Литература

1. The Ten Most Critical Web Application Security Risks [Электронный ресурс]. – URL: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_en.pdf (дата обращения: 11.05.2018).

2. Евсеев Д. Введение в тему безопасности веб-приложений [Электронный ресурс]. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/webinars/ics/Д.Евтеев_Введение_в_тему_безоп_веб_прилож.pdf. (дата обращения: 11.05.2018).

КОНТРОЛЬ БЕЗОПАСНОСТИ В КЛИЕНТ-СЕРВЕРНЫХ ПРИЛОЖЕНИЯХ ПРИ ИСПОЛЬЗОВАНИИ ФРЕЙМВОРКА MICROSOFT SIGNALR НА ОСНОВЕ КЛИЕНТСКИХ ГРУПП

В.В. Кузнецов

При разработке клиент-серверных приложений в системах информационной безопасности острой ставится задача запросов клиента к серверу, особенно учитывая проблемы связанные с несанкционированным доступом в базу данных, отправку специфических аргументов серверу и других.

Целью настоящей работы явилась разработка подхода контроля безопасности запросов клиентов к серверу.

Фреймворк Microsoft SignalR [1], обеспечивающий двустороннее взаимодействие в клиент-серверных web-приложениях позволяет на стороне сервера (backend-side) применять атрибуты клиентских групп для классов, обеспечивающих API (Application programming interface) клиентов к серверу, в результате чего исключается необходимость проверять права клиента при обработке запросов. Клиентские группы, такие как например «Пользователи» и «Администраторы» хранятся на машине (ПК) выполняющего функции сервера в разделе «Управление компьютером/Локальные пользователи и группы/Группы». Добавив соответствующие группы, предоставляется возможность их использования в добавлении аттрибутов, например [Authorize(“Custom Administrators group”)], после чего доступ к соответствующему классу или методу получат только те пользователи, имена (домены) которых включены в соответствующие группы.

Таким образом, разработан подход по контролю безопасности клиент-серверных веб-приложений при использовании фреймворка Microsoft SignalR с технологией применений атрибутов для определенных клиентских групп, указанных на серверной машине с операционной системой Windows.

Литература

1. SignalR [Электронный ресурс]. – URL: https://docs.microsoft.com/en-us/aspnet/signalr (дата обращения: 16.05.2018).

УЯЗВИМОСТИ ПОВРЕЖДЕНИЯ ПАМЯТИ В УСТРОЙСТВАХ «INTERNET OF THINGS»

В.Ф. Кулиш

Устройства «интернета вещей» используют широкий диапазон архитекур центрального процессора, но наибольшее распространение получили архитектуры ARM и MIPS. Использование таких архитектур обусловлено их низким энергопотреблением и, соответсвенно, низким количеством выделяемого тепла при работе. Однако использование таких архитектур не защищает от уязвимостей повреждения памяти. Также как и устройства с архитектурой x86, такие устройства также подвержены уязвимостям переполнения буфера и уязвимостям форматных строк.

Уязвимости переполнения буфера обнаружились еще в начале компьютерной эпохи и продолжают существовать по сей день. Уязвимостям такого типа подвержены языки программирования, в которых управление процессом выделения памяти отдано на откуп программисту (пример: C, C++). При создании программ разработчику необходимо контролировать размер помещаемых в переменную данных, память под которую была