

Защита JavaScript кода с помощью обфускации

Азаров Андрей Евгеньевич

Приамурский государственный университет им. Шолом-Алейхема

Студент

Аннотация

Доступ к исходному коду веб сайта может понизить безопасность любого сетевого ресурса. Данное исследование о методе шифрования кода языка сценариев, javascript — обфускация. Данный метод позволяет зашифровать javascript код до невозможности его прочтения, но код также будет успешно выполняться в браузере клиента.

Ключевые слова: защита данных, информационная безопасность, javascript, обфускация.

Protect JavaScript code with obfuscation

Azarov Andrey Evgenevich

Sholom-Aleichem Priamursky State University

Student

Abstract

Access to the source code of a web site can reduce the security of any network resource. This study is about a method of encrypting a scripting language code, javascript - obfuscation. This method allows you to encrypt javascript code until it is impossible to read it, but the code will also be successfully executed in the client browser.

Keywords: data protection, information security, javascript, obfuscation.

По данным компании VeriSign являющаяся авторитетным реестром доменов верхнего уровня, в интернете насчитывается 342,4 млн доменных имен. Чем больше сайтов, тем больше уязвимостей могут найти и использовать потенциальные взломщики. В отличии от настольных приложений под операционные системы, все сайты используют одни и те же технологии и языки, такие как html, css, php и javascript. Популярность и повсеместность использования языка javascript для написания сценариев, выполняемых на стороне клиента сайта, привлекает множество взломщиков. Потенциальные хакеры имея возможность изучить исходный код сайта могут воспользоваться недоработками в коде в личных интересах, например, внедрить в форму авторизации переадресацию введенных данных, если станет известно после изучения кода, что формы не валидируются.

Для борьбы со злоумышленниками, разработчики используют различные способы – это и валидации всех форм ввода, и обязательная

регистрация для использования сайта, использование различных видов шифрования, каждый из методов по отдельности полезен, но стоит использовать все методы защиты веб-сайта сразу. На любом сайте код javascript может просмотреть любой человек, поэтому для защиты и его необходимо скрыть. Одним из современных способов защиты исходного javascript кода веб-сайтов является обфускация кода.

Обфускация («obfuscation» – запутывание) – это один из методов защиты

программного кода, который позволяет усложнить процесс реверсивной инженерии кода защищаемого программного продукта. С одной стороны – любой человек также при желании будет иметь возможность просматривать исходный код сайта, эту возможность запретить невозможно, однако после процедуры обфускации данный код невозможно будет понять и следовательно изучить.

Цель данного исследования – изучить методы защиты кода с помощью обфускации.

Тема обфускации кода рассматривается не так давно по сравнению с другими аналогичными проблемами касающиеся информационной безопасности. В исследовании 2011 года, обфускация кода в контексте проблемы защиты программных продуктов [1] проводится классификация современных методов защиты программных продуктов. Предоставляется определение процесса обфускации. Сравняются методы запутывания и методы анализа программ. Также данный вопрос рассматривался А.Ю. Никольской и А.Д. Хлестовым в их общем исследовании [2] указано, что на 2015 год, процесс обфускации являлся одним из самых популярных и часто используемых методов защиты. В 2016 году М.В. Пономарев на конференции — Наука XXI века: проблемы, поиски, решения [3], также, как и вышеперечисленные авторы, описывал виды обфускации и методы модификации кода.

К 2018 году тенденция на защиту кода с помощью обфускации сохраняется, поэтому данный метод необходимо изучить детальнее.

Обфускация касается не только javascript кода, но так как данный вид кода наименее защищён от посторонних глаз, то и современные средства для обфускации ориентированы в основном на код данного языка программирования.

Процедур обфускации существует множество. Сделать код нечитаемым можно с помощью лексического приёма. Необходимо из кода удалить все комментарии, пробелы, отступы, замену имен идентификаторов (имен переменных, массивов, структур, хэшей, функций, процедур и т.д.) на произвольные длинные наборы символов, которые трудно воспринимать человеку, добавление различных личных операций, которые не используются в самих расчётах. На рисунке 1 изображен пример одного и того же кода, но второй обфусцирован с помощью лексического способа. Чтение данного кода уже затруднено в разы, но все также возможно, особенно если использовать встроенные средства отладки любого современного браузера.

обфусцирующие код являются отличным инструментом для защиты вашей работы от кражи или эксплуатации кода посторонними лицами. В данной работе были приведены основные методы обфускации, проведено исследование методов защиты кода javascript. Для максимальной защиты кода методом обфускации рекомендуется сначала использовать лексический метод и далее полный, комбинируя эти методы можно очень качественно защитить свой код.

Библиографический список

1. Лысых В.В. Обфускация кода в контексте проблемы защиты программных продуктов // информационные системы и технологии. 2011. №2 (64). С. 95-102.
2. Никольская К.Ю., Хлестов А.Д. Обфускация и методы защиты программных продуктов // Вестник УРФО. Безопасность в информационной сфере. 2015. №2 (16). С. 7-10.
3. Пономарев М.В. Обфускация как метод защиты программного продукта // Наука XXI века: Проблемы, поиски, решения. Миасс: Геотур, 2016. С. 60-63.