Статистика уязвимостей WEB-приложений в 2006 году

Сергей Гордейчик

gordey @ ptsecurity.com

Содержание

Введение

Согласно отчету корпорации Mitre [1] более четверти уязвимостей, обнаруженных в 2006 году приходится на проблемы безопасности Web-приложений. Проблемы с безопасностью в Web-приложениях достаточно легко обнаружить и использовать. В связи с этим "взлом через порт 80", является популярным инструментом в арсенале злоумышленника. Отчет «Internet Security Threat Report» [2] компании Symantec показывает, что до семидесяти процентов уязвимостей, используемых злоумышленниками, приходится на Web-приложения.

В отличие от операционных систем, СУБД и прикладного ПО, используемые в корпоративной сети Web-приложения, как правило, не проходят тщательный контроль качества. Для корректной оценки рисков, связанных с безопасностью WEB-приложений необходима достоверная информация о распространенности различных классов уязвимостей в Web-приложениях, вероятности обнаружения ошибок различного рода.

В данной публикации приведена статистика по уязвимостям Web-приложений, полученная компанией Positive Technologies в ходе работ по оценке защищенности сетей в 2006. В статье представлены данные, основанные на результатах двух видов работ: автоматизированного сканирования узлов публичного хостинг-провайдера и ручного анализа защищенности Web-приложений.

При расчете статистики уязвимости были сгруппированы на основе классификации угроз Web-приложений, разработанной Web Application Security Consortium [3]. Данная классификация представляет собой попытку собрать воедино и организовать угрозы безопасности Web-приложений. Члены Web Application Security Consortium создали этот проект для разработки и популяризации стандартной терминологии описания проблем безопасности Web-приложений. Наличие этого документа дает возможность разработчикам приложений, специалистам в области безопасности, производителям программных продуктов и аудиторам использовать единый язык для взаимодействия.

Распространенные уязвимости Web-приложений организованны в структурированный список, состоящий из шести классов:

1. Аутентификация (Authentication).
2. Авторизация (Authorization).

3. Атаки на клиентов (Client-side Attacks).

4. Выполнение кода (Command Execution).

5. Разглашение информации (Information Disclosure).

6. Логические атаки (Logical Attacks).

Для каждого из классов приведено подробное описание входящих в него разновидностей атак. Описания содержат примеры уязвимостей, приводящих к возможности реализации атаки, а так же ссылки на дополнительные материалы.

В приводимой статистике учитываются только уязвимости Web-приложений. Такие распространенные недостатки, как отсутствие актуальных обновлений безопасности ОС и неверная настройка Web-сервера не рассматриваются.

Безопасность общедоступных Web-серверов

Компания Positive Technologies совместно с хостинг-провайдером masterhost проводит постоянное бесплатное сканирование серверов, размещенных на Интернет-площадке. Сканирование проводится с помощью сканера уязвимостей XSpider 7.5 в полностью автоматическом режиме. В случае обнаружения недочетов информация об обнаруженных уязвимостях и рекомендации по устранению отправляется владельцу сервера [4].

В среднем в месяц проводится анализ 10000 различных Web-серверов. Часть из них содержит динамические Web-приложения, часть – только статический контент. Настройка политики сканирования XSpider под конкретные серверы не производится.

Всего в 2006 году было проведено 111936 сканирований, в ходе которых было обнаружено 129197 различных уязвимостей высокого и среднего уровня риска. Уязвимыми оказались 31113 сайтов. В данный отчет уязвимости низкой степени риска включены не были, в связи с низкой достоверностью обнаружения подобных ошибок в ходе полностью автоматического сканирования.

Распределение обнаруженных уязвимостей по различным классам представлено в табл. 1.

Таблица 1. Распределение уязвимостей различных классов

Уязвимость	% Уязвимостей	Уязвимые сайты
Cross-Site Scripting	72,22%	23,28%
SQL injection	14,67%	7,28%
Information Leakage	8,26%	4,20%
HTTP Response Splitting	3,47%	2,74%
SSI Injection	0,74%	0,27%
Path Traversal	0,32%	0,32%
OS Commanding	0,11%	0,03%
Directory Indexing	0,09%	0,10%
Content Spoofing	0,08%	0,06%
Bruteforce	0,05%	0,06%

В графическом виде данные статистики представлены на рисунке 1.

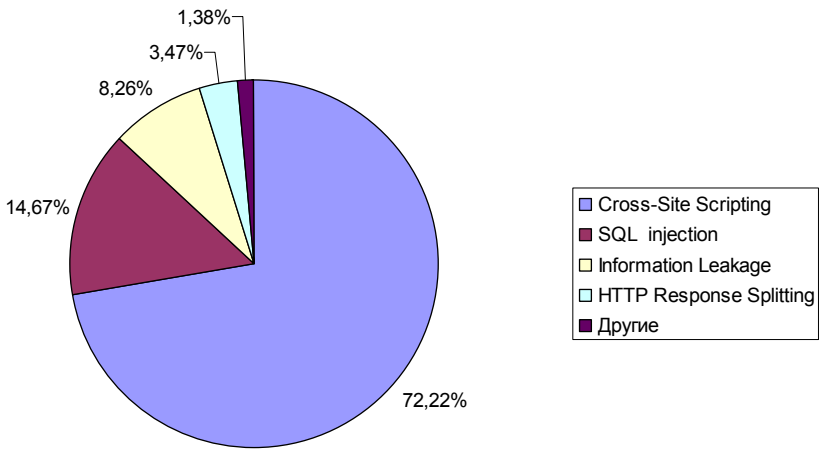

Рисунок 1 Распределение уязвимостей различных классов

На рисунке 2 представлено процент сайтов, уязвимых для разных типов ошибок.

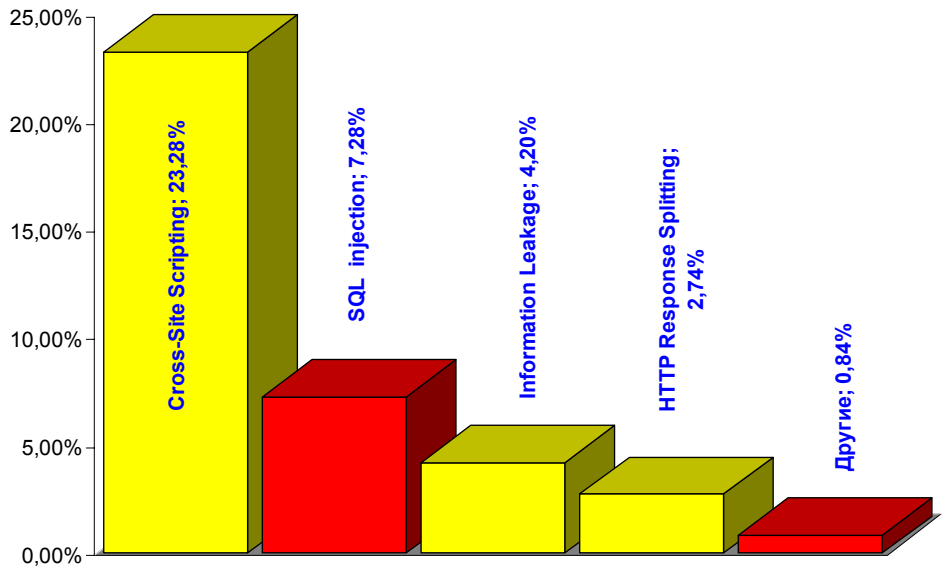

Рисунок 2. Количество уязвимых сайтов по классам

Наиболее распространена уязвимость класса «Межсайтовое выполнение сценариев» (Cross-Site Scripting, XSS). Эта ошибка средней

степени риска может использоваться для выполнения в браузере клиента произвольного кода на языках сценариев (например, JavaScript) с целью кражи идентификационных данных, подмены содержимого страниц, проведения атак типа «фишинг» и т.д. Как видно из статистики, данная уязвимость была обнаружена на 23% из всех сайтов. Количество идентифицированных XSS составляет до 72% всех обнаруженных ошибок. В среднем каждый уязвимый сайт содержит 4 уязвимости данного класса.

Вторая по полярности уязвимость класса «Внедрение операторов SQL» (SQL Injection) содержится в 7% сайтов и на неё приходится 14% общего количества ошибок. С помощью данной уязвимости злоумышленники получают возможность читать и модифицировать информацию в базе данных, используемой Web-приложением. В некоторых случаях эксплуатация SQL Injection может привести к получению полного контроля над сервером. В связи с этим, обычно уязвимости данного типа классифицируются как имеющие высокую степень риска.

На третьем месте находятся разнообразные уязвимости, приводящие к утечке важной информации с сервера (Information Leakage). На них приходится 4% серверов и 8% всех ошибок. В данную статистику включались только те из них, которые могут быть отнесены к средней степени риска.

Другие уязвимости встречаются значительно реже. На оставшиеся семь классов приходится менее 5% всех обнаруженных ошибок.

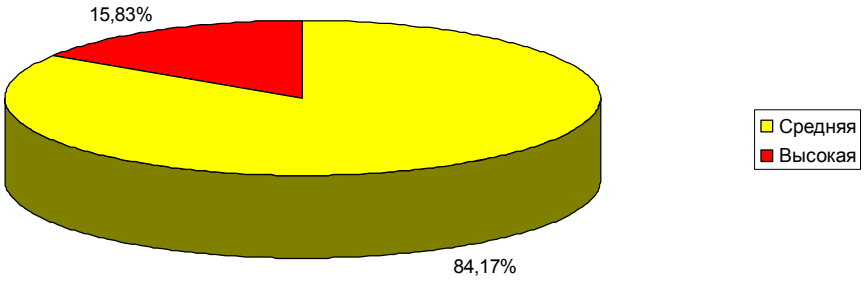

Рисунок 3. Распределение уязвимостей по степени риска

Если рассматривать распределение ошибок по степени риска, то на критичные уязвимости приходится всего 15%. Как будет показано далее, такой невысокий процент связан с ограничениями, накладываемыми используемым методом сбора данных (полностью автоматический анализ, использование единой политики сканирования для всех сайтов).

На рисунке 4 представлена суммарная вероятность обнаружения на сервере уязвимостей различной степени риска.

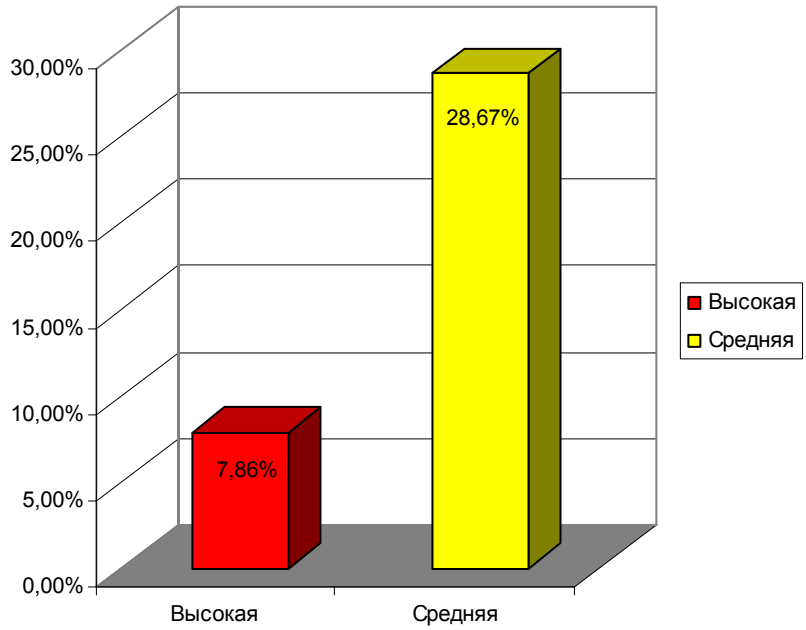

Рисунок 4 Вероятность обнаружения уязвимостей по степени риска

Безопасность корпоративных Web-приложений

Второй из представляемых вниманию читателей набор данных был получен в ходе анализа и оценки защищенности Web-приложений [5] в четвертом квартале 2006 года. Работы проводились с использованием как ручных, так и автоматизированных средств. Всего в статистику вошли данные по 35 различным Web-приложениям, таким как системы клиент-банк, электронные торговые площадки, внешние корпоративные сайты и т.д. В общей сложности на серверах было обнаружено 368 различных уязвимостей Web-приложений.

Распределение обнаруженных уязвимостей по различным классам, а также процент ошибок найденных с помощью автоматических средств представлен в табл. 2.

Таблица 2. Распределение уязвимостей различных классов

Уязвимость	% Уязвимостей	% Автоматически	% Сайтов
Cross-Site Scripting	44,8%	81%	83%
Information Leakage	21,2%	85%	80%
Predictable Resource Location	5,4%	95%	34%
SQL injection	10,1%	78%	31%
HTTP Response Splitting	3,5%	92%	29%
Insufficient Authorization	3,3%	8%	20%
Directory Indexing	3,0%	100%	20%
Insufficient Anti-automation	1,6%	0%	17%
Path Traversal	1,4%	100%	11%
Insufficient Authentication	1,1%	0%	11%
Insufficient Process Validation	1,1%	0%	11%
Bruteforce	0,8%	33%	9%
SSI Injection	1,1%	100%	6%
Content Spoofing	0,8%	100%	3%
OS Commanding	0,3%	100%	3%
LDAP Injection	0,3%	0%	3%
Weak Password Recovery Validation	0,3%	0%	3%

В отличие от статистики, полученной в ходе автоматизированного сканирования Web-серверов, ручной анализ позволил выявить гораздо большее количество ошибок. Так, уязвимость типа «Межсайтовое

выполнение сценариев» была обнаружена на 23% всех сайтов в первом случае и 83% во втором. Это связанно как с меньшей эффективностью полностью автоматизированного сканирования, так и с тем фактом, что во втором случае анализу подвергались приложения, заведомо содержащие динамический контент.

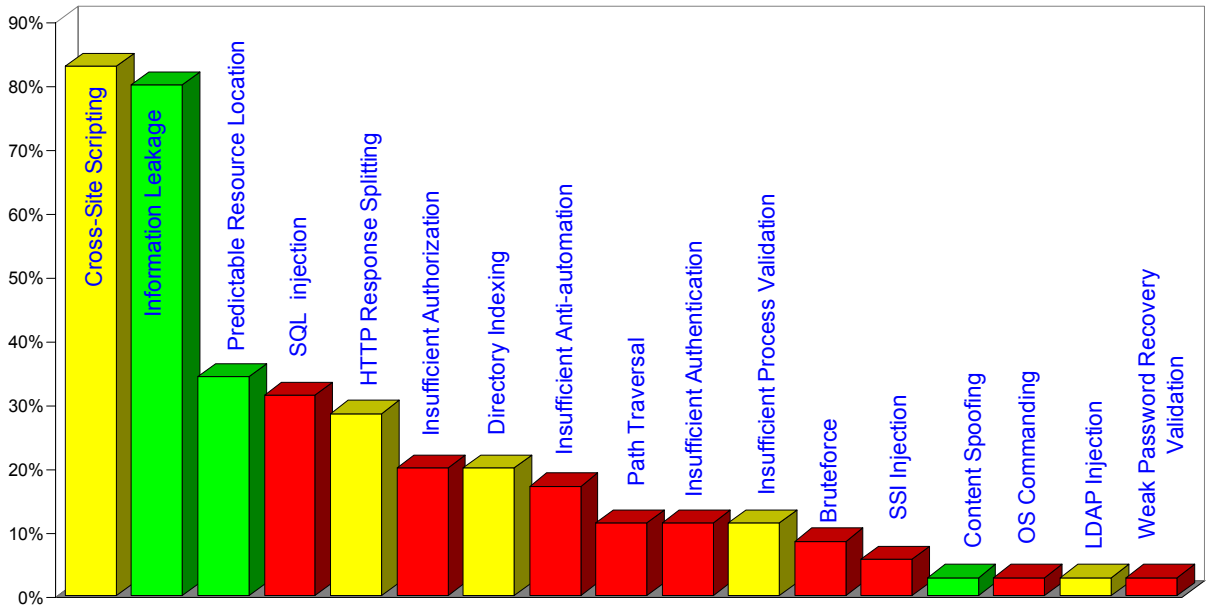

Рисунок 5. Количество уязвимых сайтов по классам

Кроме того, в статистике появились новые классы уязвимостей, такие как «Недостаточная аутентификация и авторизация» («Insufficient Authorization», «Insufficient Authentication») и др. Это связанно в первую очередь с тем, что данные недочеты относятся к так называемым «логическим ошибкам». Обнаружение уязвимостей этого типа с помощью автоматизированных средств затруднено, поскольку требует понимания бизнес-логики приложения.

Также как и в предыдущем случае, наиболее распространенной уязвимостью является «Межсайтовое выполнение сценариев», обнаруженная в 83% сайтов. Внедрение операторов SQL переместилось на третье место по количеству (10,1%) и на четвертое место по полярности (31% всех сайтов).

Второе и третье место занимаю уязвимости, связанные с разглашением информации (Information Leakage) и предсказуемым расположением ресурсов (Predictable Resource Location). Неаккуратное

разграничение доступа к Web-ресурсам, хранение в общедоступных, но «скрытых» папках конфиденциальных данных, резервные копии сценариев являются наиболее типичными примерами подобных ошибок.

В таблице 2 также приведен процент уязвимостей каждого типа, обнаруженных с помощью автоматизированных утилит. В целом, с учетом настройки под конкретные задачи сканером было обнаружено 78% всех уязвимостей. Однако ряд критичных ошибок связанных с бизнес-логикой и системой разграничения доступа был идентифицирован только при ручном анализе.

Следует отметить, что логические ошибки достаточно распространены. Так, ошибки системы авторизации, то есть возможность получения данных других пользователей, были обнаружены на 20% сайтов. Недостатки системы аутентификации встречались в 11% систем. Не смотря на относительно небольшой процент подобных уязвимостей на фоне других (суммарно 4,4%), зачастую достаточно наличия одной ошибки для полной компрометации системы.

На рисунке 6 приведено распределение количество уязвимостей по степени риска.

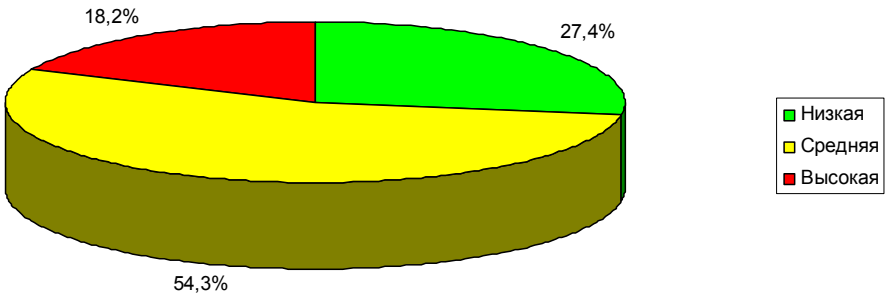

Рисунок 6 Распределение уязвимостей по степени риска

Более половины (54%) из всех обнаруженных недочетов приходится на уязвимости средней степени риска. Изрядную лепту в этот результат вносят ошибки класса «Межсайтовое выполнение сценариев». На уязвимости низкой и высокой степени риска приходится 27% и 18% соответственно.

Если рассматривать суммарную вероятность обнаружения уязвимостей различной степени риска при глубоком анализе Web-приложений, то получаем картину, приведенную на рисунке 7.

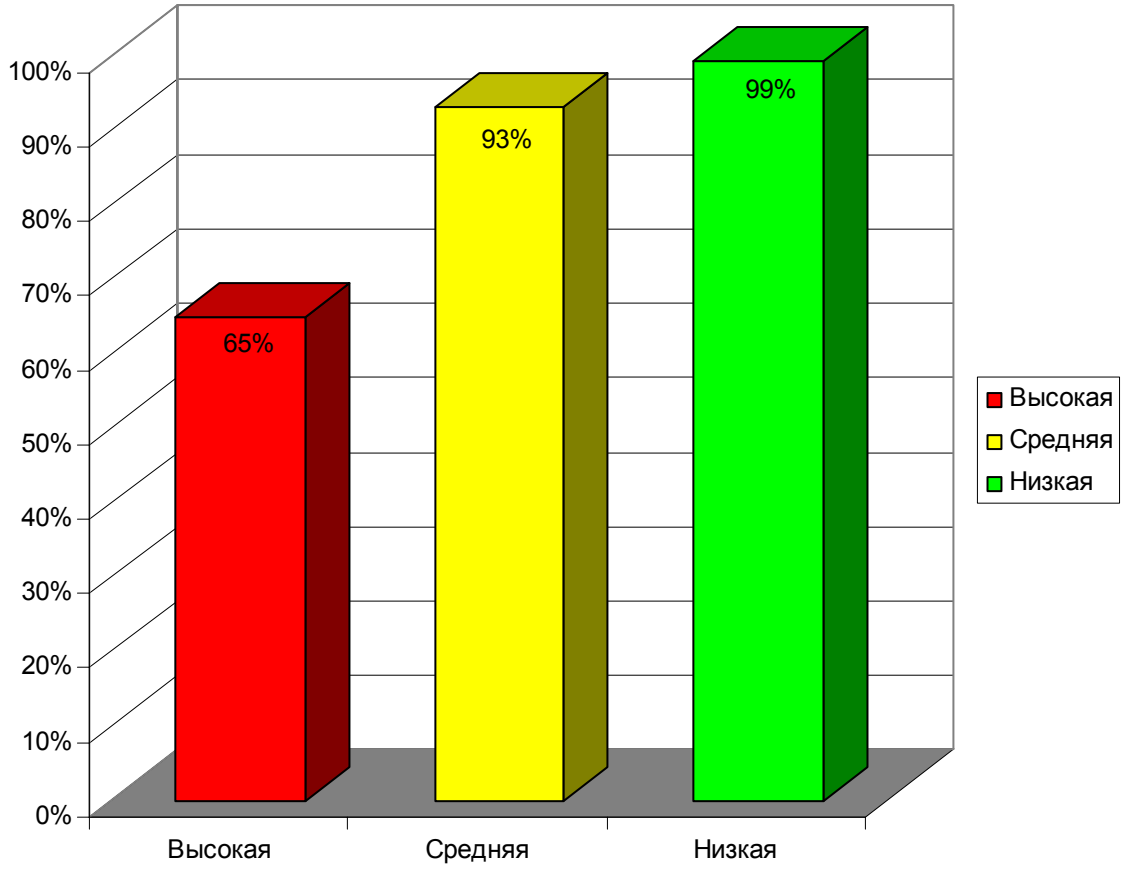

Рисунок 7 Вероятность обнаружения уязвимостей различной степени риска

То есть в 65% сайтов были обнаружены критичные уязвимости, и в 93 случаев из ста в программном обеспечении Web-приложения содержатся уязвимости средней степени риска.

Выводы

На основании полученных данных можно сделать следующие выводы:

- наиболее распространенными уязвимостями являются «Межсайтовое выполнение сценариев», «Внедрение операторов SQL» и различные варианты утечки информации.
- до 8% Web-приложений содержат уязвимости высокой степени риска, идентифицируемые с помощью автоматизированных средств;
- вероятность обнаружения критичной ошибки в динамическом Web-приложении при ручном анализе составляет 65%;
- корректное применение автоматизированных средств анализа уязвимостей позволяет идентифицировать до 80% всех недочетов;
- ряд критичных уязвимостей не может быть обнаружен с помощью автоматизированных средств.

В дальнейшем предполагается, что подобная статистика будет формироваться раз в шесть месяцев.

Об авторе

Сергей Гордейчик работает системным архитектором компании Positive Technologies (www.ptsecurity.ru), где он специализируется в вопросах безопасности приложений, безопасности беспроводных и мобильных технологий. Автор также является ведущим разработчиком курсов «Безопасность беспроводных сетей», «Анализ и оценка защищенности Web-приложений» учебного центра «Информзащита» (www.itsecurity.ru).

Опубликовал несколько десятков статей в “Windows IT Pro/RE”, SecurityLab (www.securityfocus.ru) и других изданиях. Является участником Web Application Security Consortium (WASC).

О компании Positive Technologies

Основное направление деятельности компании — защита компьютерных сетей от несанкционированного доступа. Говоря проще, мы помогаем нашим клиентам защититься от хакеров и других непрошенных виртуальных гостей.

Свою основную задачу мы решаем тремя путями:

- предоставляем услуги по тестированию на проникновение, оценке защищенности, аудиту и защите сетей и систем;
- развиваем один из лучших в мире сканеров безопасности XSpider, который клиент может использовать самостоятельно для поиска и устранения уязвимостей;
- обеспечиваем информационную поддержку профессионалам на страницах принадлежащего нам ведущего российского портала по информационной безопасности securitylab.ru.

Являясь специализированной компанией, мы способны обеспечить самый высокий уровень сервиса в своей области. В то же время, имея богатый и успешный опыт работы в сфере информационных технологий, мы по желанию клиента готовы предоставить и более комплексные решения (начиная от проектирования архитектуры локальной сети, поставки оборудования и кончая поддержкой и сопровождением всей сетевой программно-аппаратной инфраструктуры).

Ссылки

[1] Vulnerability Type Distributions in CVE
http://cwe.mitre.org/documents/vuln-trends.html

[2] Symantec Internet Security Threat Report
http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf

[3] Web Application Security Consortium
http://www.webappsec.org/projects/threat/

[4] Masterhost, «Часто задаваемые вопросы»
http://masterhost.ru/support/faq/technical/xspider/

[5] Positive Technologies, «Оценка защищенности Web-приложений»
http://www.ptsecurity.ru/serv_aud2.asp