

АНАЛИЗ УЯЗВИМОСТИ «PROTOTYPE POLLUTION» В JQUERY

М.Г. Прахоцкий, М.В. Стержанов, А.Л. Хотеев, В.Н. Теслюк

jQuery – достаточно популярная в прошлом библиотека JavaScript, фокусирующаяся на взаимодействии JavaScript и HTML [1]. Библиотека помогает легко получать доступ к любому элементу DOM, обращаться к атрибутам и содержимому элементов DOM, манипулировать ими. Также библиотека предоставляет удобный API для работы с AJAX. Хотя времена jQuery уже давно прошли, однако до сих пор существует большое количество сайтов, которые используют эту библиотеку.

Следовательно, любые недостатки, обнаруженные в библиотеке jQuery, автоматически открывают двери для атак на сотни миллионов веб-сайтов. Одной из недавно обнаруженных проблем в этой библиотеке стала уязвимость вида «Prototype Pollution». Влияние этой проблемы может быть серьезным, учитывая, что библиотека JavaScript jQuery в настоящее время используется на 74 процентах веб-сайтов в Интернете, большинство сайтов по-прежнему используют версии библиотеки 1.x и 2.x, которые подвержены уязвимости «загрязнение прототипа».

Эта уязвимость безопасности, упоминаемая и проявляющаяся как «загрязнение прототипа», позволяет злоумышленникам перезаписать прототип объекта приложения JavaScript. Когда это происходит, свойства, которыми управляет злоумышленник, могут быть внедрены в объекты, а затем либо привести к аварийной остановке приложения, либо внедриться в исходный код приложения, давая злоумышленнику полный доступ к управлению приложением [2].

Список литературы

1. Адам Фримен. jQuery для профессионалов = Pro jQuery. М.: «Вильямс», 2012. 960 с.
2. Самков Г. jQuery. Сборник рецептов. СПб.: БХВ-Петербург, 2010. 416 с.

ОСОБЕННОСТИ ПОДГОТОВКИ СПЕЦИАЛИСТОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ

З.Н. Примичева

С ростом информационного обмена и в условиях необходимости защиты информационных ресурсов страны спрос на специалистов по защите информации постоянно растет. В настоящее время преподавание должно сочетать в равной степени традиционную и современную интерактивную модели обучения. Современная интерактивная образовательная модель основывается на внедрении в процесс обучения таких инновационных методов, как метод проблемного изложения, презентация, мини-исследования и др., позволяет изменить роль преподавателя и сделать его руководителем самостоятельной творческой работы студента, предполагает большую активность обучаемого, развитие личностного потенциала студента.

Квалифицированный IT-специалист должен владеть основами информационной безопасности, уметь анализировать и оценивать ее угрозы, знать в этой области нормативную базу. Для успешного применения современных методов и средств защиты информационных систем на практике специалисту необходимо иметь всестороннюю подготовку в области математики и информационных технологий, владеть навыками абстрактного математического мышления и уметь применять абстрактные математические знания при решении конкретных задач реальной действительности. Математическая подготовка IT-специалистов должна быть ориентирована на изучение дисциплин, которые непосредственно используются в формировании основ области информационных технологий и сфер их применения.

Для повышения профессиональной компетентности специалиста по защите информации необходимы знания, которые не входят в классический курс «Высшая математика», по основам линейной алгебры (по конечным полям, кольцам, группам, линейным пространствам над конечными полями), преобразованиям Фурье и их использованию при