УДК: 004.432.2

***Проаспэт А. Г., студент магистратуры***

***1 курс, Технологический университет (прикладная информатика)***

***Россия, г. Королёв***

***Proaspat, A. G., master student***

***1 course, University of Technology (applied computer science)***

***Russia, Korolev***

**Обеспечение безопасности при использовании Node.js и CoffeeScript для разработки системы управления контентом интернет-ресурса**

***Аннотация:*** *Интернет-ресурсы, созданные с использованием системы управления контентом, менее защищены от сторонних атак, чем статические html-сайты. Однако ввиду высокой трудоёмкости процесса создания и поддержания таких ресурсов для коммерческой сферы такое решение является неприемлемым. В связи с этим необходимо обеспечение безопасности в том числе на этапе разработки корпоративной информационной системы для управления контентом интернет-ресурса.*

***Ключевые слова:*** *JavaScript, CoffeeScript, Node.js, интернет-ресурс, серверная разработка, backend, система управления контентом интернет-ресурса.*

***Abstract****:* *Internet resources created using a content management system are less protected from third-party attacks than static html sites. However, due to the high complexity of the process of creating and maintaining such resources for the commercial sphere, such a solution is unacceptable. In this regard, it is necessary to ensure security, including at the stage of development of a corporate information system for managing the content of the Internet resource.*

***Keywords****:* *JavaScript, CoffeeScript, Node.js, Internet resource, server development, backend, content management system of Internet resource.*

Когда идёт речь о разработке системы управления контентом, необходимо принимать во внимание, что пользователи системы будут осуществлять её модификацию с целью адаптации под особенности собственного ресурса. Использование JavaScript и созданных на его основе CoffeeScript и Node.js будет способствовать достижению этой цели [3, с. 902].

В настоящее время почти каждую неделю происходят серьёзные нарушения безопасности, например, в случаях LinkedIn или MySpace. Во время этих атак было украдено огромное количество пользовательских данных, а также нанесён вред корпоративной репутации. Исследования также показывают, что тикеты на ошибки, связанные с безопасностью, остаются открытыми в среднем в течение 18 месяцев в некоторых областях индустрии. С данной ситуацией необходимо бороться. При разработке программного обеспечения безопасность является одной из самых важных частей работы [7].

Если говорить о безопасности со стороны сервера, то следует изучить, какие появились нововведения в Node.js 10 в области разработки и безопасности. Недавно, 24 апреля 2018 года [9] был выпущен Node.js 10.0.0. Это — седьмой основной релиз платформы. Он, в октябре 2018, получит статус LTS. В Node 10.0.0 добавлена поддержка криптографической библиотеки OpenSSL 1.1.0, которая поддерживает протоколы TLS/SSL. Благодаря этой библиотеке появилась возможность работать с потоковым шифром ChaCha20 и алгоритмом аутентификации сообщений Poly1305. В октябре планируется расширить набор поддерживаемых криптографических технологий. Речь идёт о поддержке режимов шифрования AEAD, которые применяются для организации безопасного обмена сообщениями, и о поддержке дополнительных криптографических библиотек.

При выпуске npm 6.0 особое внимание было уделено безопасности. Отчасти это было вызвано результатами одного исследования, которое показало, что 97% JavaScript-разработчиков во всём мире полагаются, по крайней мере, в некоторых своих разработках, на опенсорсные проекты. При этом 77% разработчиков беспокоятся о безопасности подобных решений. Для того чтобы лучше документировать и исправлять уязвимости модулей и потенциальные конфликты зависимостей, компания npm приобрела проект Node Security Platform. Этот проект является основным источником сведений об уязвимости JS-пакетов.

Npm 6.0 поддерживает новую команду, направленную на анализ проблем с безопасностью: npm audit. Она позволяет рекурсивно анализировать деревья зависимостей для обнаружения потенциальных конфликтов и проблемных мест. Это позволяет разработчикам заблаговременно, не дожидаясь возникновения проблем, заменять в своих проектах устаревшие пакеты на их более новые версии, или переходить на другие пакеты, если те, что они используют, могут вызвать нежелательные эффекты [8].

Что касается защиты клиентской части, одной из наиболее распространённых ошибок является вставка HTML, позволяющая третьим лицам внедрять JavaScript в контекст безопасности информационного ресурса. Это позволяет злоумышленнику контролировать действия пользователя, полностью нарушая безопасность учетной записи. Однако безопасность на стороне сервера должна не зависеть от безопасности клиентской части. При разработке необходимо предусмотреть, что злоумышленники могут изменять HTML/CSS/Javascript информационного ресурса, чтобы попытаться получить доступ к закрытой информации и отправить на сервер данные, которые не могут быть отправлены через обычный интерфейс. Чтобы защититься от этого, необходимо проверять все пользовательские входы - рассматривать это как полностью ненадежные данные и проверять всё, что принимается сервером [10].

**Литература**

1. Программная платформа Node.js // Ubuntu. URL: http://help.ubuntu.ru/wiki/javascript (дата обращения: 15.06.2018).
2. Выразительный JavaScript: Node.js // Habr. URL: https://habr.com/post/245775/ (дата обращения: 15.06.2018).
3. Проаспэт, А.Г. Использование языка CoffeeScript для разработки системы управления контентом интернет-ресурса / А.Г. Проаспэт // сборник статей Международной научно-практической конференции 15 января 2018 г. г. Москва. [Электронный ресурс]– М.: Импульс, 2018. – 932 с.
4. Могу ли я использовать CoffeeScript вместо JS для node.js? // qa.ru. Поиск вопросов и ответов по программированию. URL: http://qaru.site/questions/34463/can-i-use-coffeescript-instead-of-js-for-nodejs (дата обращения: 15.06.2018).
5. Выбираем язык для веб-разработки // GeekBrains. URL: https://geekbrains.ru/posts/road\_to\_web\_development (дата обращения: 15.06.2018).
6. Developer Survey Results // Stack Overflow. URL: https://insights.stackoverflow.com/survey/2017#most-popular-technologies (дата обращения: 15.06.2018).
7. Безопасность. Node Hero: Глава 11 // Medium. URL: https://medium.com/devschacht/node-hero-chapter-11-c35c590f518e (дата обращения: 15.06.2018).
8. Node.js 10.0.0, What to expect as a Backend developer/Security enthusiast? // codeburst.io. URL: https://codeburst.io/node-js-10-0-0-what-to-expect-as-a-backend-developer-security-enthusiast-f8680f132320 (дата обращения: 15.06.2018).
9. Node v10.0.0 (Current) // Node.js. URL: https://nodejs.org/en/blog/release/v10.0.0/ (дата обращения: 15.06.2018).
10. Риски безопасности Javascript? // qa.ru. Поиск вопросов и ответов по программированию. URL: http://qaru.site/questions/365414/javascript-security-risks (дата обращения: 15.06.2018).

79647204962@mail.ru