ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

В качестве источника был использован модем с настраиваемой частотой и уровнем сигнала. Частота, на которой излучала антенна модема составляла 868 МГц. Ослабление выставлено 20 dB.

В результате проведенных исследований по разработке антенн с круговой поляризацией для RFID в диапазоне 868-903 МГц было выявлено несколько ключевых аспектов. RFID технология широко применяется в различных сферах, таких как логистика, медицина, производство, транспорт, розничная торговля и другие, благодаря своим преимуществам в бесконтактной идентификации и работе на различных частотах. С использованием спектрального анализатора Spectrum Rider FPH было произведено измерение распределения энергии электромагнитных колебаний в полосе частот антенны, что позволило получить детальное представление о её спектральных характеристиках. Эти результаты имеют значение для дальнейшего использования антенны в RFID системах.

Список использованных источников

1.Таратун В. Е., Лось Е. А. Исследование технологии радиочастотной идентификации и ее роль для космической отрасли // Системный анализ и логистика: журнал.: выпуск №1(23), ISSN 2007-5687. – СПб.: ГУАП., 2020 – с. 47- 54. РИНЦ.

2. Путилина М.В. RFID-технологии в продвижении. — Новосибирск // Проблемы современной экономики, 2014 г. — № 18.

3. Зиборов, И. А. Применения RFID технологий в деятельности различных субъектах хозяйствования / И. А. Зиборов. — Текст: непосредственный // Молодой ученый. — 2009. — № 12 (12). — С. 17-22.

4. Хамзаев Д.И., Хамзаев И.Х. Сравнительный анализ между RFID и NFC технологиями // Universum: технические науки: электрон. научн. журн. 2024. 1(118).

УДК 004.56

ВЛИЯНИЕ СОВРЕМЕННЫХ АТАК SQL-ИНЪЕКЦИЙ НА РАДИОЧАСТОТНЫЙ СПЕКТР: ПРИМЕРЫ И ПОСЛЕДНИЕ ТЕНДЕНЦИИ

Байжанова Диана Намиговна

diana.baizhanova00@mail.ru

Магистрант кафедры «Радиотехника, электроника и телекоммуникации» ЕНУ им. Л.Н.Гумилева, Астана, Казахстан

Научный руководитель- к.т.н профессор Бурамбаева Н.А.

В настоящее время рост числа компьютерных атак на информационные ресурсы, как государственного, так и частного сектора очевиден, что и подтверждают статистические данные от ведущих компаний, специализирующихся в области информационной безопасности. При этом, возникает закономерный вопрос о возможности снизить риски от ущерба компьютерных атак на информационные ресурсы и/или исключить возможности их реализации. С этой целью в рамках поиска решений в работе представлена модель сетевых атак типа XSS- и SQL-инъекций, позволяющая учесть различные уровни сложности их реализации, и выявить новые функциональные зависимости, которые могут быть учтены исследователями и разработчиками средств активного и пассивного тестирования веб-ресурсов [1, с.115].

В настоящее время в сфере информационной безопасности наблюдается устойчивый рост количества компьютерных атак, которые в свою очередь способствуют снижению уровня защищенности веб-ресурсов, данный факт изображен на рисунке1.

Рисунок1 - Реализация Sql-инъекций на радиочастотный спектр

Основными причинами успеха в реализации компьютерных атак, как правило, является наличие уязвимостей в программном обеспечении, отсутствием средств защиты, а также отсутствие реализации в веб-приложениях механизмов защищенного взаимодействия между клиентом и сервером. Данные факты позволяют спрогнозировать наиболее частые атаки на веб-приложения, основными из которых являются: SQL-injection (Structured Query Language - инъекция), 196 и XSS (Cross-Site Scripting).

Согласно исследований в области информационной безопасности данные атаки является наиболее распространены (в среднем, больше, чем в 75% веб-приложений была найдена XSS уязвимость) среди используемых
при разработке веб-приложений. В настоящее время для оценки защищенности веб-ресурсов применяется ряд программных средств (XSSF, XenoTix, Wapiti, XSpider (MAX-Patrol), Nemesida Scanner, Acunetix Online Web Security Scanner)), однако, достоверность результатов проведенных ими исследований не позволяют в полной мере выявить все уязвимости веб-ресурса, что подтверждается значительными финансовыми убытками компаний, что формирует практическое противоречие [2,с.89]. Данное противоречие вызвано тем, что применяемый научно-методический аппарат обладает недостаточной достоверностью результатов оценки, из-за того, что применяемые теоретические подходы не в полной мере позволяют учитывать современные способы проведения компьютерных атак, формирует.

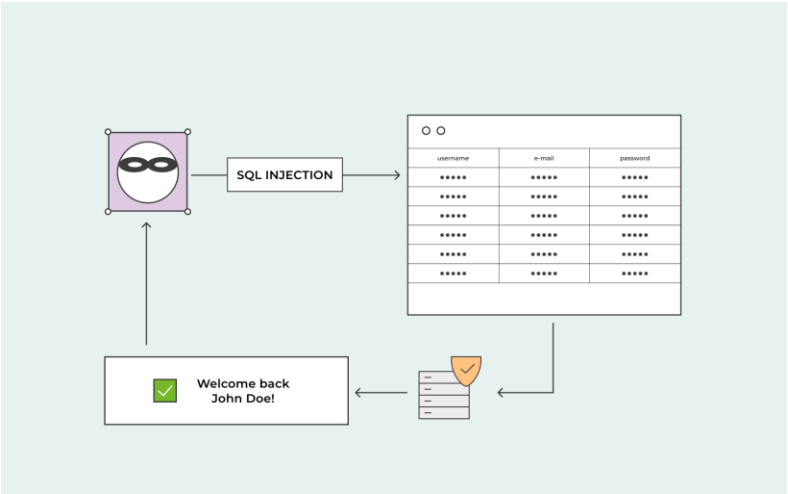

Рисунок2 - Представление Sql-инъекций на радиочастотный спектр

Для устранения представленного противоречия в теории, предлагается разработать модель сетевых атак типа XSS и SQL-инъекций на предмет их применимости, за счет учета

различных вариантов реализации атак различного уровня сложности на различные элементы атакуемого объекта. Устранение практического противоречия осуществляется за счет программное реализации сформулированной модели. Задача моделирования заключается в повышении достоверности результатов моделирования сетевых атак типа XSS и SQL-инъекция на предмет их применимости, за счет учета различных вариантов реализации атак различного уровня сложности на различные элементы атакуемого объекта.

Целью моделирования является выявление зависимости успешности проведения SQL-инъекций и XSS - атак в отношении атакуемого объекта. Цель достигается за счет аппроксимации результатов, полученных с применение имитационного стенда, реализованного в виде специализированного программного обеспечения.

Объектом атак является: веб-ресурс (информация), расположенная на вебсайте, в базах данных и других объектах ЭВТ; составные части архитектуры веб-сайта; пароли и учетные записи пользователей; аппаратные и программные средства составных частей веб-сайта.

SQL-инъекция — это атака с внедрением вредоносного кода SQL в веб-приложение. Злоумышленник вводит в форму запроса или добавляет прямо в URL-адрес специально сформированный SQL-код, который исполняется на сервере. Введенный код позволяет получить доступ к базе данных (англ. database, далее — БД) и выполнять различные операции, от просмотра до уничтожения БД. Для этого киберпреступники используют язык запросов SQL.

SQL (Structured Query Language) — самый популярный язык для работы с реляционными БД (например, MySQL или PostgreSQL). SQL позволяет взаимодействовать с объектами в БД, а также выполнять запросы и анализировать данные.

Основными угрозами являются: нарушение конфиденциальности данных (логины и пароли); нарушение доступа к данным (нарушение работоспособности вебсайта); нарушения целостности хранимой информации.

Выбор основных исходных данных необходимых для описания веб-сервера основывается прядке реализации виртуального хостинга и необходимого дополнительного программного обеспечения. С учетом рассмотрения типового веб-сайта рассматривается программное обеспечение Apache, программные средства: MySQL - сервер баз данных; PHP (Hypertext Preprocessor) - интерфейс поддержки языка программирования PHP; Perl - интерфейс поддержки языка программирования Perl, управление базами данных осуществляется через веб-интерфейс с помощью программного пакета phpMyAdmin.

Перечисленный набор программных средств и обеспечения выбран на основе статистических данных. Исходными данными необходимыми для описания XSS-инъекций являются функции, реализующие основные угрозы указанных атак: кража идентификационных данных (cookies); навязывание ложной информации для пользователя при доступе к веб-сайту; вирусная атака на отдельного пользователя.

Исходными данными необходимыми для описания SQL-инъекций являются функции, реализующие основные угрозы указанных атак: изменение входных параметров путём добавления в них конструкций языка SQL; использование ключевого слова UNION; использование сложных запросов; применение слепых инъекций; эксплуатация уязвимостей программного обеспечения (Error-based SQL injection); эксплуатация уязвимостей управления базами данных; составная SQL-инъекция [3,с.136].

Для выявления аналитической зависимости успешности проведения XSS и SQL-инъекций в отношении атакуемого объекта разработана программа для ЭВМ, позволяющая реализовывать указанные атаки на различные веб-сайты и базы данных, а так же отображать текстовую и графическую информацию о результатах моделирования. Структура стенда основанного на разработанной программе для ЭВМ по исследованию компьютерных атак типа XSS и SQL-инъекции на веб-сервер.

Модуль предназначен для моделирования следующих видов атак: Cross-site scripting (реализация передачи серверу исполняемого кода, для перенаправления на атакуемый

объект) и Challengers (реализация 10 заданий разного уровня по реализации атак типа XSS). Модуль «Атака типа SQL-инъекция» предназначен для моделирования следующих видов атак: Update (реализация SQL-инъекций, направленных на изменение данных БД); Insert (реализация SQL-инъекций, направленных на создание новых данных БД); Select (реализация SQL-инъекций, направленных на получение и вывод данных из БД); Delete (реализация SQL-инъекций, направленных на удаление данных БД); пользовательский (позволяет манипулировать данными из БД, без перехода в другие режимы); Challengers (включает 10 заданий, направленных на реализацию атак различного уровня сложности) [4,с.123].

Автоматизированное рабочее место по исследованию компьютерных атак на веб-сервер позволяет исследовать атаки, применяя критерии для манипулирования, экранирования или отклонения строки, изменяя глобальные настройки, настраивая выходные данные сервера.

Программа позволяет изменять следующие параметры:

1. Вводимые ограничения (критерии отклонения строки для атаки):
- двойные и одинарные кавычки;
- уровень ограничений (регистрово-чувствительный, регистрово-нечувствительный, пропуск обратного слэша и другие);
- вид поиска совпадений (ключевые слова, регулярное выражение);
- возможность ввода определенных слов и выражений в черный или белый список.
2. Глобальные настройки (симулирует кратковременные проблемы сервера):
- случайные ошибки;
- случайное время задержки.
3. Выходной уровень (настройка выходных данных сервера):
- результирующая строка;
- вывод ошибок;
- возможность показа нагрузки.
4. Параметры инъекции:
- строка для инъекции;
- место внедрения [5, с. 116].

Таким образом, в рамках содержательного описания модели атак XSS и SQL-инъекций выявлены аналитические выражения вероятности успешной компьютерной атаки от времени проведения атаки, при применении различного количества применяемых уязвимостей атакуемого объекта.

Разработанная имитационно-аналитическая модель удовлетворяет требованиям качества моделей и обеспечивает повышение достоверности результатов прогнозирования защищенности узлов компьютерной сети от указанных атак на 19,3 %. Разработанный программный стенд и элементы сформулированного подхода можно использовать в образовательных целях в виде семинарских и лекционных занятий в высших учебных заведениях и технических направлений средне-специализированного звена.

Список использованных литературы

1. Осипова О.С. Информационные системы. Инфра-М, 2023. - 136 с.
2. Добрышин М. М. Особенности применения информационно-технического оружия при ведении современных гибридных войн. Инфра-М, 2023. - 115 с.
3. Носиров З.А., Ажмухамедов И.М. Обнаружение XSS-уязвимостей на основе анализа полной карты веб-приложения. АСТ, 2023. - 89 с.
4. Попова И.Ю. ИС в современности. АСТ, 2024. - 123 с.
5. Яковлев И.С. Информатика и информационные системы. Просвещение, 2023. - 116 с.