# CROSS-SITE SCRIPTING

А.Ю. Сычев, Т.Д. Позняков, Ю.И. Алексеев

JavaScript – это высокоуровневый интерпретируемый динамически типизированный язык программирования, который взаимодействует с «Document Object Model» пользователя для выполнения различных функций, таких как: структурированное представление документа и определение того, как эта структура может быть доступна из программ, которые могут изменять содержимое, стиль и структуру документа. Cross-Site Scripting является одним из самых распространенных уязвимостей веб-приложений, используемая хакерами для получения несанкционированного доступа к информации. XSS осуществляется путем выполнения любого нежелательного, вредоносного или несанкционированного JavaScript сниппета (скрипта) на компьютере жертвы или в веб-приложении. Такая процедура может привести к потере информации, перенаправлению пользователя на нежелательный сайт, получения доступа к пользовательскому буферу обмена или истории браузера. Даже такие гиганты, как Facebook, подвергались атакам: в июле 2015 г. личный аккаунт М. Цукерберга был взломан и оповещен об уязвимости. Важно отметить, что любая информация, передаваемая от пользовательского до серверного, может нести в себе потенциальную угрозу или фактор

заражения. К ним относятся: параметры запроса, URL-путь, методы PUT / POST, файлы cookie, Cross-Site Scripting (XSS) и т. д. Данная уязвимость не может быть предотвращена фаерволом веб-приложения(web app firewall). Однако есть некоторые методы противодействия, например:

1) проверка и обработка вводимых пользователем данных;

2) кодирование выходных данных для конкретного элемента, особенно, если выходные данные содержат HTML теги;

3) укзаание правильных заголовков: Strict transport security, X-frame-options, X-XSS-protection, X-Content-Type-Options, Content-Security-Policy.

Предпринимая вышеуказанные меры, можно существенно сократить риск атаки, но не устранить угрозу в полной мере. Поэтому поиск эффективных мер противодействия является актуальной задачей [1, 2].

**Литература**

1. What is Cross-site Scripting and How Can You fix it? [Electronic resource]. – Access mode: https://acunetix.com/websitesecurity/cross-site-scripting/. – Date of access: 30.04.2020.

2. How does Cross-site Scripting (XSS) impact customers? | Packetlabs [Electronic resource]. – Access mode: https://www.packetlabs.net/cross-site-scripting-xss/. – Date of access: 30.04.2020.