



POSITIVE TECHNOLOGIES

ЗАО / ПОЗИТИВ ТЕКНОЛОДЖИЗ
107241 / МОСКВА / ЩЕЛКОВСКОЕ ШОССЕ / 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 ВЕБ-ПРИЛОЖЕНИЙ ЗА 2009 ГОД



POSITIVE / TECHNOLOGIES®

ОГЛАВЛЕНИЕ

| | |
|--|-----------|
| 1. ВВЕДЕНИЕ | 3 |
| 2. МЕТОДИКА | 3 |
| 3. РЕЗЮМЕ | 5 |
| 4. ПОРТРЕТ УЧАСТНИКОВ | 6 |
| 5. СТАТИСТИКА УЯЗВИМОСТЕЙ | 7 |
| 5.1. АВТОМАТИЧЕСКОЕ СКАНИРОВАНИЕ | 7 |
| 5.1.1. АНАЛИЗ УЯЗВИМОСТЕЙ НА ИНФИЦИРОВАННЫХ САЙТАХ | 10 |
| 5.1.2. ДИНАМИКА ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ | 12 |
| 5.2. ДЕТАЛЬНЫЙ АНАЛИЗ | 16 |
| 5.3. СОПОСТАВЛЕНИЕ НАБОРОВ ДАННЫХ В КОНТЕКСТЕ ТРЕБОВАНИЙ PCI DSS | 20 |
| 5.4. ОБОБЩЕННЫЕ ДАННЫЕ | 23 |
| 6. ВЫВОДЫ | 29 |
| 7. О КОМПАНИИ | 29 |
| 8. ССЫЛКИ | 30 |
| 9. ПРИЛОЖЕНИЕ 1: МЕТОДИКА ОЦЕНКИ СТЕПЕНИ РИСКА | 31 |

1. ВВЕДЕНИЕ

Многолетняя экспертиза аналитического центра PT Research, а также опыт компании Positive Technologies по проведению тестов на проникновение и аудитов информационной безопасности показывают, что ошибки в защите веб-приложений по-прежнему остаются одним из наиболее распространенных недостатков обеспечения защиты информации. Более того, уязвимости веб-приложений являются одним из наиболее распространенных путей проникновения в корпоративные информационные системы; существует множество факторов, делающих веб-сервисы привлекательной целью для атак злоумышленников.

При разработке приложений основные усилия разработчика обычно направлены на обеспечение требуемой функциональности. При этом вопросам безопасности и качества программного кода уделяется недостаточно внимания. В результате подавляющее большинство веб-приложений содержит уязвимости различной степени критичности.

Простота протокола HTTP позволяет разрабатывать эффективные методы автоматического анализа веб-приложений и выявления в них уязвимостей. Это значительно упрощает работу нарушителя, позволяя ему обнаружить большое число уязвимых веб-сайтов, чтобы затем провести атаку на наиболее интересные из них.

Кроме того, уязвимости некоторых типов допускают не только автоматическое выявление, но и автоматическую эксплуатацию. Именно таким образом производится массовое внедрение в веб-ресурсы вредоносного кода, который затем используется для создания бот-сетей из рабочих станций обычных пользователей сети Интернет. Возможность использования веб-приложений в качестве платформы для атаки на рабочие места пользователей сама по себе делает эти приложения привлекательной целью для нарушителя.

Таким образом, при подготовке атаки на информационную инфраструктуру компании нарушители в первую очередь исследуют ее веб-приложения. Недооценка риска, который могут представлять уязвимости в веб-приложениях, доступные из сети Интернет, возможно, является основной причиной низкого уровня защищенности большинства из них.

2. МЕТОДИКА

Данная публикация содержит обзорную статистику по уязвимостям в веб-приложениях, которая была получена в ходе проведения тестирований на проникновение, аудитов безопасности и других работ, выполненных экспертами компании Positive Technologies в 2009 году. В статистике собраны данные о 5560 веб-приложениях, полученные в результате проведения 6239 автоматических сканирований и детального анализа 77 веб-приложений.

В зависимости от типа выполняемых работ применялись различные методики исследования веб-приложений, от автоматизированного инструментального исследования методом «черного ящика» (black-box, blind) с использованием сканера системы контроля защищенности и соответствия стандартам 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 веб-приложениям, доступные из глобальной сети Интернет.

Обнаруженные уязвимости классифицировались согласно системе Web Application Security Consortium Web Security Threat Classification (WASC WSTCv2 [1]), в разработке которой

активное участие принимали эксперты компании Positive Technologies. Данная система представляет собой попытку классифицировать все угрозы безопасности веб-приложений. Члены Web Application Security Consortium создали этот проект для разработки и популяризации стандартной терминологии описания проблем безопасности веб-приложений. Этот документ дает возможность разработчикам приложений, специалистам в области безопасности, производителям программных продуктов и аудиторам использовать единый язык для взаимодействия.

Помимо WASC WSTCv2, в предлагаемой статистике использовался структурированный список уязвимостей, состоящий из девяти классов согласно WASC WSTCv1 [2]:

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

В приводимой статистике учитываются только уязвимости веб-приложений. Такие распространенные проблемы информационной безопасности, как недостатки процесса управления обновлениями программного обеспечения, не рассматриваются.

Степень критичности уязвимости оценивалась согласно CVSSv2 (Common Vulnerability Scoring System version 2 [3, 4]) и приводилась к классической «светофорной» оценке путем деления на 3.

3. РЕЗЮМЕ

Практически половина проанализированных систем содержали уязвимости. Суммарно во всех приложениях было обнаружено 13434 ошибок различной степени риска, зафиксировано 1412 образцов вредоносного кода, содержащихся на страницах уязвимых систем. Доля скомпрометированных сайтов распространявших вредоносное программное обеспечение составила 1,7%. Каждый из таких сайтов содержал уязвимости, позволяющие выполнять команды на сервере, что подтверждает возможность использование этих уязвимостей для компрометации системы.

Основной результат исследования неутешителен. **Вероятность обнаружения критичной ошибки в веб-приложении автоматическим сканером составляет около 35% и достигает 80% при детальном экспертном анализе.** Этот факт демонстрирует невысокую защищенность современных Web-приложений не только от атак со стороны квалифицированных злоумышленников, но и от действий атакующих, вооруженных готовыми утилитами для «автоматического взлома».

Как и ранее, наиболее распространенными ошибками, допускаемыми разработчиками приложений, являются уязвимости «Межсайтовое выполнение сценариев» и «Внедрение операторов SQL» на которые пришлось более 19% и 17% всех обнаруженных уязвимостей соответственно.

Проводя **анализ устранения выявленных уязвимостей** в 2009 году, по результатам сканирования в 2008 году, было выявлено, что **общий процент устранения всех обнаруженных уязвимостей за год составил около 20%**. В целом регулярный анализ защищенности веб-приложений и налаженный процесс устранения выявленных недостатков позволяют за год уменьшить число уязвимых сайтов в среднем втрое.

С точки зрения соответствия требованиям регуляторов (compliance management) ситуация улучшилась незначительно. **До 84% веб-приложений не удовлетворяет требованиям стандарта по защите информации в индустрии платежных карт PCI DSS и 81% не соответствуют критериям ASV-сканирования, определенного в стандарте.**

4. ПОРТРЕТ УЧАСТНИКОВ

Распределение приложений, которые были исследованы с помощью методик «черного» и «белого» ящика, по сферам деятельности их владельцев приведено в Табл. 1 и на Рис. 1.

Таблица 1. Распределение владельцев по отраслям

| Сектор экономики | Доля, % |
|-----------------------|---------|
| Телекоммуникации | 35% |
| Финансовый сектор | 13% |
| Нефтегазовый комплекс | 40% |
| Другие | 12% |



Рисунок 1. Распределение владельцев по отраслям

Подобное распределение компаний связано с тем, что наибольший интерес в 2009 г. к работам по анализу защищенности своих веб-ресурсов проявил сектор Телекоммуникации (35%) и Нефтегазовый комплекс (40%). Финансовый сектор и компании из прочих отраслей нуждались в подобных услугах в меньшей степени (13% и 12% соответственно).

Представленные данные справедливы только для компаний, ресурсы которых исследовались экспертами Positive Technologies в рамках выполнения аудитов и работ по тестированию на проникновение.

5. СТАТИСТИКА УЯЗВИМОСТЕЙ

Всего в представленную статистику вошли данные о 5560 веб-приложениях, 2023 из которых содержали уязвимости. Суммарно во всех приложениях было обнаружено 13434 ошибок различной степени риска и зафиксировано 1412 образцов вредоносного кода, содержащихся на страницах уязвимых веб-приложений. В Табл. 2 представлены данные по распределению уязвимостей, которые были получены при выполнении аудитов и путем автоматизированного сканирования.

Таблица 2. Распределение уязвимостей по методу их поиска

| Метод поиска | Узел | Уязвимых узлов | Уязвимостей | Вредоносного кода | Инфицированных сайтов |
|---|------|----------------|-------------|-------------------|-----------------------|
| Ручной метод поиска и анализ исходного кода | 77 | 77 | 442 | 4 | 1 |
| Автоматизированный метод поиска | 5483 | 1946 | 12992 | 1408 | 33 |

5.1. Автоматическое сканирование

Распределение уязвимостей, обнаруженных с помощью сканера системы контроля защищенности и соответствия стандартам MaxPatrol, по различным типам представлено в Табл. 3 и на Рис. 2. Приложения, в которых не было обнаружено уязвимостей, при расчете доли уязвимых сайтов не учитывались. Стоит отметить, что уязвимости, связанные с ошибками обработки возвращаемых (Improper Output Handling) и входных (Improper Input Handling) данных, могут служить причиной реализации большинства выявленных уязвимостей, поэтому далее они не рассматриваются.

Кроме того, в статистику, полученную при автоматическом сканировании, не вошла такая распространенная уязвимость веб-приложений, как «Подделка HTTP-запросов» (Cross-Site Request Forgery, CSRF) [5]. Эта ошибка в том или ином виде встречалась во всех исследованных приложениях.

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

| Тип уязвимости | OWASP Top Ten 2010 | CWE ID | CAPEC ID | Доля уязвимостей, % | Доля уязвимых сайтов, % |
|-------------------------|--------------------|--------|----------|---------------------|-------------------------|
| Cross-Site Scripting | A2 | 79 | 18,19,63 | 33,64% | 23,48% |
| Improper Input Handling | | 20 | | 10,31% | 6,94% |
| Malware Detect | | | | 10,84% | 1,70% |
| Fingerprinting | | 205 | 224 | 10,02% | 66,91% |
| Server Misconfiguration | A6 | 16 | | 9,25% | 61,72% |
| SQL Injection | A1 | 89 | 66 | 7,70% | 10,69% |

| | | | | | |
|---|--------|---------|---------|-------|--------|
| Improper Output Handling | | 116 | | 7,28% | 12,74% |
| Predictable Resource Location | A7 | 425 | 87 | 7,02% | 46,87% |
| Insufficient Anti-automation | A7 | 799,804 | | 6,41% | 42,81% |
| Insufficient Transport Layer Protection | A10 | 311,523 | | 5,78% | 38,54% |
| HTTP Response Splitting | | 113 | 34 | 0,65% | 1,54% |
| SSI Injection | A1 | 97 | 101 | 0,61% | 0,98% |
| Information Leakage | A6 | 200 | 118 | 0,55% | 1,75% |
| Path Traversal | A4 | 22 | 126 | 0,25% | 1,18% |
| URL Redirector Abuse | A8 | 601 | | 0,24% | 0,87% |
| Application Misconfiguration | A6 | 16 | | 0,08% | 0,51% |
| Remote File Inclusion (RFI) | | 98 | 193,253 | 0,08% | 0,41% |
| OS Commanding | A1 | 78 | 88 | 0,07% | 0,21% |
| Content Spoofing | | 345 | 148 | 0,01% | 0,05% |
| Denial of Service | A7 | 400 | 119 | 0,01% | 0,05% |
| Directory Indexing | | 548 | 127 | 0,01% | 0,05% |
| Improper File System Permissions | | 280 | 17 | 0,01% | 0,05% |
| Insufficient Authorization | A4, A7 | 284 | | 0,01% | 0,05% |

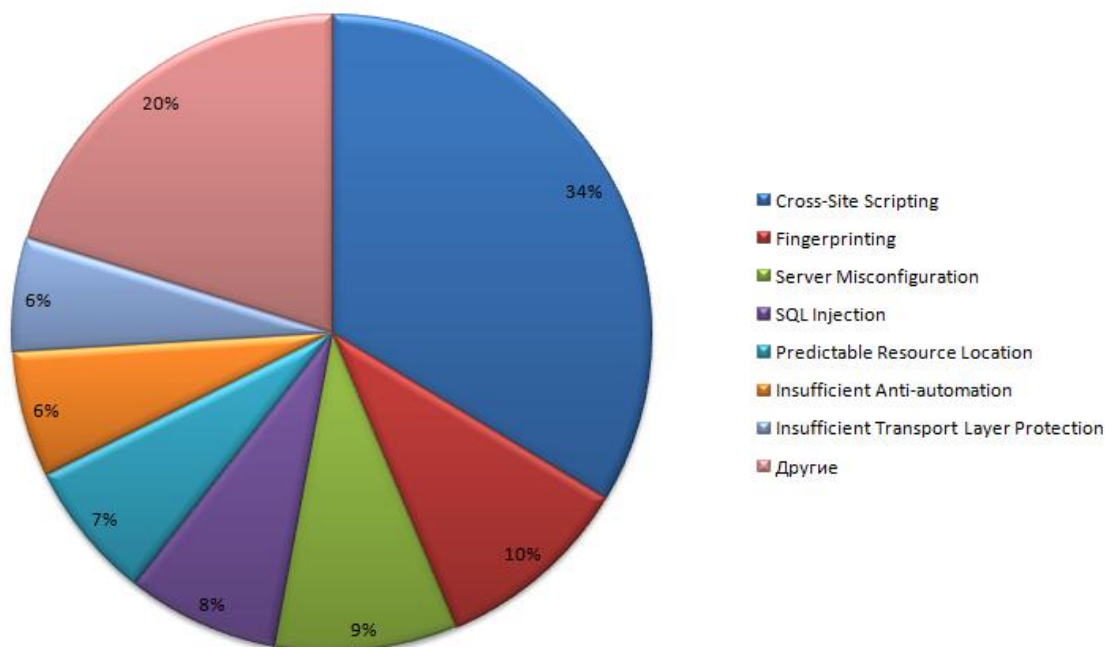


Рисунок 2. Статистика уязвимостей веб-приложений (автоматическое сканирование)

Степень распространения уязвимостей различных типов отражена на Рис. 3.

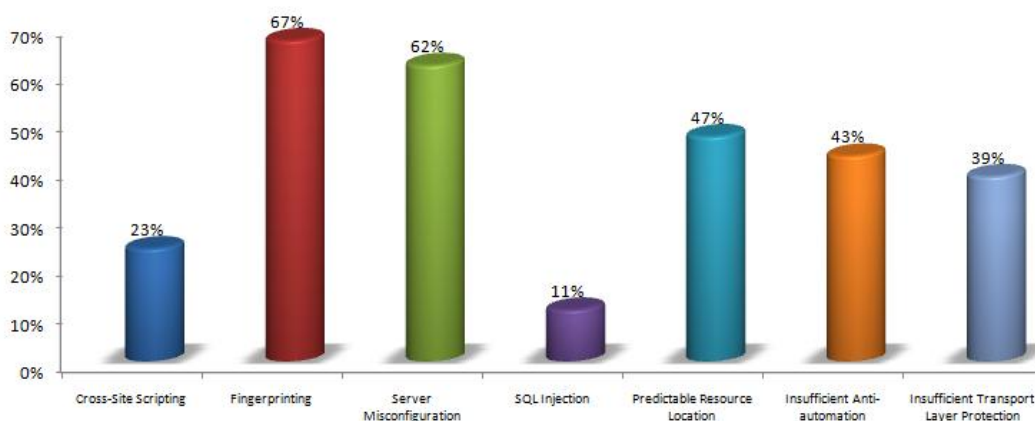


Рисунок 3. Степень распространения уязвимостей на сайтах (автоматическое сканирование)

Наиболее распространенными являются ошибки, допускаемые администраторами при обслуживании серверов (Server Misconfiguration и Fingerprinting). Такие уязвимости составляют приблизительно 20% от числа всех обнаруженных и встречаются на 62-67% исследованных сайтов. Таким образом, 2/3 сайтов содержит недостатки администрирования сервером. Основной ошибкой администраторов является использование стандартной конфигурации сервера; это во многом упрощает для злоумышленников задачу проведения и развития атаки. Тот факт, что проблемы администрирования серверов являются самыми распространенными среди уязвимостей на сайтах, объясняется также тем, что в настоящее

время широко используются системы управления сайтами; исходный код таких систем часто оказывается более защищенным, чем код приложений, разрабатываемых для конкретных сайтов. После развертывания готового «коробочного» веб-приложения администраторам следует применять на серверах защищенные конфигурации (в том числе рассмотреть возможность использования Web Application Firewall); в настоящее время большинство администраторов пренебрегает этими мерами защиты.

Другая распространенная уязвимость связана с недостаточным противодействием механизмам автоматизации (Insufficient Anti-automation). Почти в половине исследованных веб-приложений отсутствуют защитные механизмы: не используются CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), средства противодействия автоматизированному сбору email-адресов и пр.

Достаточно часто наблюдается предсказуемое расположение ресурсов (Predictable Resource Location) - такие уязвимости были обнаружены на 47% исследованных сайтов. Эта ошибка обычно бывает связана с использованием легко угадываемых названий файлов и каталогов в пространстве корневой директории веб-сервера (например, расположение панели администрирования сайтом в каталоге «admin»).

Пятое место по распространенности уязвимостей на сайтах занимает проблема передачи конфиденциальных данных без какой-либо криптографической защиты (Insufficient Transport Layer Protection). Уязвимость связана с тем, что важные данные (в том числе персональные данные пользователей) передаются по протоколу HTTP, который является открытым, вследствие чего данные могут быть перехвачены. Для решения этой проблемы рекомендуется использовать защищенный протокол SSL 3.0 или TLS 1.0 при обмене конфиденциальной информацией между сервером и клиентом.

Шестое место по распространенности заняла уязвимость «Межсайтовое выполнение сценариев» (Cross-Site Scripting, XSS), на долю которой приходится около 34% всех обнаруженных недостатков. Данная уязвимость была выявлена в 23% исследованных приложений. В отличие от недостатков, рассмотренных выше, уязвимость «Межсайтовое выполнение сценариев» связана в первую очередь с ошибками, допущенными при разработке приложений. Уязвимость «Межсайтовое выполнение сценариев», по оценке CWE/SANS [6], является наиболее распространенной ошибкой, допускаемой разработчиками приложений.

Седьмой по степени распространенности является уязвимость «Внедрение операторов SQL» (SQL Injection), на долю которой приходится приблизительно 8% всех обнаруженных ошибок. Данная уязвимость была обнаружена в 11% проанализированных приложений. Довольно часто успешная эксплуатация уязвимости «Внедрение операторов SQL» позволяет злоумышленнику нарушить все свойства обрабатываемой информации в атакуемой информационной системе. Данная уязвимость, по оценке CWE/SANS [6], является второй по распространенности ошибкой, допускаемой разработчиками приложений.

5.1.1. Анализ уязвимостей на инфицированных сайтах

Интересна позиция, которую в статистике занимает обнаружение образцов вредоносного кода (см. Табл. 3) на 34 анализируемых сайтах. Присутствие вредоносного кода свидетельствует о том, что веб-приложение содержит инфицированный код (Trojan-Spy backdoor, Code.JS, Code.I и т.д.), из-за чего на компьютеры посетителей такого сайта может быть установлено вредоносное программное обеспечение. Статистика уязвимостей с высоким уровнем опасности, обнаруженных на сайтах, которые содержат инфицированный код, показывает, что наиболее вероятным путем распространения вредоносного кода в этих приложениях является эксплуатация следующих уязвимостей:

- Внедрение операторов SQL (SQL Injection)
- Внедрение серверных расширений (SSI Injection)
- Выполнение команд ОС (OS Commanding)
- Выход за корневой каталог веб-сервера (Path Traversal)¹

Процесс эксплуатации подобных уязвимостей достаточно легко автоматизируется, а широкая распространенность таких ошибок в веб-приложениях позволяет проводить массовые «дефейсы», добавлять инфицированный код на страницы уязвимых веб-узлов.

Анализ статистики распределения критических уязвимостей на инфицированных сайтах (см. Рис. 4) показывает, что уязвимость типа «Внедрение операторов SQL» заметно преобладает на зараженных сайтах.

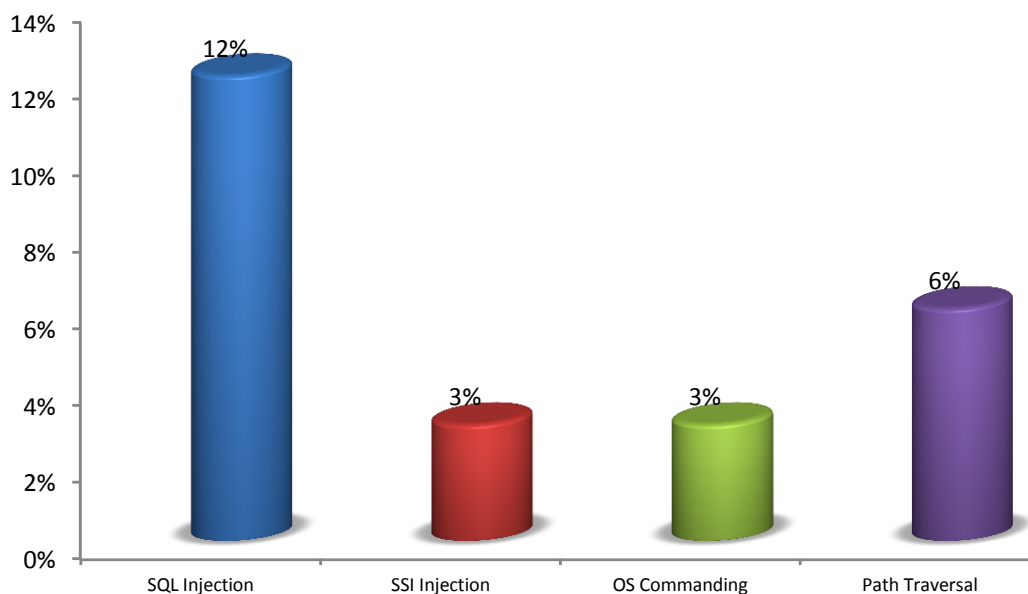


Рисунок 4. Степень распространения критических уязвимостей на инфицированных сайтах

Рассмотрим аналогичные показатели для сайтов, на которых не было обнаружено инфицированных страниц (см. Рис. 5).

¹ Следует помнить, что выход за корневой каталог веб-сервера во многих случаях позволяет выполнять команды на сервере. Это возможно, когда уязвимость содержится в функциях `include()`, `require()` и т.п.

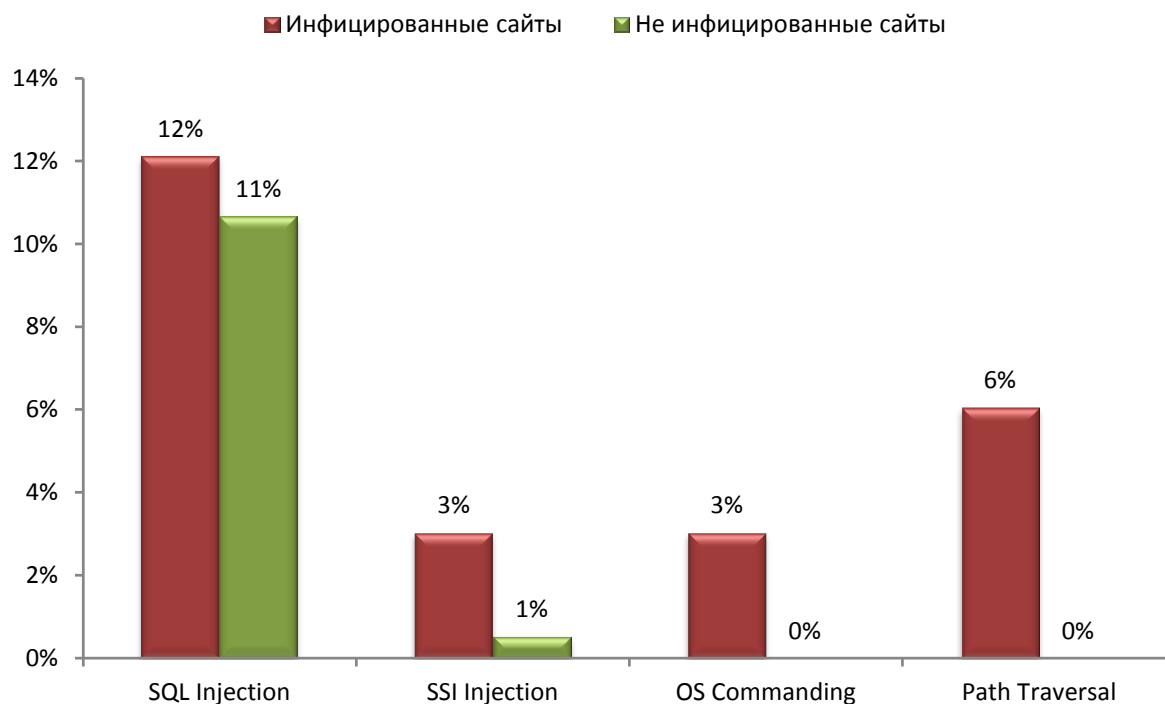


Рисунок 5. Распределение критических уязвимостей на сайтах

Таким образом можно сделать вывод, что практически все сайты, содержащие уязвимости, которые позволяют непосредственно выполнять команды на сервере, были автоматизированно заражены вредоносным кодом.

5.1.2. Динамика обнаружения уязвимостей

Данные, которые были получены при анализе результатов автоматических сканирований, проведенных за прошедшие четыре года [7,8,9], представлены в Табл. 4 и на Рис. 6.

Таблица 4. Динамика автоматизированного обнаружения уязвимостей в веб-приложениях за четыре года

| | 2006 год | 2007 год | 2008 год | 2009 год |
|-------------------|----------|----------|----------|----------|
| Узлов | 111936 | 31891 | 10400 | 5483 |
| Уровень опасности | | | | |
| Высокая | 15,83% | 23,05% | 90,96% | 13,19% |
| Средняя | 84,17% | 37,67% | 41,77% | 17,20% |
| Низкая | 0,00% | 7,72% | 12,83% | 59,60% |



Рисунок 6. Динамика обнаружения уязвимостей в веб-приложениях за четыре года (автоматическое сканирование)

Динамика получена на основе четырех наборов данных:

2006 год – пользователям предоставлена возможность бесплатно проверить защищенность своих веб-приложений. В этот набор данных вошли результаты исследования очень разнородных приложений (вплоть до статических и сайтов-«заглушек»).

2007 год – проверка защищенности веб-приложений становится платной услугой. Этим обусловлено сокращение числа сканируемых узлов в 3,5 раза. Статистика по-прежнему основана на анализе разнородных и статических сайтов, однако их количество значительно снизилось.

2008 год – набор данных в большей степени основан на анализе веб-приложений различных компаний, для которых важна реальная безопасность внешних приложений (в область сканирования входит два крупных хостинг-центра).

2009 год – период Мирового финансового кризиса. Денежные средства распределяются наиболее эффективно. Уязвимости, обнаруженные в прошлом году, устранены. Инициативы по разработке новых приложений заморожены (в область сканирования входит один крупный хостинг-центр).

Таким образом, данные за 2006-2007 годы иллюстрируют результаты сканирования «любых» приложений, данные за 2008 – результат сканирования недавно разработанных веб-приложений, а данные за 2009 год – результат сканирования приложений в компаниях, которые выполняют анализ защищенности своих веб-приложений на регулярной основе.

Процентное соотношение устранения выявленных уязвимостей в 2009 году, по результатам сканирования в 2008 году, представлено в Табл. 5 и на Рис. 7 - Рис. 8. Указанным критериям соответствовало 768 веб-приложений.

Таблица 5. % сайтов с уязвимостями различной степени риска

| | 2008 год | 2009 год | Устранение | % Устранения |
|-------------------|----------|----------|------------|--------------|
| Уровень опасности | | | | |
| Высокая | 56,77% | 19,40% | 37,37% | 65,83% |
| Средняя | 16,41% | 27,99% | -11,58% | N/A |
| Низкая | 87,50% | 60,42% | 27,08% | 30,95% |
| Итого | 95,48% | 77,03% | 18,45% | 19,33% |

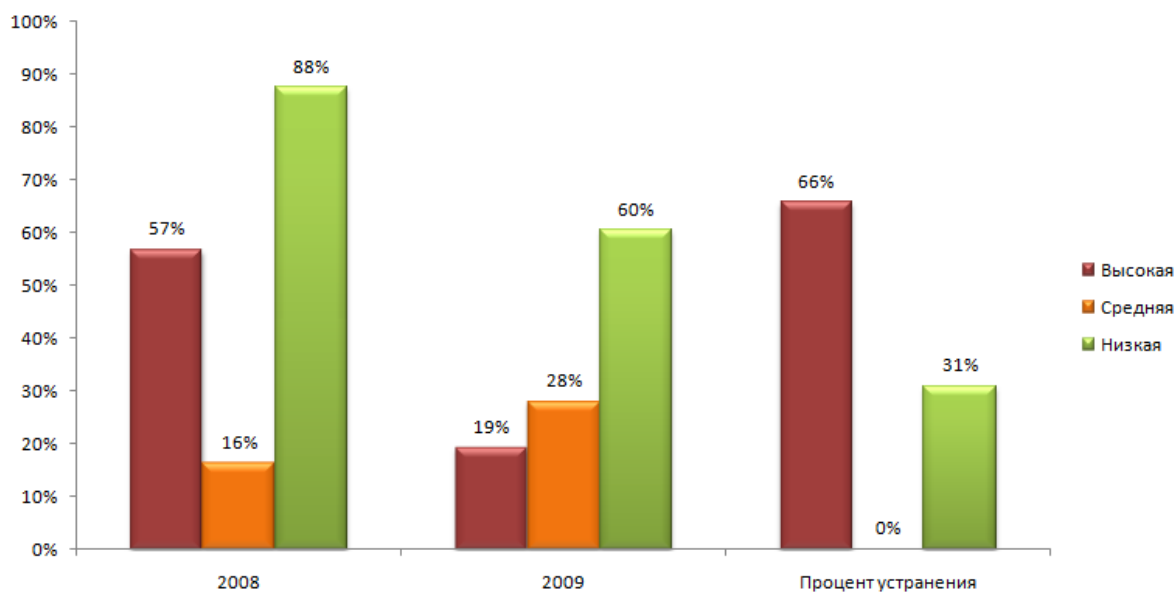


Рисунок 7. % сайтов с уязвимостями различной степени риска

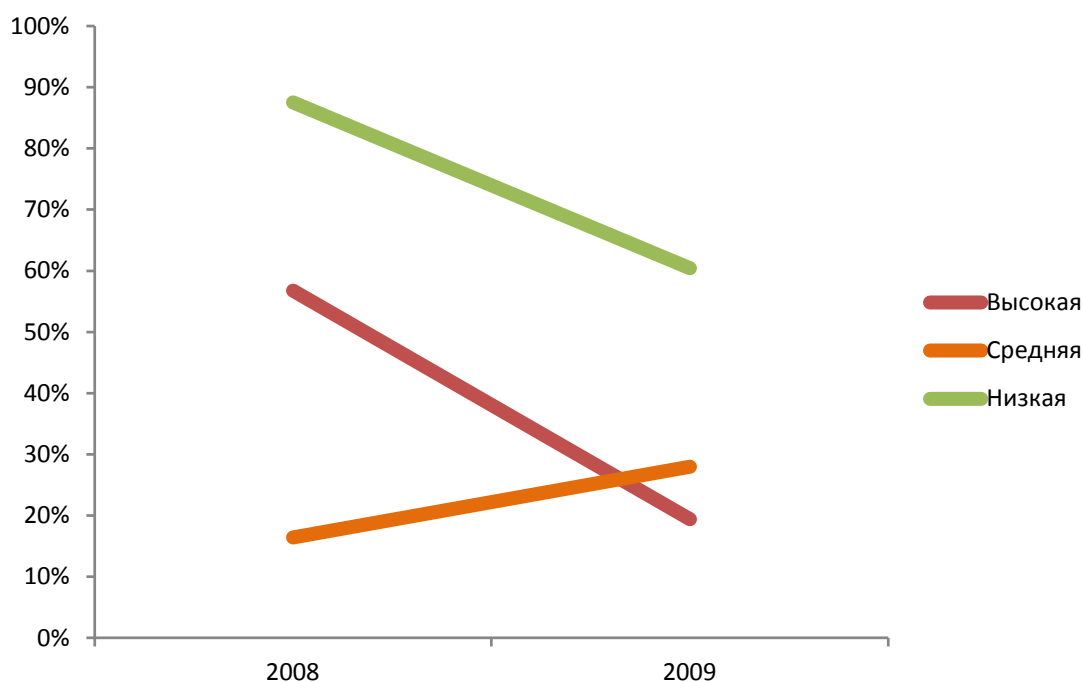


Рисунок 8. Динамика уязвимых сайтов (по уровню критичности, %)

Рассматривая процесс устранения отдельных уязвимостей на сайтах в течение года, были получены данные, представленные в Табл. 6 и на Рис. 9.

Таблица 6. % устраненных уязвимостей в веб-приложениях за год (по типу)

| | 2008 год | 2009 год | Устранение | % Устранения |
|-------------------------|----------|----------|------------|--------------|
| Узлов | | | 768 | |
| Уязвимости | | | | |
| Cross-Site Scripting | 45,05% | 13,67% | 31,38% | 69,66% |
| SQL Injection | 16,67% | 5,34% | 11,33% | 67,97% |
| Path Traversal | 1,30% | 0,26% | 1,04% | 80,00% |
| Fingerprinting | 86,85% | 29,17% | 57,68% | 66,41% |
| HTTP Response Splitting | 4,04% | 0,65% | 3,39% | 83,91% |
| Information Leakage | 16,28% | 4,95% | 11,33% | 69,59% |

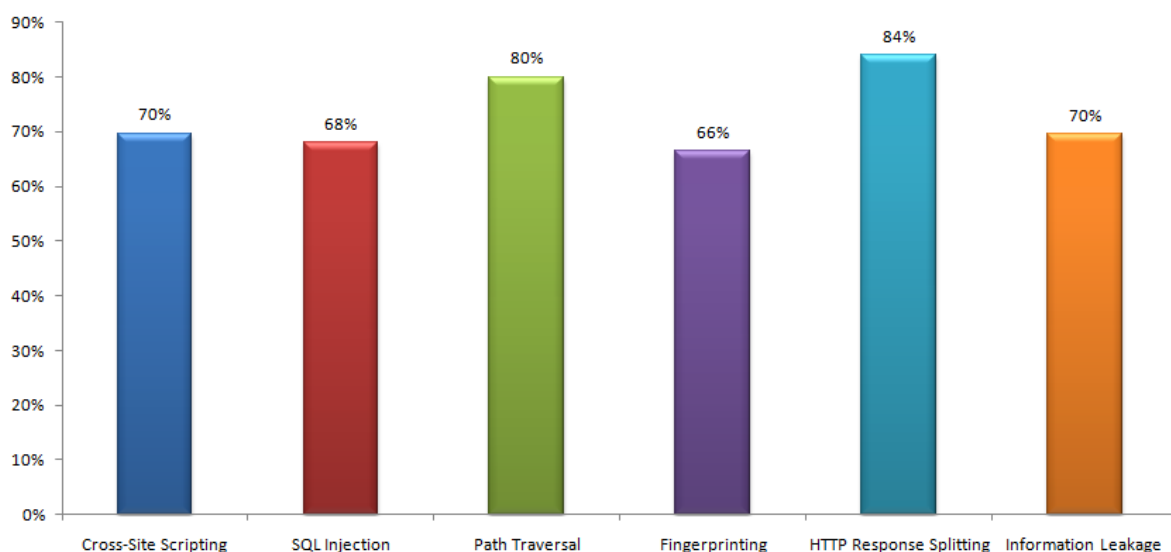


Рисунок 9. % устраненных уязвимостей в веб-приложениях за год (по типу)

Таким образом, в течение года число сайтов, содержащих критические уязвимости, снизилось на 37%, что соответствует устранению всех уязвимостей критического уровня опасности в 66% случаях. Положительная тенденция также замечена для сайтов, содержащих уязвимости с низким уровнем опасности. Так, общий процент устранения всех подобных уязвимостей составил приблизительно 31%. В отношении сайтов, содержащих уязвимости среднего уровня критичности, напротив, отмечена отрицательная тенденция, т.е. в течение года число подобных сайтов только возросло. Общий же процент устранения всех обнаруженных уязвимостей с 2008 года по 2009 год составил около 20%.

5.2. Детальный анализ

Распределение уязвимостей, обнаруженных в ходе детального анализа веб-приложений (преимущественно с использованием методики «черного-ящика») по различным типам представлено в Табл. 7 и на Рис. 10.

Таблица 7. Статистика уязвимостей веб-приложений (детальный анализ)

| Тип уязвимости | OWASP Top Ten 2010 | CWE ID | CAPEC ID | Доля уязвимостей, % | Доля уязвимых сайтов, % |
|-------------------------------|--------------------|-------------|----------|---------------------|-------------------------|
| Cross-Site Scripting | A2 | 79 | 18,19,63 | 19,23% | 27,27% |
| SQL Injection | A1 | 89 | 66 | 17,65% | 49,35% |
| Information Leakage | A6 | 200 | 118 | 12,44% | 37,66% |
| Predictable Resource Location | A7 | 425 | 87 | 11,54% | 20,78% |
| Server Misconfiguration | A6 | 16 | | 11,09% | 37,66% |
| Brute Force | A7 | 330,331,340 | 112 | 5,88% | 22,08% |

| | | | | | |
|---|-----|---------|---------|-------|--------|
| Fingerprinting | | 205 | 224 | 4,52% | 10,39% |
| Application Misconfiguration | A6 | 16 | | 4,30% | 16,88% |
| Insufficient Transport Layer Protection | A10 | 311,523 | | 2,71% | 15,58% |
| Cross-Site Request Forgery | A5 | 352 | 62 | 1,81% | 7,79% |
| OS Commanding | A1 | 78 | 88 | 1,36% | 6,49% |
| Insufficient Authentication | A3 | 287 | | 1,13% | 6,49% |
| Directory Indexing | | 548 | 127 | 0,90% | 3,90% |
| Denial of Service | A7 | 400 | 119 | 0,68% | 3,90% |
| Insufficient Authorization | A4 | 284 | | 0,68% | 3,90% |
| Path Traversal | A4 | 22 | 126 | 0,68% | 3,90% |
| SSI Injection | A1 | 97 | 101 | 0,68% | 3,90% |
| Improper File System Permissions | | 280 | 17 | 0,45% | 2,60% |
| Insufficient Session Expiration | A3 | 613 | 60 | 0,45% | 2,60% |
| Null Byte Injection | A1 | 158 | 52 | 0,45% | 2,60% |
| URL Redirector Abuse | A8 | 601 | | 0,45% | 2,60% |
| Content Spoofing | | 345 | 148 | 0,23% | 1,30% |
| Improper Input Handling | | 20 | | 0,23% | 1,30% |
| Insufficient Process Validation | | 691 | | 0,23% | 1,30% |
| Remote File Inclusion (RFI) | | 98 | 193,253 | 0,23% | 1,30% |

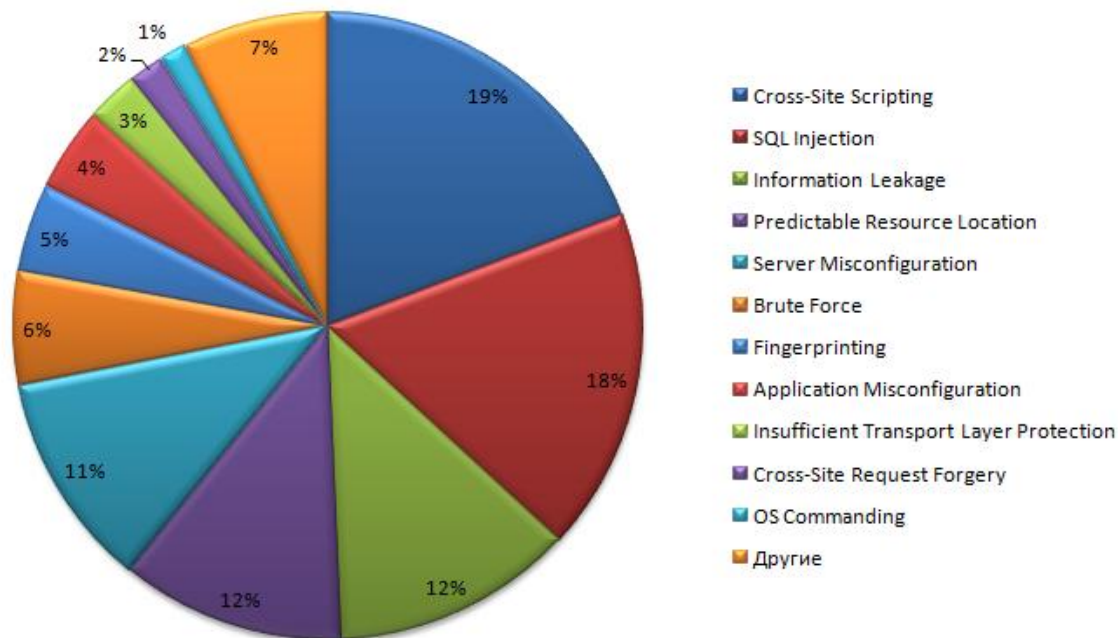


Рисунок 10. Статистика уязвимостей веб-приложений (детальный анализ)

Степень распространения уязвимостей, выявленных при детальном анализе веб-приложений, отражена на Рис. 11.

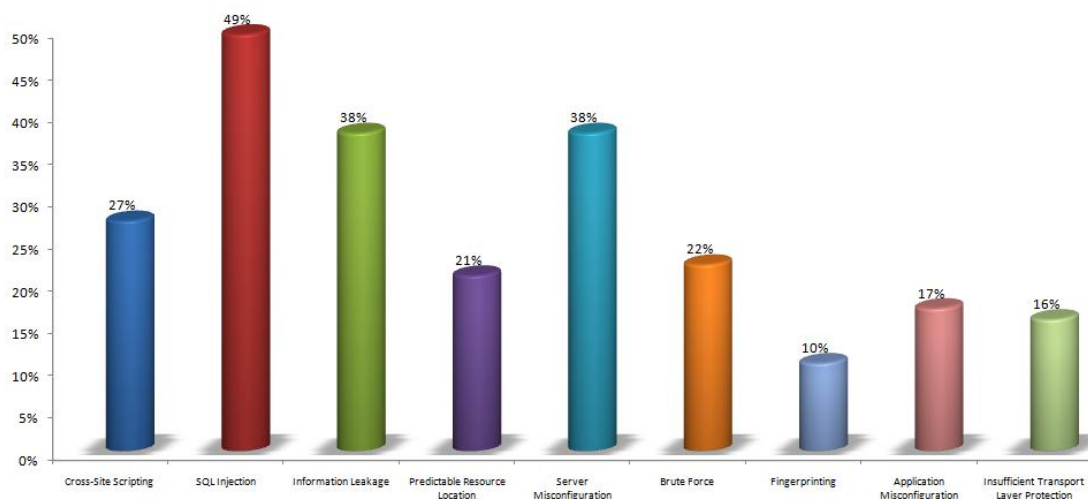


Рисунок 11. Распределение уязвимостей по сайтам (детальный анализ)

Так же, как и при автоматическом сканировании веб-приложений, при проведении детального анализа довольно часто встречались ошибки, допускаемые администраторами при обслуживании серверов (Server Misconfiguration).

С другой стороны, в отличие от автоматического сканирования веб-приложений, при проведении детального анализа наиболее часто встречалась уязвимость «Внедрение

операторов SQL» (SQL Injection). Данная уязвимость была обнаружена в 18% случаев, приблизительно в 49% всех исследуемых приложений. Таким образом, каждое второе веб-приложение содержало уязвимость «Внедрение операторов SQL».

Уязвимость, которая возглавляет список по числу обнаруженных – «Межсайтовое выполнение сценариев» (Cross-Site Scripting, XSS). На долю указанной уязвимости приходится большая часть всех обнаруженных ошибок (19%). Данная уязвимость была выявлена в 27% всех исследованных приложений.

Второе место по степени распространенности уязвимостей на сайтах занял недостаток, связанный с различными вариантами утечек конфиденциальной информации (Information Leakage). Степень возможного риска данной уязвимости может варьироваться от низкой до критической. Наиболее типичный пример таких ошибок – хранение конфиденциальных данных и резервных копий сценариев в общедоступных, но «скрытых» каталогах.

Таким образом, среди уязвимостей, связанных с разработкой веб-приложений, лидирующие позиции по вероятности обнаружения при детальном анализе занимает уязвимость на стороне веб-сервера (server-side) «Внедрение операторов SQL» (SQL Injection) и уязвимость, эксплуатируемая на стороне клиента (client-side), – «Межсайтовое выполнение сценариев» (Cross-Site Scripting, XSS).

Сравнительный анализ данных, полученных при детальном исследовании веб-приложений, и данных рейтинга TOP 25 наиболее опасных ошибок¹, допускаемых при разработке приложений, по оценке CWE/SANS за 2010 год [6] представлен на Рис. 12.

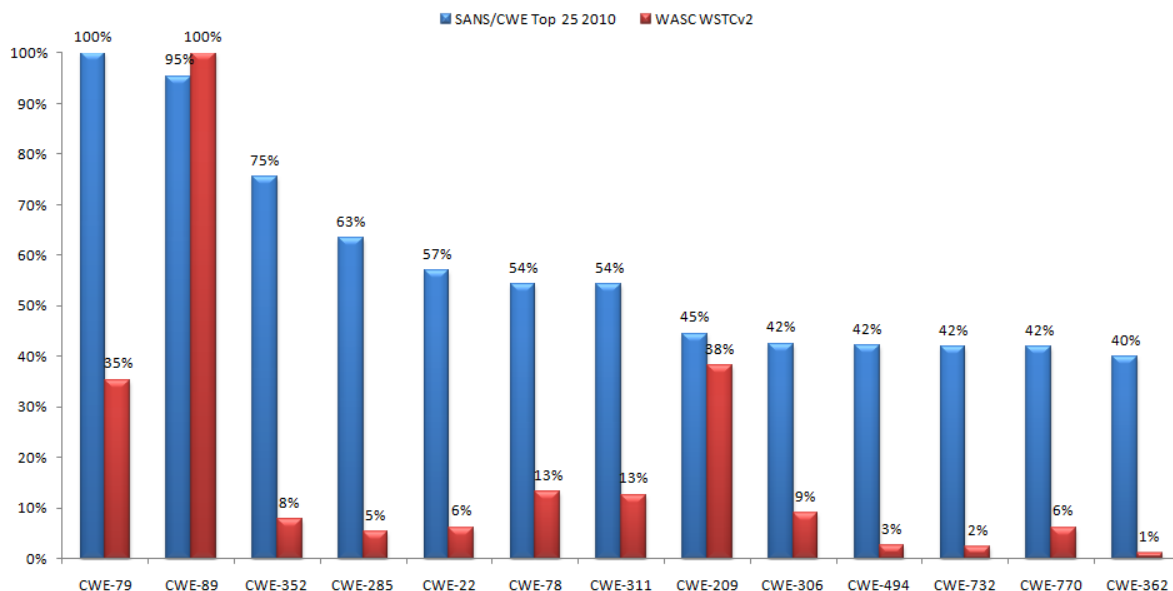


Рисунок 12. Сравнение распределения обнаруженных уязвимостей по различным типам с CWE/SANS Top 25 2010

Можно увидеть, что экспертная оценка CWE/SANS за 2010 год [6] практически сходится с данными, полученными при детальном анализе веб-приложений, для уязвимостей

¹ В качестве множителей использовались частота обнаружения уязвимости и степень ее критичности, рассчитанная по CVSSv2 [3, 4]. Для сведения различающихся наборов данных использовался подход, основанный на делении по максимальному значению из каждого набора данных. Сопоставление уязвимостей осуществлялось по разработанной матрице [10].

«Внедрение операторов SQL» (CWE-89) и различных вариантов утечки информации (CWE-209). Что же касается прочих уязвимостей, то, как показало сравнение с «живым» набором данных, степень их распространения и опасности несколько преувеличена.

5.3. Сопоставление наборов данных в контексте требований PCI DSS

Рассматривая наборы полученных данных уязвимых веб-приложений в контексте соответствия требованиям стандарта по защите информации в индустрии платежных карт PCI DSS, можно выделить те из них (см. Табл. 8), которые относятся к устранению конкретных уязвимостей в веб-приложениях. Кроме того, PCI DSS Technical and Operational Requirements for Approved Scanning Vendors (ASVs) содержит в себе схожие требования, но затрагивает только процесс ASV-сканирования по PCI (см. Табл. 9).

Таблица 8. Требования стандарта PCI DSS, регламентирующие обязательное устранение конкретных уязвимостей в веб-приложениях

| Требование PCI DSS v.1.2 | Процедура |
|---|---|
| 6.5.1 Cross-site scripting (XSS) | 6.5.1 Cross-site scripting (XSS) (Validate all parameters before inclusion.) |
| 6.5.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws. | 6.5.2 Injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries.) |
| 6.5.3 Malicious file execution | 6.5.3 Malicious file execution (Validate input to verify application does not accept filenames or files from users.) |
| 6.5.5 Cross-site request forgery (CSRF) | 6.5.5 Cross-site request forgery (CSRF) (Do not reply on authorization credentials and tokens automatically submitted by browsers.) |
| 6.5.6 Information leakage and improper error handling | 6.5.6 Information leakage and improper error handling (Do not leak information via error messages or other means.) |
| 6.5.7 Broken authentication and session management | 6.5.7 Broken authentication and session management (Properly authenticate users and protect account credentials and session tokens.) |
| 6.5.9 Insecure communications | 6.5.9 Insecure communications (Properly encrypt all authenticated and sensitive communications.) |

Таблица 9. Требования PCI DSS Technical and Operational Requirements for Approved Scanning Vendors (ASVs), регламентирующие обязательное выявление конкретных уязвимостей в веб-приложениях при проведении ASV-сканирования

| Требования Technical and Operational Requirements for Approved Scanning Vendors (ASVs) v.1.1 | Процедура |
|--|---|
| Web Server Check | <p>The ASV scanning solution must be able to test for all known vulnerabilities and configuration issues on web servers. New exploits are routinely discovered in web server products. The ASV scanning solution must be able to detect and report known exploits.</p> <p>Browsing of directories on a web server is not a good practice. The ASV scanning solution must be able to scan the web site and verify that directory browsing is not possible on the server.</p> |

| | |
|------------------------------|--|
| | The ASV scanning solution must be able to detect all known CGI vulnerabilities. |
| Custom Web Application Check | <p>The ASV scanning solution must be able to detect the following application vulnerabilities and configuration issues:</p> <ul style="list-style-type: none"> • Unvalidated parameters which lead to SQL injection attacks • Cross-site scripting (XSS) flaws |

Оценка полученных статистических данных по критериям, приведенным в Табл. 8 и Табл. 9, представлена в Табл. 10 и на Рис. 13–15.

Таблица 10. Доля сайтов, не соответствующих требованиям стандарта PCI DSS при оценке веб-приложений различными методами

| Требование PCI DSS v.1.2 | Суммарная доля несоответствия, обобщенные данные (доля сайтов, %) | Доля несоответствия при автоматическом сканировании (доля сайтов, %) | Доля несоответствия при детальном анализе (доля сайтов, %) |
|---|---|--|--|
| 6.5.1 Cross-site scripting (XSS) | 23,43% | 23,48% | 27,27% |
| 6.5.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws. | 14,88% | 13,16% | 58,44% |
| 6.5.3 Malicious file execution | 1,68% | 1,70% | 1,30% |
| 6.5.5 Cross-site request forgery (CSRF) | Не применимо | Не применимо | 7,79% |
| 6.5.6 Information leakage and improper error handling | 15,03% | 14,29% | 37,66% |
| 6.5.7 Broken authentication and session management | 1,53% | 0,10% | 33,77% |
| 6.5.9 Insecure communications | 37,47% | 38,54% | 15,58% |
| Требование Technical and Operational Requirements for Approved Scanning Vendors (ASVs) v.1.1 | | | |
| Web Server Check | Не применимо | 61,77% | Не применимо |
| Application Server Check | Не применимо | 0,51% | Не применимо |
| Custom Web Application Check | Не применимо | 31,65% | Не применимо |

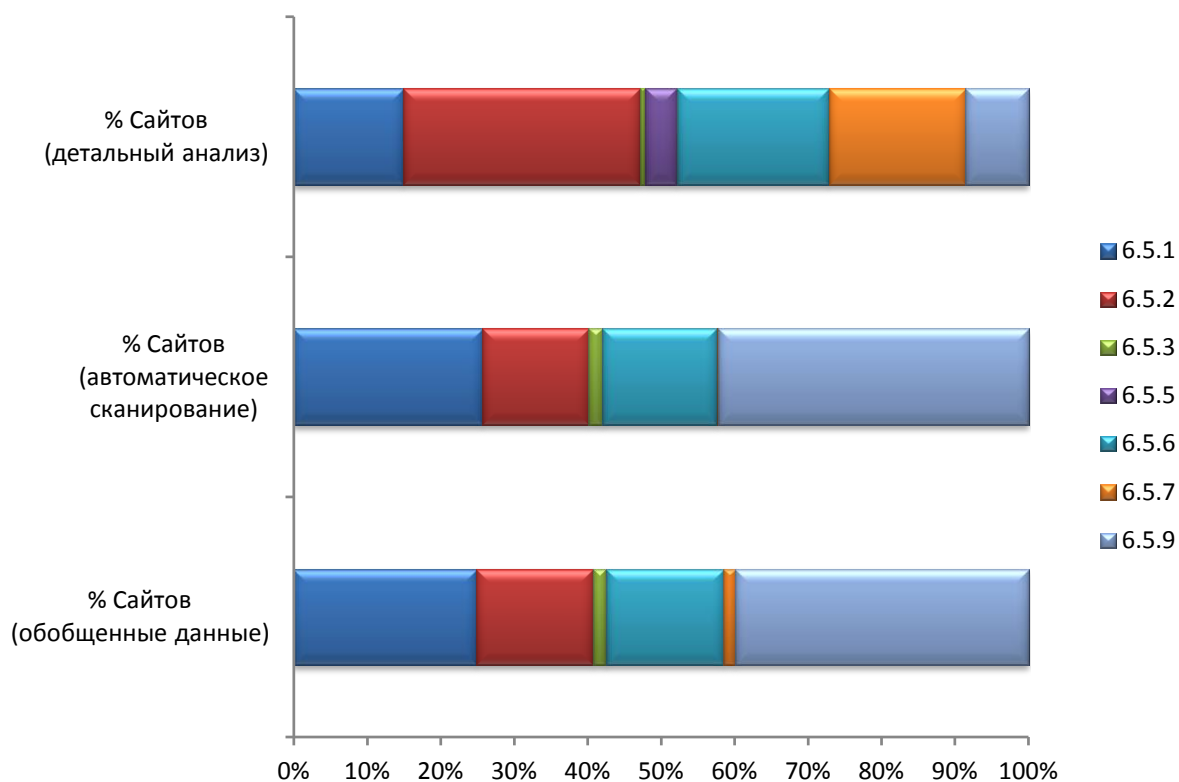


Рисунок 13. Распределение сайтов, не удовлетворяющих требованиям стандарта PCI DSS

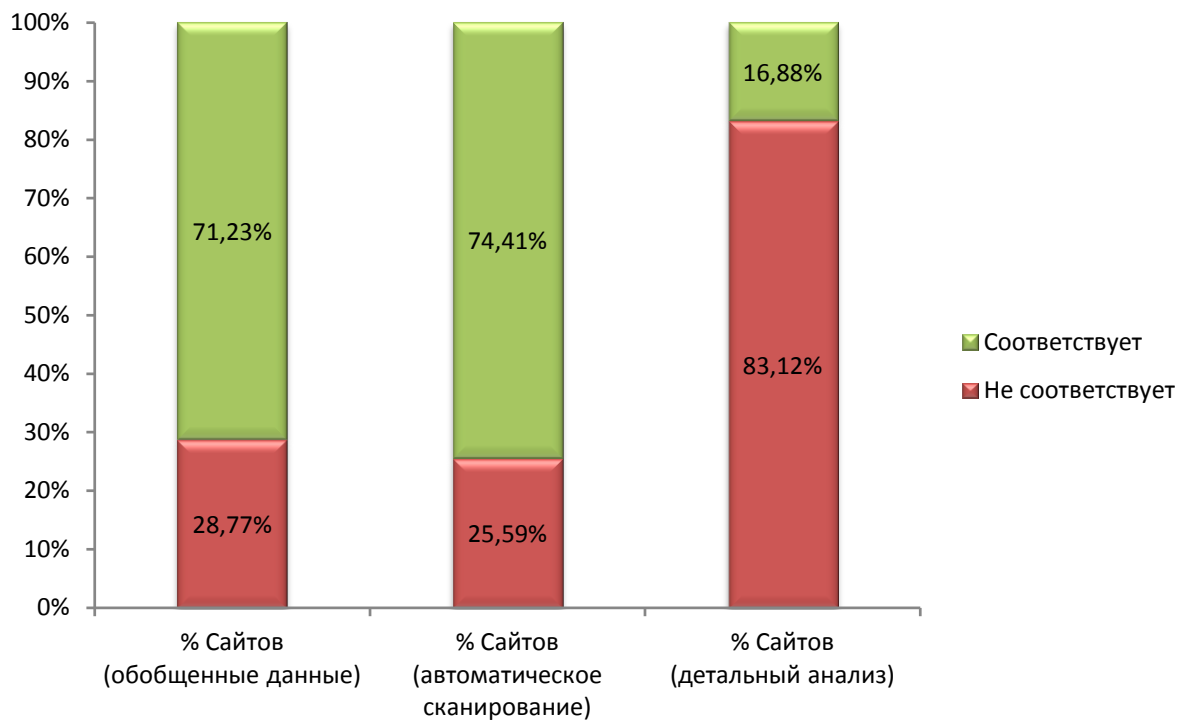


Рисунок 14. Уровень соответствия анализируемых веб-приложений требованиям стандарта PCI DSS (QSA)

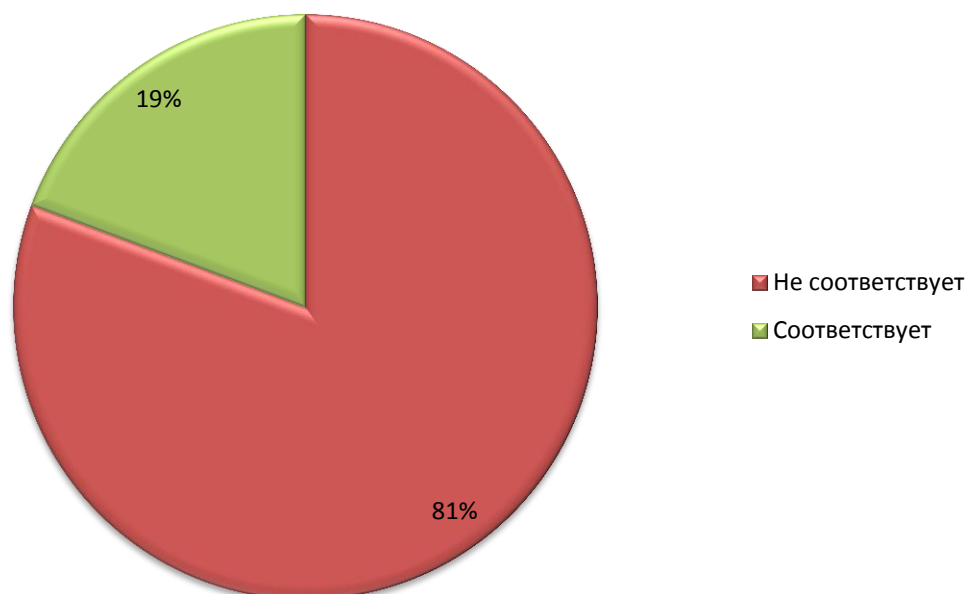


Рисунок 15. Уровень соответствия анализируемых веб-приложений требованиям стандарта PCI DSS (ASV)

Таким образом, при проведении ASV-сканирования веб-приложений около 81% из них оказались несоответствующими требованиям стандарта PCI DSS. В то же время при проведении более глубокого анализа было выявлено, что 84% веб-приложений не удовлетворяет требованиям стандарта по защите информации в индустрии платежных карт.

5.4. Обобщенные данные

Обобщенные результаты анализа распределения уязвимостей, обнаруженных с помощью детального анализа веб-приложений и при автоматическом сканировании, по различным типам WSTCv2 и классам WSTCv1 представлены в Табл. 11 и на Рис. 16.

Таблица 11. Статистика уязвимостей веб-приложений (обобщенные данные)

| Тип уязвимости | Автоматическое сканирование | | Детальный анализ | |
|-------------------------|-----------------------------|----------------------------|------------------------|----------------------------|
| | Доля уязвимостей, % | Доля уязвимых сайтов, % | Доля уязвимостей, % | Доля уязвимых сайтов, % |
| Cross-Site Scripting | 33,64% | 23,48% | 19,23% | 27,27% |
| Improper Input Handling | 10,31% | 6,94% | 0,23% | 1,30% |
| Fingerprinting | 10,02% | 66,91% | 4,52% | 10,39% |
| Server Misconfiguration | 9,25% | 61,72% | 11,09% | 37,66% |
| SQL Injection | 7,70% | 10,69% | 17,65% | 49,35% |

| | | | | |
|---|-------|--------|--------|--------|
| Improper Output Handling | 7,28% | 12,74% | 0% | 0% |
| Predictable Resource Location | 7,02% | 46,87% | 11,54% | 20,78% |
| Insufficient Anti-automation | 6,41% | 42,81% | 0% | 0% |
| Insufficient Transport Layer Protection | 5,78% | 38,54% | 2,71% | 15,58% |
| HTTP Response Splitting | 0,65% | 1,54% | 0% | 0% |
| SSI Injection | 0,61% | 0,98% | 0,68% | 3,90% |
| Information Leakage | 0,55% | 1,75% | 12,44% | 37,66% |
| Path Traversal | 0,25% | 1,18% | 0,68% | 3,90% |
| URL Redirector Abuse | 0,24% | 0,87% | 0,45% | 2,60% |
| Application Misconfiguration | 0,08% | 0,51% | 4,30% | 16,88% |
| Remote File Inclusion (RFI) | 0,08% | 0,41% | 0,23% | 1,30% |
| OS Commanding | 0,07% | 0,21% | 1,36% | 6,49% |
| Content Spoofing | 0,01% | 0,05% | 0,23% | 1,30% |
| Denial of Service | 0,01% | 0,05% | 0,68% | 3,90% |
| Directory Indexing | 0,01% | 0,05% | 0,90% | 3,90% |
| Improper File System Permissions | 0,01% | 0,05% | 0,45% | 2,60% |
| Insufficient Authorization | 0,01% | 0,05% | 0,68% | 3,90% |
| Brute Force | 0% | 0% | 5,88% | 22,08% |
| Cross-Site Request Forgery | 0% | 0% | 1,81% | 7,79% |
| Insufficient Authentication | 0% | 0% | 1,13% | 6,49% |
| Improper File System Permissions | 0% | 0% | 0,45% | 2,60% |
| Insufficient Session Expiration | 0% | 0% | 0,45% | 2,60% |
| Null Byte Injection | 0% | 0% | 0,45% | 2,60% |
| Insufficient Process Validation | 0% | 0% | 0,23% | 1,30% |

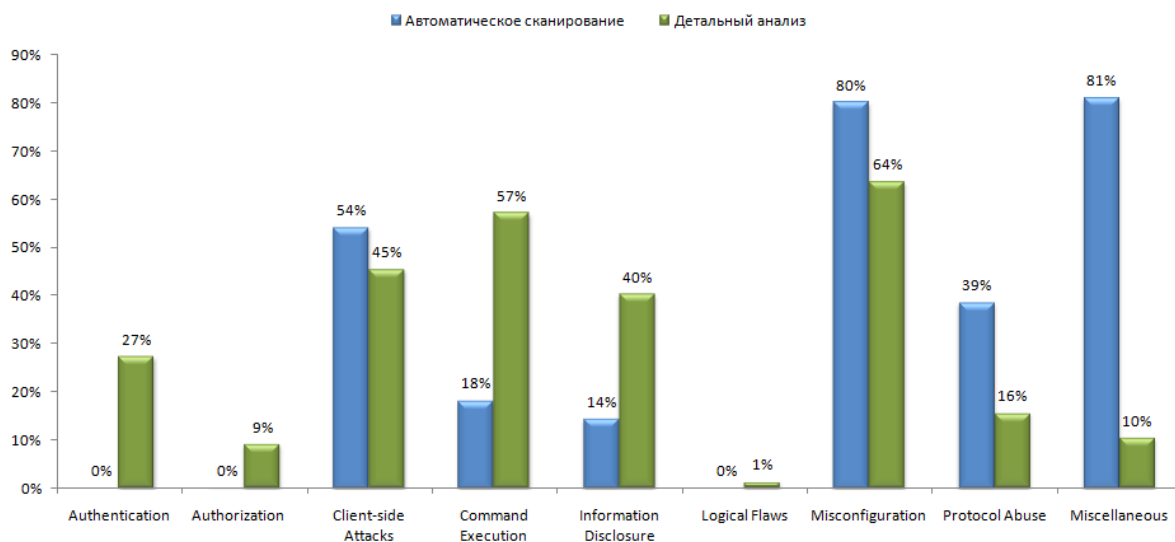


Рисунок 16. Распределение уязвимостей на сайтах по классам WSTCv1 (обобщенные данные)

Анализ количества уязвимостей различной степени риска (Рис. 17 и 18) показывает, что среди ошибок, обнаруженных при автоматическом сканировании, наиболее распространенными являются уязвимости с низкой степенью критичности (Рис. 17), а среди ошибок, обнаруженных при детальном анализе, – уязвимости с высокой степенью критичности (Рис. 18).

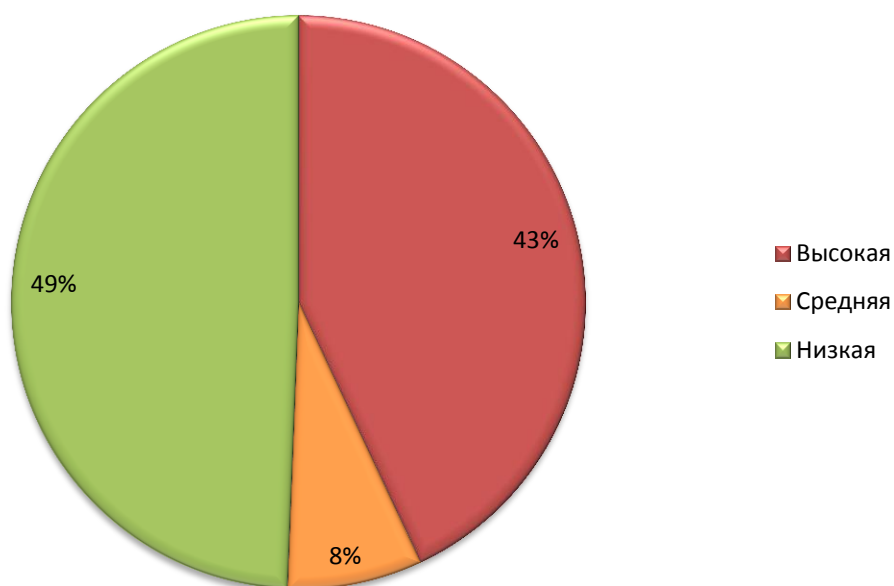


Рисунок 17. Количество уязвимостей различной степени риска (автоматизированное сканирование)

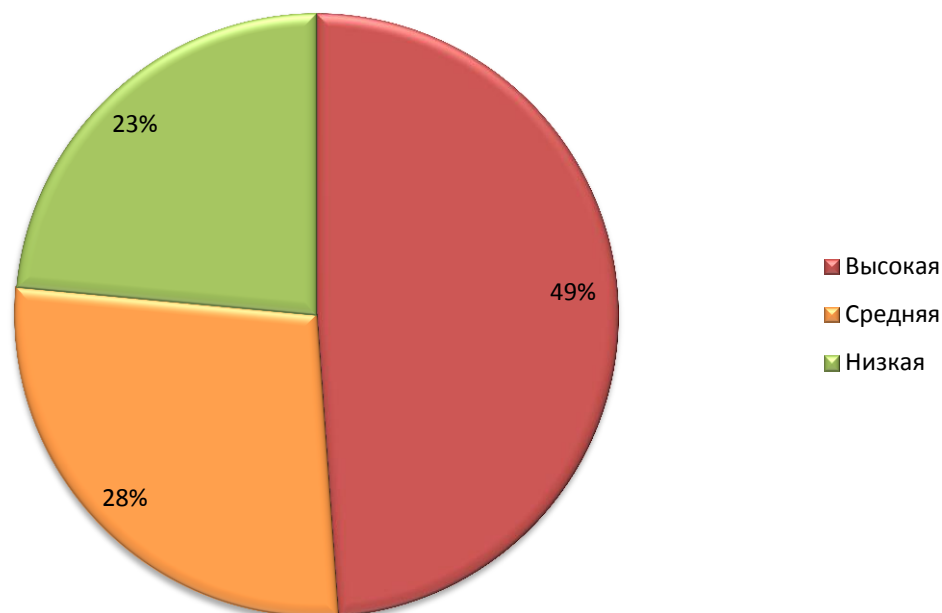


Рисунок 18. Количество уязвимостей различной степени риска (детальный анализ)

Анализ уязвимостей, связанных с ошибками разработки веб-приложений (Рис. 19), показывает, что наиболее часто здесь встречаются уязвимости типа «Межсайтовое выполнение сценариев» (Cross-Site Scripting) и «Внедрение операторов SQL» (SQL Injection).

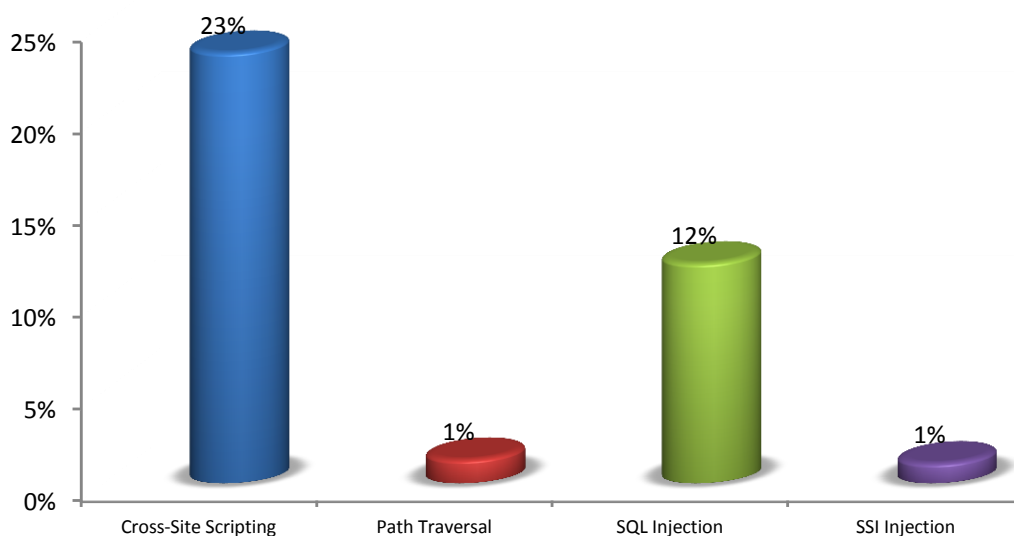


Рисунок 19. Наиболее распространенные уязвимости, допускаемые разработчиками веб-приложений (обобщенные данные)

Данные о распределении уязвимостей и уязвимых сайтов по природе возникновения ошибок (согласно классам WASC WSTCv2) представлены на Рис. 20.

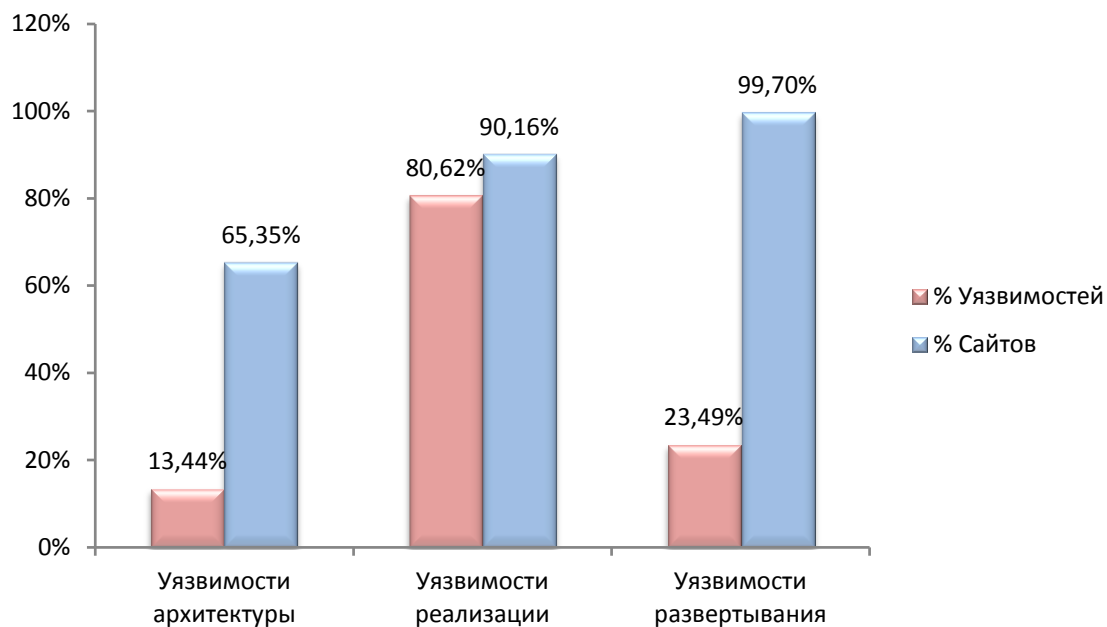


Рисунок 20. Распределение уязвимостей согласно классам WASC WSTCv2 (обобщенные данные)

Таким образом, в значительной степени преобладают сайты, содержащие ошибки, связанные с механизмом развертывания веб-приложения. Гораздо реже встречаются уязвимости архитектуры и сайты, содержащие такие уязвимости. Уязвимости разработки (реализации приложения) были выявлены на 90% анализируемых сайтов.

На Рис. 21 представлено распределение узлов по степени опасности обнаруженных на них уязвимостей. Как видно из гистограммы, на восьми сайтах из десяти при их детальном анализе (преимущественно с использованием методики «черного ящика») можно обнаружить уязвимость высокого уровня опасности. Вероятность обнаружения уязвимости аналогичного уровня риска с помощью автоматизированных средств анализа составляет 35%.

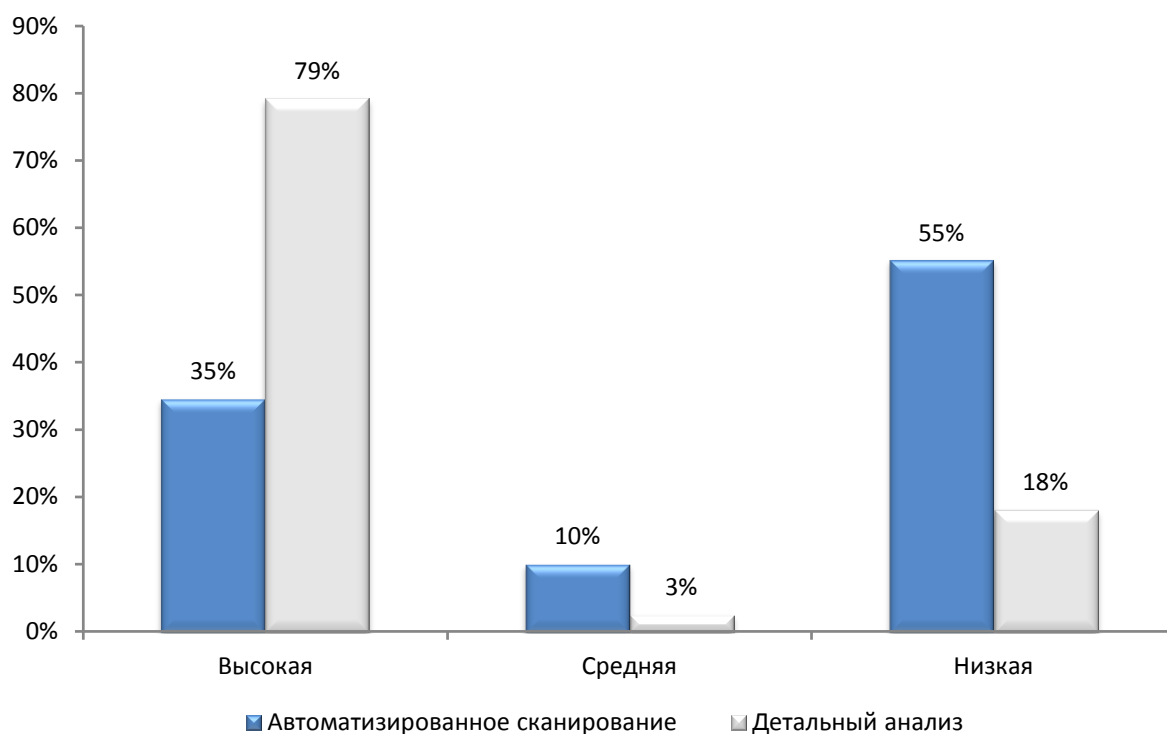


Рисунок 21. Распределение узлов по максимальному уровню обнаруженных на них уязвимостей (доля сайтов, %)

Рассмотрим суммарную вероятность обнаружения уязвимостей различной степени риска при использовании разных подходов к анализу веб-приложений (Рис. 22).

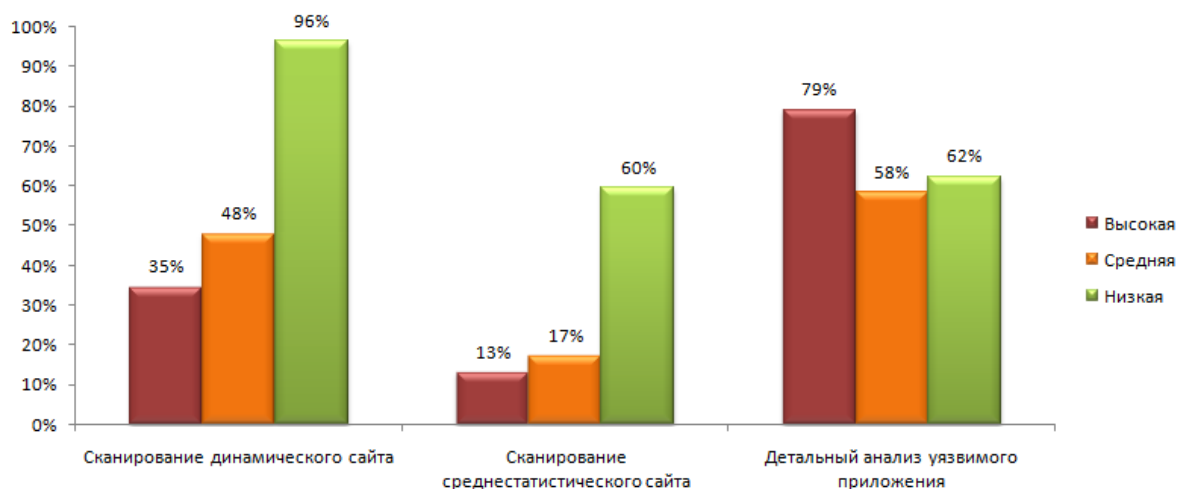


Рисунок 22. Вероятность обнаружения уязвимостей различной степени риска

Из гистограммы видно, что на каждом втором сайте были обнаружены критические уязвимости, и в 58% случаев в программном обеспечении веб-приложения содержались уязвимости средней степени риска.

6. ВЫВОДЫ

На основании полученных данных можно сделать следующие выводы:

- наиболее распространенными ошибками, допускаемыми разработчиками приложений, являются уязвимости «Межсайтовое выполнение сценариев» и «Внедрение операторов SQL»;
- если сайт содержит уязвимости, которые позволяют непосредственно выполнять команды на сервере, то вероятность автоматизированного заражения вредоносным кодом такого ресурса достигает 100%;
- уязвимостей, связанных с недостатками администрирования, встречается на 10% больше, чем уязвимостей, связанных с ошибками при разработке систем;
- 84% веб-приложений не удовлетворяет требованиям стандарта по защите информации в индустрии платежных карт и 81% не соответствуют критериям ASV-сканирования по PCI DSS;
- регулярный анализ защищенности веб-приложений и налаженный процесс устранения выявленных недостатков позволяют за год уменьшить число уязвимых сайтов в среднем втрое;
- вероятность обнаружения критичной ошибки в динамическом веб-приложении составляет порядка 35% при проведении автоматического сканирования методикой «черного ящика» и 79% при детальном экспертном анализе;
- ситуация со степенью защищенности веб-приложений в 2009 году по результатам исследований улучшилась в сравнении предыдущими четырьмя годами [7,8,9].

7. О КОМПАНИИ

«Позитив Текнолоджиз» (Positive Technologies) - лидирующая компания на рынке информационной безопасности.

Основные направления деятельности компании:

- разработка систем комплексного мониторинга информационной безопасности (XSpider, MaxPatrol);
- оказание консалтинговых услуг в области ИБ;
- предоставление сервисных услуг в области ИБ;
- развитие ведущего российского портала по ИБ Securitylab.ru.

Компания «Позитив Текнолоджиз» (Positive Technologies) – это команда квалифицированных разработчиков и консультантов. Эксперты компании имеют большой практический опыт, являются членами международных организаций, активно участвуют в развитии отрасли.

8. ССЫЛКИ

- [1] Web Application Security Consortium, "Web Security Threat Classification v2.0"
<http://projects.webappsec.org/Threat-Classification>
- [2] Web Application Security Consortium, "Web Security Threat Classification v1.0"
<http://projects.webappsec.org/Threat-Classification-Previous-Versions>
- [3] Common Vulnerability Scoring System
<http://www.first.org/cvss/>
- [4] Сергей Гордейчик, "Насколько "дыра" широка?"
<http://www.osp.ru/win2000/2006/02/1156304/>
- [5] Сергей Гордейчик, Cross-Site Request Forgery - много шума из-за ничего
<http://www.securitylab.ru/analytics/292473.php>
- [6] CWE/SANS Top 25 Most Dangerous Programming Errors 2010
http://cwe.mitre.org/top25/archive/2010/2010_cwe_sans_top25.pdf
- [7] Статистика уязвимости веб-приложений за 2008 год
<http://www.ptsecurity.ru/download/Статистика%20уязвимости%20Web-приложений%202008.pdf>
- [8] Positive Technologies, "Статистика уязвимостей WEB-приложений в 2007 году"
<http://www.ptsecurity.ru/stat2007.asp>
- [9] Positive Technologies, "Статистика уязвимостей WEB-приложений в 2006 году"
<http://www.ptsecurity.ru/webstat2006.asp>
- [10] Блог компании Positive Technologies, WASC WSTCv2 Mapping Proposal
<http://ptresearch.blogspot.com/2010/04/wasc-wstcv2-mapping-proposal.html>

9. ПРИЛОЖЕНИЕ 1: МЕТОДИКА ОЦЕНКИ СТЕПЕНИ РИСКА

Таблица 12. Методика оценки степени риска

| Threat Classification | Basic CVSS Score | PCI DSS Risk |
|-------------------------------|----------------------------------|--------------|
| Abuse of Functionality | 4 (AV:N/AC:H/Au:N/C:P/I:P/A:N) | Medium |
| Brute Force Attack | 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Critical |
| Buffer Overflow | 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) | Urgent |
| Content Spoofing | 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N) | High |
| Credential/Session Prediction | 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Critical |
| Cross-Site Scripting | 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N) | Critical |
| Cross-Site Request Forgery | 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N) | High |
| Denial of Service | 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C) | High |
| Format String Attack | 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) | Urgent |
| HTTP Request Splitting | 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N) | Critical |
| HTTP Response Splitting | 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N) | Critical |
| HTTP Request Smuggling | 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N) | Critical |
| HTTP Response Smuggling | 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N) | Critical |
| Integer Overflow | 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) | Urgent |
| LDAP Injection | 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) | Urgent |
| Mail Command Injection | 5 (AV:N/AC:L/Au:N/C:N/I:P/A:N) | High |
| OS Commanding | 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) | Urgent |
| Path Traversal | 7.8 (AV:N/AC:L/Au:N/C:C/I:N/A:N) | Critical |
| Predictable Resource Location | 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N) | High |
| Remote File Inclusion | 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) | Urgent |

| | | |
|---------------------------------|----------------------------------|----------|
| Routing Detour | 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N) | High |
| SOAP Array Abuse | 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C) | High |
| SSI Injection | 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) | Urgent |
| Session Fixation | 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Critical |
| SQL Injection | 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) | Urgent |
| URL Redirectors | 2.6 (AV:N/AC:H/Au:N/C:N/I:P/A:N) | Medium |
| XPath Injection | 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) | Urgent |
| XML Attribute Blowup | 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N) | High |
| XML External Entity | 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N) | High |
| XML Entity Expansion | 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N) | High |
| XML Injection | 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P) | Critical |
| XQuery Injection | 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) | Urgent |
| Application Misconfiguration | 5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P) | Medium |
| Directory Indexing | 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N) | High |
| Fingerprinting | 0 (AV:N/AC:L/Au:N/C:N/I:N/A:N) | Low |
| Improper Parsing | 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) | Urgent |
| Improper Permissions | 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) | Urgent |
| Information leakage | 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N) | High |
| Insecure Indexing | 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N) | High |
| Insufficient Anti-automation | 4 (AV:N/AC:H/Au:N/C:P/I:P/A:N) | Medium |
| Insufficient Authentication | 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Critical |
| Insufficient Authorization | 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Critical |
| Insufficient Data Protection | 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N) | High |
| Insufficient Process Validation | 4 (AV:N/AC:H/Au:N/C:P/I:P/A:N) | Medium |

| | | |
|---|----------------------------------|----------|
| Insufficient Session Expiration | 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P) | Critical |
| Insufficient Transport Layer Protection | 4 (AV:N/AC:H/Au:N/C:P/I:P/A:N) | Medium |
| Server Misconfiguration | 5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P) | Medium |
| Improper File System Permissions | 4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P) | Medium |