившей название ORM, существует класс приложений, в которых данная проблема актуальна до сих пор. Например, приложения, написанные на основе относительно старых технологий, приложения, связанные с обеспечением работы программно-аппаратных средств на низком уровне(близкому к аппаратному), и др.

В качестве базового средства анализа SQL инъекций https://habr.com/ru/articles/725134/ https://xakep.ru/2011/12/06/57950/ используется SQL Map https://hackware.ru/?p=1928 https://kmb.cybber.ru/net/sqlmap/main.html

Так как деятельность по проверке WEB и других приложений на наличие возможность осуществления SQL инъекций не является без согласия правообладателя ресурса является незаконной, то работу по анализу наличия выполнения SQL инъекций будет проводится на основе следующих оффлайн площадок, разворачиваемых на виртуальных машинах.

1. DVWA. https://hackware.ru/?p=1956 https://hackware.ru/?p=2069
2. BwAPP, или виртуальной машине, уже содержащей предустановленную версию данного ПО, получившую название be-box https://kali.tools/?p=2330.

При этом в рамках данной работы предполагается выполнение работы на всех уровнях платформы DVWA, таких как low, medium, height. Более подробно инструкцию по работе с данной платформой и выполнению атак с её помощью, можно посмотреть на следующих ресурсах.

1) https://www.youtube.com/watch?v=i1yle_9cJXw
2) https://dzen.ru/media/timcore/42-uiazvimost-dvwa-sqlinjection-blind-uroven-medium--timcore-5ff5bcdffe4e686f6a7d0320
3) https://timcore.ru/2021/04/12/1-ujazvimost-dvwa-sql-injection-uroven-low/
4) https://www.youtube.com/watch?v=IR1JsaSQLMc
5) https://www.youtube.com/watch?v=U1bgjOQZgwQ

3. Оборудование

Персональный компьютер с количеством процессорных ядер не менее 2, работающих на частоте не менее 2 GHz, работающий под управлением операционной системы Kali Linux, Ubuntu Linux с пакетом дополнений Forensic Tools, Windows 7, или более новая. Видеокарта с поддержкой технологий

CUDA или Open CL. Не менее 4 GB оперативной памяти. Не менее 20GB свободного места на HDD.

4. Задание на работу

4.1 Установите DVWA и проведите его настройку.

4.2 Установить Metasploitable 2 в комплекте с платформой DVWA.

4.3 Установить уровень Low на платформе DVWA и выполнить следующие действий, получить список таблиц БД, получить список полей таблицы пользователей СУБД. Получить имена пользователей и хеши паролей пользователей. Расшифровать пароль администратора при помощи JhonTheRipper, или HashCat и представить скриншот каждого этапа.

4.4 Установить уровень Medium на платформе DVWA и выполнить следующие действия, получение списка пользователей и хешей их паролей и представить скриншот выполнения этапа.

4.5 Установить уровень Height на платформе DVWA и выполнить следующие действия, получение списка пользователей и хешей их паролей и представить скриншот выполнения этапа.

4.6 Установить платформу bWApp https://habr.com/ru/articles/250551/ и выполнить атаку на раздел, содержащий SQL Injection на основе следующего руководства https://hackware.ru/?p=1956 и передоставть запрос, приведший к получению администратора и его хеша пароля и скриншот окна, содержащий подтверждение его получения.

4.7 Сделать выводы о проделанной работе.

6. Оформление отчета

Отчет оформляется в тетради или листах формата А4 и должен содержать:

- название курса, название и номер лабораторной работы;
- цель работы и задание на исследование;
- базовая информация об исследуемых SQL инъекциях;
- скриншоты окон выполнения запросов и прохождения заданий машин;
- краткие выводы о проделанной работе.

7. Контрольные вопросы

7.1 Понятие SQL инъекций?

7.2 Основные виды SQL инъекций?

7.3 Основные средства, используемые для выявлении SQL инъекций?

7.4 Назначение и основные возможности среды SQL Map?

7.5 Основные команды среды SQL Map?

7.6 Различие между различными уровням осуществления инъекций на платформе DVWA?

7.7 Особенности платформы bwAPP в области реализации SQL инъекций?

7.8 Основные различия между платформами DVWA и bwAPP в области реализации SQL инъекций?

7.9 Правовые ограничения применения методов анализа на наличие SQL инъекций?

7.10 Какая юридическая ответственность наступит, или может наступить в случае анализа уязвимостей на сайте https://tulsu.ru/? **!!!Внимание!!!** Сканировать любые сайты, кроме настроенных в рамках данной работы, категорически запрещается!