

## БЕЗОПАСНОСТЬ В JAVASCRIPT

И.В. Чибисов, И.А. Клапатов, В.В. Шиманский

JavaScript является самым популярным языком, используемым в веб-разработке. Из-за этого существуют десятки методов, которые используют уязвимости этого языка программирования. Главной целью хакера являются данные пользователей, поэтому они нацелены на файлы cookie, данные сессии, пароли и логины. В основном злоумышленник использует уязвимые поля пользовательского ввода, незащищенные элементы отправки HTTP-запросов, а также пользовательский ввод, который требуется серверной команде. Самые распространенные виды атак это Межсайтовый скриптинг (XSS), Подделка межсайтовых запросов (CSRF) и Серверная JavaScript-инъекция. Все они используют вышеперечисленные уязвимости, чтобы завладеть данными пользователей. Но все уязвимости можно компенсировать и не допустить утечки данных. Изучая методы защиты было установлено, что безопасность использования JavaScript полностью зависит от разработчика, который должен всегда использовать все необходимые методы защиты в своем приложении. Используя поля для пользовательского ввода, разработчику нужно использовать специальный синтаксис escape, также можно использовать экранирование JavaScript и HTML. Чтобы исключить вредоносные HTTP-запросы достаточно в элементы отправки внедрить токены, которые будут генерироваться каждый раз при начале нового сеанса, а сервер будет проверять эти токены

перед отправкой запроса. Также разработчик должен избегать использования и знать такие команды JavaScript, которые являются небезопасными и могут исполнить и скомпилировать код.

Подводя итог можно сказать, что в современных веб-приложениях есть много уязвимостей и вся ответственность за безопасность приложения ложится на плечи разработчика, который должен разбираться в своем деле и знать основы безопасного использования JavaScript.

### **Литература**

1. Форристал Д., Брумс К. Защита от хакеров Web-приложений. – М.: Компания АйТи; ДМК Пресс. – 496 с.
2. Фленов М.Е. Web-сервер глазами хакера. – СПб.: БХВ-Петербург, 2009. – 320 с.