ЗАО / ПОЗИТИВ ТЕКНОЛОДЖИЗ
107241 / МОСКВА / ЩЕЛКОВСКОЕ ЩОССЕ / Д.23А
ТЕЛ.: +7 (495) 744 01 44 / ФАКС: +7 (495) 744 01 87 / PT@PTSECURITY.RU
WWW.PTSECURITY.RU / WWW.MAXPATROL.RU / WWW.SECURITYLAB.RU

СТАТИСТИКА УЯЗВИМОСТЕЙ WEB-ПРИЛОЖЕНИЙ ЗА 2008 ГОД

ДМИТРИЙ ЕВТЕЕВ

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Как показывает многолетний опыт компании Positive Technologies по проведению работ по тестированию на проникновение и аудитов информационной безопасности - уязвимости в Web-приложениях по-прежнему остаются одним из наиболее распространенных недостатков обеспечения защиты информации. Другие часто встречающиеся проблемы - это низкая осведомленность сотрудников в вопросах ИБ, слабая парольная политика или повсеместное ее несоблюдение, недостатки в процессах управления обновлениями ПО, использование небезопасных конфигураций, и как это может показаться парадоксальным, не эффективное межсетевое разграничение доступа.

Несмотря на то, что уязвимости Web-приложений неоднократно описаны в «научно-популярной» и специализированной литературе, достаточно редко встречаются превентивные защитные механизмы, снижающие риски эксплуатации различных уязвимостей в них.

Проблема защищенности Web-приложений усугубляется еще и тем, что при разработке Web-приложений, зачастую не учитываются вопросы, связанные с защищенностью этих систем от внутренних и внешних угроз, либо не достаточно внимания уделяется данному процессу. Это в свою очередь порождает ситуацию, в которой проблемы ИБ попадают в поле зрения владельца системы уже после завершения проекта. А устранить уязвимости в уже созданном Web-приложении является более расходной статьей бюджета, чем при его разработке и внедрении.

Недооценка серьезности риска реализации угроз ИБ с использованием Web-приложений, доступных со стороны сети Интернет, возможно, является основным фактором текущего низкого состояния защищенности большинства из них.

2. МЕТОДИКА

Данная публикация содержит обзорную статистику уязвимостей Web-приложений, полученную из двух источников:

- В ходе работ по тестированию на проникновение, аудитов безопасности и других работ, выполненных экспертами компании Positive Technologies в 2008 году.
- По итогам повышения безопасности сайтов клиентов Хостинг-Центра РБК в рамках услуги "Проверка Безопасности Сайта", осуществляемая на основе системы MaxPatrol (модуль Pentest) компании Positive Technologies.

Всего в статистике участвуют данные о 10459 Web-приложениях. Данные основываются на проведении 16121 автоматических сканирований, детальном анализе 59 Web-приложений, в том числе с проведением анализа исходного кода более 10-ти из них.

В зависимости от типа выполняемых работ были задействованы различные методики проведения обследования Web-приложений, от автоматизированного инструментального обследования методом «черного ящика» (black-box, blind) с использованием сканеров безопасности XSpider и MaxPatrol, до проведения всех проверок вручную методом «белого ящика» (white-box), включая частичный и полный анализ исходного кода. В статистику вошли данные только по внешним Web-приложениям, доступным из глобальной сети Интернет.

Обнаруженные уязвимости классифицировались согласно Web Application Security Consortium Web Security Threat Classification (WASC WSTCv2 [1]). Данная классификация представляет собой попытку собрать воедино 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 девяти классов (WSTCv2):

- Аутентификация (Authentication)
- Авторизация (Authorization)
- Атаки на клиентов (Client-side Attacks)
- Выполнение кода (Command Execution)
- Разглашение информации (Information Disclosure)
- Логические недостатки (Logical Flaws)
- Не безопасные конфигурации (Misconfiguration)
- Недостатки протокола (Protocol Abuse)
- Другие (Miscellaneous)

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 проблемы ИБ, как недостатки процесса управления обновлениями ПО не рассматриваются.

Критичность уязвимости, оцениваемая согласно CVSSv2 (Common Vulnerability Scoring System version 2 [2, 3]), приводилась к классической «светофорной» оценке путем деления на 3.

3. ПОРТРЕТ УЧАСТНИКОВ

Распределение приложений, исследуемых методом «белого ящика», в зависимости от сферы деятельности владельца приведено в Табл. 1 и на Рис. 1.

Таблица 1. Распределение владельцев по отрасли

Сектор экономики	Доля, %
Телекоммуникации	48
Финансовый сектор	8
Нефтегазовый комплекс	39
Другие	5

Подобное распределение респондентов связано с тем, что наибольший интерес в 2008 г. к работам по анализу защищенности своих Web-ресурсов проявил сектор Телекоммуникации (48%) и Нефтегазовый комплекс (39%). В меньшей степени, востребованность в подобных услугах за 2008 г., была у Финансового сектора (8%) и компаний в различных отраслях (5%). Однако это обусловлено, прежде всего тем, что для данного сектора экономики проводились более детальные исследования Web-приложений путем анализа исходного кода.

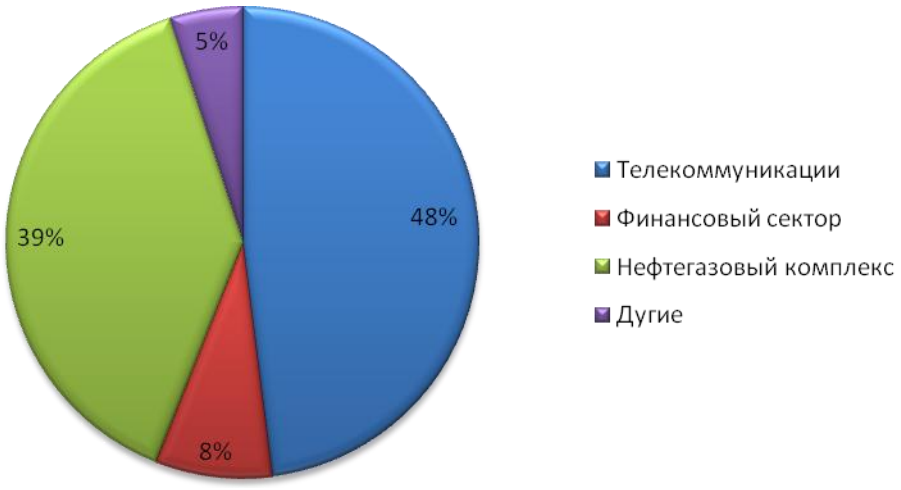

Рисунок 1. Распределение владельцев по отрасли

Представленные данные справедливы только для участников исследования, ресурсы которых обследовались экспертами Positive Technologies в рамках аудитов и работ по тестированию на проникновение.

4. СТАТИСТИКА УЯЗВИМОСТЕЙ

Всего в представленную статистику вошли данные по 10459 Web-приложениям, 7861 из которых содержали одну и более уязвимостей. Суммарно во всех приложениях было обнаружено 33931 ошибок различной степени риска. В Табл. 2 представлены данные по распределению уязвимостей, выявленные в ходе аудитов и путем автоматизированного сканирования.

Таблица 2. Распределение уязвимостей по методу их поиска

Метод поиска	Хостов	Уязвимых хостов	Уязвимостей
Ручной метод поиска и анализ исходного кода	59	59	428
Автоматизированный метод поиска	10400	7802	33503

Таким образом, вероятность обнаружения уязвимостей в одном Web-приложении (т.е. эффективность оценки защищенности) при его детальном анализе выше этого показателя при автоматическом сканировании на 26% (см. Рис. 2). Такое соотношение обусловлено, прежде всего тем, что анализ исходного кода и выполнение ручных проверок позволяет добиться лучших результатов, чем при автоматизированном сканировании. Кроме того, в работах по исследованию Web-приложений ручным способом применялись методы проверки приложений на основе системных журналов, исходных кодов, что увеличивает охват API системы, и как следствие, позволяет получить более объективную оценку защищенности исследуемых систем. При автоматизированном сканировании настройка профилей сканирования под конкретное Web-приложение не выполнялась, и сканирования производились методом «черного ящика».

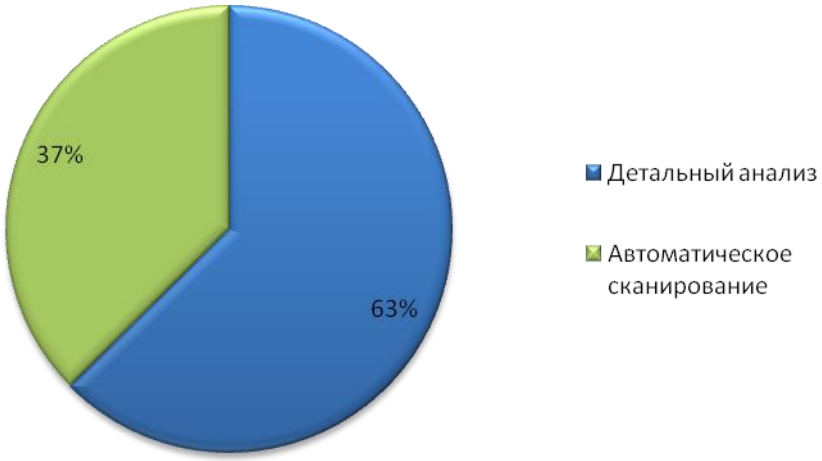

Рисунок 2. Вероятность обнаружения уязвимости различными методами их поиска

4.1. Автоматическое сканирование

Распределение обнаруженных уязвимостей по различным типам с помощью автоматизированных средств представлено в Табл. 3 и на Рис. 3. Данные указаны с учетом систем, для которых были обнаружены от одной до нескольких уязвимостей. При расчете процента уязвимых сайтов были исключены web-приложения, у которых не было обнаружено уязвимостей.

Стоит отметить, что в статистику не вошла распространенная уязвимость Web-приложений – «Подделка HTTP-запросов» (Cross-Site Request Forgery, CSRF) [4]. Эта ошибка в том или ином виде встречалась во всех проанализированных приложениях.

Таблица 3. Статистика уязвимостей Web-приложений (автоматическое сканирование)

Тип уязвимости	% Уязвимостей	% Уязвимых сайтов
Cross-Site Scripting	30,08	50,10
Information Leakage	29,82	97,19
Insufficient Transport Layer Protection	11,18	53,25
Fingerprinting	9,59	45,68
SQL Injection	7,95	15,50
Malware detect	5,52	1,32
Improper Parsing	3,92	6,62
HTTP Response Splitting	0,84	2,07
SSI Injection	0,42	0,42
Remote File Inclusion	0,22	0,44
Path Traversal	0,23	0,70
OS Commanding	0,08	0,06
Content Spoofing	0,06	0,19
Denial of Service	0,05	0,23
Insufficient Authorization	0,02	0,10
Brute Force	0,01	0,06
Directory Indexing	0,01	0,05

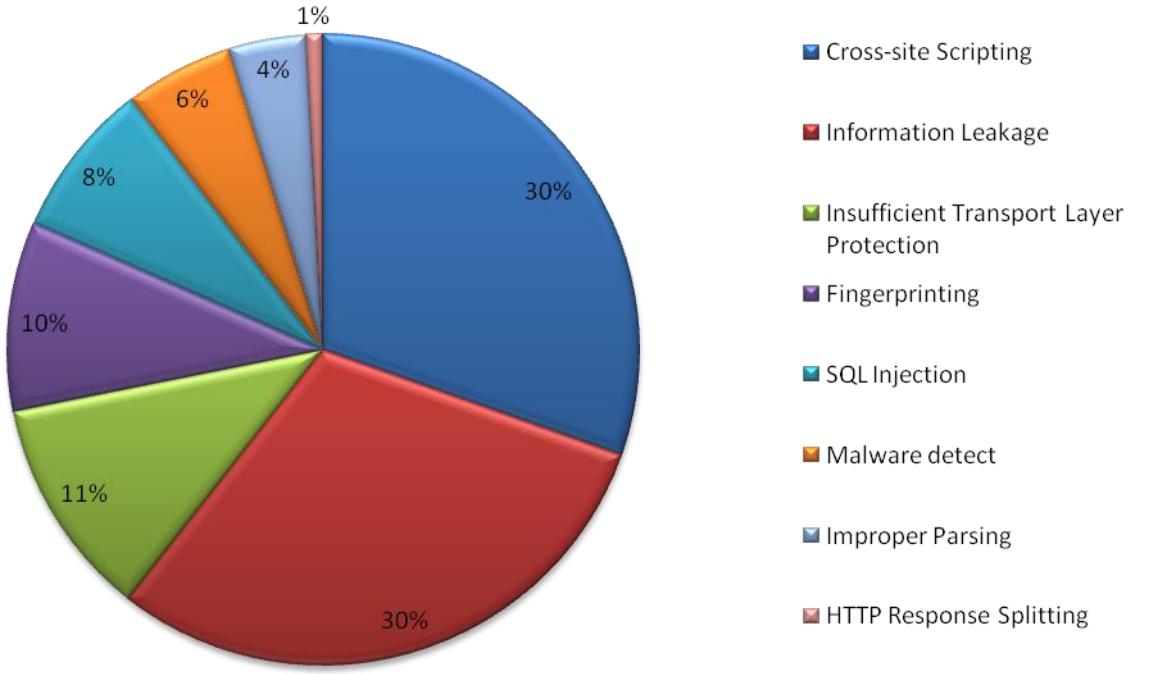

Рисунок 3. Статистика уязвимостей Web-приложений (автоматическое сканирование)

Если рассматривать уязвимости с точки зрения распространенности, то будут получены результаты, представленные на Рис. 4.

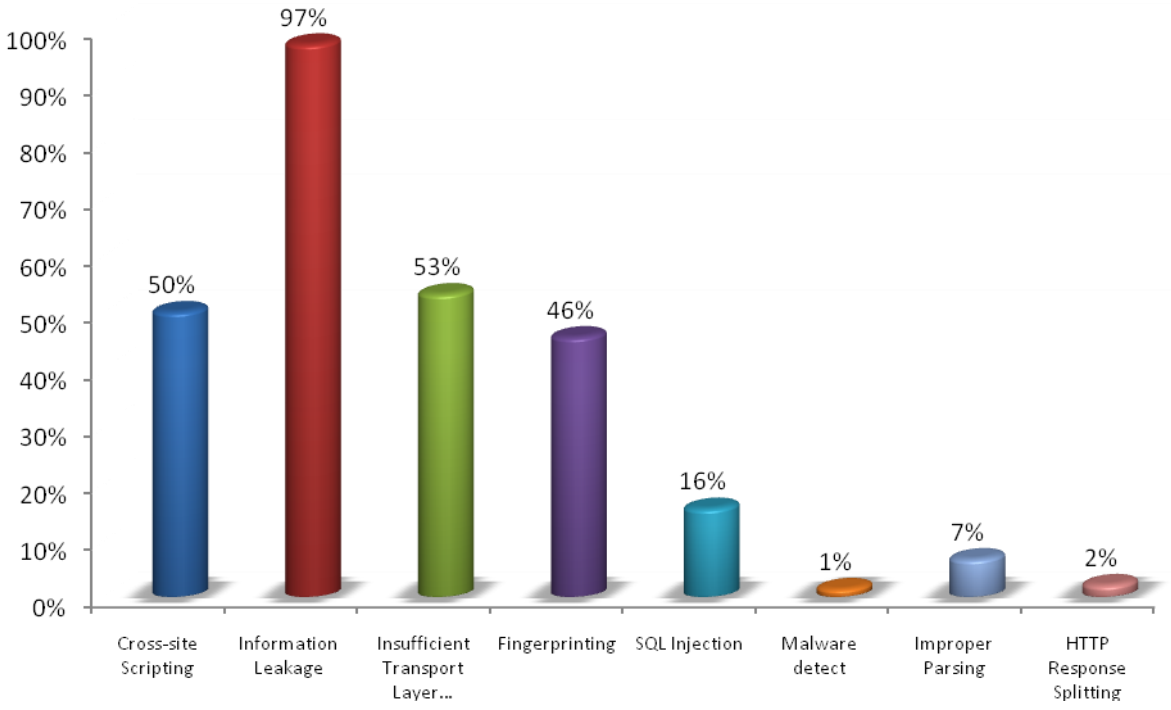

Рисунок 4. Распределение уязвимостей по сайтам (автоматическое сканирование)

Наиболее распространенной уязвимостью является «Межсайтовое выполнение сценариев» (Cross-Site Scripting, XSS), на долю которой приходится приблизительно 30% всех ошибок.

Данная уязвимость встречалась в 50% всех проанализированных приложений. То есть каждый второй сайт содержит подобную уязвимость.

Другая распространенная уязвимость, вплотную приблизившаяся к «Межсайтовому выполнению сценариев», связана с различными вариантами утечки информации. Уязвимость данного типа собрала в себе такие распространенные ошибки, как доступ к исходному коду серверных сценариев, раскрытие пути каталога Web-сервера, получение различной чувствительной информации и прочее. Ошибки, связанные с данной уязвимостью, встречались практически на каждом обследуемом сайте.

Таким образом, лидирующую позицию по вероятности обнаружения уязвимости в Web-приложении при автоматическом сканировании, занимает уязвимость – «Утечка информации» (Information Leakage). Стоит отметить, что степень возможного риска данной уязвимости может варьироваться от низкой до критической. Ошибки в разграничении доступа к Web-ресурсам, хранение в общедоступных, но «скрытых» папках конфиденциальных данных, резервных копий сценариев являются наиболее типичными примерами подобных недостатков. В некоторых случаях аудиторам удавалось получить доступ к критичной системной или бизнес информации (например, базам учетных записей, журналам транзакций), используя только механизм «Forced Browsing», т.е. подбор имен файлов, доступных со стороны сети Интернет.

Интересную позицию в статистике занимает уязвимость «Malware detect», на долю которой приходится приблизительно 6% всех выявленных уязвимостей при автоматическом сканировании (см. Рис. 3). Присутствие данной уязвимости свидетельствует о том, что Web-приложение содержит инфицированный код (Trojan-Spy backdoor, Code.JS, Code.I и т.д.), вследствие чего на компьютеры посетителей такого сайта может быть установлено злонамеренное программное обеспечение. Статистика уязвимостей с высоким уровнем опасности, обнаруженных на сайтах, содержащих инфицированный код (см. Рис. 5), показывает, что наиболее вероятные пути распространения инфицированного кода в этих приложениях – это использование следующих уязвимостей:

- Внедрение операторов SQL (SQL Injection)
- Выполнение команд ОС (OS Commanding)
- Внедрение серверных расширений (SSI Injection)

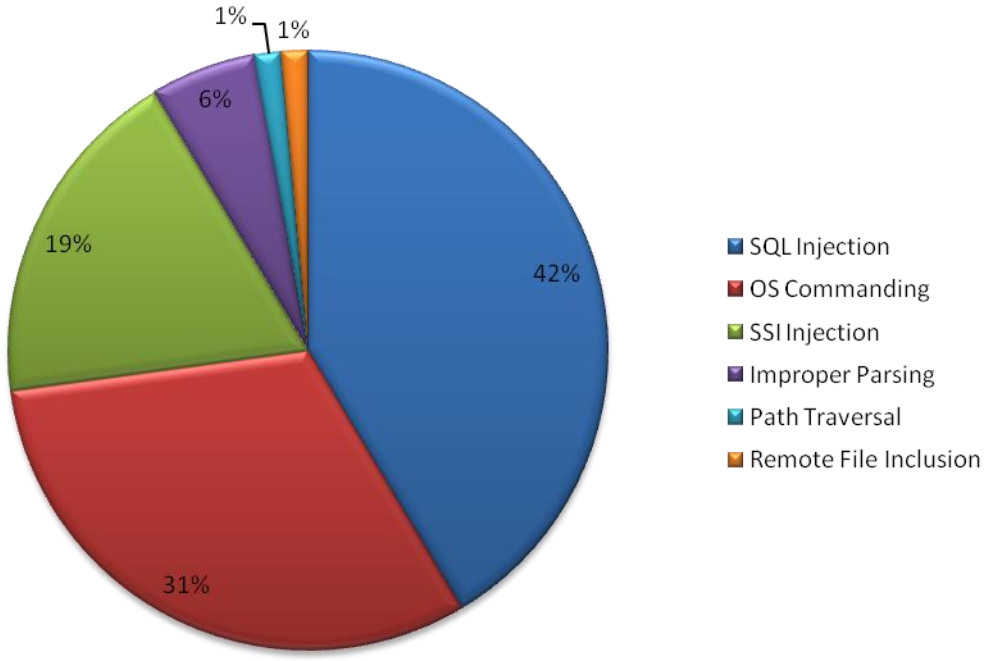

Рисунок 5. Статистика критических уязвимостей на сайтах, содержащих инфицированный код

Процесс эксплуатации подобных уязвимостей может быть достаточно легко автоматизирован, а распространненость подобных ошибок в Web-приложениях позволяет проводить массовые «дефейсы», добавлять инфицированный код на страницы уязвимых Web-узлов.

Если посмотреть на статистику распределения критических уязвимостей по инфицированным сайтам (см. Рис. 6), то можно сделать вывод, что основным вектором заражения Web-приложения автоматизированным способом, является эксплуатация уязвимости «Внедрение операторов SQL».

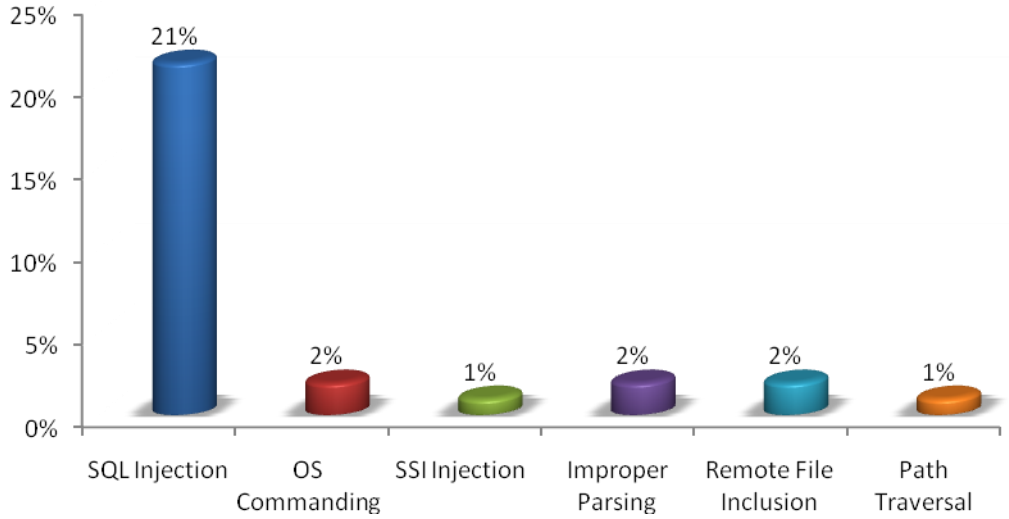

Рисунок 6. Распределение критических уязвимостей по инфицированным сайтам

Сравнивая аналогичные показатели по сайтам, на которых не было обнаружено инфицированных страниц (см. Рис. 7), можно сделать вывод, что приблизительно 15-20%

Web-приложений может быть заражено автоматизированным способом, при условии настроек среды Web-сервера, позволяющих провести подобную атаку.

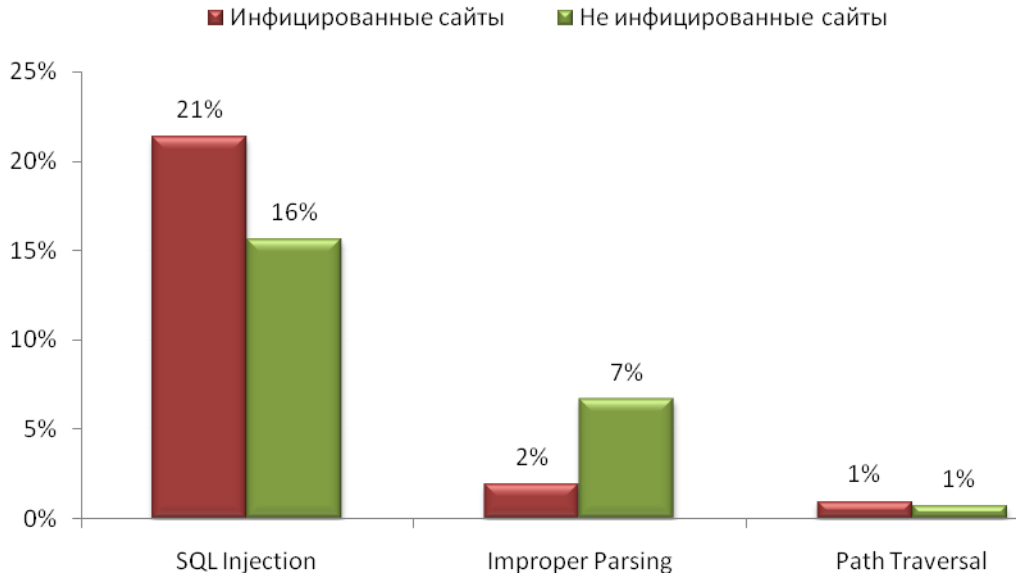

Рисунок 7. Распределение критических уязвимостей на сайтах

4.2. Детальный анализ

Распределение обнаруженных уязвимостей по различным типам, выявленных с помощью детального анализа Web-приложений представлено в Табл. 4 и на Рис. 8.

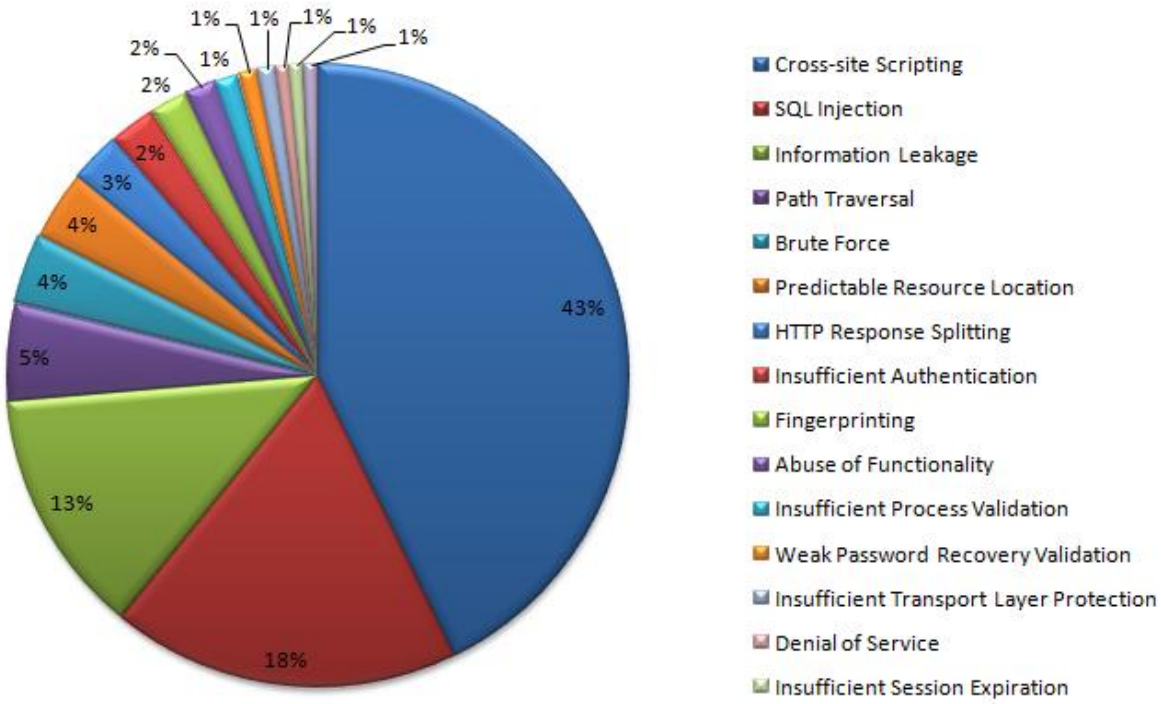

Рисунок 8. Статистика уязвимостей Web-приложений (детальный анализ)

Таблица 4. Статистика уязвимостей Web-приложений (детальный анализ)

Тип уязвимости	% Уязвимостей	% Уязвимых сайтов
Cross-Site Scripting	41,75	61,01
SQL Injection	17,69	67,79
Information Leakage	12,50	16,94
Path Traversal	4,95	11,86
Brute Force	3,54	18,64
Predictable Resource Location	3,54	22,03
HTTP Response Splitting	2,59	5,08

Тип уязвимости	% Уязвимостей	% Уязвимых сайтов
Insufficient Authentication	2,36	15,25
Fingerprinting	1,89	10,16
Abuse of Functionality	1,65	6,77
Insufficient Process Validation	1,18	5,08
Weak Password Recovery Validation	0,94	6,77
Insufficient Transport Layer Protection	0,94	3,38
Denial of Service	0,71	5,08
Insufficient Session Expiration	0,71	5,08
Remote File Inclusion	0,71	3,38
Credential/Session Prediction	0,47	3,38
Directory Indexing	0,47	3,38
Insufficient Anti-automation	0,47	3,38
OS Commanding	0,47	3,38
Session Fixation	0,24	1,69
Mail Command Injection	0,24	1,69

Если рассматривать наиболее часто встречаемые уязвимости при детальном анализе Web-приложения с точки зрения распространенности, то будут получены результаты, представленные на Рис. 9.

Также как и при автоматическом сканировании Web-приложений, при проведении детального анализа, наиболее распространенной уязвимостью по-прежнему является «Межсайтовое выполнение сценариев» (Cross-Site Scripting, XSS), на долю которой приходится приблизительно 43% всех ошибок. Данная уязвимость встретилась в 61% всех проанализированных приложений.

На втором месте, при детализированном анализе защищенности Web-приложений, оказалась уязвимость «Внедрение операторов SQL» (SQL Injection). Данная уязвимость встретилась в 18% случаев, приблизительно на 68% всех исследуемых приложений.

Таким образом, лидирующие позиции по вероятности обнаружения уязвимости в Web-приложении при его детальном анализе, занимает уязвимость на стороне Web-сервера (server-side) – «Внедрение операторов SQL» (SQL Injection) и уязвимость, эксплуатируемая

на стороне клиента (client-side) – «Межсайтовое выполнение сценариев» (Cross-Site Scripting, XSS).

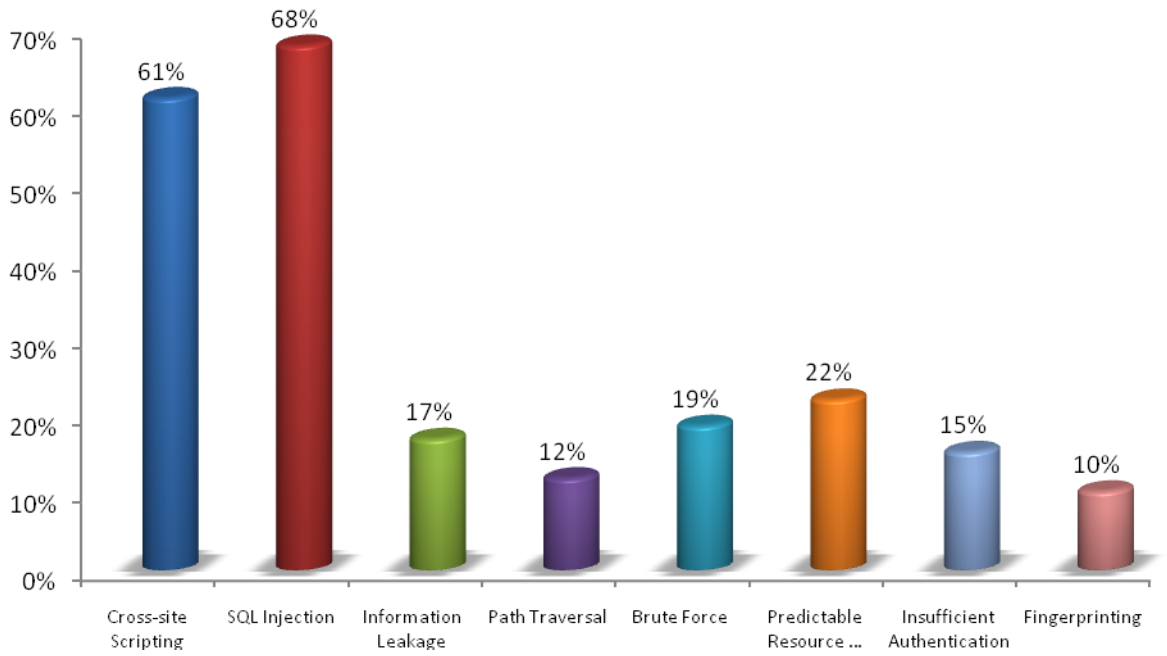

Рисунок 9. Распределение уязвимостей по сайтам (детальный анализ)

Небольшой процент распределения уязвимости типа «Утечка информации» (Information Leakage) по сравнению с автоматическим сканированием обусловлено используемой методикой при проведении детального анализа защищенности Web-приложений. Так, многие недостатки, которые сканер безопасности относит к данному типу уязвимости и суммирует их, при экспертном анализе, группировались в одну уязвимость или оказывались признаками других, более серьезных проблем (например, ошибками разграничения доступа).

4.3. Обобщенные данные

Обобщенные результаты по распределению обнаруженных уязвимостей по различным типам и классам WSTCv2, выявленных с помощью детального анализа Web-приложений и при автоматическом сканировании представлено в Табл. 5 и на Рис. 10.

Таблица 5. Статистика уязвимостей Web-приложений (обобщенные данные)

Тип уязвимости	Автоматическое сканирование		Детальный анализ	
	% Уязвимостей	% Уязвимых сайтов	% Уязвимостей	% Уязвимых сайтов
Cross-Site Scripting	30,08	50,10	41,75	61,01
SQL Injection	7,95	15,50	17,69	67,79

Тип уязвимости	Автоматическое сканирование		Детальный анализ	
	% Уязвимостей	% Уязвимых сайтов	% Уязвимостей	% Уязвимых сайтов
Information Leakage	29,82	97,19	12,50	16,94
Path Traversal	0,23	0,70	4,95	11,86
Brute Force	0,01	0,06	3,54	18,64
Predictable Resource Location	0	0	3,54	22,03
HTTP Response Splitting	0,84	2,07	2,59	5,08
Insufficient Authentication	0	0	2,36	15,25
Fingerprinting	9,59	45,68	1,89	10,16
Abuse of Functionality	0	0	1,65	6,77
Insufficient Process Validation	0	0	1,18	5,08
Weak Password Recovery Validation	0	0	0,94	6,77
Insufficient Transport Layer Protection	11,18	53,25	0,94	3,38
Denial of Service	0,05	0,23	0,71	5,08
Insufficient Session Expiration	0	0	0,71	5,08
Remote File Inclusion	0,22	0,44	0,71	3,38
Credential/Session Prediction	0	0	0,47	3,38
Directory Indexing	0,01	0,05	0,47	3,38
Insufficient Anti-automation	0	0	0,47	3,38
OS Commanding	0,08	0,06	0,47	3,38
Session Fixation	0	0	0,24	1,69
Mail Command Injection	0	0	0,24	1,69

Тип уязвимости	Автоматическое сканирование		Детальный анализ	
	% Уязвимостей	% Уязвимых сайтов	% Уязвимостей	% Уязвимых сайтов
Malware detect	5,52	1,32	0	0
Improper Parsing	3,92	6,62	0	0
SSI Injection	0,42	0,42	0	0
Content Spoofing	0,06	0,19	0	0
Insufficient Authorization	0,02	0,10	0	0

Рисунок 10. Распределение уязвимостей по сайтам в соответствии классам WSTCv2 (обобщенные данные)

При анализе количества уязвимостей по степени риска (Рис. 11 и 12) видно, что наиболее распространенными являются недочеты низкой степени критичности при автоматическом сканировании (Рис. 11) и средней степени критичности при детальном анализе (Рис. 12).

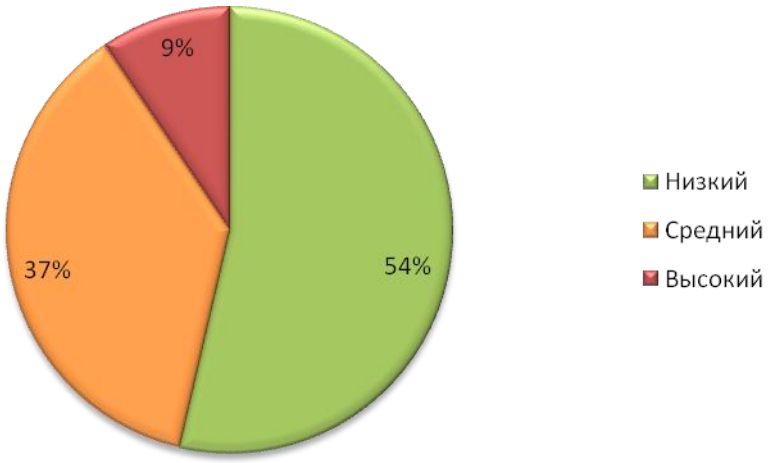

Рисунок 11. Количество уязвимостей по степени риска (автоматизированное сканирование)

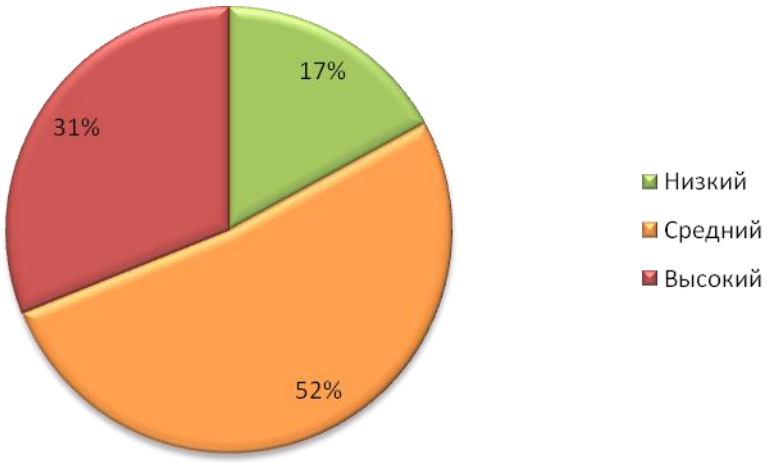

Рисунок 12. Количество уязвимостей по степени риска (детальный анализ)

Если анализировать распространенность уязвимостей высокого степени риска (Рис. 13), то здесь наиболее часто встречаются ошибки типа «Внедрение операторов SQL» (SQL Injection). Возможность несанкционированного доступа к базе данных была обнаружена в 67% случаев при детальном анализе Web-приложения и 16% при автоматическом сканировании. Также широко распространены ошибки «Чтения произвольных файлов» (Path Traversal), «Подбор пароля» (Brute Force) и ошибки в реализации и настройке системы авторизации и аутентификации.

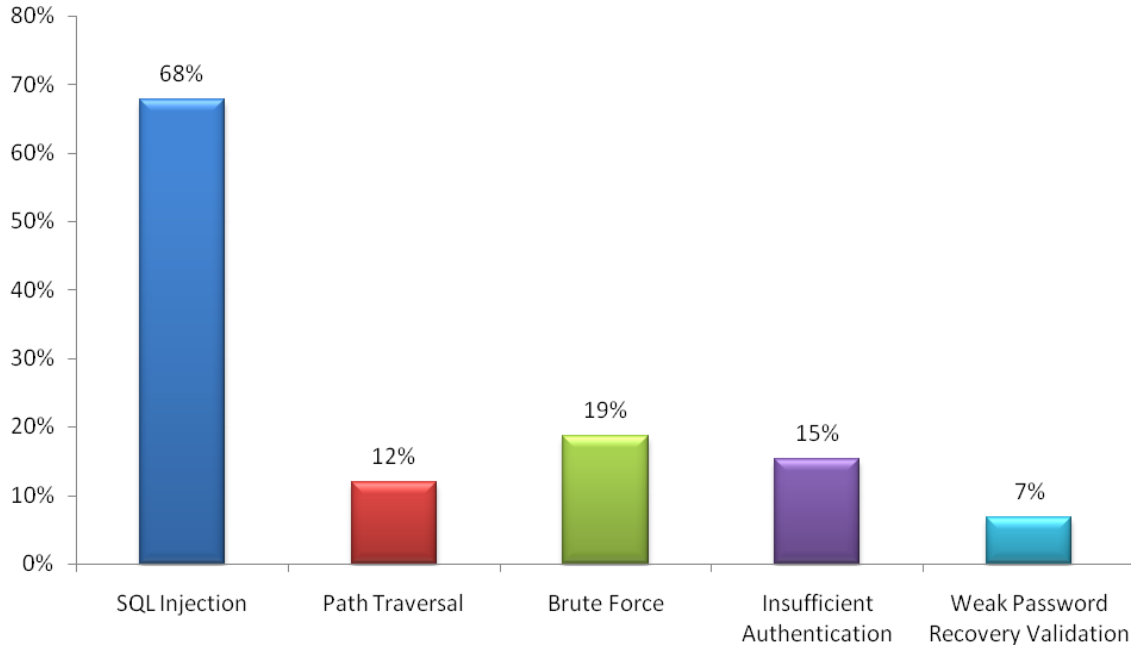

Рисунок 13. Наиболее часто встречаемые критические уязвимости

Если рассматривать суммарную вероятность обнаружения уязвимостей различной степени риска при использовании разных подходов к анализу Web-приложений, то получаем картину, приведенную на Рис. 14.

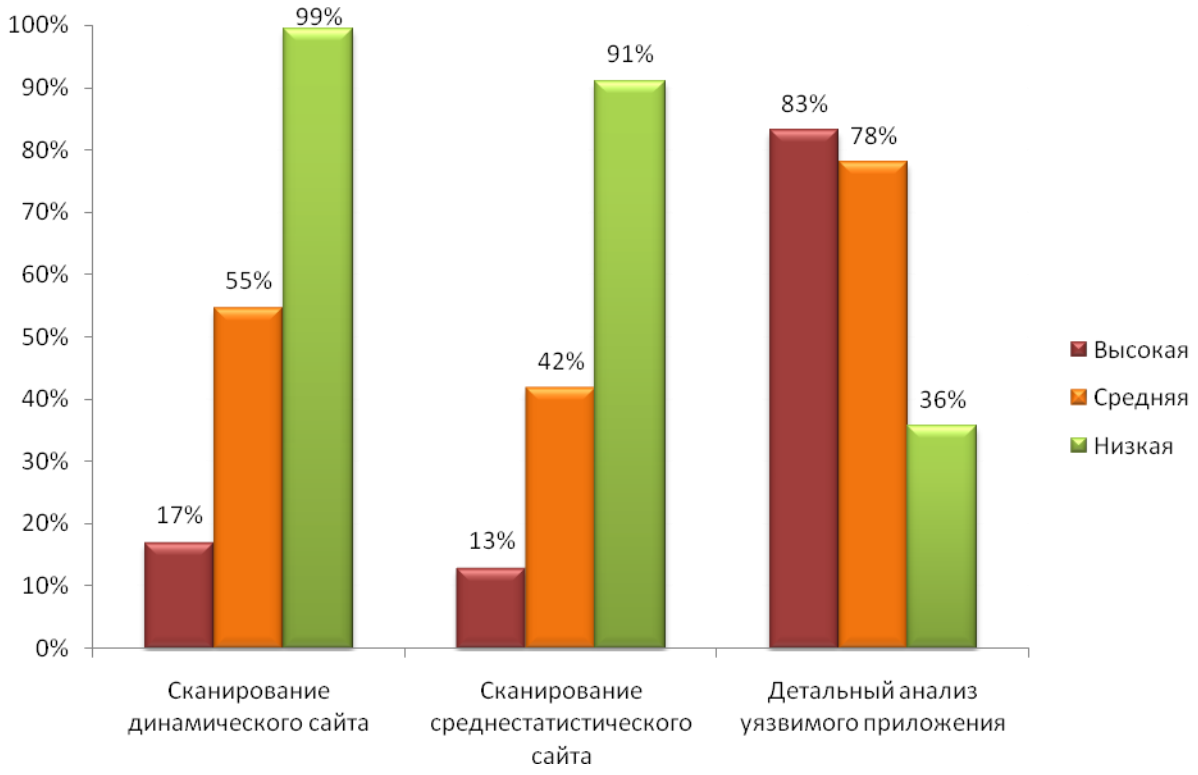

Рисунок 14. Вероятность обнаружения уязвимостей различной степени риска

То есть в 83% сайтов были обнаружены критичные уязвимости, и в 78% случаев из ста в программном обеспечении Web-приложения содержатся уязвимости средней степени риска.

5. ВЫВОДЫ

На основании полученных данных можно сделать следующие выводы:

- наиболее распространенными уязвимостями являются "Межсайтовое выполнение сценариев", "Внедрение операторов SQL", различные варианты утечки информации, "Чтение произвольных файлов" и подбор паролей;
- вероятность обнаружения критичной ошибки в динамическом Web-приложении составляет порядка 17% при проведении автоматического сканирования методом «черного ящика» и 83% при всестороннем экспертном анализе методом «белого ящика»;
- вероятность автоматизированного инфицирования страниц уязвимого Web-приложения составляет приблизительно 15-20%;
- ситуация с защитой Web-приложений в 2008 году является более оптимистичной по сравнению с результатами исследований предыдущих двух лет [5,6].

6. ССЫЛКИ

[1] Web Application Security Consortium, "Web Security Threat Classification"

http://webappsec.org/projects/threat/

[2] Common Vulnerability Scoring System

http://www.first.org/cvss/

[3] Сергей Гордейчик, "Насколько "дыра" широка?"

http://www.osp.ru/win2000/2006/02/1156304/

[4] Сергей Гордейчик, Cross-Site Request Forgery - много шума из-за ничего

http://www.securitylab.ru/analytics/292473.php

[5] Positive Technologies, "Статистика уязвимостей WEB-приложений в 2007 году"

http://www.ptsecurity.ru/stat2007.asp

[6] Positive Technologies, "Статистика уязвимостей WEB-приложений в 2006 году"

http://www.ptsecurity.ru/webstat2006.asp

ОБ АВТОРЕ

Дмитрий Евтеев, эксперт по информационной безопасности отдела консалтинга и аудита компании Positive Technologies. Специализируется в вопросах проведения тестирований на проникновение, аудита информационных систем и анализа защищенности Web-приложений. Имеет профессиональные звания и сертификаты (MCSE:Security, MCTS).

О КОМПАНИИ

Positive Technologies www.ptsecurity.ru - одна из ведущих российских компаний в области информационной безопасности.

Основные направления деятельности компании - разработка систем комплексного мониторинга информационной безопасности (XSpider, MaxPatrol); предоставление консалтинговых и сервисных услуг в области информационной безопасности; развитие специализированного портала Securitylab.ru.

Заказчиками Positive Technologies являются более 40 государственных учреждений, более 50 банков и финансовых структур, 20 телекоммуникационных компаний, более 40 промышленных предприятий, компании ИТ-индустрии, сервисные и ритейловые компании России, стран СНГ, Балтии, а также Великобритании, Германии, Голландии, Израиля, Ирана, Китая, Мексики, США, Тайланда, Турции, Эквадора, ЮАР, Японии.

Positive Technologies - это команда высококвалифицированных разработчиков, консультантов и экспертов, которые обладают большим практическим опытом, имеют профессиональные звания и сертификаты, являются членами международных организаций и активно участвуют в развитии отрасли.