электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

 # 02, февраль 2016

УДК 004.056.53

Оценка количества и типов атак на веб-приложения

***Смолянинова К.А.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»

Научный руководитель: Алешин В.А., к.т.н, доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Информационная безопасность»
v.aleshin@bmstu.net

За последние шесть месяцев наблюдались некоторые очень интересные тенденции при сравнении стран, где порождаются различные атаки и стран, на которые направлены эти атаки. Чтобы показать эти результаты, специалисты охарактеризовали и представили данные в отношении наиболее распространенных категорий атак. Анализ, проведенный для этого доклада, определяет эти категории атак, как угрозы с высокой степенью риска для большинства, если не для всех сетей, и поэтому, они должны быть на первом месте у специалистов по безопасности [1]. Это HTTP атаки на серверной стороне, HTTP атаки на клиентской стороне, PHP Remote File Include, Cross-Site Scripting и наконец, SQL-инъекции. Как и следовало ожидать, есть некоторые перекрытия в этих категориях, последние три являются подмножеством первых двух категорий.

SQL инъекции включают в себя «SQL инъекции, использующие SQL оператор Select», «SQL инъекции, использующие строковые функции», и, «SQL инъекции с использованием логической идентификации». Наиболее заметны «PHP Remote File Include» атаки, которые ищут небольшой запрос HTTP, который включает в себя ссылку на другой сайт как параметр, содержащий очень специфический метод уклонения, используемый большим количеством атак для повышения надежности своих атак. Также следует отметить очень специфическую атаку против приложения «Zeroboard PHP». Последний тип атаки, включенный в эту статистику является одним из наиболее распространенных – «HTTP Connect Tunnel», которая остается главной атакой на серверную сторону HTTP. Эти атаки используются, для отправки спама через неправильно сконфигурированные сервера HTTP.

На рисунке 1 видно, что Соединенные Штаты являются главной целью атаки для категории атак на серверную сторону HTTP.

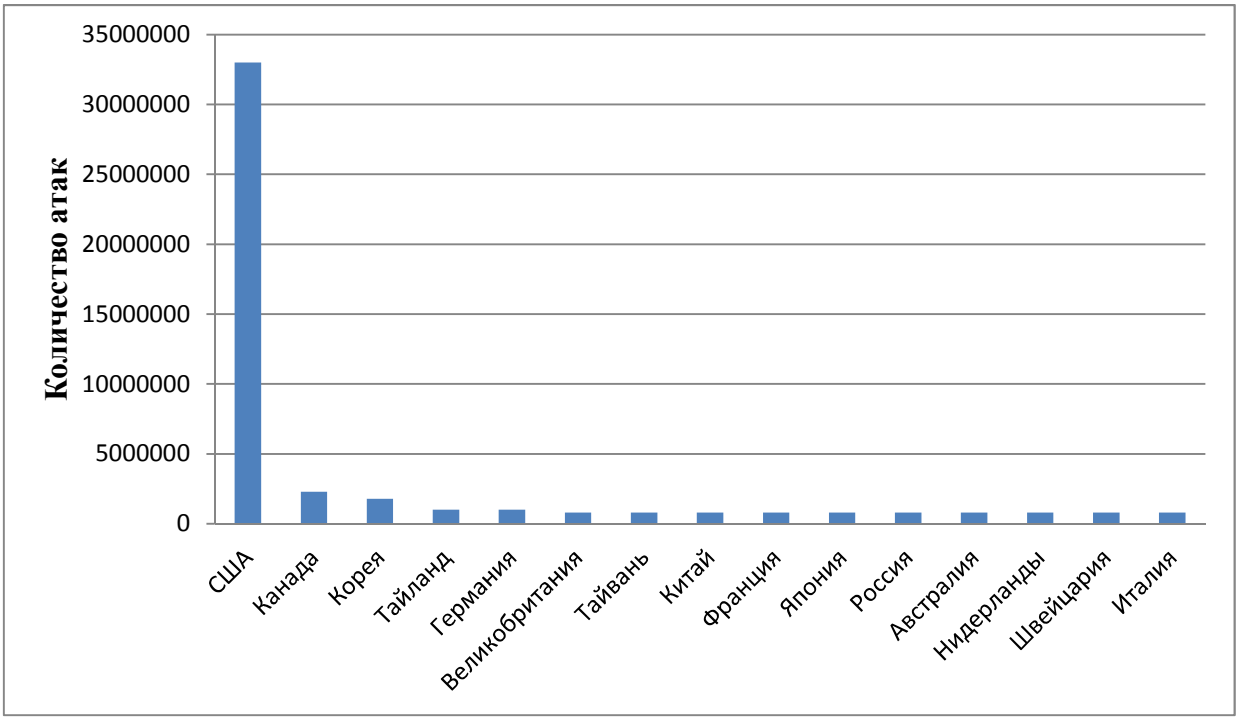

Рис. 1. Страны, которые являются целью атаки на серверную сторону

В течение многих лет атаки, нацеленные на США, представляли большую ценность для злоумышленников, поэтому в этой статистике нет ничего удивительного.

За последние шесть месяцев было обнаружено много SQL иньекций. Некоторые типичные ситуации возникали в США, которые лидируют как в топе источников угроз, так и в топе целей SQL инъекций.

SQL инъекции можно разделить на две подкатегории: *легитимные SQL-инъекции (legitimate SQL Injection – англ.)* и вредоносные SQL-инъекции. Многие веб-приложения в интернете по-прежнему используют SQL-инъекции для нормального функционирования. Разница в целях. Веб-приложения, которые на законных основаниях используют SQL инъекции, гарантированно будут уязвимы для инструментов и методов, используемых злоумышленниками для выполнения вредоносных SQL-инъекций. Серверы, содержащие эти приложения более подвержены риску не только потому, что являются уязвимыми, но и потому что они должны различать законные и вредоносные инъекции для определения атаки.

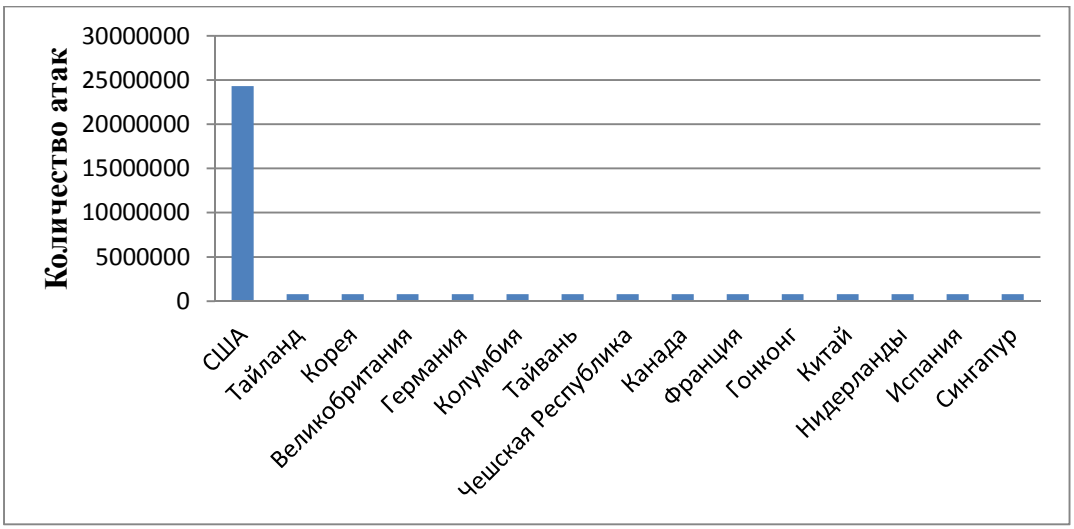

Рис. 2. Страны, которые являются целью для SQL-инъекций

На рисунке 2 видно широкомасштабное число SQL-инъекций, отмеченных в разделе атак на серверную сторону HTTP.

Очень большой всплеск SQL-инъекций в июле был в основном вызван онлайн рекламой, которая распространяла код для многих филиалов, используя SQL инъекции, в качестве функционала.

Приложение быстро разошлось, приводя к значительному провалу некоторых мероприятий в августе.

Источники таких атак более разнообразны, чем цели. Китай в настоящее время является крупнейшим источником за пределами Соединенных Штатов.

Опять же в подавляющем большинстве место для этих атак – Соединенные Штаты (рис.3).

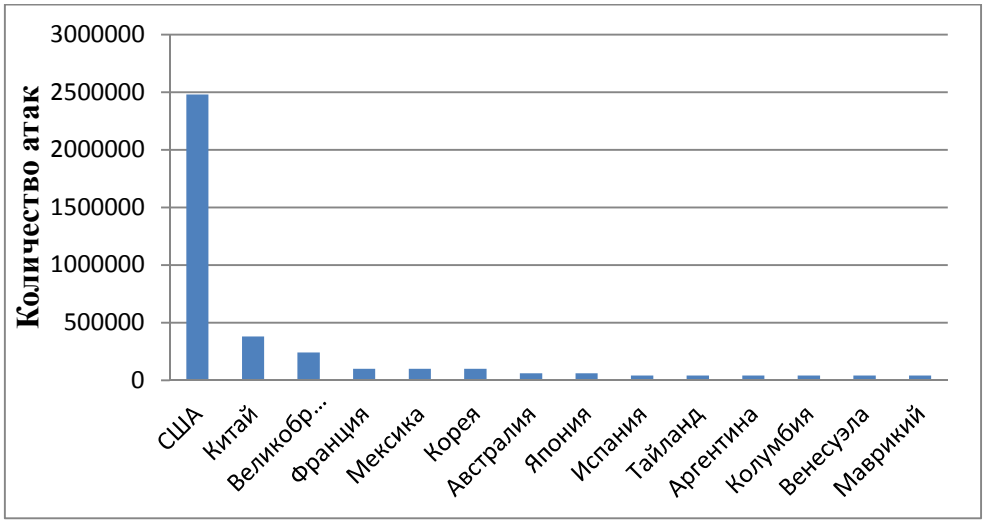

Рис. 3. Источники SQL-инъекций

Хотя атаки «PHP File Include» были популярны, сейчас очевидно заметное снижение их в общем количестве атак. За исключением основных атак из Таиланда в апреле, число «PHP File Include» атак в августе составили меньше половины среднего числа с марта.

Существует много способов для защиты от таких атак. Настройка Apache, обработка ввода и оборудование безопасности сетей очень хорошо сдерживают эти атаки, так что вполне вероятно, что падение общего числа атак связанно с использованием этих средств разработчиками приложений, системными администраторами и специалистами по безопасности. Тем не менее, в связи с чрезвычайной простотой этой атаки и огромного преимущества (произвольный код PHP выполняется на сервере), такие атаки, скорее всего, останутся популярными в течение некоторого времени.

Основные источники «PHP File Include» атак приведены на рисунке 4.

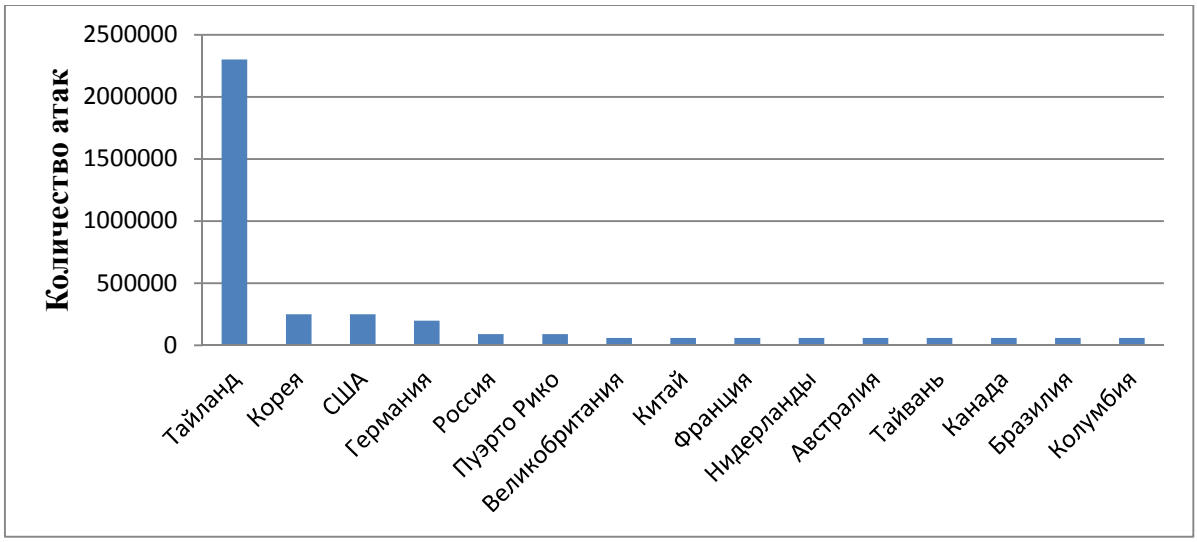

Рис. 4. Источники атак PHP File Include

Cross Site Scripting (XSS) является одной из наиболее распространенных ошибок в современных веб-приложениях. К сожалению, разработчики часто попадают в ловушку введения XSS ошибки при создании кода, который соединяет все различные веб-технологии. Другими весьма распространенными «пользователями» XSS является различные рекламные и аналитические системы. Например, *баннер (banner – англ.)* рекламодателя, который отображает некоторый JavaScript на HTTP сервере рекламодателя для отслеживания результатов, может быть встроен в веб-страницу. Тем не менее, в данном случае, есть небольшой риск, что сайт, о котором идет речь (обычно) имеет полный контроль над страницей, запрос на сайт рекламодателя как правило, не

вредоносный. Эти отражения, наряду с атаками, которые используют недостатки в обработке данных, составляют подавляющее большинство XSS атак, которые были известны за последние шесть месяцев.

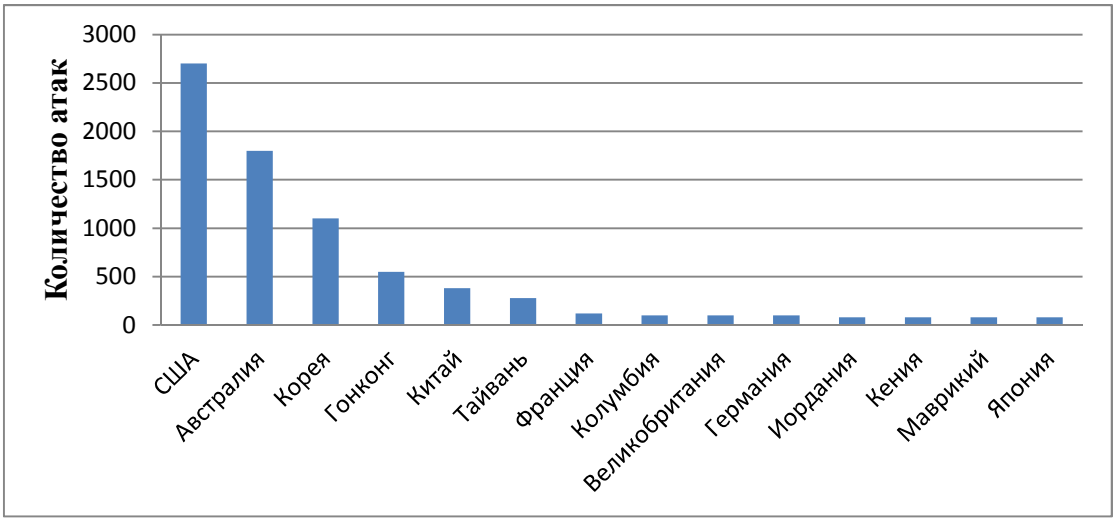

Рис. 5. Источники XSS атак

На рисунке 5 представлены страны, которые являются источниками XSS атак за последние шесть месяцев. Атаки из США постоянно снижались месяц за месяцем. В Республике Корея замечено снижение на 50% за последние 30 дней. Однако, эти два события, были скомпенсированы резким увеличением на 20% атак из Австралии.

Пример реального использования клиентской стороны HTTP.

В этом разделе показан пример реальной атаки против организации, что привело к потере важных для организации данных.

В ходе этой атаки «Acme Widgets Corporation» был нанесен серьезный ущерб от злоумышленников, которые подвергли опасности всю инфраструктуру внутренней сети, используя два самых мощных и распространенных типа атак на сегодня: эксплуатация программного обеспечения клиента, и атаки pass-the-hash против Windows.

Шаг 1: Атакующий размещает контент на доверенном сайте.

На первом шаге, злоумышленник размещает *контент (content – англ.)* на доверенных сторонних веб-сайтах, например, в социальных сетях, блогах, сервисах обмена фотографиями или видео, или на любой другой веб-сервер, который принимает контент, размещенный рядовыми пользователями. Контент атакующего включает *эксплойт (exploitation – англ.)* для необновленного программного обеспечения на стороне клиента.

Шаг 2: Эксплутация клиентской стороны.

На шаге 2 пользователь во внутренней корпоративной сети Acme Widgets просматривает страницы в интернете с машины Windows, через необновленную на стороне клиента программу, например, медиа-плеер (Real Player, Windows Media Player, ITunes, и т.д.), программу просмотра документов (например, Acrobat Reader) или компонента офисного пакета (например, Microsoft Word, Excel, Powerpoint и т.д.). После получения контента атакующего с сайта, браузер пользователя вызывает уязвимую программу на стороне клиента, через эксплойт. Этот эксплойт позволяет злоумышленнику устанавливать или выполнять программы на зараженном компьютере, используя привилегии пользователя, запустившего браузер.

Атака частично скомпенсирована, потому что пользователь-жертва не имеет прав администратора в этой системе. Тем не менее, злоумышленник может запускать программы с ограниченными правами пользователя.

Шаг 3: Создание *бэкдора (backdoor – англ.),* использующего HTTPS.

На шаге 3, эксплойт атакующего устанавливает бэкдор на компьютер жертвы. Эта программа дает злоумышленнику доступ к зараженной машине через командную строку, связь между этой системой и системой атакующего осуществляется по протоколу HTTPS. Бэкдор шифрует исходящий трафик, поскольку на предприятии установлен *фаервол (firewall – англ.).*

Шаги 4 и 5: Дамп хешей (dump hashes – англ.) и использование Pass-The-Hash атаки на опорную точку.

На шаге 4, злоумышленник использует командный доступ к системе жертвы, чтобы загрузить программу эксплойт с локальными привилегиями пользователя. Эта программа позволяет злоумышленнику перейти с ограниченных привилегий пользователя к полному доступу к системе на этой машине. Хотя производители часто выпускают *патчи (patches – англ.),* чтобы остановить атаки на изменение привилегий, многие организации не устанавливают такие патчи достаточно быстро, потому что такие предприятия, как правило, сосредотачиваются исключительно на исправлении уязвимостей дистанционного доступа. У злоумышленника теперь есть дамп хэшей паролей для всех учетных записей на этом локальном компьютере, в том числе локальная учетная запись администратора в системе.

На шаге 5, вместо взлома пароля локального администратора, злоумышленник использует программу pass-the-hash для Windows для аутентификации к другой машине Windows во внутренней сети предприятия, с полностью обновленной клиентской

системой, на которой этот же пользователь имеет полный административный доступ. Используя NTLMv1 или NTLMv2, машины на Windows используют хэши, а не пароли для аутентификации доступа к сети через SMB протокол, позволяя злоумышленнику получить доступ к файловой системе или запускать программы на полностью обновленной системе с правами локального администратора. Используя эти права, атакующий сбрасывает хэши паролей для всех локальных учетных записей на этой машине Windows.

Шаг 6: Pass the hash для получения доступа над *контроллером домена (domain controller – англ.).*

На шаге 6, злоумышленник использует хэш пароля от локальной учетной записи на обновленном клиенте Windows для доступа к системе контроллера домена, снова используя атаку pass-the-hash, чтобы получить командный доступ к контроллеру домена. Так как пароль для локальной учетной записи администратора совпадает с паролем для учетной записи администратора домена, хэши паролей идентичны. Таким образом, злоумышленник может получить полный доступ к контроллеру домена с правами администратора, что дает атакующему полный контроль над всеми другими учетными записями и машинами в этом домене.

Шаги 7 и 8: Отступление.

На шаге 7, с полными привилегиями администратора домена, атакующий ставит под угрозу сервер, где хранятся секретные данные организации. На шаге 8, злоумышленник извлекает конфиденциальную информацию, состоящую более чем из 200 мегабайт данных. Злоумышленник загружает эти данные через интернет с сервера, используя HTTPS для шифрования, сводя к минимуму вероятность обнаружения.

Заключение

В статье рассмотрена проблема безопасности веб-приложений, которая является очень актуальной в настоящее время. С каждым годом количество атак на веб-приложения увеличивается. Разработчики устраняют одни уязвимости, но злоумышленники находят все новые и новые, нанося серьезный ущерб компаниям.

Анализ источников и целей атак, проведенный в статье, показывает, что наибольшее количество атак приходится на США. Причем США являются как источником, так и целью для атак.

Список литературы

[1]. Низамутдинов М. Ф. Тактика защиты и нападения на Web-приложения. СПб.: БХВ-Петербург, 2010. 432 с.

[2]. The Top Cyber Security Risks September 2011. Available at: http://www.tippingpoint.com, accessed 20.03.2015.

[3]. Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines. Available at: http:// http://csis.org/files/publication/Twenty_Critical_Controls_for_Effective_Cyber_Defense_CAG.ppd, 21.03.2015.