УДК 0.004 **Информационные технологии**

Дьяченко Никита Владимирович, *магистрант*
Донского государственного технического университета

АТАКА С ПОДДЕЛЬНЫМИ МЕЖСАЙТОВЫМИ ЗАПРОСАМИ

Аннотация: Стремительный рост веб-приложений и широкое использование Интернета произвели революцию в том, как мы взаимодействуем с информацией и сервисами. Однако эта цифровая эволюция также привела к росту киберугроз, поскольку злоумышленники постоянно разрабатывают новые методы использования уязвимостей. Одна из таких угрожающих атак известна как "Атака с поддельными межсайтовыми запросами", вариант хорошо известной атаки с подделкой межсайтовых запросов (CSRF). В этой статье исследуется природа этих поддельных межсайтовых запросов, их потенциальное воздействие и меры защиты от этой развивающейся угрозы веб-безопасности.

Ключевые слова: атака, межсайтовой запрос, злоумышленник, данные.

Annotation: The rapid growth of web applications and the widespread use of the Internet made a revolution in how we interact with information and services. However, this digital evolution also led to an increase in cyberurosis, since attackers are constantly developing new methods of using vulnerabilities. One of these threatening attacks is known as the “attack with fake intersight requests”, a variant of a well -known attack with fake intersight requests (CSRF). This essay examines the nature of these fake intersight requests, their potential impact and protection measures from this developing threat of web security.

Keywords: attack, intersyate request, attacker, data.

Введение

Атака с использованием поддельных межсайтовых запросов, также

называемая "Поддельным CSRF" или "CSRF с поддельными запросами", представляет собой вредоносный метод, при котором злоумышленники подделывают межсайтовые запросы для манипулирования действиями пользователей в веб-приложениях. Эта атака основана на неявном доверии между браузером пользователя и веб-приложением, используя тот факт, что браузер автоматически включает файлы cookie для аутентификации пользователя в каждый запрос к приложению.

Цель злоумышленника состоит в том, чтобы обманом заставить браузер пользователя отправить запрос целевому веб-приложению, в результате чего от имени пользователя будут выполняться несанкционированные действия. Эти действия могут включать изменение конфиденциальных настроек учетной записи, инициирование финансовых транзакций или даже распространение вредоносного ПО. Пользователь, не подозревающий об атаке, непреднамеренно выполняет эти вредоносные действия, что приводит к потенциально серьезным последствиям.

Последствия атаки с поддельными межсайтовыми запросами

Последствия поддельных атак CSRF могут быть далеко идущими и разрушительными как для отдельных лиц, так и для организаций:

1. Финансовые потери: злоумышленники могут манипулировать сеансом пользователя для инициирования транзакций или платежей, что приводит к несанкционированным финансовым потерям жертвы.

2. Кража личных данных: личная информация может быть изменена или украдена, что позволяет осуществлять кражу личных данных и дальнейшее использование присутствия пользователя в сети.

3. Репутационный ущерб: организации, ставшие жертвами таких атак, могут столкнуться с серьезным репутационным ущербом, потеряв доверие и лояльность клиентов.

4. Юридические последствия: юридическая ответственность может возникнуть, если веб-приложение будет скомпрометировано из-за поддельной атаки CSRF, особенно если это касается конфиденциальных пользовательских

данных.

5. Подрыв доверия пользователей: пользователи могут испытывать опасения по поводу использования веб-приложений, что препятствует росту онлайн-сервисов и электронной коммерции.

Защита от атак с помощью поддельных межсайтовых запросов.

Чтобы противостоять растущей угрозе поддельных атак CSRF, необходимо внедрить несколько надежных механизмов защиты:

1. Токены CSRF: введите уникальные, непредсказуемые токены, которые включаются в каждый запрос. Сервер проверяет эти токены, гарантируя, что запрос является законным.

2. Файлы cookie для одного сайта: внедряйте файлы cookie, которые ограничены одним и тем же исходным доменом, предотвращая несанкционированные межсайтовые запросы.

3. Заголовки ссылок: проверьте заголовок ссылки, чтобы убедиться, что запросы исходят из известных, надежных источников.

4. Двойная отправка файлов cookie: реализуйте комбинацию токенов, относящихся к сеансу, и токенов, специфичных для запроса, чтобы предотвратить атаки CSRF.

5. Политика безопасности контента (CSP): используйте CSP для ограничения доменов, с которых может загружаться контент, снижая риск внедрения вредоносного кода.

6. Методы безопасного кодирования: разработчики должны следовать методам безопасного кодирования, включая проверку ввода и кодирование вывода, чтобы предотвратить различные векторы атак.

7. Регулярные проверки безопасности: проводите периодические проверки безопасности и тестирование на проникновение для активного выявления и устранения уязвимостей.

Заключение

Распространение веб-приложений принесло многочисленные преимущества как пользователям, так и предприятиям, но оно также поставило

нас перед новыми вызовами безопасности. Атака с поддельными межсайтовыми запросами, как вариант атак CSRF, представляет серьезную угрозу безопасности веб-приложений. Используя доверие пользователей и манипулируя их браузерами, злоумышленники могут выполнять несанкционированные действия с далеко идущими последствиями. Вебразработчики, специалисты по безопасности и пользователи обязаны сохранять бдительность и внедрять надежные меры защиты от этой угрозы веб-безопасности. Осведомленность, образование и сотрудничество необходимы для защиты цифрового ландшафта и сохранения доверия пользователей к онлайн-среде.

Библиографический список:

1. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / Под. ред. А.С.Маркова. - М.: Радио и связь, 2012. 192 с.

2. Барабанов А.В., Евсеев А.Н. Применение международного стандарта для поиска уязвимостей // Безопасные информационные технологии: Сборник трудов Пятой Всероссийской научно-технической конференции. - М., 2015. - С. 50-52.

3. Барабанов А.В., Федичев А.В. Разработкатиповой методики анализауязвимостей в веб приложениях при проведении сертификационных испытаний по требованиям безопасности информации Вопросы кибербезопасности. 2016. № 2 (15). С. 2-8.

4. N. Jovanovic, E. Kirda, and C. Kruegel. Preventing cross site request forgery attacks. In the IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm) , pages 1-10, September 2006.