Лабораторная работа №5

БАЗОВЫЕ МЕТОДЫ ИССЛЕДОВАНИЯ УРОНЯ ЗАЩИЩЁННОСТИ WEB ПРИЛОЖЕНИЙ

1. Цель и задачи работы

Ознакомится с основными методами поиска уязвимостей в WEB приложениях, основанных на использовании инструментов анализа и модификации сетевого трафика.

2. Теоретические положения

Не смотря на массовый переход ИТ направления на приоритетное использование мобильных приложений, особенно в сегменте B2C бизнеса, количество WEB приложений в мире всё равно увеличивается. Дополнительными предпосылками для развития WEB приложений, является использование совмещённых архитектур, заключающихся в том, что для обслуживания мобильного приложения создаётся WEB сервер. Кроме этого широкое распространение получает микросерверная архитектура, которая так же расширяет спектр применения WEB приложений. WEB приложения не стрит воспринимать, исключительно как WEB сайты, поэтом средства анализа WEB сайтов будут рассмотрены в рамках дополнительного задания, но приоритет при выполнении данной работе будет отдан средствам анализа трафика.

Как правило современные WEB приложения строятся по следующим схемам. Построение типа монолит, ввиду простоты исключим из рассмотрения.

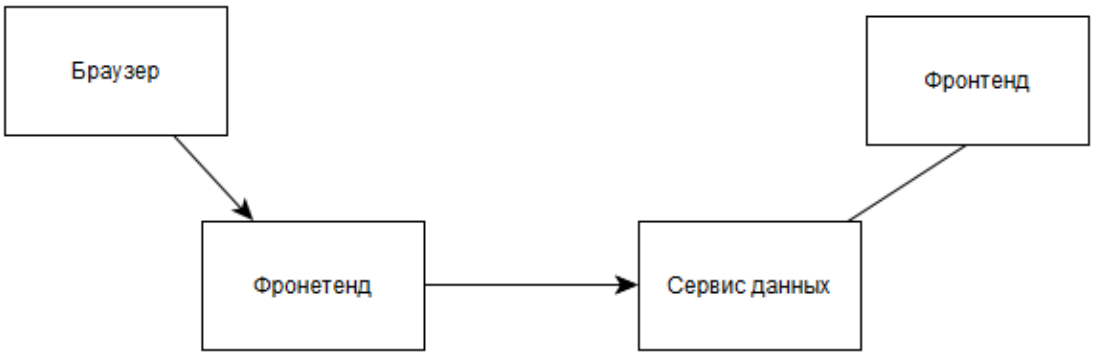

Рисунок 1. Типовая структура построения WEB приложения.

Браузер в данной схеме используется в качестве средства, обеспечивающего взаимодействие пользователя и приложения. При этом браузер служит для отображения графического интерфейса пользователя и получения информации, о действиях пользователя, которые он совершил во время сеанса работы с приложением. В качестве браузера, в современной контексте может выступать как браузер ОС, так и браузер встроенный в

приложении, или само приложение, например, мобильное, написанное с использованием браузера.

Фронтенд – часть приложения, основной задачей которого, является получением информации от браузера о действиях пользователей от браузера и формирование на его основе запросов к серверной части приложения. При этом наиболее часто используемым протоколом в WEB приложениях является HTTP и HTTPS. Фронтенд часть приложения может функционировать как в составе монолитного приложения, так и размещена на отдельном сервере, от бакенда, так и на том же сервере, на котором расположен бакенд, что крайне не рекомендуется, так как нагрузка на сервер бакенда в данном случае сильно увеличится. Наиболее часто Фронтенд часть приложения пишется на семействе языков программирования, основанных на языке JavaScript. На выходе фронтенд приложения уже имеет смысл анализ трафика.

Сервис данных – расширение Бакенда, которое занимается преобразованием запросов, поступающих с фронтенда в вид удобный для последующей обработки бакенд части приложения. Данный модуль необходим, так как запросы с фронтенда отправляются по стандартным каналам связи и по спецификации передачи данных должны быть на низких уровнях модели OSI в виде набора байт, которые содержат заголовки протоколов и названия и значений параметров. Поэтому для извлечения данных из запросов необходим дополнительный модуль. Его может не быть в явном виде, так как он может быть встроен в фреймворк на основе которого написан бакенд. Например, фабрика контроллеров в ASP.NET MVC, или Django, или YII, или его аналоги на различных языках программирования. Роль данного сервиса, может выполнять сервис обработки данных страницы, или входной микросервис в микросервисной архитектуре.

Бакенд – серверная часть приложения, на которой как правило располагается вся бизнес-логика приложения, включая алгоритмы взаимодействия с базами данных и интеграции со сторонними сервисами. При этом корректность работы данной части приложения крайне зависит от корректности поступивших входных данных и корректности задания его конфигурационных параметров. При этом бакенд может представлять из себя как один сервис, так и несколько связанных между собой сервисов, на которые может быть установлен балансировщик нагрузок, отвечающий за равномерное разделение нагрузки между различными сервисами.

Для просмотра и анализ трафика необходимо реализовать схему, аналогичную схеме, используемой при атаке человек посередине, которая в упрощённом виде приведена на рисунке 2.

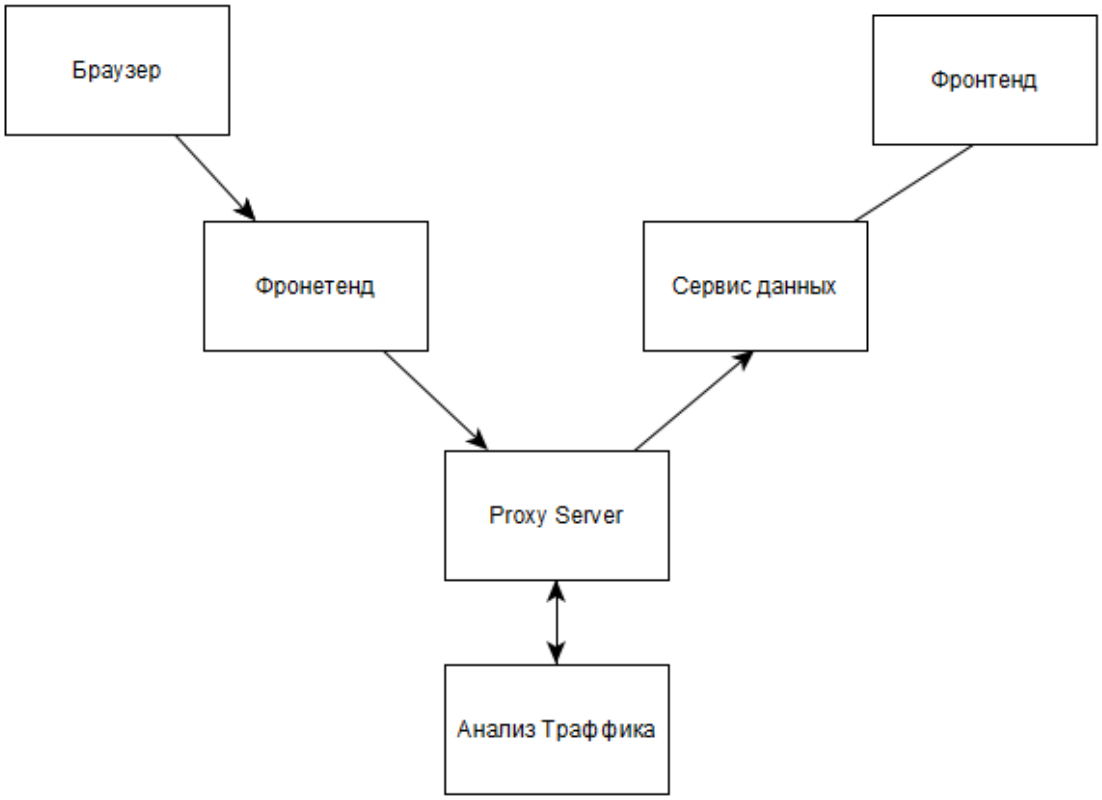

Рисунок 2. Упрощённая схема анализа трафика.

Пара Proxy Server и анализатор трафика, должна быть установлена между любыми элементами схемы построения WEB приложения, единственным условием её внедрения является передача запросов через сеть и возможность установки данной пары.

В качестве Proxy Server, возможно использование различных решений. При этом в рамках данной работы в качестве прокси сервера будет использована бесплатная версия Burp Suite, в качестве плагина, необходимого для обеспечения взаимодействия браузера и прокси сервера будет использован Foxy Proxy. При этом в случае наличия возможности, или возникновении проблем в работе приложения Burp Suite в качестве альтернативы возможно использование комплекса Owasp ZAP, являющегося бесплатной альтернативой Burp Suite.

Proxy Server – в данной схеме используется для перехвата трафика с целью получения информации о входящих запросах к бакенду приложения и запросах, поступающих от него.

При этом в качестве полей запроса, представляющих интерес, можно выделить следующие.

1. Метод отправки запроса GET, POST, PUT, SET.
2. Тело запроса.
3. Информация о заголовках запроса.
4. Информация о переданных параметрах пользователя и их значениях.
5. Информация о Coockie файлах пользователей переданных по сети.

6. Информация о токенах защиты приложения, переданных по сети.
7. Информация об адресах отправки запросов.
8. Идентификаторы и типы пользовательских элементов, активация которых привела к выполнению запроса.

Рассмотрим модули, входящие в комплекс BurpSuite более подробно.

1. Scanner – сканер уязвимостей, встроенный в комплекс.
2. Spider (паук или краулер) – средство, позволяющее собирать информацию об архитектуре WEB приложения.
3. Proxy – прокси сервер, входящий в комплекс.
4. Intruder – модуль позволяющий проводить различные атаки, например, подбор паролей.
5. Repeater – модуль, необходимы для повторной отправки и модификации запросов и анализа ответов приложения.
6. Compare – модуль, необходимы для выявления различий в данных.
7. Sequencer – утилитка для выявления алгоритмов генерации очередей, используемых в приложении.
8. Extenter – модуль необходимых для установки дополнительных расширений в среду BurpSuite, которые могут быть получены из магазина расширений, или написаны самостоятельно.

Так как деятельность, направленная на исследование уязвимостей в WEB приложениях является лицензируемой, то в целях обучения работы с предложенными методами анализа будет использовать комплект уязвимых приложений, получивший название metasploitable-2, или площадка DVWA.

Порядок выполнения работы с комплексом Burp Suite.

1. Установить ОС Kali Linux, или запустить соответствующую виртуальную машину.
2. Запустить Burp Suite, который уже установлен в данной версии ОС.
3. Использовать настройки по умолчанию, так как бесплатная версия Burp Suite предполагает работу только со временными проектами.
4. Установить плагин Foxy Proxy в браузере Firefox, входящего в состав ОС Kali Linux, используя поиск в Addons браузера.
5. Нажать на кнопку Options плагина Foxy Proxy.
6. Перейти во вкладку Proxy и добавить локальный прокси, с параметрами localhost или 127.0.0.1 в качестве порта, задать порт Burp Suite по умолчанию 8080.
7. Нажать кнопку Save.
8. Зайти на Web интерфейс Burp Suite, по умолчанию расположенный по адресу 127.0.0.1:8080 и выпустить сертификат Burp Suite, нажав на кнопку CA Certificate.
9. Скачать сгенерированный сертификат и добавить его в браузер. Для этого перейдите в раздел Privacy and Security / Certificates / Import и добавить скаченный сертификат.
10. Включить Proxy Server в Foxy Proxy.
11. В среде Burp Suite включить перехват запросов. Для этого необходимо перейти на вкладку Proxy и выбрать пункт Intecept is on.

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 и NMap, 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 Burp Suite и проведите его настройку.

4.2 Установить Metasploitable 2 в комплекте с платформой DVWA.

4.3 Изучить документацию по основам работы с Metasplitable 2. https://docs.rapid7.com/metasploit/metasploitable-2/

4.4 Изучить методику исправления конфигурации приложения Mutillidae для работы с приложением Burp Suite https://cyberarms.wordpress.com/2015/05/01/mutillidae-database-errors-in-metasploitable-2/

4.5 Установите программный комплекс Metasploitable

4.6 Выполните привязку двух машин (Kali Linux и Metasploitable). Чтобы узнать адрес машины Metasploitable, используйте команду ifconfig. После проверьте работоспособность схемы с помощью команды:
ping IP-адрес Metasploitable (по умолчанию ping 10.7.7.7).

4.7 В результаты выполнения работы добавьте скриншот результатов выполнения команды ping.

4.8 2Зайдите через браузер Kali Linux на Metasploitable.

4.9 Введите в строку запросов IP-адрес машины, на которую установлен Metasploitable.

4.10 Выбрать тренировочную площадку DVWA.

4.11 В качестве логина и пароля для входа используйте admin/password.

4.12 Перейдите в настройки и выберите уровень безопасности low.

4.13 Выполнить задания во вкладках:

4.13.1 SQL Injection,

4.13.2 XSS Reflected,

4.13.3 XSS Stored.

4.14 В качестве дополнительного задания: пройдите SQL Injection, XSS Reflected и XSS Stored на уровне безопасности medium.

4.15 Привести скриншот выполнения задания SQL Injection содержащий подбор правильного запроса к БД.

4.16 Привести скриншот выполнения задания XSS Stored содержащий побор правильного скрипта, извлекающего cookie текущей сессии. включающий скрипт и скриншот результата запроса.

4.17 Привести скриншот выполнения задания XSS Reflected содержащий информацию о получении доменной части источника происхождения

текущего документа, включающий скрипт и скриншот результата работы скрипта.

4.18 Настроить Mutillidae для работы с metaspoitable2, как показано на ресурсе https://cyberarms.wordpress.com/2015/05/01/mutillidae-database-errors-in-metasploitable-2/

4.19 Настроить и провести атаку типа Sniper» в приложении Mutillidae (входит в состав Metasploitable 2).

4.20 Дождаться окончания атаки средством Intruder и проанализировать полученные результаты. При этом, как правило, успешно выполненные запросы отличаются либо кодом состояния, либо своей длиной.

4.21 Проверите результат инъекции ‘or 1=1 or ”=’. Для этого необходимо выбрать вкладку Response, а в ней Render, чтобы узнать, успешно ли прошла ваша инъекция и какие данные вы смогли получить.

4.22 Привести скриншот содержащий результат выполнения запроса.

4.23 В качестве дополнительного задания пришлите примеры успешных запросов и результат атак в виде скриншотов.

5. Порядок выполнения работы

5.1 Установить Kali Linux.

5.2 Настройте Burp Suite.

5.3 Установите Metasploitable 2.

5.4 Настройте Mutillidae.

5.5 Выполнить задания на работу в предложенном порядке.

5.6 Предоставить скриншот каждого этапа выполнения задания.

5.7 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 уязвимостях;
- скриншоты окон выполнения запросов и прохождения заданий машин;
- краткие выводы о проделанной работе.

7. Контрольные вопросы

7.1 Типовые структуры построения WEB приложений?

7.2 Методы проксирования трафика и принципы подключения Proxy Server?

7.3 Методы связывания Proxy Server с источниками запросов?

7.4 Состав и основные возможности приложения Burp Suite?

7.5 Состав и основные возможности приложения OWASP ZAP?

7.6 Метод связи Burp Suite и Foxy Proxy?

7.7 Основное назначение комплекса Metasploitable 2?

7.8 Базовые сведения об атаках типа SQL Injection?

7.9 Базовые сведения об атаках типа XSS Reflected?

7.10 Базовые сведения об атаках типа XSS Stored?

7.11 Базовые сведения об атаках типа перебор значения параметра («Sniper» в Burp Suite)?

7.12 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!