МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

“ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ”

Факультет компьютерных наук

Кафедра Технологии обработки и защиты информации

Межсайтовая подделка запросов (CSRF), подделка серверных запросов (SSRF)

Анализ уязвимостей и защита программного обеспечения

10.03.01 Информационная безопасность

Безопасность компьютерных систем

Обучающийся _____Домарев К.В., 4 курс, д/о

Руководитель _____М.А.Дрюченко, к.т.н., доцент

Воронеж 2023

Введение

Межсайтовая подделка запросов (CSRF) и подделка серверных запросов (SSRF) - это две распространенные уязвимости веб-приложений, которые могут привести к серьезным последствиям для безопасности данных и систем. Обе атаки используются злоумышленниками для получения доступа к конфиденциальной информации или выполнения нежелательных действий от имени авторизованных пользователей.

Межсайтовая подделка запросов (CSRF) происходит путем отправки поддельного запроса на уязвимое веб-приложение от имени авторизованного пользователя. Атака основана на том, что приложение не проверяет, откуда приходит запрос, и выполняет его в соответствии с переданными параметрами. Чтобы защититься от CSRF-атак, разработчики должны использовать токены CSRF, которые генерируются при каждой новой сессии пользователя и проверяются при каждом запросе, отправленном на сервер.

Подделка серверных запросов (SSRF) - это атака, которая позволяет злоумышленнику получить доступ к внутренним ресурсам сервера, таким как базы данных или файловые системы. Атака происходит путем отправки поддельного запроса на сервер с помощью уязвимого веб-приложения. Чтобы защититься от SSRF-атак, разработчики должны внимательно проверять все внешние URL-адреса, используемые в приложении, и ограничивать доступ к внутренним ресурсам сервера, если это возможно.

Защита от CSRF и SSRF-атак - это важный аспект безопасности веб-приложений, который требует внимательного технического и процессуального подхода. Разработчики и пользователи должны быть осведомлены о возможных уязвимостях и принимать меры для защиты своих данных и систем от злоумышленников.

Межсайтовая подделка запросов (CSRF)

Межсайтовая подделка запросов (CSRF) - это атака на веб-приложение, которая происходит путем отправки поддельного запроса с вредоносным кодом на сайт, который пользователь уже авторизован и доверяет. В результате запроса происходят действия, которые могут быть опасны для пользователя, например, изменение пароля, отправка сообщения или создание новой записи.

Методы GET, HEAD, OPTIONS и TRACE не подвержены CSRF, потому что предназначены только для получения информации и не изменяют состояние сервера. Методы POST, PUT, DELETE и PATCH должны быть защищены от CSRF.

Атака основана на том, что многие веб-сайты не проверяют, откуда приходят запросы, и просто выполняют их в соответствии с переданными параметрами. Это позволяет злоумышленникам манипулировать запросами и выполнить действия от имени авторизованного пользователя.

Пример атаки CSRF может выглядеть так: злоумышленник создает веб-страницу, содержащую скрытый тег <img> или <iframe>, который ссылается на уязвимое веб-приложение. Когда пользователь посещает эту страницу, скрытый тег отправляет поддельный запрос на уязвимое веб-приложение. Запрос может содержать параметры, которые заставят приложение выполнить нежелательные действия, такие как удаление записи или изменение настроек пользователя.

Чтобы защититься от CSRF-атак, разработчики веб-приложений должны использовать токены CSRF, которые генерируются при каждой новой сессии пользователя и проверяются при каждом запросе, отправленном на сервер. Токены CSRF можно реализовать с помощью различных технологий, таких как сессионные cookie или скрытые поля ввода формы.

Токен

Токены (или synchronizer token) — это способ защиты со стороны сервера. Сервер генерирует случайный уникальный токен для браузера пользователя и проверяет его для каждого запроса. Токен находится в скрытом поле, должен быть непредсказуемым случайным числом и иметь небольшое время жизни, без возможности переиспользования. Токен должен

- удовлетворять следующим условиям:
- быть уникальным в пределах каждой операции;
- использоваться один раз;
- иметь размер устойчивый к подбору;
- генерироваться криптографически стойким генератором псевдослучайных чисел;
- иметь ограниченное время жизни.

Для чувствительных действий, вроде перевода денег или смены пароля, требуйте дополнительное действие от юзера (ввод капчи или кода подтверждения).

Важно отметить, что CSRF-атаки могут быть выполнены только в том случае, если злоумышленник знает, какие запросы необходимо отправлять на уязвимое веб-приложение, и какие параметры нужно передать в запросе. Поэтому, чтобы защититься от CSRF-атак, необходимо также ограничить доступ к конфиденциальной информации, такой как токены CSRF, и не разглашать их.

В общем, чтобы предотвратить CSRF-атаки, веб-разработчики должны быть осведомлены о возможных уязвимостях и принимать меры для защиты веб-приложений от таких атак.

Подделка серверных запросов (SSRF)

Подделка серверных запросов (SSRF) - это атака на веб-приложение, которая позволяет злоумышленнику получить доступ к внутренним ресурсам сервера, таким как базы данных или файловые системы. Атака происходит путем отправки поддельного запроса на сервер с помощью уязвимого веб-приложения (рисунок 1). Запрос может быть сформирован таким образом, чтобы использовать в качестве адреса URL внутренний адрес сервера, например, 127.0.0.1 или localhost.

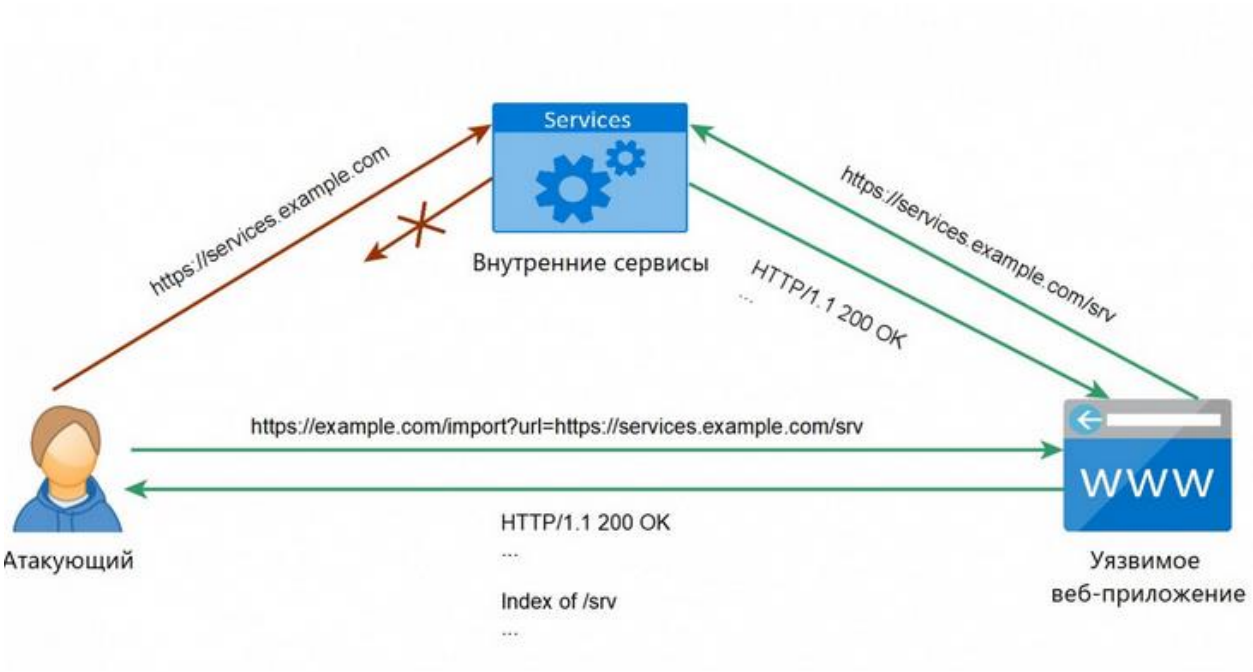

Рисунок 1 – Пример атаки SSRF

SSRF-атаки могут быть выполнены на любом уязвимом веб-приложении, которое позволяет пользователю отправлять запросы на внешние ресурсы. Злоумышленник может использовать эту возможность, чтобы отправить запрос на внутренний ресурс сервера, например, базу данных, которая содержит конфиденциальную информацию. В результате злоумышленник может получить доступ к внутренним ресурсам сервера

(рисунок 2), что может привести к утечке конфиденциальной информации или выполнению злонамеренных действий.

Рисунок 2 – Функции SSRF

Пример атаки SSRF может выглядеть так: злоумышленник отправляет запрос на уязвимое веб-приложение, который содержит в качестве адреса URL внутренний адрес сервера, например, 127.0.0.1 или localhost. Запрос может быть выполнен с помощью различных методов, таких как GET, POST или HEAD. В результате запроса злоумышленник может получить доступ к внутренним ресурсам сервера и выполнять нежелательные действия.

Чтобы защититься от подделки серверных запросов, разработчики должны внимательно проверять все внешние URL-адреса, используемые в приложении, и ограничивать доступ к внутренним ресурсам сервера, если это возможно. Одним из способов защиты от SSRF-атак является ограничение диапазона IP-адресов, которые могут быть использованы в запросах. Это позволит разрешить доступ только к определенным адресам, которые являются доверенными.

Также, чтобы защититься от подделки серверных запросов, необходимо следить за обновлением и патчами безопасности веб-приложений и операционной системы на серверах. Рекомендуется использовать надежные библиотеки и фреймворки для разработки веб-приложений, которые обеспечивают защиту от известных уязвимостей.

В общем, подделка серверных запросов (SSRF) - это серьезная угроза безопасности веб-приложений и требует сочетания технических и процессуальных мер для защиты от нее. Разработчики и пользователи должны быть осведомлены о возможных уязвимостях и принимать меры для защиты своих данных и систем от злоумышленников.