0.1. *Шумилин О.П., Вичугова А.А.* **Основы информационной безопасности в веб-программировании. Современные методы и средства защиты от SQL-инъекций**

SQL-инъекция является одним из самых распространенных методов взлома программ и сайтов, работающих с базами данных. Это атака на базу данных, которая позволяет выполнять какие-либо действия, которые раннее не планировались создателем скрипта. SQL–атакастановится возможной из-за некорректной обработки входных данных, используемых в запросах.Данная уязвимость является одной из самых распространенных и наиболее опасной в вопросе безопасности. SQL–инъекции считаются опасными, потому что они предоставляют данные для хакеров через веб-интерфейс. После удачного проведения атаки, злоумышленник распорядится вашей информацией как посчитает нужным: получит пароли от учетных записей, удалит таблицы из базы данных или внесет в них изменения. SQL-инъекции это чисто программная ошибка, и не имеет ничего общего с хост-провайдером. За безопасность базы данных полностью отвечает разработчик [1].

Современные программные платформы разработки, предлагающие набор методов и средств реализации программного обеспечения и называемые фреймворки, содержат инструменты защиты от SQL-инъекций. Например, Laravel, выбранный для реализации проектируемой системы «Мобильный горожанин». Также популярными средствами этой категории являются ZendFramework, Lumen, Symphony, Yii2 и многие другие. В настоящее время использование фреймворков считается хорошим стилем программирования и становится стандартом де-факто [2]. Поэтому очень важно следить за новинками рынка программного обеспечения и выбирать соответствующие инструменты разработки для эффективной и качественной реализации поставленных задач.

Список литературы

[1] PHP: SQL-инъекции – Manual. Адрес доступа: http://php.net/manual/ru/security.database.sql-injection.php (дата обращения: 21.09.2015).

[2] Приход новой эры PHP-фреймворков. Адрес доступа: http://blogerator.ru/page/prihod-novoj-ery-php-frejmvorkov (дата обращения: 21.09.2015)