МЕЖСАЙТОВЫЕ АТАКИ С ВНЕДРЕНИЕМ СЦЕНАРИЯ

А.С. Михайлов, А.П. Турлай, С.Б. Саломатин

Рассматриваются следующие алгоритмы возможных атак в рамках схемы работы межсайтовой атаки с внедрением сценария.

Хранимые XSS (постоянные) – один из самых опасных типов уязвимостей, так как позволяет злоумышленнику получить доступ к серверу и уже с него управлять вредоносным кодом (удалять, модифицировать).

Отраженные XSS (непостоянные): в этом случае вредоносная строчка выступает в роли запроса жертвы к зараженному веб-сайту.

DOM-модели: в этом варианте возможно использование как хранимых XSS, так и отраженных.

Правила безопасности. Защита применяется последовательно, без исключений и упрощений, желательно с самого начала разработки веб-приложения.

Рассматриваются следующие варианты: проверка входных данных, экранирование данных на выходе.

Заключение. Разработанные алгоритмы, реализованные в виде программ, позволяют повысить эффективность защиты веб-приложения от атак. Они значительно упрощают процесс тестирования веб-ресурса разработчиком, благодаря функционалу формирования отчета с рекомендациями по устранению найденных уязвимостей.

Литература

1. Элхади А.М. Полное пособие по межсайтовому скриптингу.

2. Элхади А.М. Уязвимости веб-приложений: пора анализировать исходный код.

3. Джатана Н., Агравал А., Собти.К. Пост эксплуатация XSS: продвинутые методы и способы защиты.