Алексей ФОРТУНА, МЭА

БЕЗОПАСНОСТЬ WEB 2.0 ПРИЛОЖЕНИЙ

Abstract: *Ajax, RIA and web-services are critically important new generation components of web-applications. In current report are widely covered only some of possible security problems of these technologies.*

WEB 2.0 – это новый термин, применяемый для нового поколения web-приложений. Появление приложений такого типа внесло ряд новых проблем безопасности. На сегодняшний день атаки на WEB-приложения являются наиболее серьезной угрозой безопасности ИТ инфраструктур, из-за которых подвергаются риску конфиденциальная корпоративная информация и конфиденциальные данные пользователей.

Межсайтовый скриптинг в AJAX во много раз увеличил опасность XSS атак. Примером того могут послужить новые черви, распространяющиеся через WEB 2.0 приложения. Они в основном написаны на JavaScript и распространяются с огромной скоростью. Уже пострадали от нового вида червей такие проекты как, MySpace и Yahoo Mail. WEB 2.0 базирующиеся приложения очень часто используют AJAX. И разработчики очень часто используют проверку данных на стороне клиента и забывают производить повторную проверку на серверной стороне, что в большинстве случаев приводит к XSS и SQL инъекциям.

С ростом популярности XML, как основного языка онлайновых бизнес-транзакций, атаки на SOAP WEB-сервисы становятся все более частыми.

Атака направлена на конечную точку (сервер) с целью произвести несанкционированные действия, например, получить или уничтожить данные либо манипулировать содержимым SOAP-сообщений. В результате сервер потребляет избыточные ресурсы и в конце концов перестает отвечать на запросы. Данный вид атаки может привести к раскрытию информации либо вызвать отказ сервиса.

Еще одним видом атаки на WEB-сервисы, использующие SOAP как протокол обмена данными, являются XPATH-инъекции. Часто большие XML-файлы содержат добавленные конечным пользователем секции когда, формирующие отрывки XPATH, за счет которых уязвимым становится весь документ. Если внедренный код запускается успешно, взлом может спровоцировать потерю данных. Единственный способ блокировать этот способ проникновения – проверять XPATH запросы, прежде чем передавать в ответ на них ценную информацию.

RSS и Atom ленты тоже привнесли свои проблемы. RRS /Atom инъекции – это новый вид атак, позволяющих внедрить в RSS / Atom ленты злонамеренный код. Данных вид атаки может привести к похищению cookies, а в худшем случае к выполнению вредоносного кода. Также данный вид атаки очень хорошо подходит для распространения спама.

Rich Internet Applications (RIA) – это приложения с очень богатым пользовательским интерфейсом (Flash, ActiveX Controls, Апплеты). В последнее время очень часто разработчики переносят логику аутентификации и других важных процессов WEB-приложений во flash-ролики и java-апплеты, забывая о том, что RIA приложения можно довольно легко декомпилировать и изменить логику работы приложения.

Из-за простоты использования приложения, которую во многих случаях хотят добиться разработчики, возникают также серьезные проблемы безопасности. Например, чтобы не утруждать пользователя системы при восстановлении пароля кликать на ссылку и запоминать новый сгенерированный пароль, разработчики зачастую принимают решение хранить пароли в открытом виде, и на запрос о забытом пароле просто высылается письмо на адрес владельца с его паролем.

Злоупотребление функциональными возможностями приложений является не новым видом атаки на web-приложения, но в WEB 2.0 приложениях из-за очень насыщенного пользовательского интерфейса данный вид атаки становится все более распространенным. Данные атаки направлены на использование функций Web-приложения с целью обхода механизмов разграничение доступа. Некоторые механизмы Web-приложения, включая функции обеспечения безопасности, могут быть использованы для этих целей. Наличие уязвимости в одном из, возможно, второстепенных компонентов приложения может привести к компрометации всего приложения. Уровень риска и потенциальные возможности злоумышленника в случае проведения атаки очень сильно зависят от конкретного приложения.

Методы анализа WEB 2.0 приложений.

Одним из основным инструментов анализа WEB 2.0 приложений являются WEB-краулеры (web crawler). Это поисковые роботы, переходящие по ссылкам WEB-ресурсов и умеющие обрабатывать вызовы AJAX. Они позволяют сократить время на поиск всех мест, где происходят AJAX- вызовы.

Для анализа клиентских Ajax-приложений необходимо рассмотреть каждое из событий досконально, чтобы не потерять логику работы приложения. Один из путей анализа работы – это построчный разбор всего кода. Лучшим средством анализа является браузер Firefox. С помощью его плагинов, таких как Firebug и WEB-Developer можно

производить отладку и анализ яваскриптов любой сложности.

Заключение

Ajax, Rich Internet Applications и WEB-сервисы критически важные компоненты нового поколения web-приложений. Чтобы идти в ногу с этими технологиями и соблюдать новые стандарты безопасности необходимо использовать разные методологии и инструменты. Один из них – эффективное использование браузера.

Литература:

1. Фактор XML, Лори Маквитти (http://www.ccc.ru/magazine/depot/04_13/print.html?0203.htm)
2. Top 10 Web 2.0 Attack Vectors, Shreeraj Shah (http://www.net-security.org/article.php?id=949)
3. AJAX. Не повторяйте ошибок, Никита Вакорин (http://www.umade.ru/log/2005/06/73.html)
4. Web Application Security Assessment, Chaudhry, S. Clarke, S. Veney, E. Rachner, J. Sutton