УДК 665.73

Студ. В.Д. Нигриенко
Науч. рук. доц. Н.А. Жиляк
(кафедра информационных систем и технологий, БГТУ)

МЕЖСАЙТОВЫЙ СКРИПТИНГ(XSS)

Уязвимость XSS (Cross-SiteScripting) – одна из немногих уязвимостей, которая присутствует на очень многих сайтах даже сейчас. Данная уязвимость состоит в том, что хакеру удается внедрить на страницу свой вредоносный JavaScript-код. Этот код будет выполняться каждый раз, когда обычные пользователи будут заходить на страницу приложения, куда этот код был добавлен.

Итак, существует несколько типов XSS:

– хранимый XSS возможен, когда злоумышленнику удается внедрить на сервер вредоносный код, выполняющийся в браузере каждый раз при обращении к странице. Его примером может послужить плохая фильтрация входных данных в базу данных или ее отсутствие при написании комментарий на каком-либо сайте. Stored XSS очень опасная уязвимость, поскольку может иметь свойство червя – распространяться;

– отраженный XSS или по-другому Reflected XSS. Является очень распространенной XSS. Эти уязвимости появляются, когда данные, предоставленные веб-клиентом, появляются чаще всего в параметрах HTTP-запроса или в форме HTML. Отражённая XSS-атака срабатывает, когда пользователь переходит по ссылке, в которую вставлена полезная нагрузка;

– XSS в Dom или DOM-based XSS. Данная XSS реализуется через DOM и не зависит от платформы и языка программного интерфейса, позволяющий программам и сценариям получать доступ к содержимому HTML и XML-документов, а также изменять содержимое, структуру и оформление таких документов.

Далее опишем некоторые рекомендациям по предотвращению XSS изOWASP XSS Prevention Cheatsheet.

Параметры, получаемые веб-приложением, должны проходить процессы санитизации и фильтрации для предотвращения исполнения управляющих конструкций.

При формировании страницы веб-приложения проводить санитизацию и экранирование управляющих конструкций из динамически собирающихся данных.