УДК 004.(491+738.5.057.4):65.012.8

АНАЛИЗ АТАКИ ТИПА МЕЖСЕТЕВОЙ СКРИПТИНГ

Герасименко А.В., Баранов А.А.
Государственный ВУЗ «Национальный горный университет», nmu.org.ua, alex0392@gmail.com

Многие сайты, такие как форумы, блоги, социальные сети и т.п., стреляться предоставить пользователю возможность вставлять на страницу свой контент. Для удобства пользователей изобретаются редакторы, делающие процесс добавления красивого комментария легким и приятным. Но за всем этим скрывается угроза безопасности. В данной статье рассмотрены основные понятия, касающиеся XSS-атак и методов борьбы с ними.

Ключевые слова – XSS; межсайтовый скриптинг; угроза.

ВВЕДЕНИЕ

XSS (Cross Site Scripting) – межсайтовый скриптинг. Это тип атаки на уязвимые интерактивные информационные системы в вебе. XSS-уязвимость – это уязвимость на сервере, которая позволяет внедрить в генерируемую и затем передаваемую пользователю страницу формата HTML некий произвольный код, порой весьма вредоносный.

ПРИНЦИП АТАКИ

Для проведения атаки используется так называемая нефильтруемая переменная – такая переменная, которая перед ее использованием в скрипте не проверяется на корректность и наличие в ней запретных символов. Вначале значение данной переменной передается от страницы, загруженной в браузере пользователя, некоторому скрипту. А если злоумышленник подставит в передаваемые значения некоторый код, то данный код выполнится интерпретатором без всяких условий. Достаточно лишь найти эту самую XSS-уязвимость.

Данная уязвимость преимущественно присутствует на страницах, где допустим прямой вывод пользовательского html кода в необработанном виде. Если пользователь откроет зараженную страницу - на его компьютере выполнится скрипт, который может выполнить потенциально опасные действия, например отправить cookies на сервер злоумышленника, что может позволить злоумышленнику авторизоваться на сайте от имени пользователя.

Также злоумышленник может переадресовать пользователя на другой ресурс, где, пользователь, авторизовавшись, передаст в руки злоумышленников свои пароли и логины в открытом виде.

При наличии XSS-уязвимости у злоумышленника также появляется возможность, помимо кражи cookies, осуществить кражу конфиденциальной информации – об установленной операционной системе, текущем IP-адресе, посещенных пользователем сайтах, о браузерах, используемых на компьютере и т.д.

Так же возможно значительно замедлить работу сайта, если поместить в его код скрипт, производящий загрузку большого объема данных (или небольшого объема, но с медленных серверов).

МЕХАНИЗМ ОБНАРУЖЕНИЯ АТАКИ

Для обнаружения данной уязвимости можно проанализировать фильтрацию данных, вводимых пользователями. Так же можно попробовать добавить скрипт (например alert(‘Ups’);) на страницу всеми возможными способами. В случае успеха – исправить фильтры, отвечающие за обработку данных содержащих скрипт.

МЕХАНИЗМ ЗАЩИТЫ

Для того чтобы обезопасить себя от данного типа атак необходимо фильтровать все данные, вводимые пользователями на предмет возможных скриптов. Данные скрипты могут находиться как в html тэгах, так и в их атрибутах вида OnClick и др. Так же следует держать под контролем остальные данные, поступающие в скрипт извне.

Еще один способ защиты – ассоциировать с сессией ключ, который будет передаваться посредством POST-запросов и проверяться сервером, во время каждого такого запроса. Это сделает бесполезной кражу cookies (информация будет бесполезна без данного ключа).

Также методом защиты служит типизация всех недоверенных данных. Как можно ближе к месту появления таких данных в компоненте, необходимо обеспечить их приведение к ожидаемым типам. Реализация типизации дает гарантию, что в компоненте будут обрабатываться данные именно тех типов, на работу с которыми он рассчитан.

Сразу после типизации, семантику полученных объектов необходимо проверить на соответствие функционалу компонента. Например, для целочисленных типов или даты/времени – это будет проверка диапазона (например, появление в нем, отрицательных номеров страниц или сумм денежного перевода соответствует ожиданиям функционала), для строковых, в большинстве случаев, будет достаточно проверки на соответствие регулярным выражениям, а для объектов более комплексных типов необходимо реализовывать проверку семантики каждого из его полей и свойств.

ВЫВОДЫ

Сложность этой атаки состоит в том, что алгоритм фильтрации входящих данных не должен создавать необоснованных ограничений легальным пользователям, но в то же время должен делать невозможной XSS-атаку со стороны злоумышленника. Противодействие атакам данного

типа должно идти в качестве второго эшелона защиты и не должно использоваться в качестве средства устранения уязвимостей.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Межсайтовый_скриптинг (Электрон. ресурс) / Способ доступа: URL: http://ru.wikipedia.org/wiki/ Межсайтовый_скриптинг

2. Вся правда об XSS или Почему межсайтовое выполнение сценариев не является уязвимостью? (Электрон. ресурс) / Способ доступа: URL: http://habrahabr.ru/post/149152/

3. XSS уязвимость (Электрон. ресурс) / Способ доступа: URL: http://thelocalhost.ru/xss-uyazvimost-dlya-novichkov/