СТАТИСТИКА УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ 2012

Москва, 2013

ОГЛАВЛЕНИЕ

Введение.....3

1. Методика исследования.....4

2. Резюме.....5

3. Портрет участников.....7

4. Статистика уязвимостей.....10

4.1. Наиболее распространенные уязвимости.....10

4.2. Поквартальная динамика.....12

4.3. Уязвимости, характерые для различных средств разработки веб-приложений.....18

4.4. Уязвимости, характерные для различных веб-серверов.....22

4.5. Статистика для различных отраслей экономики.....25

Заключение.....31

Ссылки.....31

Приложение А.....32

ВВЕДЕНИЕ

В связи с непрерывным развитием сети Интернет и информационных технологий в целом веб-приложения стали неотъемлемой частью корпоративной информационной системы любой современной организации вне зависимости от рода ее деятельности и сферы экономики. Не только коммерческие компании создают и развивают собственные веб-ресурсы: государственный сектор активно включается в процесс развития веб-сервисов, обеспечивающих предоставление онлайн-услуг.

Веб-приложения обеспечивают всевозможные преимущества, однако их уязвимости являются одним из наиболее распространенных путей проникновения в корпоративные информационные системы. Разумеется, что при разработке веб-приложений в первую очередь решаются задачи, связанные с обеспечением основных функций системы. Безопасность сайта не всегда является приоритетной целью для разработчика, что обуславливает появление уязвимостей различной степени риска.

Доступность сайта компании любому пользователю сети Интернет делает данный вектор атаки наиболее выгодным для злоумышленника способом проникновения в корпоративную сеть организации. Подтверждением этому служат статистические исследования, ежегодно проводимые специалистами компании Positive Technologies.

Настоящее исследование посвящено анализу данных, полученных в ходе проведения работ по оценке уровня защищенности веб-приложений в 2012 году, и разработке статистики наиболее распространенных уязвимостей веб-приложений в зависимости от различных параметров рассмотренных систем.

1 МЕТОДИКА ИССЛЕДОВАНИЯ

Данный отчет содержит обзорную статистику уязвимостей веб-приложений, полученную в ходе работ по анализу защищенности, выполненных экспертами компании Positive Technologies в 2012 году. В общей сложности в 2012 году специалисты компании Positive Technologies изучили порядка 400 веб-приложений в рамках различных работ, начиная от инструментального сканирования и заканчивая анализом исходного кода. С целью получения объективной оценки уровня защищенности были выделены 67 веб-приложений, для которых проводился углубленный анализ защищенности с наиболее полным покрытием проверок. Результаты анализа защищенности веб-приложений, полученные в ходе таких работ, как инструментальное сканирование или тестирование на проникновение, в данном исследовании не затрагиваются.

Для выделенных 67 сайтов было обнаружено 576 уязвимостей различной степени риска. Оценка защищенности проводилась ручным способом методами черного, серого и белого ящиков с использованием вспомогательных автоматизированных средств. Метод черного ящика заключается в проведении работ по оценке защищенности информационной системы без предварительного получения какой-либо информации о ней со стороны владельца. Метод серого ящика аналогичен методу черного ящика, при этом в качестве нарушителя на данном этапе рассматривается пользователь, обладающий определенными привилегиями в системе. Метод белого ящика заключается в том, что для оценки защищенности информационной системы используются все необходимые данные о ней, включая исходный код приложений. В статистику вошли только данные о внешних веб-приложениях, доступных из глобальной сети Интернет.

Обнаруженные уязвимости классифицировались согласно соответствующим угрозам по системе Web Application Security Consortium Threat Classification (WASC TC v2 [1]). Ошибки обработки входных и возвращаемых данных (Improper Input Handling и Improper Output Handling) не были классифицированы, поскольку они могут использоваться при эксплуатации множества других уязвимостей.

В настоящей статистике приведены только уязвимости веб-приложений. Другие распространенные проблемы информационной безопасности (к примеру, недостатки процесса управления обновлениями ПО) не рассматриваются.

Степень риска уязвимостей оценивалась согласно системе Common Vulnerability Scoring System (CVSS v2 [2]); на основе этой оценки выделялись высокий, средний и низкий уровни риска.

2 РЕЗЮМЕ

В данном разделе приведены наиболее значимые заключения по статистическому анализу уязвимостей, выявленных на исследуемых веб-ресурсах.

1 Все веб-приложения содержат различные проблемы безопасности, при этом **45% рассмотренных систем содержат уязвимости высокой степени риска.** Данный показатель существенно ниже соответствующих показателей по результатам 2010 (76%) и 2011 (61%) годов, однако доля сайтов с уязвимостями высокого уровня риска по-прежнему крайне велика.

2 **9 из 10 веб-приложений содержат уязвимости среднего уровня риска**, что близко к результатам прошедших двух лет.

3 Наиболее распространенный недостаток по итогам 2012 года — возможность идентификации программного обеспечения (Fingerprinting), которая встречается в 72% приложений. На втором месте межсайтовое выполнение сценариев (Cross-Site Scripting), которому подвержены 63% рассмотренных систем. **В топ-10 вошли две критические уязвимости — внедрение SQL-кода (SQL Injection) и обход каталога (Path Traversal)**, которым подвержены **33%** и **18%** исследованных веб-ресурсов соответственно.

4 Наибольшее количество веб-приложений, содержащих уязвимости высокой степени риска, было выявлено **в телекоммуникационной отрасли**, где **78%** приложений подвержены критическим уязвимостям. По результатам прошлых лет, данный сектор экономики также был наиболее уязвим.

5 PHP оказался самым популярным языком для разработки веб-приложений. На нем написано 36% исследованных систем. Эти системы оказались наименее защищенными: **83% веб-ресурсов, разработанных с помощью PHP, содержат критические уязвимости**. Этот показатель почти в три раза выше, чем у следующего за ним Perl (29%).

6 **Веб-приложения, разработанные на платформе ASP.NET, наименее подвержены уязвимостям высокой степени риска** (10% уязвимых приложений), однако еще 80% приложений на ASP.NET содержат уязвимости средней критичности. Таким образом, о высоком уровне защищенности этих приложений говорить все же не приходится.

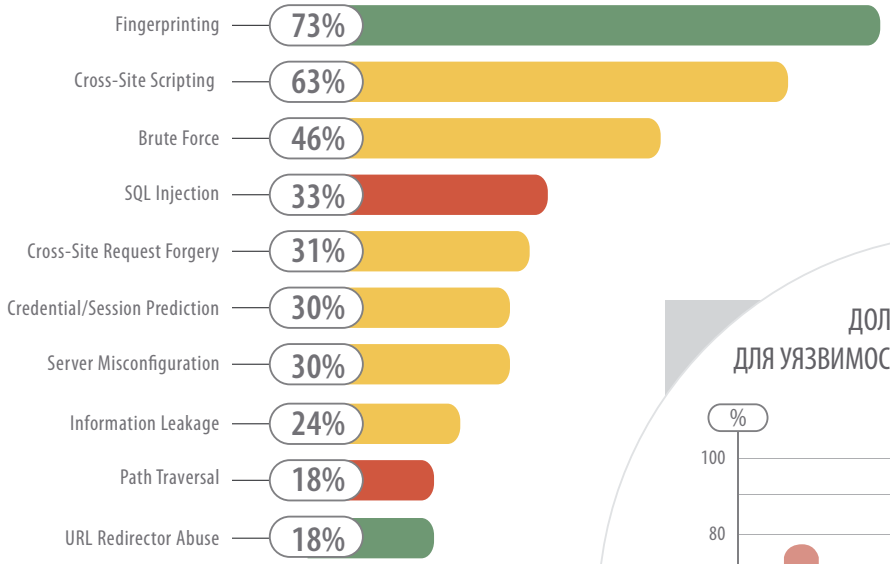
7 В 2012 году наиболее распространенным веб-сервером оказался Nginx. **Наиболее подверженным уязвимостям высокой степени риска является Apache: 88% использующих его веб-ресурсов подвержены критическим уязвимостям.**

8 **Только 30% исследованных веб-ресурсов использовали Web Application Firewall (WAF).** Учитывая, что на каждом из рассмотренных сайтов были обнаружены различные уязвимости, наличие такого дополнительного средства превентивной защиты могло бы снизить соответствующие риски, однако на сегодняшний день немногие владельцы веб-приложений прибегают к использованию таких средств.

POSITIVE TECHNOLOGIES

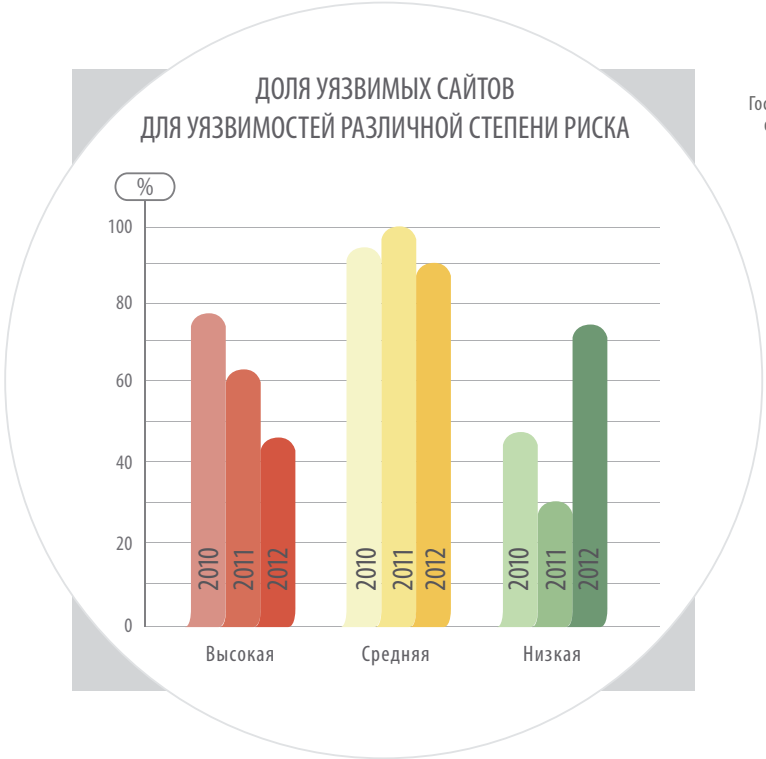
АНАЛИТИКА • 2012 СТАТИСТИКА УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ УЯЗВИМОСТИ
(доля сайтов, %)

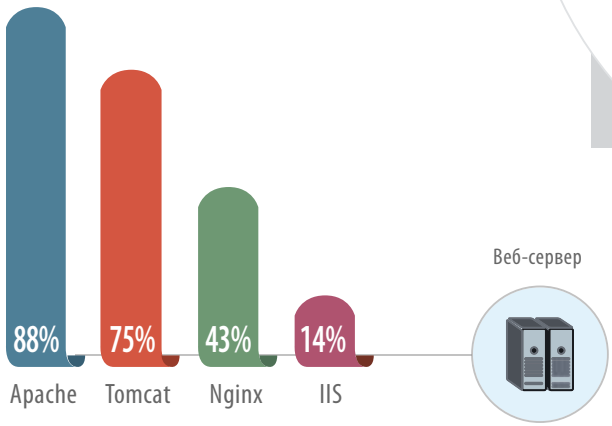


ДОЛЯ САЙТОВ, ПОДВЕРЖЕННЫХ УЯЗВИМОСТЯМ РАЗЛИЧНЫХ УРОВНЕЙ РИСКА
(для каждой из рассмотренных сфер экономики)

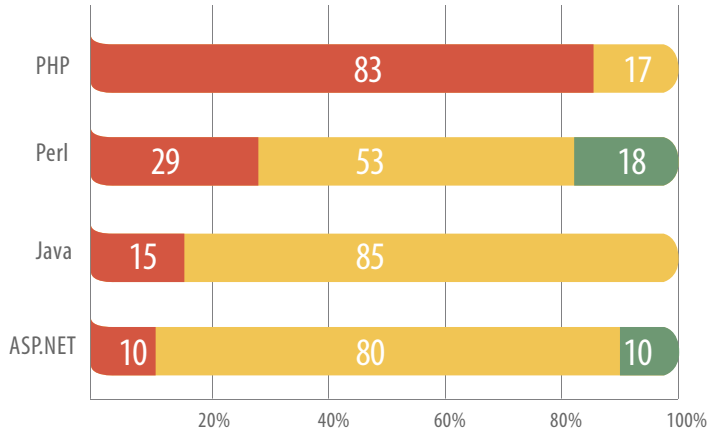
ДОЛЯ УЯЗВИМЫХ САЙТОВ ДЛЯ УЯЗВИМОСТЕЙ РАЗЛИЧНОЙ СТЕПЕНИ РИСКА



ВЕБ-ПРИЛОЖЕНИЯ С КРИТИЧЕСКИМИ УЯЗВИМОСТЯМИ
(по типу веб-сервера)



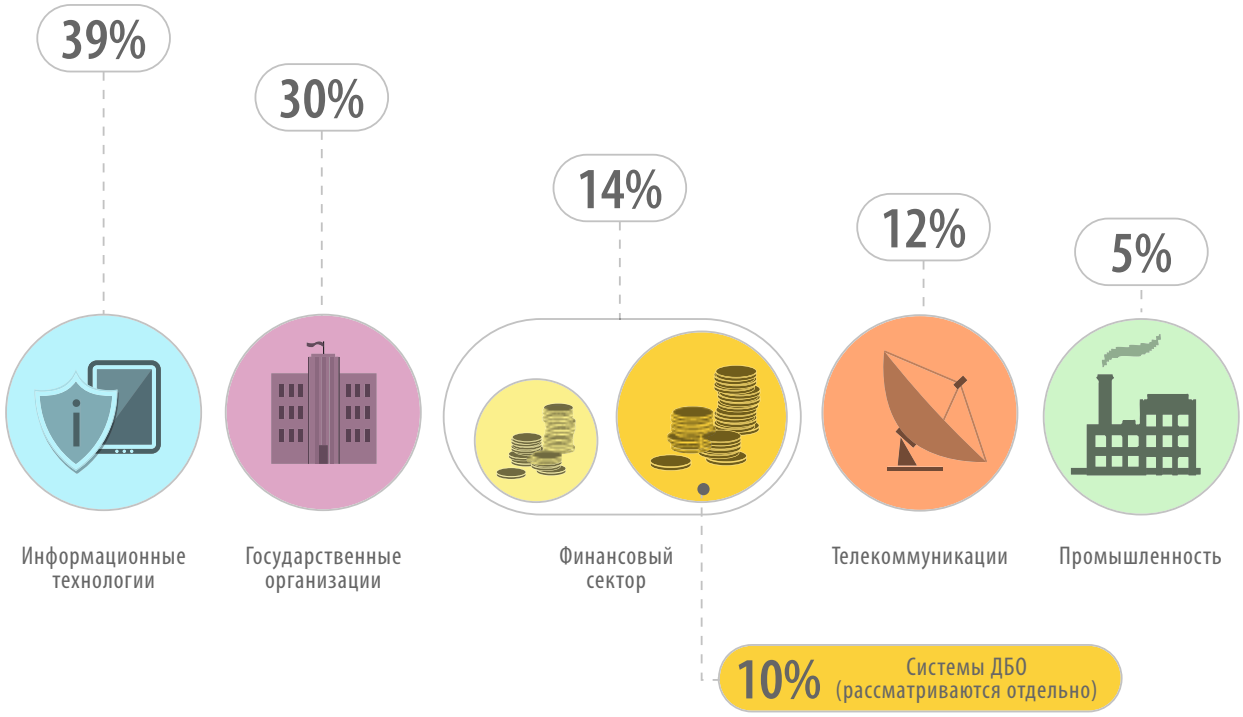
ДОЛЯ ВЕБ-ПРИЛОЖЕНИЙ ПО МАКСИМАЛЬНОМУ УРОВНЮ РИСКА УЯЗВИМОСТЕЙ



3 ПОРТРЕТ УЧАСТНИКОВ

Веб-приложения, глубоко проанализированные в 2012 году, относятся к различным отраслям экономики. С точки зрения отраслевой принадлежности были выделены следующие группы владельцев сайтов: информационные технологии и информационная безопасность, государственный и финансовый секторы, телекоммуникации, промышленность. Наиболее широко представлены сектор информационных технологий и информационной безопасности (39%) и сайты государственных организаций (30%). Большое внимание анализу защищенности веб-приложений уделяют также представители финансового сектора (14%), в частности банки.

РАСПРЕДЕЛЕНИЕ ВСЕХ ВЕБ-ПРИЛОЖЕНИЙ, ПРОАНАЛИЗИРОВАННЫХ В 2012 ГОДУ, ПО ОТРАСЛЯМ ЭКОНОМИКИ



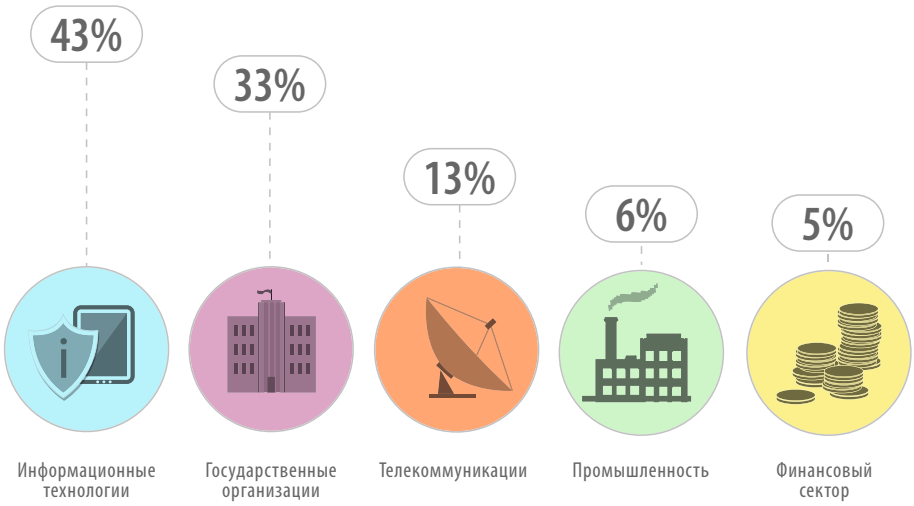
В выборку веб-приложений для настоящего исследования не были включены системы дистанционного банковского обслуживания. Уязвимости данных систем были рассмотрены отдельно, а результаты опубликованы в отчете «Статистика уязвимостей систем дистанционного банковского обслуживания (2011—2012 гг.)». Прочие оставшиеся системы, относящиеся к данному сектору, составляют лишь незначительную долю всех исследованных систем и представляют собой различные сайты информационного характера. В силу малого числа рассмотренных веб-приложений финансового сектора отдельная статистика по этой отрасли экономики в данном документе не приводится.

РАСПРЕДЕЛЕНИЕ УЧАСТНИКОВ ПО ОТРАСЛЯМ ЭКОНОМИКИ

ОТРАСЛЬ ЭКОНОМИКИ	ДОЛЯ, %
Информационные технологии и информационная безопасность	43
Государственные организации	33
Телекоммуникации	13
Промышленность	6
Финансовый сектор	5

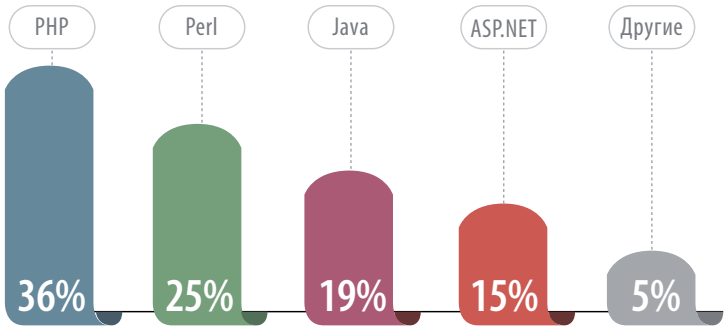
В итоговой выборке доля сектора информационных технологий и информационной безопасности составила 43%, а доля государственных учреждений — 33%; прочие секторы составляют менее значительную часть выборки.

РАСПРЕДЕЛЕНИЕ СИСТЕМ ПО ОТРАСЛЯМ ЭКОНОМИКИ



Все рассмотренные системы можно разделить на четыре группы в зависимости от средства разработки (ASP.NET, Java, Perl и PHP). Большинство веб-приложений разработано на языках PHP (36%) и Perl (25%). Существенная доля исследованных систем разработана с помощью Java (19%) и ASP.NET (15%). Значительно реже применялись другие языки программирования.

РАСПРЕДЕЛЕНИЕ СИСТЕМ В ЗАВИСИМОСТИ ОТ СРЕДСТВА РАЗРАБОТКИ

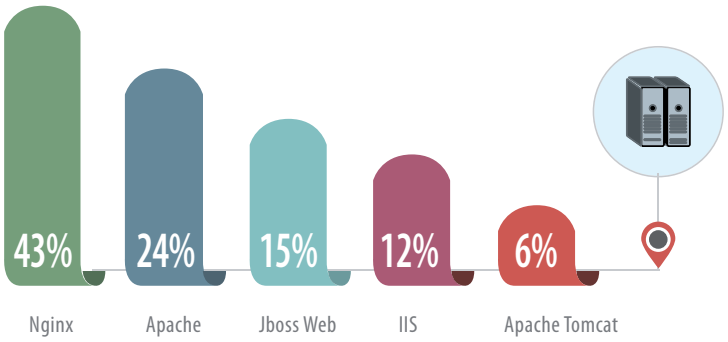


Среди рассмотренных веб-приложений большинство функционирует под управлением веб-серверов Nginx (43%). Практически четверть всех систем управляются веб-серверами Apache, которые в 2010—2011 годах были наиболее популярны. Менее других распространены серверы Jboss Web, Microsoft Internet Information Services (IIS) и Apache Tomcat.

РАСПРЕДЕЛЕНИЕ ВЕБ-ПРИЛОЖЕНИЙ ПО ИСПОЛЬЗУЕМОМУ ВЕБ-СЕРВЕРУ

ВЕБ-СЕРВЕР	ДОЛЯ, %
NGINX	43
APACHE	24
JBOSS WEB	15
IIS	12
APACHE TOMCAT	6

РАСПРЕДЕЛЕНИЕ СИСТЕМ ПО ТИПУ ИСПОЛЬЗУЕМОГО ВЕБ-СЕРВЕРА



В рассмотренных в 2012 году веб-приложениях только в двух случаях применялись коммерческие системы управления содержимым (CMS). Во всех остальных случаях CMS не использовались, поскольку приложения представляли собой специфические системы, разработанные для конкретных заказчиков. В связи с этим статистические исследования уровня защищенности сайтов в зависимости от используемой системы CMS не проводились.

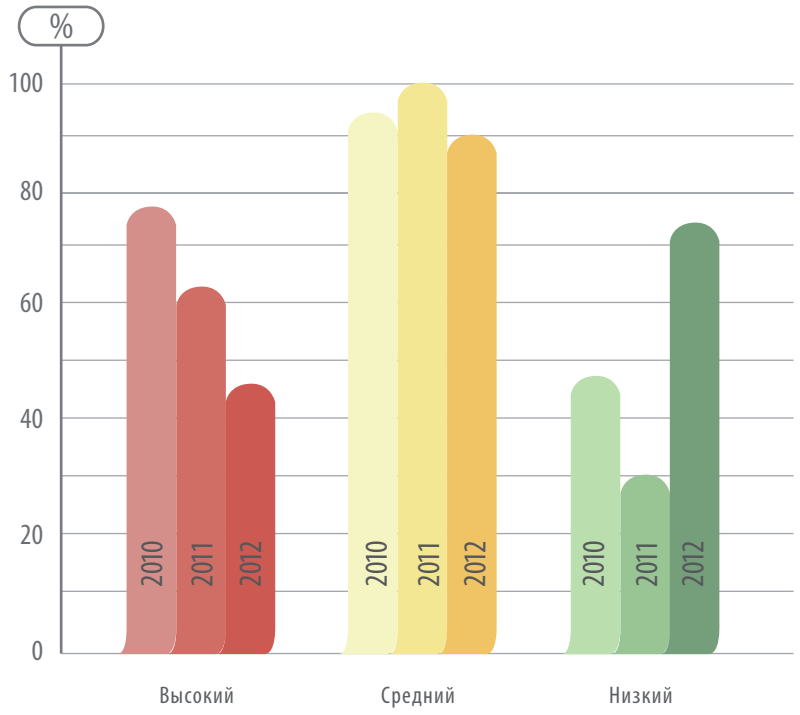
4 СТАТИСТИКА УЯЗВИМОСТЕЙ

Данная глава содержит анализ распространенности и уровней риска уязвимостей различных типов, классифицированных согласно угрозам, представленным в WASC TC v2.

4.1. НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ

В результате проведенных в 2012 году исследований уязвимости были обнаружены во всех проверенных веб-приложениях, при этом 45% систем содержали уязвимости высокой степени риска и практически все системы (90%) — уязвимости средней степени риска.

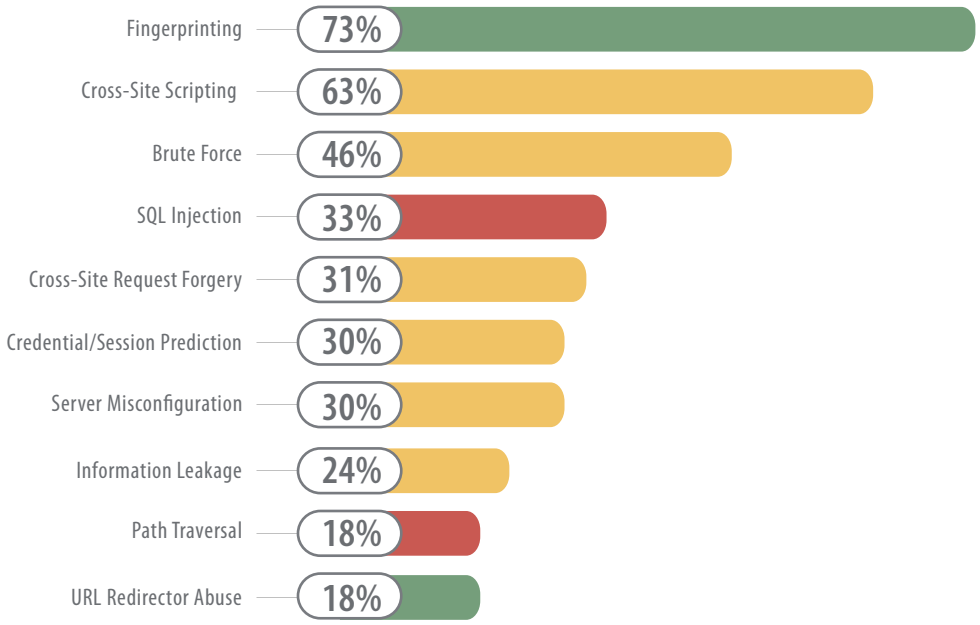
ДОЛЯ УЯЗВИМЫХ САЙТОВ В ЗАВИСИМОСТИ ОТ СТЕПЕНИ РИСКА УЯЗВИМОСТЕЙ



На рисунке показаны также результаты статистического анализа за 2010 и 2011 годы. Согласно полученным данным, наблюдается постепенное уменьшение доли систем, подверженных критическим уязвимостям. Доля таких систем уменьшилась с 76% в 2010 году до 45% в 2012 году. Доля систем, в которых были найдены уязвимости средней степени риска, остается крайне велика (более 90%), при этом в 2011 году абсолютно все рассмотренные системы были подвержены таким уязвимостям. Существенно возросла доля систем, подверженных уязвимостям низкой степени риска: более чем в два раза по сравнению с 2011 годом, когда данный параметр был на достаточно низком уровне (30%).

В 2012 году получила распространение уязвимость низкого уровня риска Fingerprinting. Данной уязвимости подвержены три четверти исследованных ресурсов (73%). На втором месте в топ-10 — ошибки, позволяющие осуществить межсайтовое выполнение сценариев (уязвимости обнаружены в 63% веб-приложений, которые были проверены специалистами Positive Technologies). Почти в половине систем (46%) присутствуют недостатки, позволяющие автоматизировано подбирать учетные данные и пароли пользователей (Brute Force). Уязвимость высокой степени риска, позволяющая осуществить внедрение SQL-кода, не вошла в тройку самых распространенных, однако ей подвержена треть всех рассмотренных систем.

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ (доля сайтов, %)



Согласно статистике веб-уязвимостей за 2010 и 2011 годы, десятку распространенных уязвимостей веб-ресурсов возглавляла уязвимость подделки запросов (Cross-Site Request Forgery CSRF), которой был подвержен 61% исследованных ресурсов. В первую десятку входили три критические уязвимости, позволяющие осуществить внедрение SQL-кода (SQL Injection), выполнение команд ОС (OS Commanding) и обход каталога (Path Traversal). Уязвимости были обнаружены в 47%, 28% и также 28% веб-приложений соответственно.

В 2012 году доля веб-приложений с уязвимостями высокой степени риска сократилась: SQL Injection — 33%, Path Traversal — 18%, а ошибки, позволяющие осуществлять атаку OS Commanding, стали встречаться еще реже (16%).

4.2. ПОКВАРТАЛЬНАЯ ДИНАМИКА

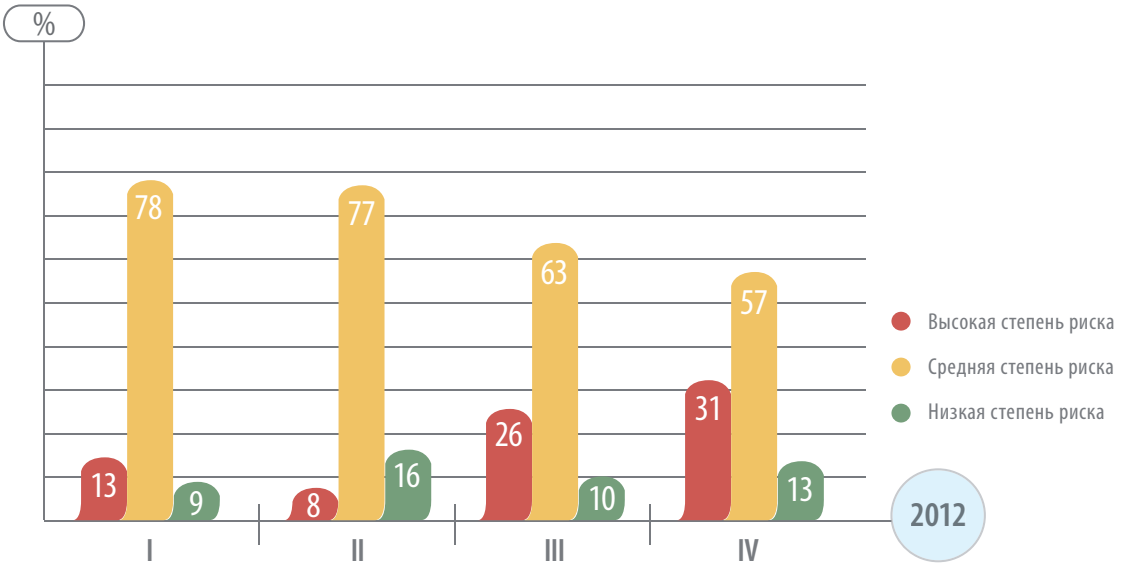
В данном разделе представлены статистические данные по уязвимостям разного уровня риска в веб-приложениях, детальный анализ защищенности которых был проведен в 2012 году.

Как показывает проведенное исследование, доля систем, содержащих уязвимости высокой степени риска, существенно возросла во втором полугодии (более чем в два раза). Если в первом квартале 2012 года таких систем насчитывалось менее 30% от общего числа рассмотренных, то в третьем квартале их оказалось более 80%. При этом доля уязвимостей среднего и низкого уровней риска в третьем квартале 2012 года также достигает максимальных значений (100% и 91% соответственно). В четвертом квартале наблюдается уменьшение доли веб-приложений, в которых обнаружены уязвимости высокой степени риска — на 12%, средней — на 20%, низкой — на 61%. Как показывает статистика, число систем, подверженных уязвимостям высокой степени риска, к концу года остается на отметке, в два раза превышающей уровень начала года. Даже с учетом снижения числа систем, подверженных уязвимостям среднего и низкого уровня риска, статистика позволяет судить об ухудшении ситуации в данной области.

ДОЛЯ ВЕБ-ПРИЛОЖЕНИЙ, ПОДВЕРЖЕННЫХ УЯЗВИМОСТЯМ РАЗНОЙ СТЕПЕНИ РИСКА
(поквартальная статистика)

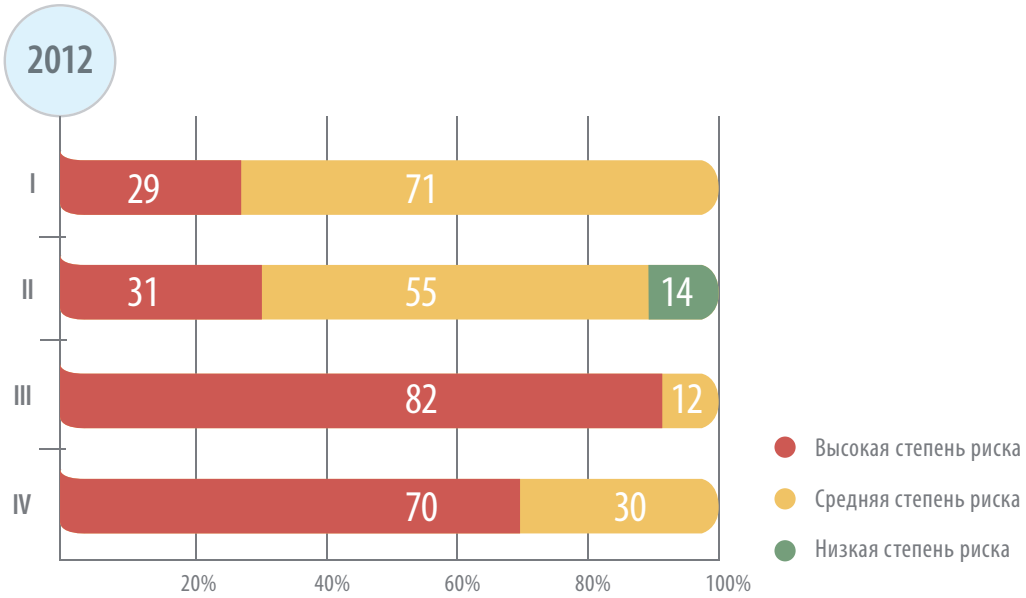
На следующей диаграмме показана статистика по степени риска уязвимостей, обнаруженных в течение каждого из кварталов 2012 года. Прослеживается заметное уменьшение доли уязвимостей средней степени риска в течение года, доля уязвимостей низкой степени риска остается примерно на одном уровне, около 13%. При этом доля уязвимостей высокой степени риска ко второму кварталу года существенно уменьшилась и составила всего 8% от общего числа обнаруженных в этот период уязвимостей. К концу года данный показатель существенно ухудшился: практически треть всех обнаруженных в четвертом квартале 2012 года уязвимостей характеризуются высокой степенью риска.

УРОВЕНЬ РИСКА УЯЗВИМОСТЕЙ (поквартальная статистика)



Ухудшение показателей к концу 2012 года подтверждается также и диаграммой, отображающей соотношения максимальных уровней риска уязвимостей исследованных систем.

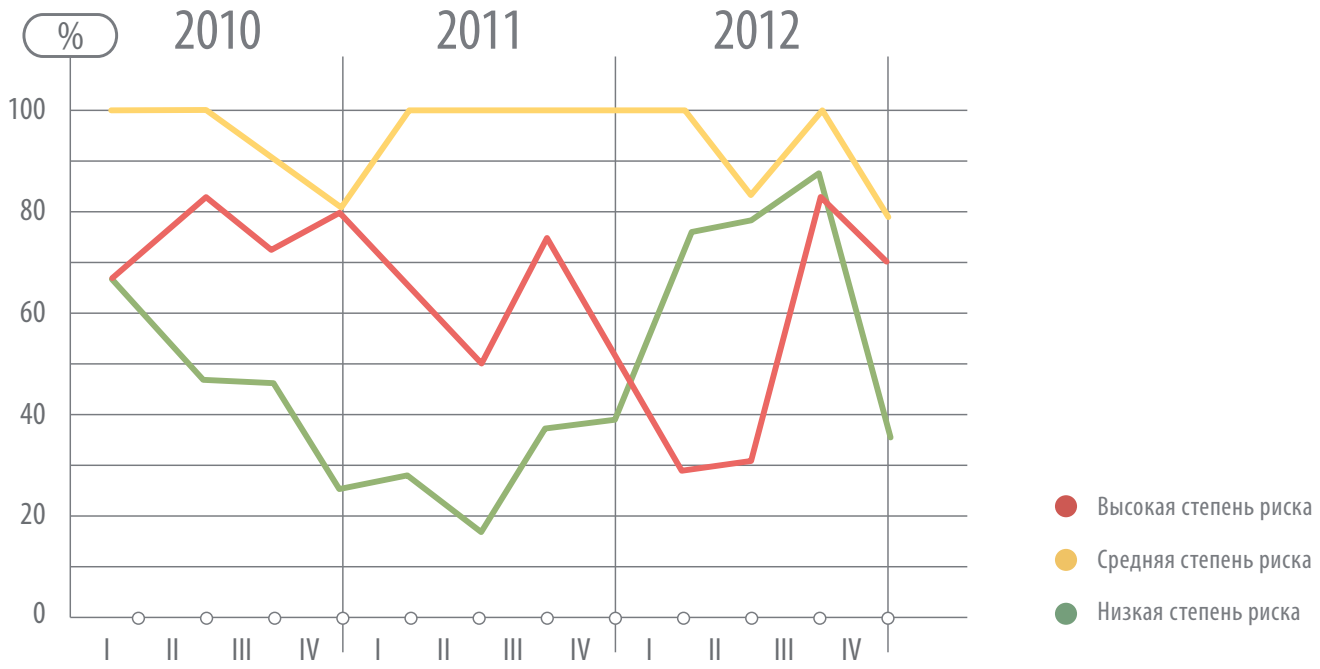
ДОЛЯ ВЕБ-ПРИЛОЖЕНИЙ ПО МАКСИМАЛЬНОМУ УРОВНЮ РИСКА ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ



В начале года треть всех рассмотренных систем содержали уязвимости высокого уровня риска, при этом остальные содержали уязвимости среднего и низкого уровней риска. Во втором квартале 2012 года доля веб-приложений с критическими уязвимостями осталась примерно на том же уровне, однако в остальном ситуация несколько улучшилась: 14% рассмотренных веб-приложений содержали уязвимости только низкого уровня риска. В третьем квартале статистика существенно хуже: более 80% всех исследованных в этот период систем оказались подвержены критическим уязвимостям. Ситуация лишь незначительно улучшилась к концу 2012 года.

Более информативно в данном случае сравнение динамических показателей трех лет (2010—2012 гг.). Ниже представлена диаграмма, отражающая динамику изменения доли уязвимых сайтов для разных степеней риска.

ДИНАМИКА ДОЛЕЙ САЙТОВ С УЯЗВИМОСТЯМИ РАЗНОЙ СТЕПЕНИ РИСКА



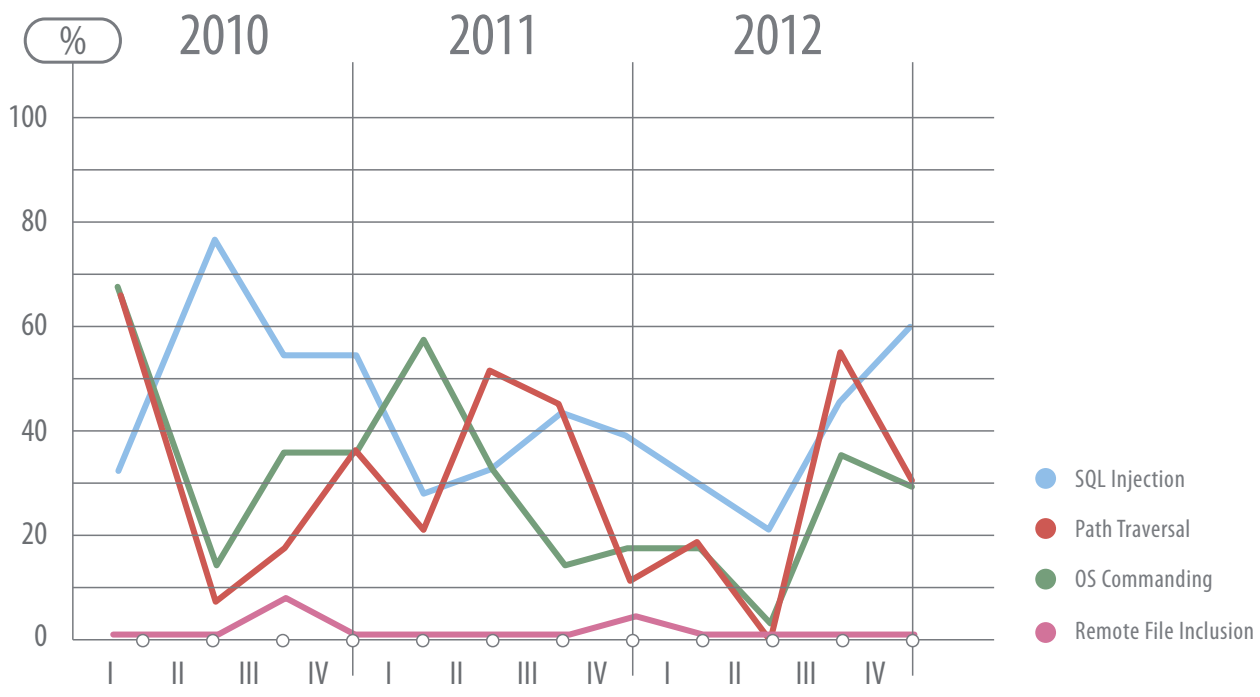
Согласно полученной статистике, в период первого полугодия 2012 года существенно сократилась доля веб-приложений, подверженных уязвимостям высокой степени риска, при этом возросло количество уязвимостей низкого уровня риска. Наименьшее количество критических уязвимостей зафиксировано в первом квартале 2012 года. Во втором полугодии 2012 года количество уязвимостей высокого уровня риска снова достигло уровня показателей начала 2010 года и составило 70—80%. Уязвимости среднего уровня риска оказались наиболее распространенными в 2012 году, также как и в предыдущие периоды. Им было подвержено порядка 90% исследованных систем в течение года, что соответствует уровню конца 2010 года и ниже уровня 2011 года, когда данные уязвимости были обнаружены во всех системах.

В таблице представлена динамика за 2010—2012 гг. доли исследованных веб-приложений, которые подвержены наиболее распространенным критическим уязвимостям, таким как SQL Injection, Path Traversal, OS Commanding и Remote Inclusion (выполнение удаленных файлов).

ДИНАМИКА ДОЛИ САЙТОВ С КРИТИЧЕСКИМИ УЯЗВИМОСТЯМИ (%)

УЯЗВИМОСТЬ	2010				2011				2012			
	I	II	III	IV	I	II	III	IV	I	II	III	IV
SQL Injection	33	77	55	55	29	33	4	39	29	21	45	60
Path Traversal	67	8	18	36	21	50	44	11	18	—	55	30
OS Commanding	67	15	36	36	57	33	15	18	18	3	36	30
Remote File Inclusion	—	—	9	—	—	—	—	4	—	—	—	—

На диаграмме представлен соответствующий график для каждой из перечисленных уязвимостей.



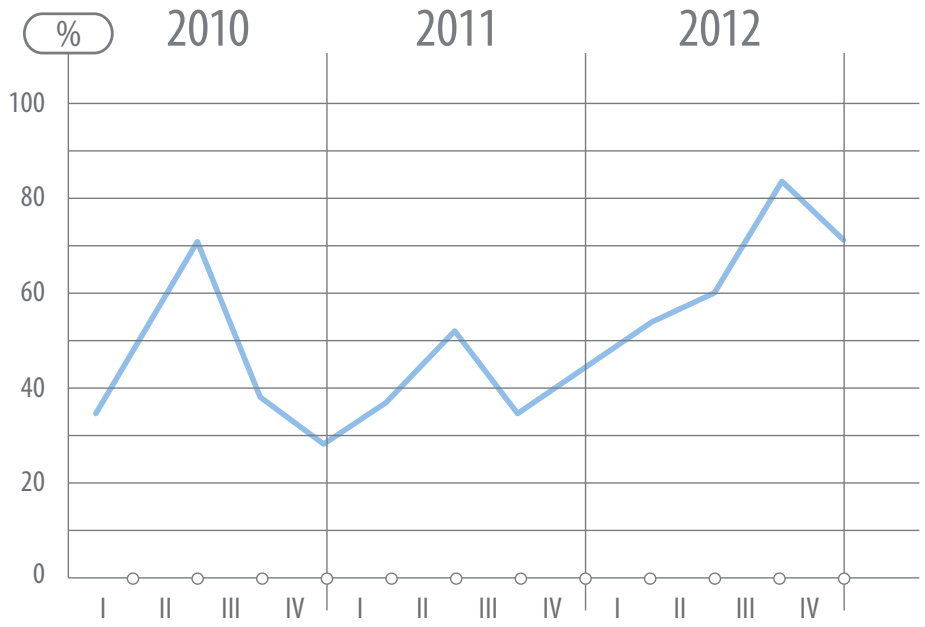
Согласно результатам проведенного анализа, наиболее распространенной уязвимостью является SQL Injection. Доля сайтов, подверженных данной уязвимости, значительно уменьшилась к концу 2011 года. Тенденция к снижению доли уязвимых ресурсов сохранилась и в начале 2012 года: во втором квартале наблюдается минимальное значение доли ресурсов, подверженных SQL Injection, за трехлетний период исследований. К концу 2012 года доля уязвимых систем значительно увеличилась и достигла 60%.

Наименее распространенной среди рассмотренных уязвимостей является Remote File Includion: она была обнаружена в системах только в середине 2010 и конце 2011 годов, в 2012 году не выявлено ни одной системы, содержащей данную уязвимость.

В таблице представлена динамика доли веб-ресурсов, содержащих уязвимости межсайтового выполнения сценариев (XSS), в процентах за три года. На диаграмме представлен соответствующий график.

ДОЛИ САЙТОВ, УЯЗВИМЫХ ДЛЯ XSS (%)

УЯЗВИМОСТЬ	2010				2011				2012			
	I	II	III	IV	I	II	III	IV	I	II	III	IV
Cross-Site Scripting	33	69	36	27	36	50	32	43	53	59	82	70

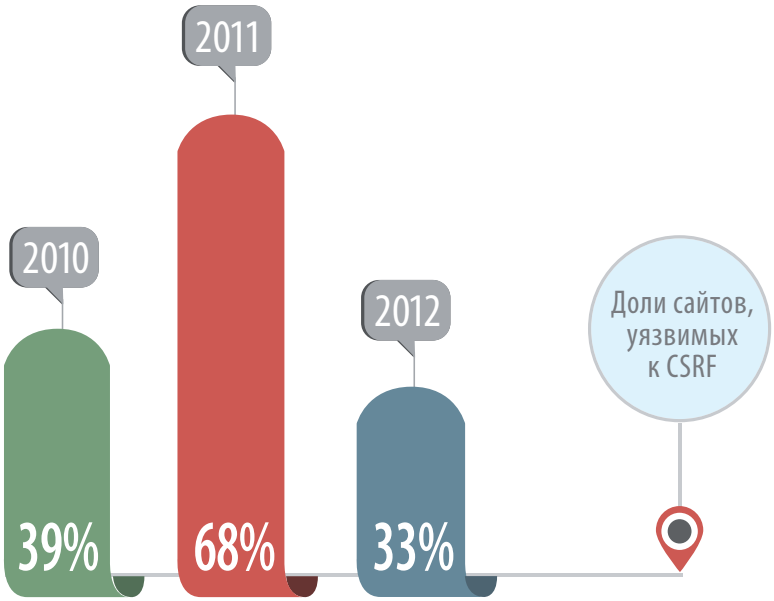


В 2012 году наблюдается постепенное увеличение доли веб-приложений, подверженных уязвимости межсайтового выполнения сценариев. Лишь в четвертом квартале года данный показатель незначительно снизился и составил 70%. Максимальное значение доли уязвимых сайтов за весь трехлетний период исследований приходится на третий квартал 2012 года, когда он составил более 80%.

В таблице представлена динамика доли веб-ресурсов, содержащих уязвимости CSRF.

ДОЛИ САЙТОВ, УЯЗВИМЫХ ДЛЯ CSRF (%)

УЯЗВИМОСТЬ	2010	2011	2012
Cross-Site Request Forgery	39	68	33



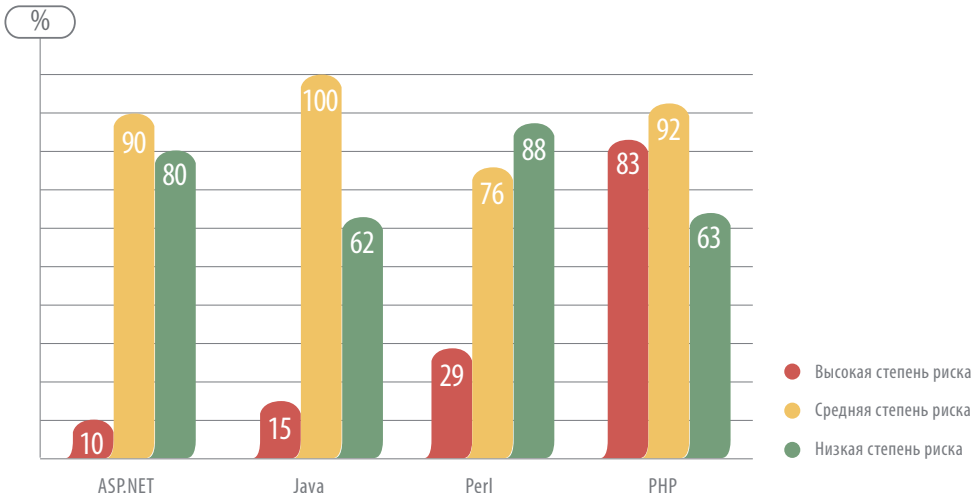
В целом изменения доли уязвимостей разного уровня риска на протяжении трех лет позволяют выделить начало 2012 года как наиболее успешный период в борьбе с критическими веб-уязвимостями, но к концу 2012 года показатели защищенности систем снова снизились до уровня трехлетней давности.

4.3. УЯЗВИМОСТИ, ХАРАКТЕРНЫЕ ДЛЯ РАЗЛИЧНЫХ СРЕДСТВ РАЗРАБОТКИ ВЕБ-ПРИЛОЖЕНИЙ

Проведенное исследование позволило установить соотношения уровней риска уязвимостей, обнаруженных для различных средств разработки веб-приложений. Результаты представлены на диаграмме.

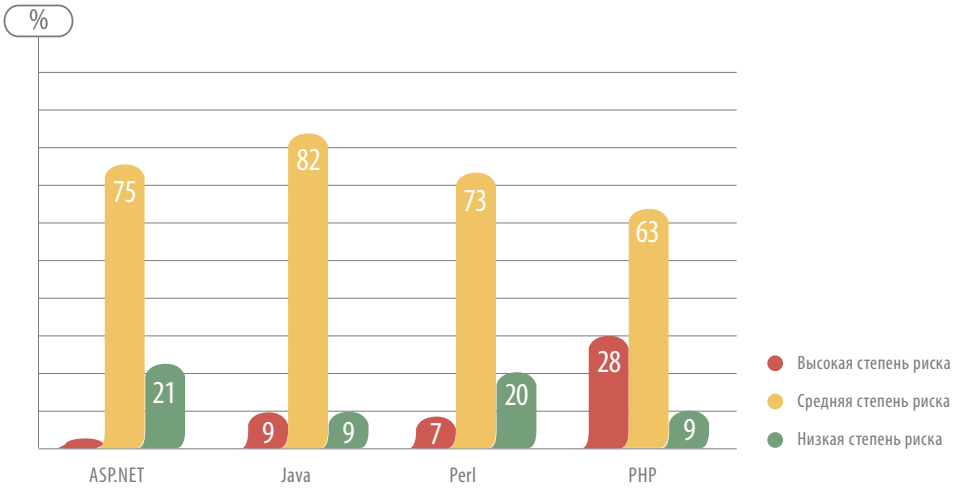
Наибольшее количество систем (83%), подверженных критическим уязвимостям, выявлено среди веб-приложений, разработанных на языке PHP. Системы, разработанные на языке Perl, оказались менее подвержены уязвимостям средней степени риска, при этом все веб-приложения, написанные на Java, содержат уязвимости среднего уровня риска. Наименьшее количество систем, подверженных уязвимостям высокой степени риска, разработано на платформе ASP.NET.

ДОЛИ СИСТЕМ С УЯЗВИМОСТЯМИ РАЗНОЙ СТЕПЕНИ РИСКА (по средствам разработки)



На следующей диаграмме показана статистика по уровню риска обнаруженных уязвимостей для каждого вида систем. Всего 1% уязвимостей, обнаруженных в веб-приложениях, разработанных на платформе ASP.NET, имеют высокую степень риска, в то время как каждая третья уязвимость PHP-систем характеризуется высоким уровнем риска. Наиболее распространены среди всех видов систем уязвимости средней степени риска (60—80%).

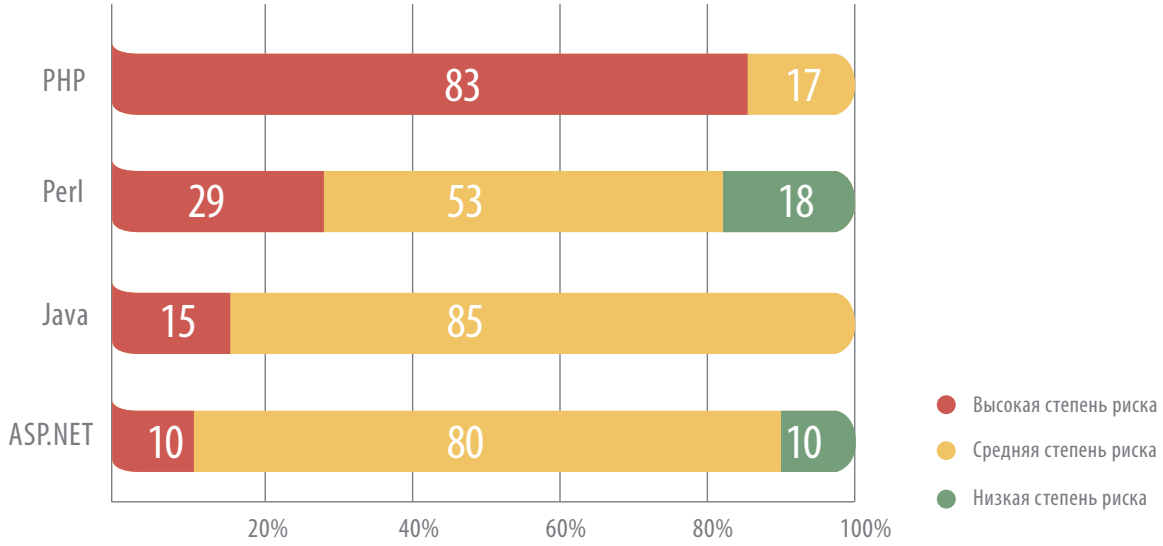
СООТНОШЕНИЕ ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ ПО УРОВНЮ РИСКА ДЛЯ ЧЕТЫРЕХ ИНСТРУМЕНТОВ РАЗРАБОТКИ ВЕБ-ПРИЛОЖЕНИЙ



Согласно результатам проведенного исследования, 83% веб-приложений, разработанных на языке PHP, содержат критические уязвимости, остальные 17% таких систем содержат уязвимости средней и низкой степени риска. На втором месте Perl: практически треть систем, содержат уязвимости высокого уровня риска.

Максимальный уровень риска для различных типов рассмотренных систем представлен на диаграмме.

ДОЛЯ ВЕБ-ПРИЛОЖЕНИЙ ПО МАКСИМАЛЬНОМУ УРОВНЮ РИСКА УЯЗВИМОСТЕЙ

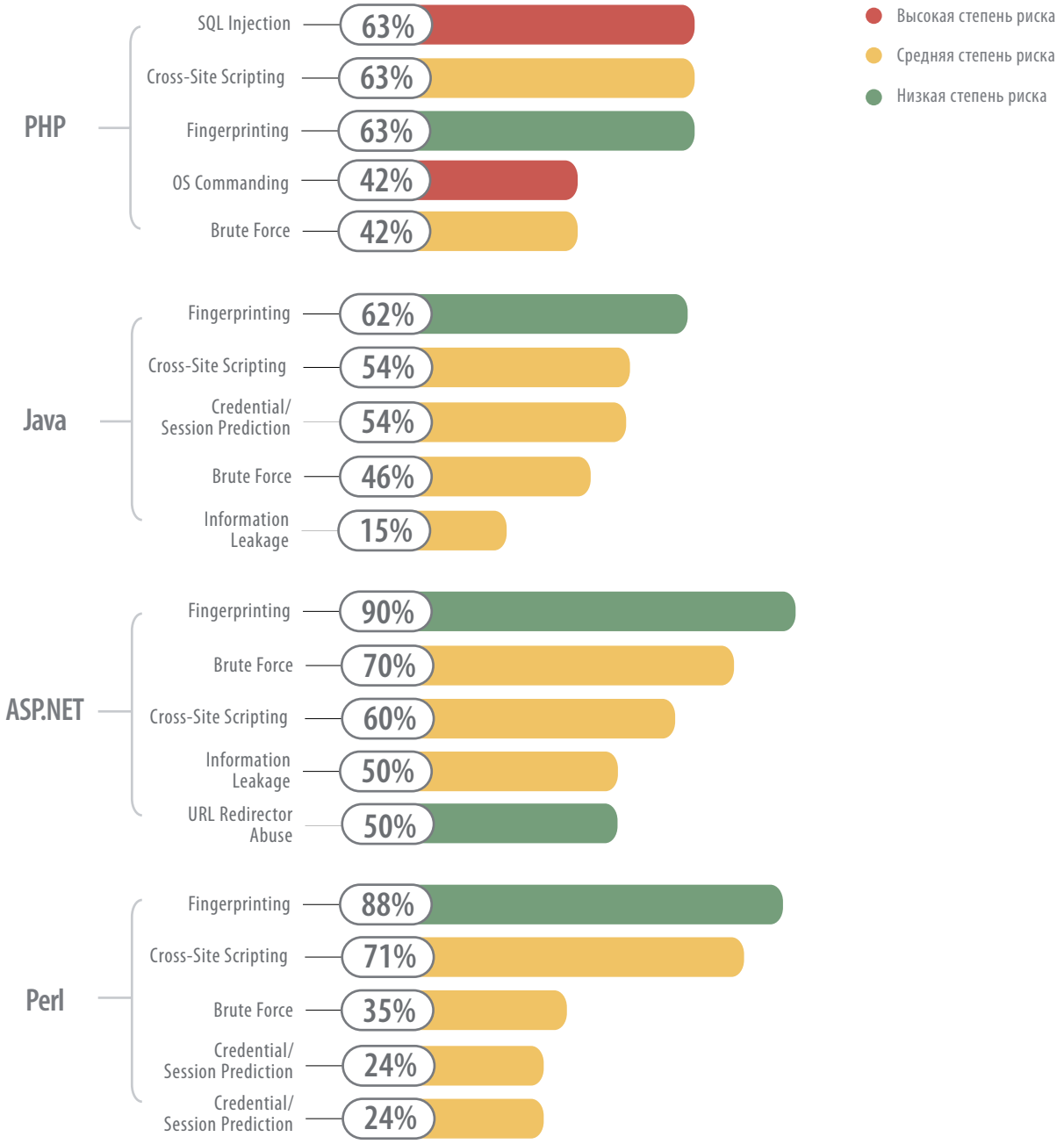


Для Java было выявлено 15% приложений, содержащих критические уязвимости, при этом все приложения подвержены уязвимостям как минимум среднего уровня риска. Стоит отметить, что большинство рассмотренных приложений на Java относились к одному крупному проекту, разработчики которого регулярно проводят анализ защищенности и устраняют уязвимости. Таким образом, подобная статистика по Java во многом является результатом целенаправленной работы по устранению уязвимостей в рамках конкретного проекта, в то время как в целом ситуация с безопасностью Java-приложений может быть гораздо хуже. Так, для приложений на Java, не относящихся к указанному проекту, доля уязвимостей высокого уровня риска достигает 66%.

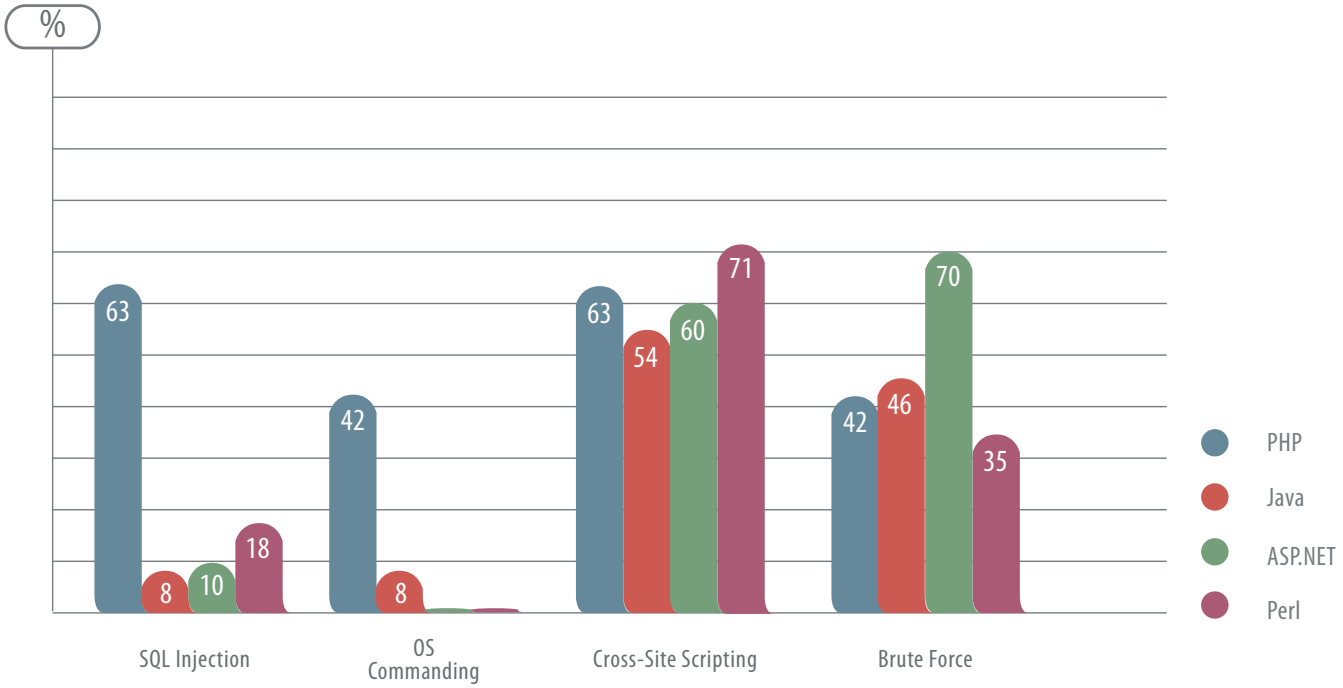
Лишь десятая часть веб-приложений, разработанных с помощью ASP.NET, содержит уязвимости высокой степени риска, такая же доля систем подвержена уязвимостям низкого уровня риска. Таким образом, можно выделить веб-приложения, разработанные на платформе ASP.NET, как наиболее безопасные среди рассмотренных в 2012 году. Однако, учитывая, что 90% сайтов на ASP.NET содержат уязвимости как минимум среднего уровня риска, говорить о достижении приемлемого уровня защищенности данных приложений пока не приходится.

На рисунке представлены доли систем, подверженных наиболее распространенным уязвимостям, в зависимости от используемого инструмента разработки. В данную статистику входят лишь две критические уязвимости (SQL Injection и OS Commanding), которые были обнаружены лишь в веб-приложениях, разработанных на языке PHP. При этом наиболее распространенной оказалась уязвимость низкого уровня риска — Fingerprinting. Данная уязвимость наиболее часто встречается в системах, разработанных на Java, ASP.NET и Perl.

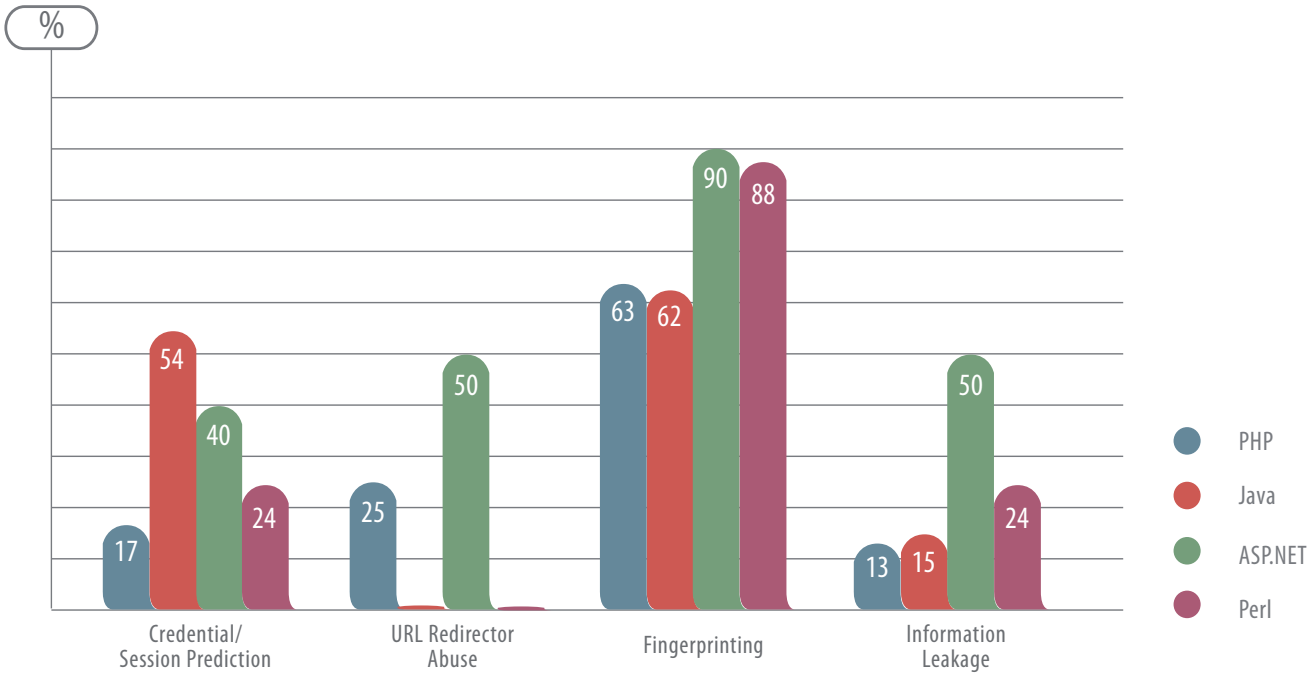
НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ
(в зависимости от средства разработки)



ДОЛЯ САЙТОВ С НАИБОЛЕЕ РАСПРОСТРАНЕННЫМИ УЯЗВИМОСТЯМИ В ЗАВИСИМОСТИ ОТ СРЕДСТВА РАЗРАБОТКИ (ЧАСТЬ 1)



ДОЛЯ САЙТОВ С НАИБОЛЕЕ РАСПРОСТРАНЕННЫМИ УЯЗВИМОСТЯМИ В ЗАВИСИМОСТИ ОТ СРЕДСТВА РАЗРАБОТКИ (ЧАСТЬ 2)



Критическая уязвимость SQL Injection была обнаружена также в других системах, разработанных с помощью Java, ASP.NET и Perl, но доля уязвимых систем в этих случаях не превышает 20%. Уязвимости OS Commanding подвержены также веб-приложения, разработанные на Java. Доля таких систем составила 8% в 2012 году.

Существенная доля веб-ресурсов подвержена уязвимостям Fingerprinting, Brute Force и Cross-Site Scripting для всех рассмотренных инструментов разработки. Уязвимость URL Redirector Abuse (злоупотребление перенаправлением URL) была выявлена только в системах, разработанных на PHP и ASP.NET.

Уязвимость подбора паролей наиболее распространена в веб-приложениях, разработанных на ASP.NET. Этот факт объясняется тем, что данная технология как правило используется в коммерческих приложениях, где предполагается использование централизованного хранилища идентификационных данных пользователей (Active Directory). При разворачивании подобного продукта владелец системы полагается на разработчика в вопросах обеспечения безопасности, забывая о необходимости использования таких механизмов защиты как двухфакторная аутентификация, CAPTCHA и блокирование попыток подбора учетных данных. В то же время наличие интеграции с Active Directory часто делает такие приложения наиболее интересной целью для злоумышленников с точки зрения подбора идентификаторов и паролей пользователей.

4.4. УЯЗВИМОСТИ, ХАРАКТЕРНЫЕ ДЛЯ РАЗЛИЧНЫХ ВЕБ-СЕРВЕРОВ

По результатам исследования, 88% сайтов под управлением сервера Apache оказались подвержены критическим уязвимостям. На втором месте по данному показателю веб-приложения под управлением серверов Apache Tomcat.

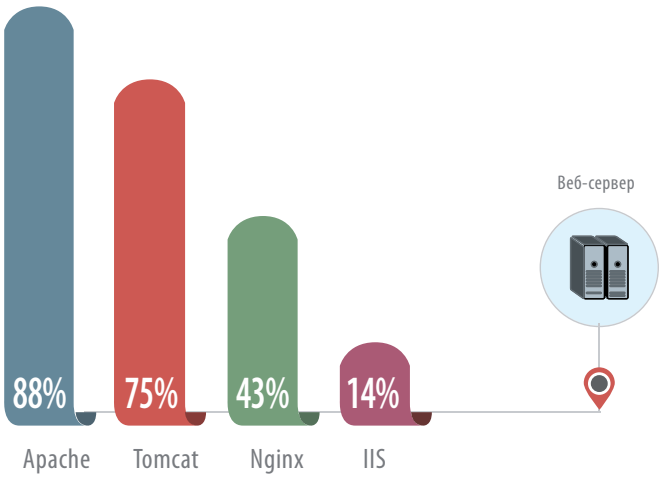
ДОЛИ САЙТОВ С КРИТИЧЕСКИМИ УЯЗВИМОСТЯМИ

ВЕБ-СЕРВЕР	ДОЛЯ, %
Apache	88
Apache Tomcat	75
Nginx	43
IIS	14
Jboss Web	-

Все исследованные системы под управлением веб-сервера Jboss Web относились к одному из крупных заказчиков Positive Technologies. Услуги по анализу защищенности данных систем осуществлялись на периодической основе. Таким образом, на момент подведения результатов исследования большинство уязвимостей были устранены, чем объясняется результат 0% в рассматриваемой категории. В целом уровень защищенности приложений на JBoss может быть существенно ниже.

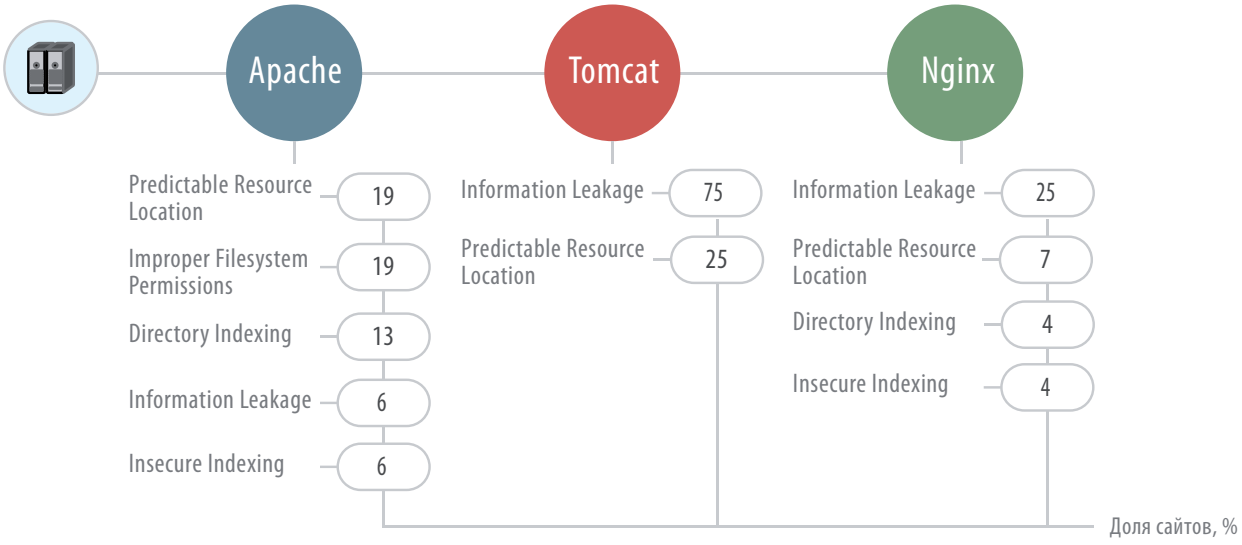
В 2010 и 2011 годах наиболее уязвимыми были веб-серверы Nginx и Apache, при этом наименее подвержены критическим уязвимостям были веб-приложения под управлением веб-сервера Microsoft IIS. В 2012 году веб-приложения под управлением серверов IIS оказались столь же безопасны: всего 14% исследованных сайтов содержали уязвимости высокой степени риска.

ВЕБ-ПРИЛОЖЕНИЯ С КРИТИЧЕСКИМИ УЯЗВИМОСТЯМИ (по типу веб-сервера)

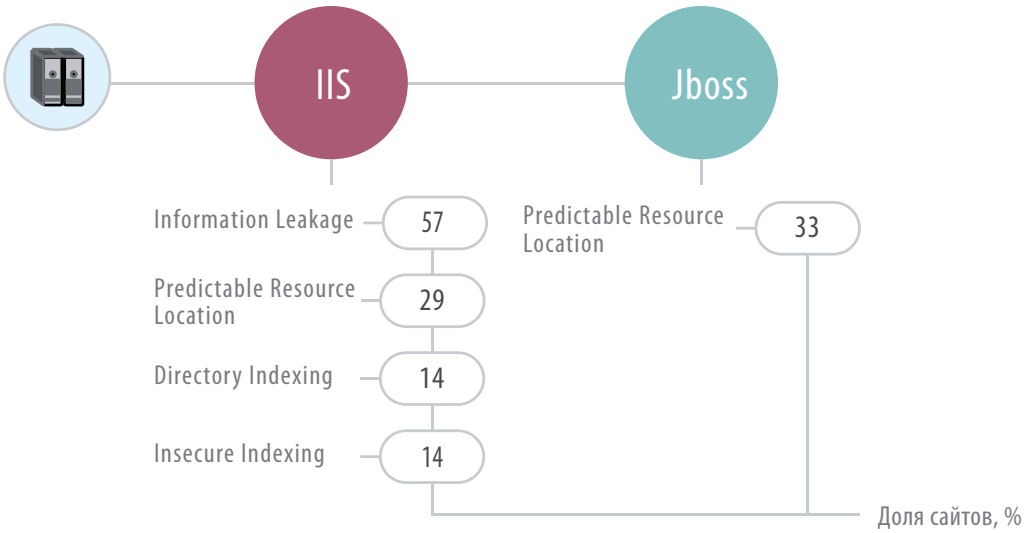


Многие уязвимости веб-приложений, выделенные согласно классификации WASC TC v2, связаны с ошибками администрирования. В нижеследующих таблицах приведен рейтинг таких уязвимостей, отсортированных по доле уязвимых сайтов, которые работают под управлением Apache Tomcat, Microsoft IIS, Nginx и Jboss Web. Все рассмотренные в таблице уязвимости характеризуются средней степенью риска.

РЕЙТИНГ УЯЗВИМОСТЕЙ, СВЯЗАННЫХ С ОШИБКАМИ АДМИНИСТРИРОВАНИЯ, ДЛЯ РАЗЛИЧНЫХ СЕРВЕРОВ (часть 1)



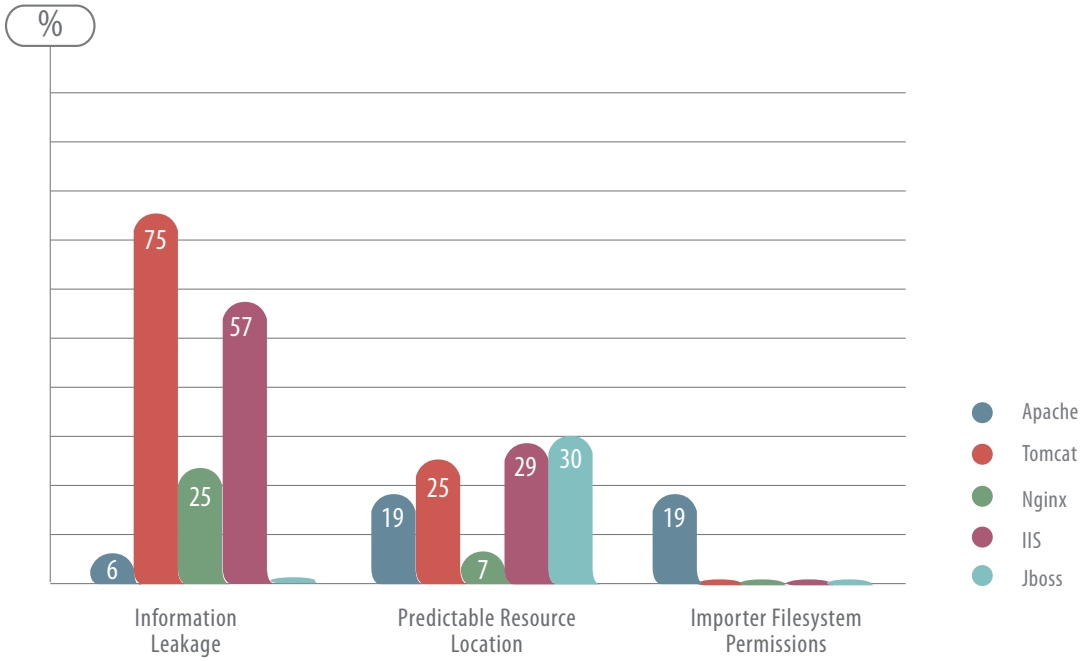
РЕЙТИНГ УЯЗВИМОСТЕЙ, СВЯЗАННЫХ С ОШИБКАМИ АДМИНИСТРИРОВАНИЯ, ДЛЯ РАЗЛИЧНЫХ СЕРВЕРОВ (часть 2)



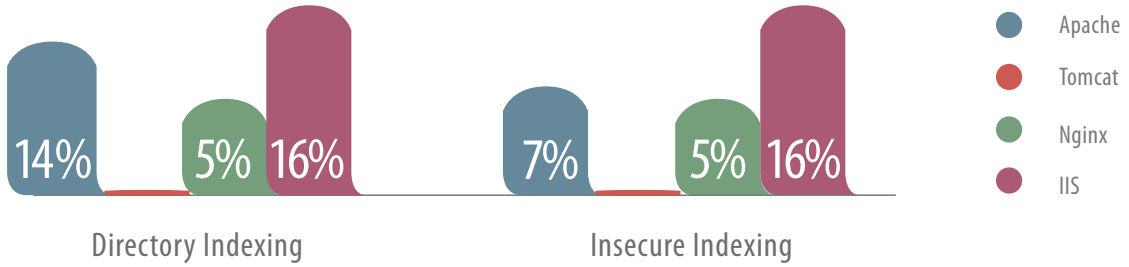
Для большинства веб-серверов наиболее распространенной ошибкой администрирования является Information Leakage (утечка информации), как и в 2010—2011 гг. Наиболее распространена данная уязвимость в системах под управлением веб-сервера Apache Tomcat: уязвимы 75% систем. В случае применения веб-сервера Microsoft IIS подобные ошибки администрирования были обнаружены более чем в половине исследованных систем.

Более подробное сравнение по распространенным уязвимостям, связанным с конфигурацией и функционированием веб-серверов, приведено на диаграммах.

ДОЛИ УЯЗВИМЫХ САЙТОВ НА РАЗЛИЧНЫХ ВЕБ-СЕРВЕРАХ (часть 1)



ДОЛИ УЯЗВИМЫХ САЙТОВ НА РАЗЛИЧНЫХ ВЕБ-СЕРВЕРАХ (часть 2)



На сайтах под управлением веб-сервера Apache ошибка администрирования Information Leakage встретилась всего в 6% рассмотренных систем, при этом уязвимость Improper Filesystem Permissions (некорректные разрешения файловой системы) оказалась характерна только для сайтов под управлением Apache и при этом наиболее распространенной, наравне с уязвимостью Predictable Resource Location (предсказуемое расположение ресурсов). Доля систем, подверженных уязвимостям Directory Indexing (индексация каталогов) и Secure Indexing (небезопасная индексация), не превышает 14% в случае применения веб-сервера IIS. Веб-приложения под управлением сервера Jboss содержат только ошибку администрирования Predictable Resource Location: уязвима треть рассмотренных сайтов, однако, как говорилось ранее, данные результаты относятся к ресурсам одного заказчика и могут не отражать общую картину для JBoss.

Согласно полученным результатам, системы, использующие веб-сервер Nginx, оказались наименее подвержены ошибкам администрирования. Стоит отметить, что и в 2010—2011 гг. веб-сервер Nginx превосходил все остальные веб-серверы по количеству уязвимых сайтов для всех типов уязвимостей, связанных с ошибками администрирования.

4.5. СТАТИСТИКА ДЛЯ РАЗЛИЧНЫХ ОТРАСЛЕЙ ЭКОНОМИКИ

В рамках проведенного исследования были рассмотрены веб-приложения, относящиеся к пяти областям экономики: промышленность, информационные технологии и информационная безопасность, государство, финансовый и телекоммуникационный секторы. Для каждой из перечисленных областей выявлены уязвимости разных степеней риска. В силу малого количества рассмотренных систем финансового сектора результаты их исследования не включены в данный раздел.

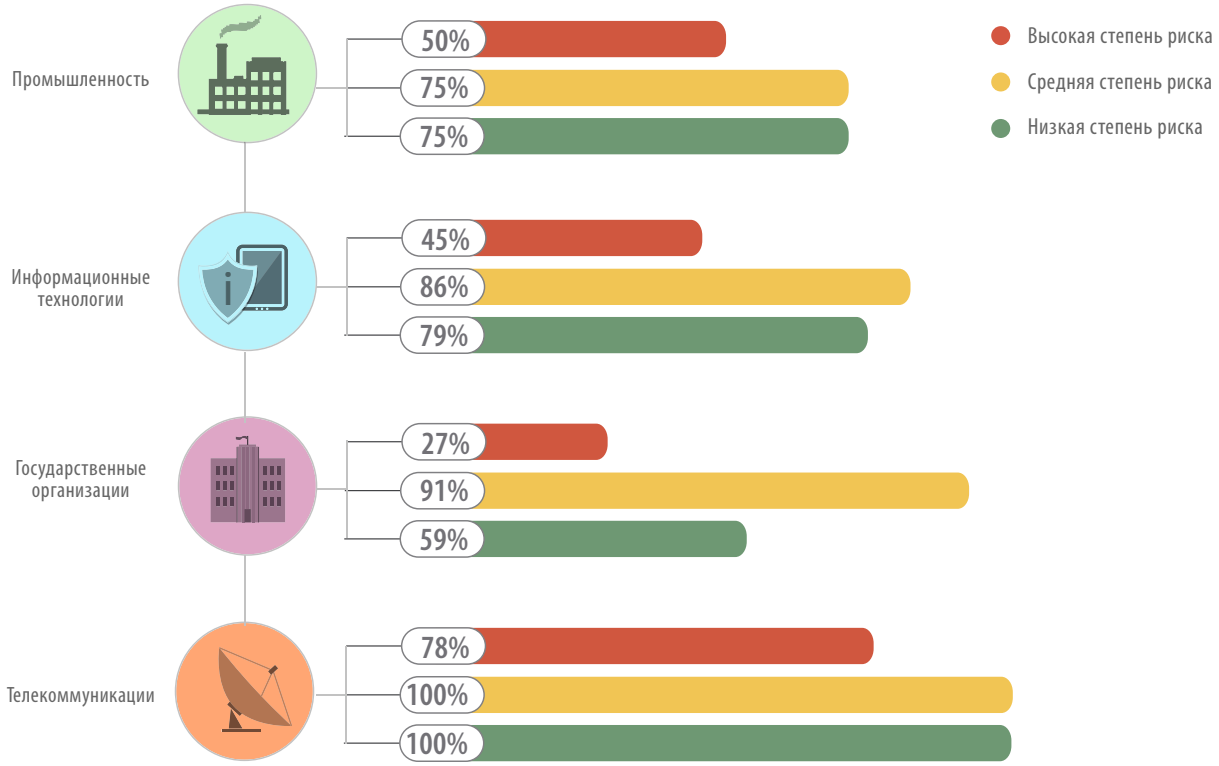
Наибольшее количество систем, содержащих уязвимости высокой степени риска, было выявлено в телекоммуникационной отрасли экономики и составило 78% от общего количества уязвимостей, выявленных в данном секторе. В промышленной сфере таких ресурсов ровно половина, затем следуют сайты IT- и ИБ-компаний. В государственных организациях примерно каждое третье веб-приложение содержит уязвимость высокого уровня риска.

В исследовании за 2012 год к уязвимостям IT-организаций была добавлена статистика по веб-приложениям компаний, специализирующихся на ИБ. Возможно, это и повлияло на улучшение ситуации в данном сегменте. Если в исследовании за 2010 и 2011 годы доля сайтов с уязвимостями высокого уровня риска составляла 75%, то сейчас показатель снизился до 45%. Особенностью компаний данного сектора является наличие уязвимостей, позволяющих осуществить XPath-инъекцию. В остальном все сходится с общей статистикой: в веб-приложениях много критических ошибок OS Commanding, Path Traversal и SQL Injection. Обнаружены также уязвимости, позволяющие вызвать отказ в обслуживании (Denial of Service), а у одной из компаний IT-отрасли, веб-приложение которой было построено на популярной коммерческой CMS, были обнаружены полтора десятка уязвимостей SQL Injection.

ДОЛИ САЙТОВ С УЯЗВИМОСТЯМИ ВЫСОКОГО УРОВНЯ РИСКА

ОТРАСЛЬ ЭКОНОМИКИ	ДОЛЯ, %
Телекоммуникации	78
Промышленность	50
Информационные технологии и информационная безопасность	45
Государственные организации	27

ДОЛЯ САЙТОВ, ПОДВЕРЖЕННЫХ УЯЗВИМОСТЯМ ОПРЕДЕЛЕННОГО УРОВНЯ РИСКА, ДЛЯ КАЖДОЙ ИЗ РАССМОТРЕННЫХ СФЕР ЭКОНОМИКИ



Половина рассмотренных веб-приложений промышленных компаний содержат критические уязвимости — ровно столько же, сколько и в 2010—2011 годы. Сотрудникам служб ИБ в подобных компаниях следует обращать внимание на недостатки, которые могут привести к осуществлению OS Commanding и SQL Injection, а также на менее перспективные с точки зрения злоумышленника, но весьма многочисленные уязвимости Cross-Site Scripting. Системы данного сектора экономики наименее подвержены уязвимостям средней степени риска — при том что доля уязвимых веб-приложений достигает 75%.

Исследование показало, что треть веб-приложений государственных организаций содержат уязвимости высокой степени риска. Год назад этот показатель равнялся 65%. В этом году на результатах исследования существенно сказался крупный государственный проект, в рамках которого успешно устранялись обнаруженные ранее уязвимости. Если не рассматривать веб-приложения данного проекта, то доля веб-приложений с критическими уязвимостями в государственном секторе составит 50%, что совпадает с показателями промышленной сферы (см. рис. на стр. 27). С одной стороны, снижение доли приложений с критическими уязвимостями в государственном секторе свидетельствует о позитивной динамике, но с другой стороны, доля уязвимых приложений все еще крайне велика, особенно учитывая интенсивный переход ряда государственных услуг, а значит и огромных объемов конфиденциальной информации, в сеть Интернет. Наиболее опасные для сайтов госорганов векторы атак: SQL Injection, Path Traversal, OS Commanding и Denial of Service. Кроме того, именно в этой сфере в 2012 году обнаружен единственный крупный корпоративный сайт, зараженный вирусом.

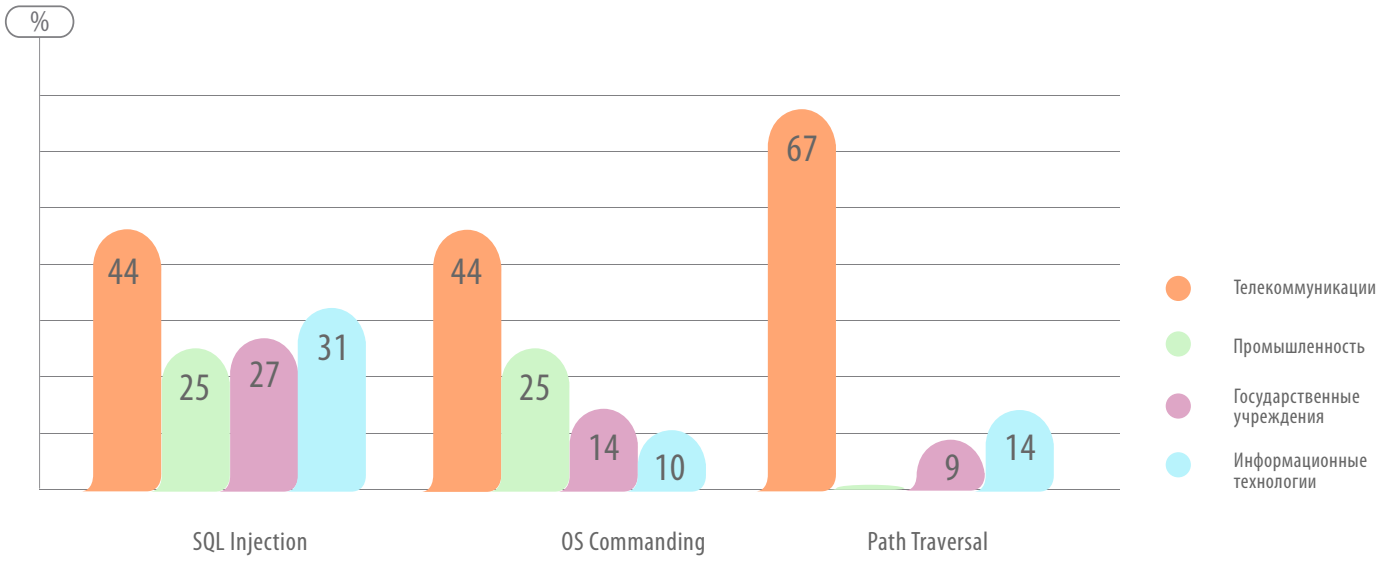
ДОЛИ САЙТОВ С УЯЗВИМОСТЯМИ ВЫСОКОГО УРОВНЯ РИСКА, ПРИНАДЛЕЖАЩИХ РАЗНЫМ ОТРАСЛЯМ ЭКОНОМИКИ

ОТРАСЛЬ ЭКОНОМИКИ	ДОЛЯ, %
Телекоммуникации	78
Промышленность	50
Государственные организации (выборочно)	50
Информационные технологии и информационная безопасность	45

Наиболее уязвимыми в 2012 году оказались веб-приложения телекоммуникационного сектора. Уязвимости среднего и низкого уровня риска были обнаружены во всех системах, чуть менее 80% систем подвержены уязвимостям высокого уровня риска. Эта цифра весьма велика, но все-таки ниже 88%, полученных в 2010 и 2011 годах. Как и прежде, профильные для отрасли веб-приложения часто подвержены атакам на пользователей (Client-Side Attacks) и насыщены недостатками, позволяющими реализовать Cross-Site Scripting. Среди наиболее опасных уязвимостей следует отметить распространенные в веб-приложениях этого сектора Path Traversal и SQL Injection, а также на OS Commanding и XML Injection, которые встречаются немного реже.

На рисунке ниже представлены доли систем, подверженных таким критическим уязвимостям, как SQL Injection, Path Traversal и OS Commanding. В 2012 году сохранилась неутешительная ситуация в телекоммуникационном секторе, где доля уязвимых систем наиболее велика для трех рассматриваемых видов уязвимостей. В сфере промышленности и в государственных учреждениях данные показатели существенно ниже, доля уязвимых систем в них не превышает 27%. Наблюдается также тенденция к повышению уровня защищенности систем в сфере информационных технологий и информационной безопасности: доля уязвимых веб-приложений уменьшилась в 2—4 раза для различных уязвимостей. В то же время доля уязвимых систем все еще не позволяет говорить о достаточном уровне безопасности сайтов в данной области экономики.

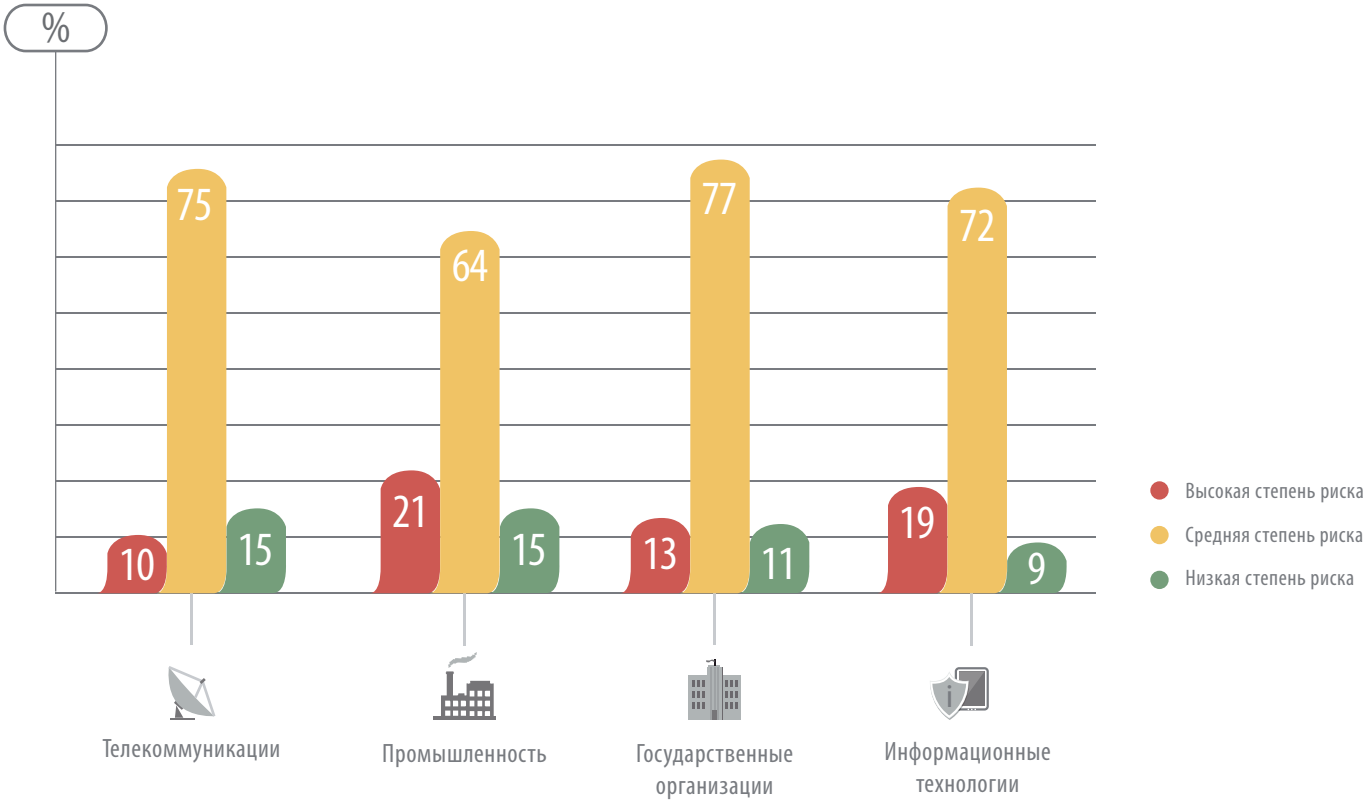
ДОЛИ УЯЗВИМЫХ САЙТОВ ДЛЯ РАЗЛИЧНЫХ ОТРАСЛЕЙ ЭКОНОМИКИ



Ниже представлено соотношение обнаруженных уязвимостей по уровню риска для соответствующих областей экономики. Результаты проведенного исследования показывают, что наиболее распространены уязвимости веб-приложений среднего уровня риска: примерно 65—75% уязвимостей в каждой сфере экономики.

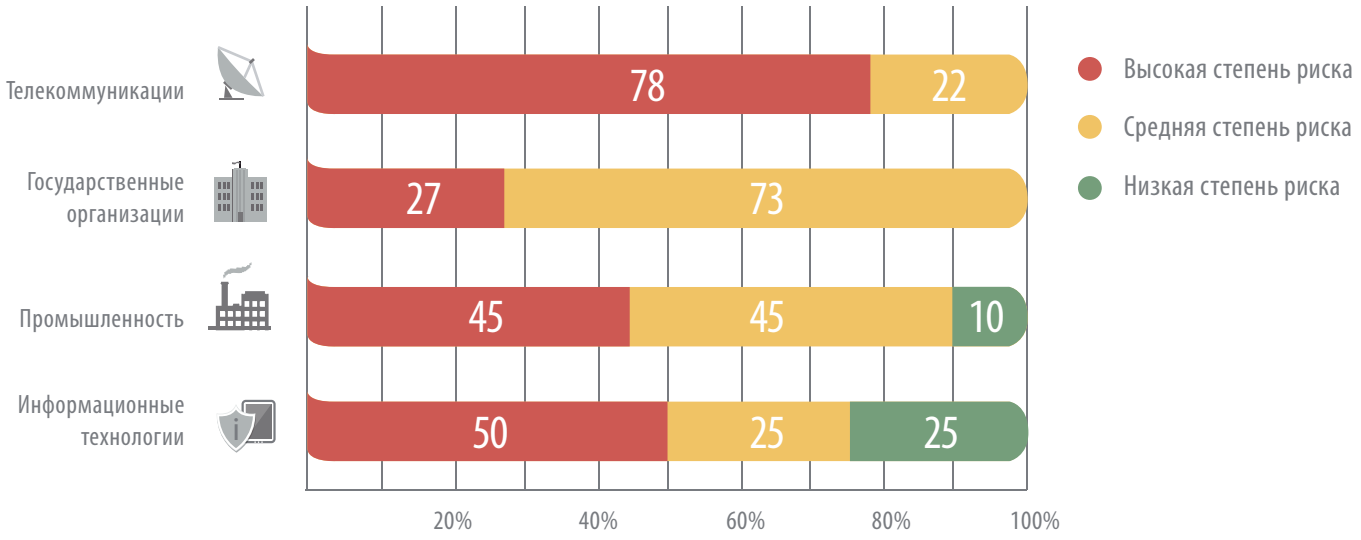
Полученная статистика оказалась довольно сбалансированной. Среди рассмотренных сфер экономики выделяется лишь сектор IT , веб-приложения которого содержали более 20% уязвимостей высокой степени риска. Приближаются к данному уровню и телекоммуникационные компании: здесь показатель достигает 19%. Наблюдается относительно небольшой процент уязвимостей низкого уровня риска (10—20% во всех сферах экономики). В целом показатели различных областей экономики в рассматриваемом соотношении оказались практически одинаковы.

СООТНОШЕНИЕ ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ ПО УРОВНЮ РИСКА ДЛЯ РАССМАТРИВАЕМЫХ ОБЛАСТЕЙ ЭКОНОМИКИ



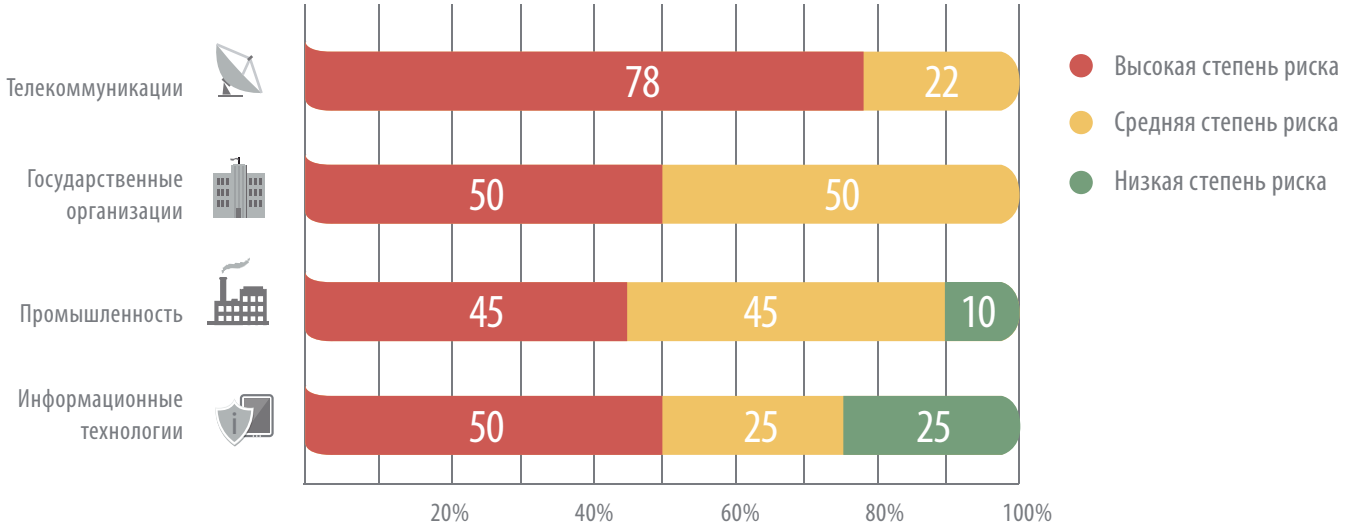
В части анализа максимальных уровней риска обнаруженных уязвимостей веб-приложений необходимо выделить сферу телекоммуникаций. Здесь наблюдается существенное преобладание систем, подверженных уязвимостям высокого уровня риска. Только среди веб-приложений веб-приложений промышленного сектора, а также IT- и ИБ-компаний выявлены системы, имеющие уязвимости низкой степени риска. В сфере промышленности доля таких систем достигает 25%. При этом в данной сфере достаточно велика доля веб-приложений, в которых обнаружены критические уязвимости (50%).

ДОЛЯ ВЕБ-ПРИЛОЖЕНИЙ ПО МАКСИМАЛЬНОМУ УРОВНЮ РИСКА УЯЗВИМОСТЕЙ



Проведенные исследования показали, что в 2012 году наилучшая ситуация наблюдается в государственной сфере, где было выявлено наименьшее количество веб-приложений, подверженных уязвимостям высокой степени риска. Однако данные показатели можно объяснить тем, что существенную долю систем государственного сектора составили веб-приложения одного крупного заказчика, для приложений которого анализ и устранение уязвимостей проводились на регулярной основе. Статистика по приложениям, имеющим уязвимости с различным максимальным уровнем риска, без учета данного проекта приведена на рисунке ниже.

ДОЛЯ ВЕБ-ПРИЛОЖЕНИЙ ПО МАКСИМАЛЬНОМУ УРОВНЮ РИСКА УЯЗВИМОСТЕЙ
(без учета государственного проекта с повторной оценкой защищенности)



ЗАКЛЮЧЕНИЕ

В ходе проведенного исследования мы продемонстрировали, насколько уязвимы современные веб-приложения.

Средний уровень защищенности веб-приложений по сравнению с 2011 годом стал немного выше. Доля сайтов, содержащих критические уязвимости, уменьшилась на 15% и составила почти 45%. Было обнаружено только одно зараженное веб-приложение, тогда как ранее 10% сайтов содержали вредоносный код. С другой стороны, есть и признаки стагнации: никак не изменилась доля веб-приложений с уязвимостями высокого уровня риска в промышленной сфере, а сайты телеком-сектора повышают уровень безопасности очень медленно.

Общая поквартальная динамика показала, что первое полугодие 2012 года характеризуется снижением количества веб-приложений, содержащих уязвимости высокой степени риска, но в третьем квартале года данные показатели вновь приближаются к уровню предыдущих лет.

ССЫЛКИ

1. WASC Threat Classification v. 2.0: http://projects.webappsec.org/Threat-Classification.
2. Common Vulnerability Scoring System: http://www.first.org/cvss.
3. OWASP Top Ten Project: https://www.owasp.org/index.php/OWASP_Top_Ten_Project.

ПРИЛОЖЕНИЕ А

МЕТОДИКА ОЦЕНКИ СТЕПЕНИ РИСКА

Классификация угроз	Базовая оценка по шкале CVSS
Abuse of Functionality	4 (AV:N/AC:H/Au:N/C:P/I:P/A:N)
Brute Force Attack	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Buffer Overflow	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Content Spoofing	5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
Credential/Session Prediction	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Cross-Site Scripting	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)
Cross-Site Request Forgery	5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
Denial of Service	7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
Format String Attack	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
HTTP Request Splitting	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)
HTTP Response Splitting	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)
HTTP Request Smuggling	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)
HTTP Response Smuggling	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)
Integer Overflow	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
LDAP Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Mail Command Injection	5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
Null Byte Injection	5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
OS Commanding	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Path Traversal	7.8 (AV:N/AC:L/Au:N/C:C/I:N/A:N)
Predictable Resource Location	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Remote File Inclusion	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Routing Detour	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
SOAP Array Abuse	7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
SSI Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Session Fixation	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
SQL Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
URL Redirectors	2.6 (AV:N/AC:H/Au:N/C:N/I:P/A:N)

Классификация угроз	Базовая оценка по шкале CVSS
XPath Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
XML Attribute Blowup	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
XML External Entity	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
XML Entity Expansion	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
XML Injection	7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
XQuery Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Application Misconfiguration	5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
Directory Indexing	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Fingerprinting	0 (AV:N/AC:L/Au:N/C:N/I:N/A:N)
Improper Parsing	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Improper Permissions	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Information leakage	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Insecure Indexing	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Insufficient Anti-automation	4 (AV:N/AC:H/Au:N/C:P/I:P/A:N)
Insufficient Authentication	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Insufficient Authorization	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Insufficient Data Protection	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Insufficient Password Recovery	5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
Insufficient Process Validation	4 (AV:N/AC:H/Au:N/C:P/I:P/A:N)
Insufficient Session Expiration	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Insufficient Transport Layer Protection	4 (AV:N/AC:H/Au:N/C:P/I:P/A:N)
Server Misconfiguration	5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
Improper File System Permissions	4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)