БЕЗОПАСНОСТЬ В JAVASCRIPT

М.А. Аниховский, И.Ю. Изгачёв, В.А. Ковалёв, В.Я. Анисимов

В данной работе описываются наиболее распространенные угрозы безопасности веб-сайтов: XSS, SQL-инъекции и CSRF. Рассмотрим их подробнее. XSS или межсайтовый скриптинг (от англ. Cross Site Scripting) - тип атаки на веб-системы, заключающийся во внедрении в страницу вредоносного кода. Уязвимость вызвана недостатками клиентских языков сценариев, таких как HTML и JavaScript. Через XSS злоумышленники могут внедрять сторонний JavaScript код для выполнения вредоносных задач. XSS-атаки могут привести к краже личных данных и распространению вирусов, а иногда и к удаленному управлению браузером пользователя. Предотвратить потенциальные XSS угрозы можно с помощью экранирования пользовательского ввода [1].

Уязвимости SQL-инъекций дают злоумышленникам возможность выполнять произвольный SQL код в базе данных, позволяя им получать, изменять или удалять данные независимо от разрешений пользователя. Типы внедрения SQL включают: внедрение на основе ошибок, внедрение на основе логических ошибок и внедрение на основе времени. Данная уязвимость имеет место быть, если пользовательский ввод напрямую передается в SQL запрос без надлежащего экранирования потенциально опасных символов [2].

CSRF или подделка межсайтовых запросов (от англ. Cross Site Request Forgery) – уязвимость, позволяющая злоумышленникам отправлять авторизованные запросы,

используя данные сессии жертвы. Многие веб-приложения используют cookies для хранения сессии пользователя. Для проведения простейшей CSRF атаки злоумышленнику необходимо оставить ссылку с кодом, который будет отправлять запрос с данными, выгодными злоумышленнику. При переходе по ссылке браузер автоматически прикрепит к запросу cookies жертвы, включая данные его сессии. Для защиты от CSRF уязвимостей чаще всего используются уникальные CSRF-токены для каждой пользовательской сессии (один токен в теле запроса, второй, идентичный – в cookie) [3]. Также можно защитить потенциально опасные действия паролем, который должен ввести сам пользователь.

Литература

1. Palmer S. Web Application Vulnerabilities.
2. Yaworksi P. Real-World Bug Hunting: A Field Guide to Web Hacking.
3. Stuttard D., Pinto M. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.