Ошибки путаницы привилегий, подделка межсайтовых запросов в веб-приложениях.

Cross-site request forgery(CSRF)

Аристид Жан Лоэнс Аристобуль Надаль

19 октября 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Аристид Жан Лоэнс Аристобуль Надаль
- Студент
- Российский университет дружбы народов

Вводная часть

Объект и предмет исследования

- Уязвимости веб-сайтов
- безопасность веб-приложений
- роли и разрешения пользователей

Цели и задачи

- Понять, что такое подделка межсайтовых запросов
- Защитите веб-приложение от такой уязвимости

Материалы и методы

- обычные инструменты, такие как html, javascript
- веб-браузер
- подключение к интернету

Элементы презентации

Актуальность

- Дайте представление о потенциальных уязвимостях вашего веб-приложения
- Предоставьте методы, позволяющие не стать жертвой CSRF-атаки

Что такое CSRF?

- Подделка межсайтовых запросов (CSRF) - это атака, которая заставляет конечного пользователя выполнять нежелательные действия в веб-приложении, в котором он в данный момент аутентифицирован.

CSRF scenario

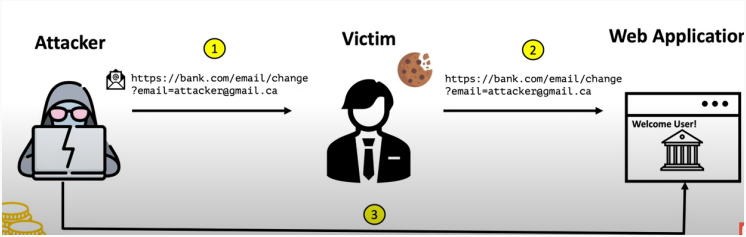

Рис. 1: CSRF scenario

Намерения злоумышленников

- изменить электронную почту или пароль жертвы
- купить что-то
- Получить личные данные

Условия CSRF

- Соответствующее действие
- Обработка сессии на основе куки
- Отсутствие непредсказуемых параметров запроса

Предотвращение уязвимостей CSRF

- CSRF token
- cookies SameSite

Токен CSRF

- непредсказуемый
- привязан к сессии пользователя
- проверяется перед удовлетворением запроса

Cookies SameSite

- Strict
- Lax
- None

```
Set-Cookie: session=test; SameSite=Strict

Set-Cookie: session=test; SameSite=Lax

Set-Cookie: flavor=choco; SameSite=None; Secure
```

Сканеры уязвимостей веб-приложений (WAVS)

- acunetix
- arachni
- wapiti
- Burp Suite

Итоговый слайд

- Веб-приложения подвержены множеству уязвимостей, о которых веб-разработчик должен знать при программировании своего веб-приложения. Веб-разработчик должен принять необходимые меры для защиты своего сайта от этих уязвимостей, чтобы сохранить данные пользователей и избежать взлома их аккаунтов.

Sources

- https://owasp.org/www-community/attacks/csrf
- Web Application Security: Exploitation and Countermeasures for Modern Web Applications by Andrew Hoffman