УДК 004.056

АНАЛИЗ УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ. СПОСОБЫ ИХ ПРЕДОТВРАЩЕНИЯ

Булатова А.Р[1], студент гр. ИБТС-01, V курс
[1]Поволжский государственный университет телекоммуникаций и информатики, г. Самара

В данной статье рассматриваются актуальные уязвимости веб-приложений, которые способны привести к утечке конфиденциальных данных и компрометации безопасности пользователя. Описываются распространенные типы уязвимостей веб-приложений, а также методы их предотвращения. Автором предложены методы по обеспечению безопасности веб-приложений и предотвращению потенциальных угроз.

*Ключевые слова: уязвимости веб-приложений, информационная безопасность, киберугроза, кибербезопасность***.**

Уязвимость веб-приложения – это недостаток в системе, который может быть использован злоумышленником для выполнения атаки на приложение, получения несанкционированного доступа к данным или системе. Уязвимости могут возникать из-за ошибок в коде программы, недостаточного уровня аутентификации и авторизации пользователей, отсутствия защиты. Это может привести к потере конфиденциальной информации и создать угрозы безопасности данных и системы.

Распространенные типы уязвимостей веб-приложений включают в себя:

1. Внедрение SQL-инъекций
2. Межсайтовый скриптинг (XSS атака)
3. Подделка межсайтовых запросов (CSRF)
4. Атака типа «Отказ в обслуживании» (DoS)
5. Перехват сеанса
6. Небезопасное криптографическое хранилище

При проведении атаки «Внедрение SQL-инъекций» злоумышленник получает доступ к базе данных, в которой хранится конфиденциальная информация, используемая веб-приложениями. Путем внедрения вредоносного SQL-кода происходит хищение данных, выполнение привилегированных действий, изменение или удаление информации.

Для защиты от атаки SQL-инъекций необходимо использовать инструменты аутентификации, ограничение прав доступа пользователей, особенно в отношении типа и объема данных, к которым они могут получить доступ. Также следует применять фильтрацию входных данных, использовать

параметризованные запросы вместо динамических строк и устанавливать антивирусное программное обеспечение.

Межсайтовый скриптинг представляет собой тип атаки на веб-приложения, при которой злоумышленник внедряет вредоносный скрипт в веб-сайт или страницу, используя уязвимость в коде. Вредоносный код запускается, когда пользователь открывает скомпрометированное приложение – зараженную страницу. Скрипт выполняется в браузере, тем самым может вызвать раскрытие конфиденциальных данных, перенаправление на фишинговые сайты, а также выполнение действий от имени пользователя [1].

Для того чтобы защититься от XSS атаки, необходимо:

- Использовать библиотеки безопасности (фреймворк), которые автоматически очищают ввод и вывод данных пользователя.
- Проводить проверку входных данных и кодирование выходных данных.
- Включать заголовки политики безопасности контента (CSP) для ограничения источников скриптов.

Атака типа «Подделка межсайтовых запросов» происходит, когда злоумышленник заставляет авторизованного пользователя выполнять непреднамеренные действия в веб-приложении. Для выполнения атаки CSRF злоумышленники используют различные методы, такие как внедрение вредоносного кода, социальную инженерию или отправку ссылок на вредоносные сайты. Данный вид атаки используется для изменения пароля пользователя, отправки вредоносных сообщений, совершения финансовых транзакций и выполнения любых действий от имени пользователя.

Для предотвращения данной атаки необходимо отключать функции автоматического запоминания данных в приложении, генерировать уникальные токены CSRF для каждого пользователя и включать их в формы или запросы для проверки. Также необходимо обновлять пароли, сессионные ключи и проводить тестирование безопасности.

При проведении атак DoS злоумышленник пытается помешать пользователям получить доступ к системе, перегружая ее запросами, тем самым вызывая сбой. Целью атаки является создание ситуации, когда из-за огромного объема трафика и обслуживания ложных запросов пользователь не может получить доступ к необходимым ресурсам [2]. Данный вид атаки может использовать различные методы для достижения цели, включая переполнение сети или сервера запросами, отправку вредоносных пакетов.

Предотвратить атаку «Отказ в обслуживании» возможно следующими способами:

- Увеличение пропускной способности сети поможет справиться с большим объемом трафика, что может сделать атаку менее эффективной.
- Правильная конфигурация брандмауэра и систем предотвращения вторжений (IPS) может помочь в обнаружении и предотвращении атак.

- Распределение нагрузки на несколько серверов или облачных ресурсов делает атаку менее успешной, так как каждый сервер получает только некоторую долю трафика.

Наиболее распространенный метод атаки «Перехват сеанса» называется IP-spoofing, когда злоумышленник использует IP-пакеты, маршрутизируемые источником, для вставки команд в коммуникацию между двумя узлами сети и маскируется под одного из прошедших проверку подлинности пользователей. Этот тип атаки возможен, поскольку аутентификация обычно выполняется только в начале сеанса TCP. Другой тип перехвата сеанса известен как атака "человек посередине", при которой злоумышленник использует сниффер для наблюдения за обменом данными между устройствами и сбора данных по мере их передачи.

Для предотвращения перехвата сеанса необходимо внедрить меры безопасности как на уровне приложения, так и на сетевом уровне; использовать пакетное шифрование пакетов, чтобы злоумышленник не мог расшифровать заголовки пакетов и получить информацию для подмены, а также использовать протоколы для обеспечения безопасности данных IPSEC, SSL, SSH.

Небезопасное криптографическое хранилище относится к неправильной обработке и хранению конфиденциальных данных в веб-приложении. Это возникает, когда криптографические функции либо плохо реализованы, либо полностью игнорируются, что приводит к раскрытию конфиденциальной информации, такой как пароли, номера кредитных карт, личные данные.

Для защиты от данного типа атаки можно применить следующие меры:

- Использование надежных и проверенных алгоритмов шифрования.
- Регулярное обновление криптографических библиотек и платформ, которые используются для работы с зашифрованными данными.
- Обеспечение безопасного хранения ключей шифрования. Ключи шифрования должны быть достаточно длинными и сложными, а также должны храниться отдельно от зашифрованных данных.

Анализ уязвимостей веб-приложений и их последующее устранение должны быть непрерывным процессом в рамках обеспечения безопасности данных пользователей. Правильные меры предосторожности и систематический подход к защите веб-приложений помогут предотвратить потенциальные киберугрозы и обеспечить безопасность пользователей и их данных. Для обеспечения безопасности веб-приложений возможны комбинированные методы анализа уязвимостей, например, регулярное обновление программного обеспечения, соблюдение правил безопасной разработки и обучение персонала по вопросам информационной безопасности.

Список литературы:

1. Крылов И.Д. ЭФФЕКТИВНЫЕ СПОСОБЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ XSS-УЯЗВИМОСТЕЙ САЙТОВ // StudNet. 2021. №2. Режим доступа: https://cyberleninka.ru/article/n/effektivnye-sposoby-

obnaruzheniya-i-predotvrascheniya-xss-uyazvimostey-saytov [Электронный ресурс]

2. Лупорев Сергей Николаевич, Волосенков Владимир Олегович СПОСОБЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ // НАУ. 2015. №2-3 (7). Режим доступаhttps://cyberleninka.ru/article/n/sposoby-obespecheniya-informatsionnoy-bezopasnosti-veb-prilozheniy [Электронный ресурс]