ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ САЙТОВ

канд. техн. наук, доц. С.Ю. Гавриленко, магистр Д.В. Богуш,
Национальный технический университет "Харьковский политехнический институт", г. Харьков

Характерной чертой развития современного общества является информационная интеграция в глобальную мировую систему, основанная на повсеместном использовании компьютерных и телекоммуникационных средств. В этих условиях важнейшей задачей становится защита информационных ресурсов от несанкционированных действий [1].

Наибольшая часть всех компьютерных преступлений приходиться на компьютерные взломы, в том числе и на взломы сайтов. Особенный интерес представляют сайты с большим количеством посетителей.

Как свидетельствует статистика, многие крупнейшие предприятия в мире так или иначе используют уязвимое программное обеспечение с открытым кодом. Причина – отсутствие в приложениях оперативной системы оповещения об обнаруженной в них уязвимости, а также наличие автоматического обновления.

Анализ литературы показал, что уязвимость сайтов чаще всего связана с XSS или Cross Site Scripting. "Межсайтовый скриптинг" XSS – это тип уязвимости интерактивных информационных веб-систем. Он возникает тогда, когда во время генерации сервером страниц в них по различным причинам попадают скрипты пользователей. XSS можно условно разделить на активные и пассивные. Активные XSS характерны тем, что вредоносный скрипт находится на самом сервере. Срабатывание происходит во время открытия страницы сайта в браузере сайта-жертвы. Пассивные исходят из того, что для срабатывания пассивной XSS потребуется дополнительное воздействие в браузере жертвы, например, переход по ссылке, специально для этого сформированной.

Следует также отметить, что современные браузеры определяют кодировку страницы "на лету" и интерпретируют HTML-код в соответствии с результатом этой процедуры. У хакера имеется возможность вставки злонамеренного HTML-кода, обходя фильтрацию символов.

Для выявления уязвимостей сайтов используют специальный тест на проникновение (penetration test, пентест), который является наиболее эффективным способом определения защищенности сайтов. Тест на проникновение позволяет смоделировать сценарии взлома сайта злоумышленниками.

Список литературы: 1. *Гавриленко С.Ю.* Защита данных в компьютеризированных управляющих системах / *С.Ю. Гавриленко, С.Г. Семенов, В.В. Давыдов*. Deutschland: LapLambertAcademicpublishing, 2014. – 236 с.