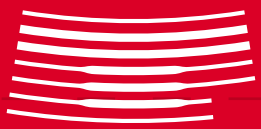
СТАТИСТИКА УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ

(2013 ГОД)



POSITIVE TECHNOLOGIES

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

На сегодняшний день информатизация является одним из приоритетных направлений развития всех экономических отраслей. Практически каждая организация, коммерческая или государственная, имеет свой интернет-сайт, вводит всевозможные онлайн-услуги. В электронном виде хранятся персональные данные клиентов и сотрудников, финансовая информация и данные о хозяйственной деятельности. В связи с этим задача обеспечения безопасности веб-приложений становится важнее год от года.

К сожалению, разработчики корпоративных информационных систем не всегда следуют требованиям безопасности — из-за отсутствия необходимого опыта или просто сосредоточиваясь на иных целях при разработке системы. Ежегодные исследования компании Positive Technologies свидетельствуют, что большое количество веб-приложений содержат уязвимости высокой степени риска, которые могут стать причиной финансового или репутационного ущерба.

Именно атака на веб-приложения зачастую становится первым этапом при взломе сетей крупных компаний, а публикация порочащей владельца информации на официальных веб-сайтах служит оружием в информационной войне. Немалую роль уязвимые веб-приложения могут сыграть в успехе крайне распространенных на сегодняшний день распределенных атак, направленных на отказ в обслуживании (DDoS). Если на сетевом уровне специальные услуги от провайдеров и устройства для защиты трафика могут справиться с наиболее примитивными и массовыми DDoS-атаками, то в случае когда злоумышленник эмулирует действия легитимного пользователя приложения и использует специальные ресурсоемкие запросы к сайту, даже небольшой объем трафика может привести к полной недоступности сайта.

Настоящее исследование посвящено анализу данных, полученных в результате работ по анализу защищенности веб-приложений в 2013 году, и обзору наиболее распространенных уязвимостей веб-приложений (в зависимости от 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 2013 году. В общей сложности специалисты компании изучили порядка 500 веб-приложений в рамках различных работ, начиная от инструментального сканирования и заканчивая анализом исходного кода. С целью получения объективной оценки уровня защищенности было выделено 61 веб-приложение, 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 61 сайта было обнаружено 953 уязвимости 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 v. 2 [1]), за исключением Improper Input Handling и Improper Output Handling, поскольку они реализуются 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 v. 2 [2]); на этой основе выделялись качественные оценки высокого, среднего и низкого уровней риска.

2. РЕЗЮМЕ

1. Все веб-приложения содержат те или иные уязвимости, при этом **62% рассмотренных систем содержат уязвимости высокой степени риска;** данный показатель существенно выше прошлогоднего (45%). Уязвимости среднего уровня риска содержались в 95% систем.
2. Наиболее распространенная уязвимость по итогам 2013 года — межсайтовое выполнение сценариев (Cross Site Scripting), которое встречается в 78% приложений, на втором месте — возможность подбора идентификатора или пароля (Brute Force), которой подвержены 69% рассмотренных систем. **В топ-10 вошли две уязвимости высокой степени риска: «Внедрение операторов SQL», которому подвержены 43%** исследованных веб-ресурсов, а также **«Внедрение внешних сущностей XML», которому оказались подвержены 20%** анализируемых систем.
3. Наибольшее количество веб-приложений, содержащих уязвимости высокой степени риска, было выявлено среди **веб-приложений, принадлежащих СМИ, где 80% приложений подвержены критическим уязвимостям.**
4. **76% систем, написанных на языке программирования PHP, оказались подвержены критическим уязвимостям.** Этот показатель выше, чем у других языков, как по общей доле уязвимых систем, так и по среднему количеству уязвимостей на систему.
5. В 2013 году наиболее распространенным веб-сервером оказался Apache, при этом наиболее подверженными уязвимостям высокой степени риска являются веб-приложения, функционирующие на базе Apache Tomcat и Microsoft IIS: критические уязвимости обнаружены в 75 и 71% веб-ресурсов соответственно.
6. Половина рассмотренных систем ДБО содержали критические уязвимости, при этом **полностью требованиям PCI DSS не соответствовала ни одна из исследованных систем.**
7. **Тестирование методом белого ящика в среднем позволяет обнаружить в 10 раз больше критических уязвимостей,** а также примерно в два раза больше уязвимостей средней и низкой степени риска, чем тестирование только методами черного и серого ящиков.

3. ПОРТРЕТ УЧАСТНИКОВ

Исследованные веб-ресурсы принадлежат компаниям, относящимся к различным отраслям экономики — информационным технологиям, телекоммуникациям, промышленности, государственным учреждениям, банковскому сектору и средствам массовой информации. Большая часть веб-ресурсов принадлежит банкам (57%). Существенная часть сайтов относится к государственному сектору (21%), прочие отрасли представлены менее широко.

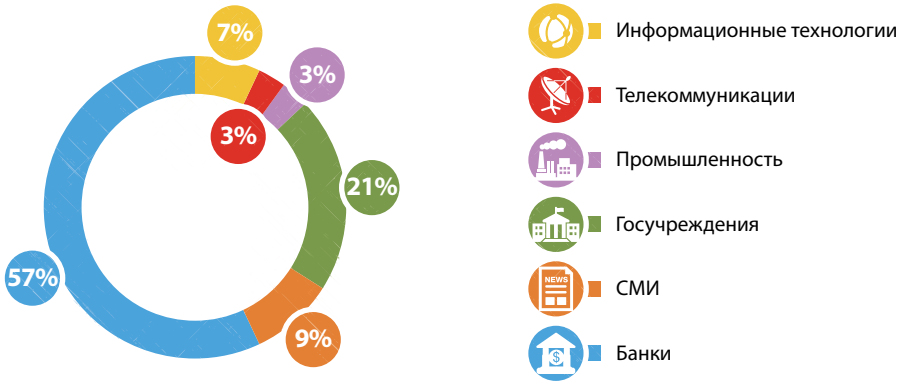
Банки традиционно уделяют большое внимание анализу защищенности веб-приложений, это объясняется наличием в инфраструктуре банков критически важных для бизнеса приложений, в которых осуществляются финансовые операции, и наличием требований регулирующих органов по проведению анализа защищенности (например, согласно стандарту PCI DSS). При этом в 2013 году спрос на анализ защищенности в банковском секторе заметно возрос, что связано с активным вводом в эксплуатацию новых систем, а также с повышением внимания к вопросам анализа кода банковских приложений со стороны Банка России и отрасли в целом. Также стоит отметить возросший спрос на анализ защищенности веб-приложений со стороны средств массовой информации, причиной которого послужили, вероятно, недавние громкие случаи хакерских атак с последующим распространением заведомо ложных новостей (к примеру, заявления об отставке президента ОАО «Российские железные дороги» Владимира Якунина, распространенного от имени пресс-службы правительства).

Исследуемые веб-ресурсы были разработаны с использованием различных технологий и языков программирования. Наиболее распространенными среди анализируемых систем оказались такие средства разработки как PHP (39%), Java (37%) и ASP.NET (20%). В категорию «Другое» вошли языки программирования, которые используются для разработки веб-приложений значительно реже, такие как Perl и Ruby.

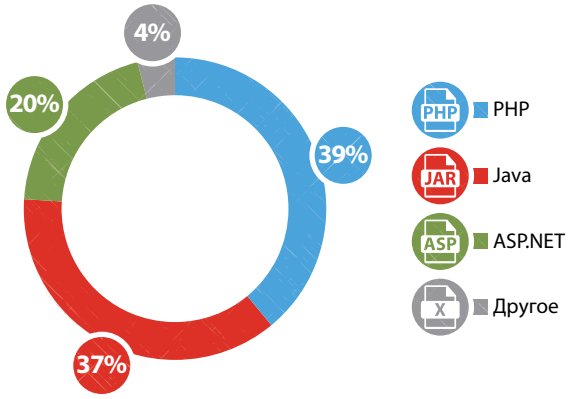
Кроме того, все веб-приложения можно разделить на пять групп в зависимости от типа используемого веб-сервера. Большинство сайтов функционирует на базе веб-сервера Apache (39%). Другим распространенным веб-сервером является Nginx: он обеспечивает работу 37% рассмотренных систем и, как правило, используется на уровне фронтэнда. Менее популярными оказались веб-серверы Jboss, Oracle Application Server и специализированное проприетарное ПО, которые были объединены в категорию «Другое» вследствие малого количества систем, использующих данные веб-серверы. Полное распределение веб-приложений приведено на диаграмме ниже.

Как и в 2012 году, коммерческие системы управления содержимым (CMS) применялись крайне редко, в связи с чем статистические исследования уровня защищенности сайтов в зависимости от используемой системы CMS не проводились.

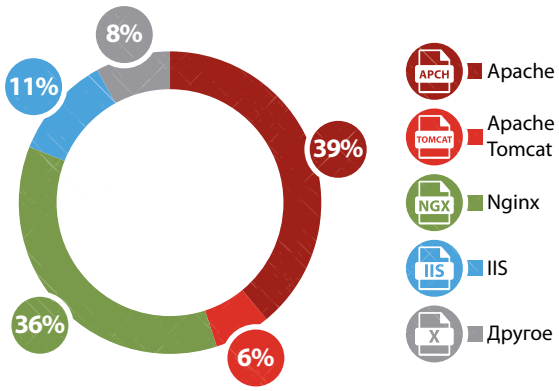
РАСПРЕДЕЛЕНИЕ СИСТЕМ ПО ОТРАСЛЯМ ЭКОНОМИКИ



РАСПРЕДЕЛЕНИЕ СИСТЕМ ПО СРЕДСТВАМ РАЗРАБОТКИ



РАСПРЕДЕЛЕНИЕ СИСТЕМ ПО ТИПУ ИСПОЛЬЗУЕМОГО ВЕБ-СЕРВЕРА



4. СТАТИСТИКА УЯЗВИМОСТЕЙ

Данная глава содержит анализ распространенности и уровней риска уязвимостей различных типов, классифицированных согласно угрозам, представленным в WASC TC v. 2.

4.1. НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ

Исследования, проведенные в 2013 году, показали, что большая часть систем (62%) содержит уязвимости высокой степени риска и практически все системы (95%) — уязвимости средней степени риска.

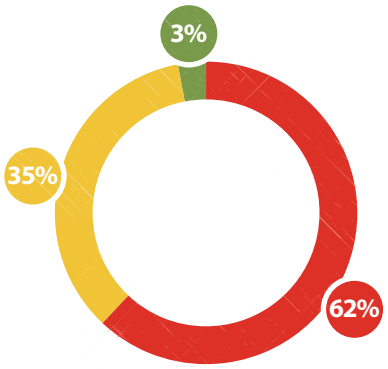
В целом в каждом веб-приложении были обнаружены те или иные уязвимости.

По сравнению с результатами предыдущих лет заметно увеличилась доля систем, содержащих уязвимости средней и высокой степени риска. Количество веб-приложений, подверженных уязвимостям низкой степени риска, снизилось, однако в целом можно говорить об ухудшении ситуации в области защищенности веб-приложений.

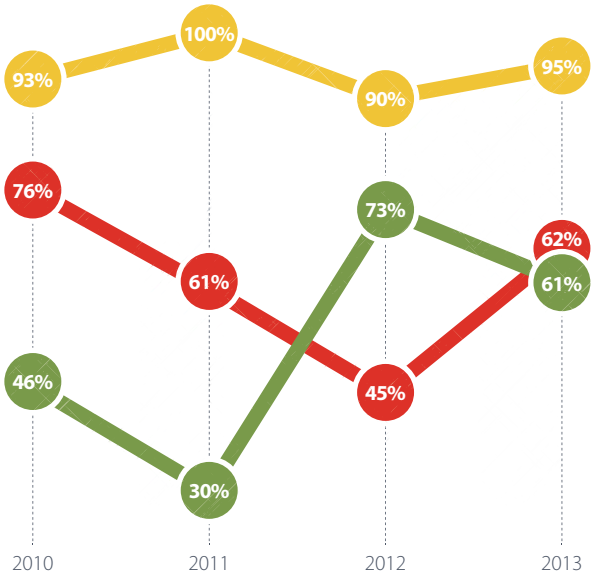
Наиболее распространенной по результатам исследования в 2013 году оказалась уязвимость «Межсайтовое выполнение сценариев» (Cross-Site Scripting, XSS). Данной уязвимости подвержены 78% ресурсов. Второе место занимают недостатки, позволяющие автоматизировано подбирать учетные данные и пароли пользователей (Brute Force), которые были обнаружены в 69% исследованных систем. Почти две трети (63%) веб-ресурсов содержат уязвимости, связанные с недостаточной защитой сессий пользователей (Credential/Session Prediction). В 2012 году десятку распространенных уязвимостей веб-ресурсов возглавляла уязвимость идентификации программного обеспечения (Fingerprinting), выявленная в 73% исследованных ресурсов, теперь она была выявлена менее чем в половине приложений (49%) и опустилась на четвертое место.

ДОЛЯ УЯЗВИМЫХ САЙТОВ В ЗАВИСИМОСТИ ОТ СТЕПЕНИ РИСКА УЯЗВИМОСТЕЙ

ДОЛЯ УЯЗВИМЫХ САЙТОВ В ЗАВИСИМОСТИ ОТ МАКСИМАЛЬНОЙ СТЕПЕНИ РИСКА



ДОЛЯ УЯЗВИМЫХ САЙТОВ (ПО СТЕПЕНИ РИСКА УЯЗВИМОСТЕЙ)



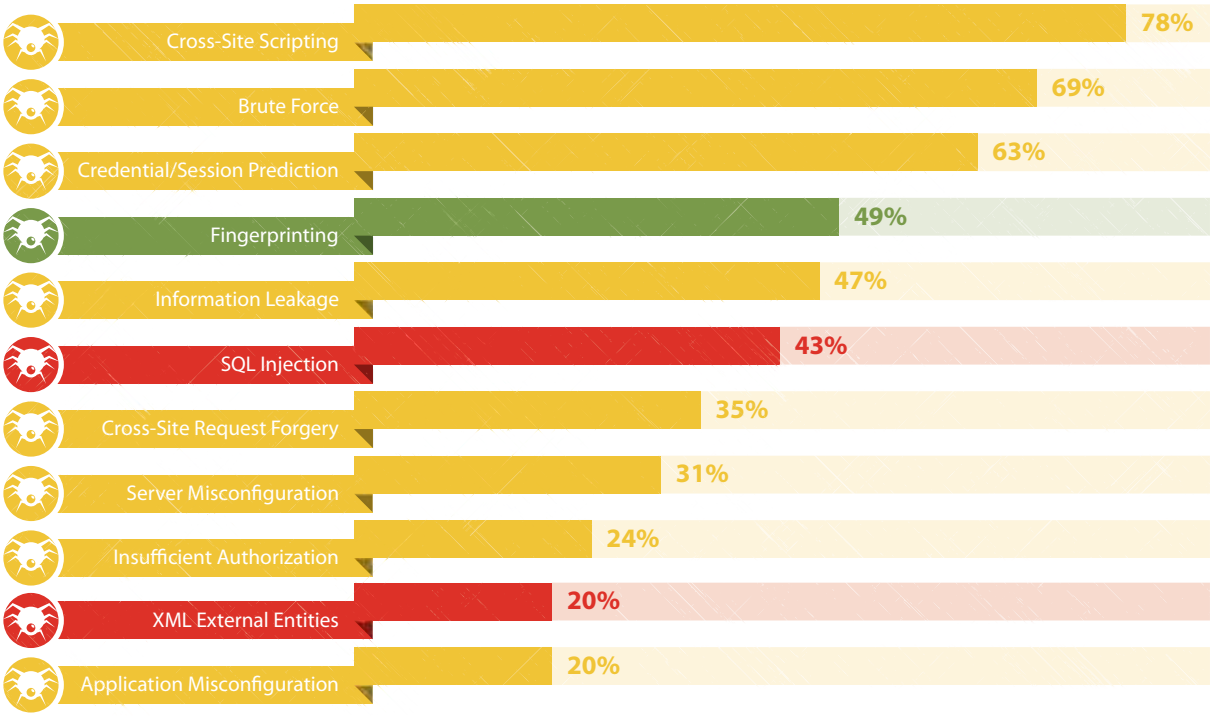
Также в топ-10 вошла уязвимость высокой степени риска «Внедрение операторов SQL» (SQL Injection), которой оказались подвержены 43% исследованных в 2013 году веб-ресурсов. Несмотря на то что в общем рейтинге по распространенности этот недостаток спустился с 4-го места на 6-е, в целом уязвимых приложений стало больше: их доля возросла на 10% по сравнению с 2012 годом. Уязвимость типа «Внедрение внешних сущностей XML» (XML External Entities) встретилась в каждом пятом приложении (ранее она не входила в десятку самых распространенных). Это можно объяснить возникновением новых техник атак, таких как XML Out-Of-Band Data Retrieval, которая была разработана специалистами Positive Technologies и признана одной из лучших техник атак на веб-приложения в 2013 году. Эксплуатация уязвимости может привести к получению доступа к сторонним ресурсам по различным протоколам, чтению файлов на сервере, а также к полному отказу в обслуживании веб-приложения.

Стоит обратить внимание, что в десятку самых распространенных вошли уязвимости, связанные с недостатками авторизации пользователей (24%). Несмотря на то что в общем случае уязвимости присвоен средний уровень риска, данный недостаток зачастую, в зависимости от бизнес-логики приложения, может приводить к серьезным последствиям, например к несанкционированному проведению транзакций в системах дистанционного банковского обслуживания или возможности оформления покупок в интернет-магазинах без оплаты товара.

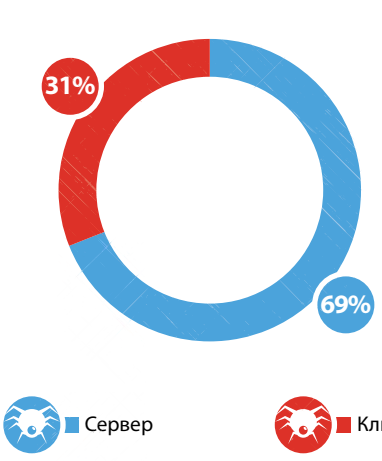
Большая часть недостатков (69%) позволяет проводить атаки на серверные компоненты веб-приложений. Среди уязвимостей, позволяющих проводить атаки на пользователей, наиболее распространены межсайтовое выполнение сценариев и подделка межсайтовых запросов.

Подавляющее большинство (89%) недостатков являются ошибками в программном коде, и лишь 11% возникли вследствие некорректной конфигурации веб-приложений.

НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ (ДОЛЯ САЙТОВ, %)



РАСПРЕДЕЛЕНИЕ УЯЗВИМОСТЕЙ ПО ОБЪЕКТАМ АТАКИ

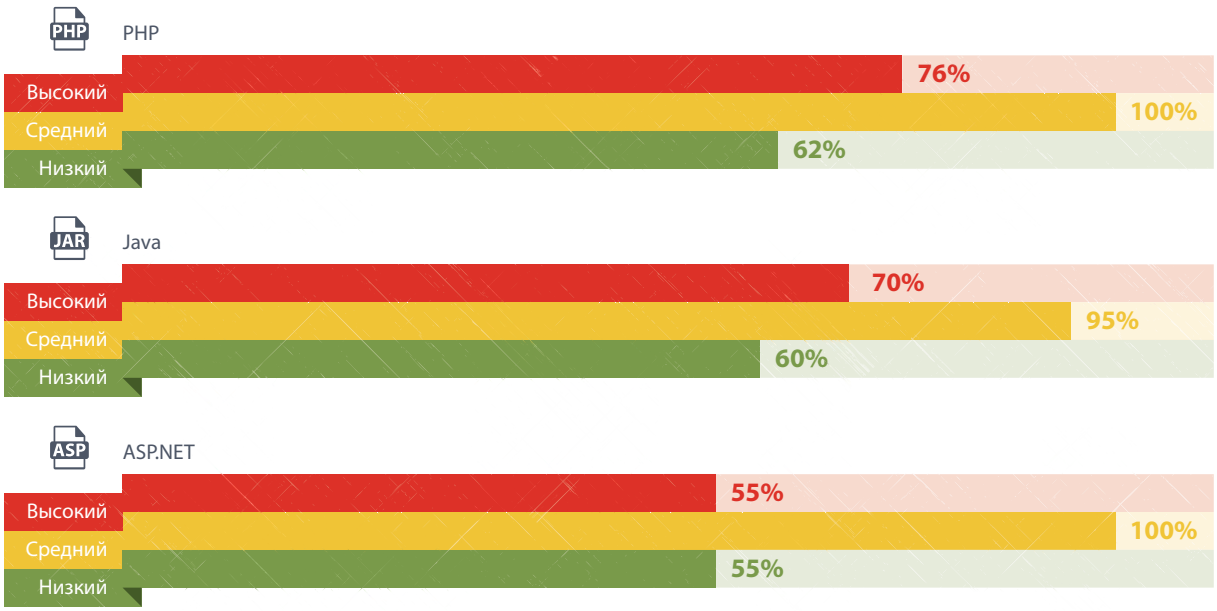


РАСПРЕДЕЛЕНИЕ УЯЗВИМОСТЕЙ ПО ПРОИСХОЖДЕНИЮ

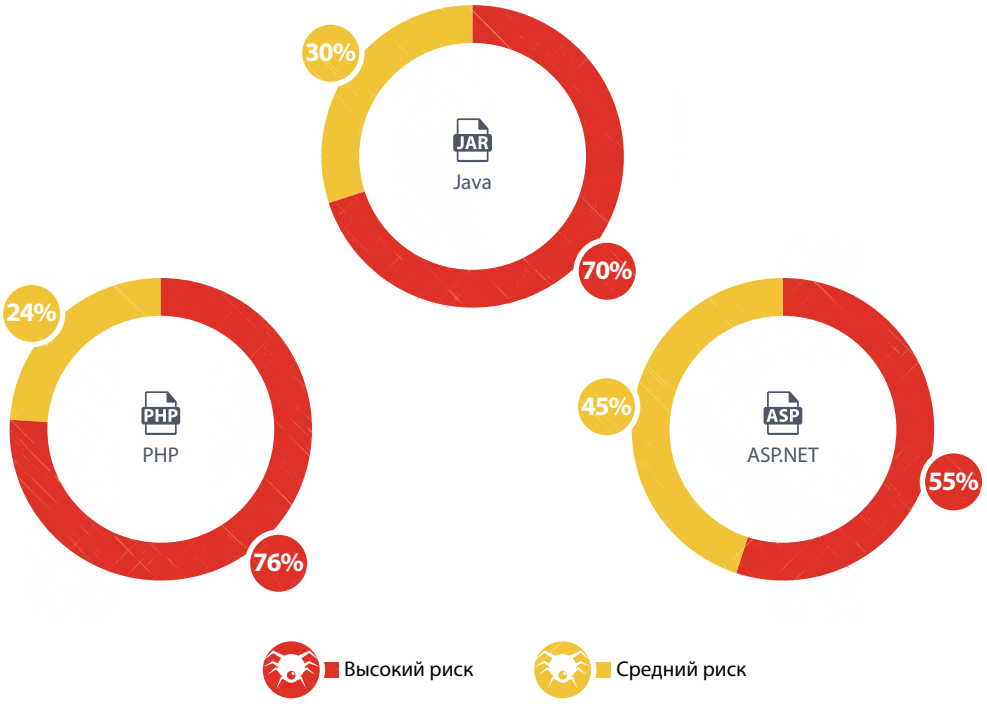
4.2. УЯЗВИМОСТИ, ХАРАКТЕРНЫЕ ДЛЯ РАЗЛИЧНЫХ СРЕДСТВ РАЗРАБОТКИ ВЕБ-ПРИЛОЖЕНИЙ

В данном разделе приведена статистика по уязвимостям для трех наиболее распространенных средств разработки веб-приложений: PHP, Java и ASP.NET. Три четверти (76%) сайтов, написанных на языке программирования PHP, содержат критические уязвимости. Веб-ресурсы, написанные на Java и ASP.NET, оказались менее уязвимыми: 70 и 55% приложений соответственно содержат критические уязвимости. Все приложения, написанные на трех указанных языках программирования содержат уязвимости как минимум средней степени риска.

ДОЛИ СИСТЕМ С УЯЗВИМОСТЯМИ РАЗНОЙ СТЕПЕНИ РИСКА (ПО ЯЗЫКАМ ПРОГРАММИРОВАНИЯ)



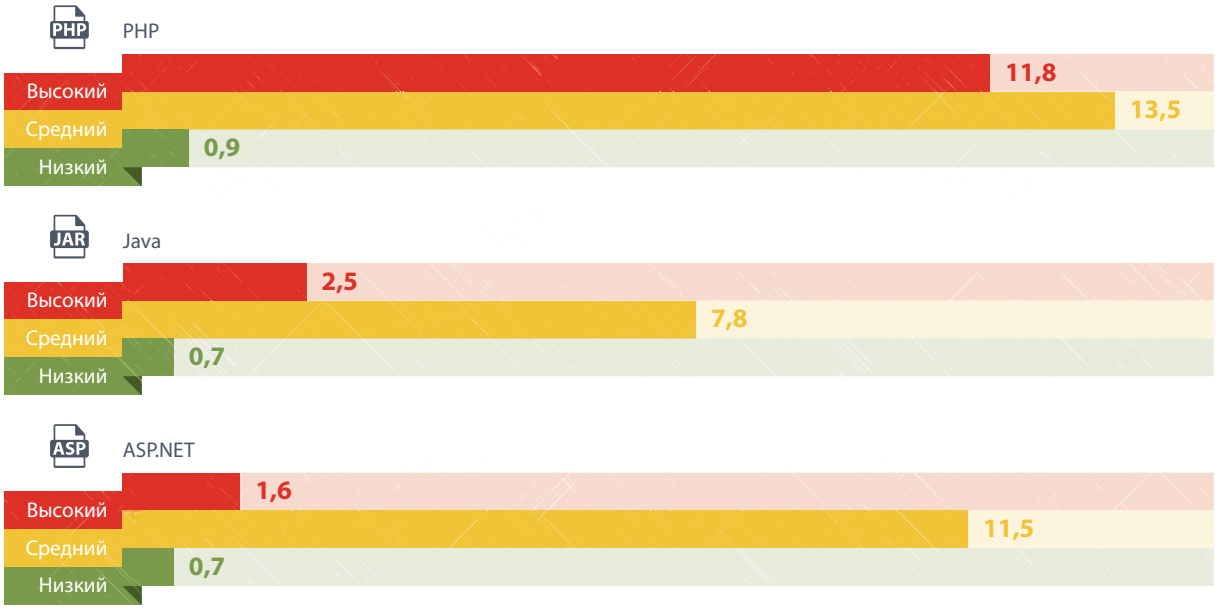
ДОЛЯ ВЕБ-ПРИЛОЖЕНИЙ ПО МАКСИМАЛЬНОМУ УРОВНЮ РИСКА УЯЗВИМОСТЕЙ



О том, что веб-приложения, разработанные на PHP, более уязвимы, свидетельствует и среднее количество уязвимостей, приходящихся на одну систему. Так, в каждом PHP-приложении в среднем было найдено 12 критических уязвимостей, тогда как приложения на Java и ASP.NET в среднем содержат по 2 и 1 критической уязвимости соответственно.

В таблице представлены статистические данные о распространенности часто встречающихся уязвимостей на ресурсах, созданных при помощи разных языков программирования.

СРЕДНЕЕ КОЛИЧЕСТВО УЯЗВИМОСТЕЙ В ОДНОЙ СИСТЕМЕ (ПО ЯЗЫКУ РАЗРАБОТКИ)



РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ (ПО ЯЗЫКАМ ПРОГРАММИРОВАНИЯ)

PHP	Доля сайтов, %	Java	Доля сайтов, %	ASP.NET	Доля сайтов, %
Cross-Site Scripting	90	Cross-Site Scripting	80	Cross-Site Scripting	73
Credential/Session Prediction	86	Fingerprinting	60	Brute Force	73
Brute Force	81	Brute Force	45	Fingerprinting	55
Information Leakage	67	Credential/Session Prediction	45	Cross-Site Request Forgery	55
SQL Injection	62	Server Misconfiguration	35	Credential/Session Prediction	45
Fingerprinting	43	Information Leakage	30	Information Leakage	45
Cross-Site Request Forgery	43	XML External Entities	30	Server Misconfiguration	36
Server Misconfiguration	29	SQL Injection	25	Application Misconfiguration	36
Insufficient Authorization	29	Cross-Site Request Forgery	25	XML External Entities	36
Application Misconfiguration	19	Insufficient Authorization	15	SQL Injection	27

Для всех языков программирования самой распространенной оказалась уязвимость «Межсайтовое выполнение сценариев». Ей подвержены 90, 80 и 73% приложений, написанных на PHP, Java и ASP.NET соответственно.

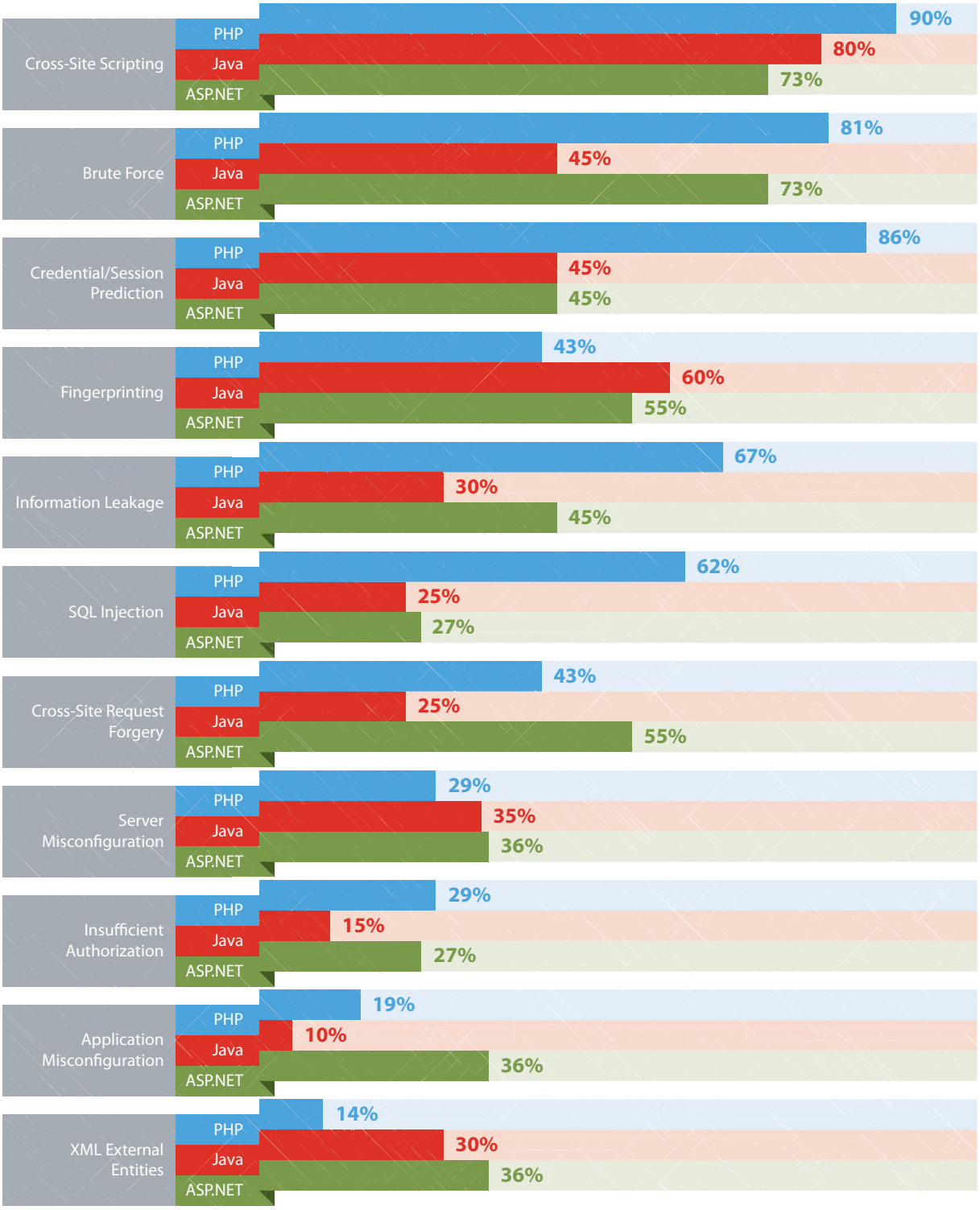
Критическая уязвимость «Внедрение операторов SQL» встречается в 62% сайтов, написанных на языке PHP. Для других языков данный показатель значительно ниже, но все же хуже, чем в прошлом году: для приложений на Java внедрение операторов SQL теперь встречается в каждой четвертой системе, а для приложений на ASP.NET — в 27% случаев. Высокую распространенность данной уязвимости среди приложений, разработанных на PHP, можно объяснить тем, что в этом языке программирования

не с первых версий появилась возможность создания параметризованных SQL-запросов. Как следствие, многие книги и интернет-ресурсы, по которым учатся программисты, содержат примеры, где обращение к базе данных осуществляется небезопасным образом.

Уязвимость «Внедрение внешних сущностей XML», напротив, для языка PHP встречается реже, чем для других: доля сайтов на PHP, содержащая эту уязвимость, — 14%, тогда как для Java и ASP.NET это 30 и 36% соответственно. Подобная ситуация может быть связана с тем, что устранить этот недостаток при использовании PHP относительно просто, а для двух других языков исправление ошибки может потребовать сложных изменений в коде приложения.

В целом, согласно полученным результатам, самым небезопасным для разработки веб-приложений языком программирования является PHP.

ДОЛИ САЙТОВ С РАСПРОСТРАНЕННЫМИ УЯЗВИМОСТЯМИ



4.3. УЯЗВИМОСТИ, ХАРАКТЕРНЫЕ ДЛЯ РАЗЛИЧНЫХ ВЕБ-СЕРВЕРОВ

Как и в 2012 году, наибольшая доля сайтов с критическими уязвимостями (75%) функционировала на базе веб-сервера Apache Tomcat. Значительно возросло число уязвимых ресурсов под управлением веб-сервера Microsoft IIS (71%), Nginx (57%), и только в отношении сайтов под управлением Apache заметна положительная динамика: 60% ресурсов вместо прошлогодних 88% содержат критические уязвимости.

ВЕБ-ПРИЛОЖЕНИЯ С УЯЗВИМОСТЯМИ ВЫСОКОЙ СТЕПЕНИ РИСКА (ПО ТИПУ ВЕБ-СЕРВЕРА)

Некоторые уязвимости веб-приложений, выделенные согласно классификации WASC TC v. 2, являются следствием некорректного администрирования веб-приложения. Далее приведена статистика по уязвимостям для наиболее распространенных веб-серверов среди систем, исследованных в 2013 году, — Apache, Nginx и Microsoft IIS. Веб-приложения, функционирующие на базе Apache Tomcat, не содержали ошибок администрирования: все выявленные недостатки соответствующих систем были связаны с ошибками в коде (Java). Это не означает, впрочем, что ошибки администрирования не характерны для данного веб-сервера, поскольку количество рассмотренных в 2013 году систем на этой платформе невелико (4 шт.).

Наиболее распространенные ошибки, а также доли уязвимых сайтов под управлением веб-серверов Apache, IIS и Nginx приведены в таблице (все представленные уязвимости характеризуются средней степенью риска).

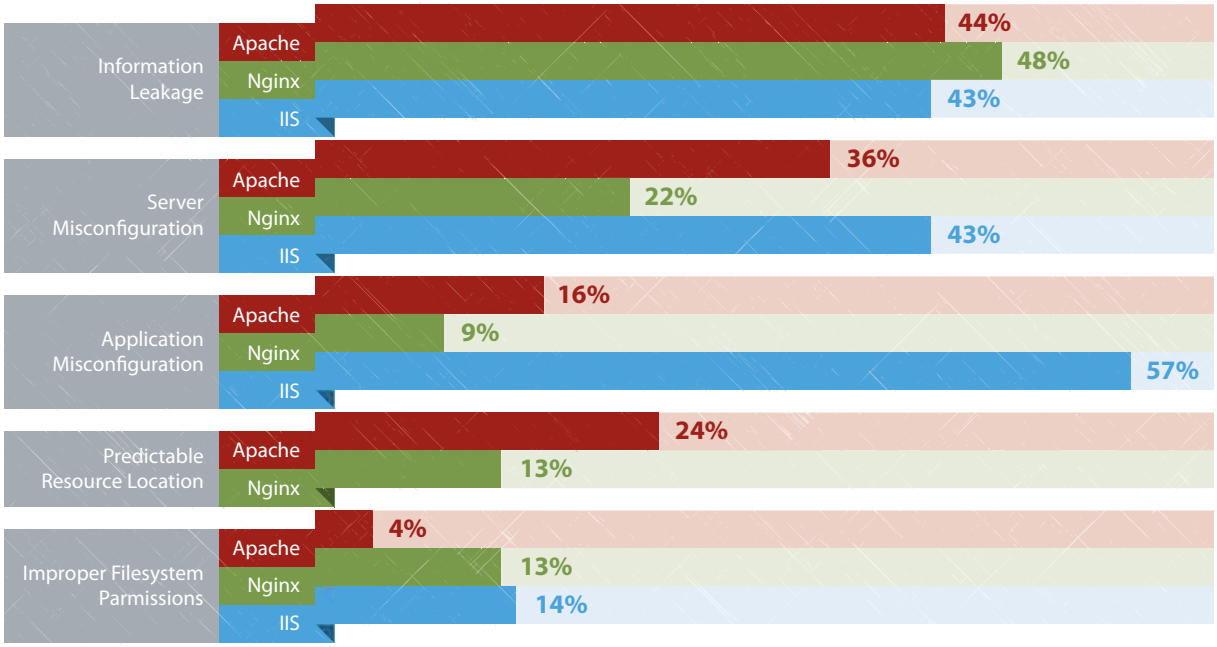
РЕЙТИНГ УЯЗВИМОСТЕЙ, СВЯЗАННЫХ С ОШИБКАМИ АДМИНИСТРИРОВАНИЯ

IIS	Доля сайтов, %	Nginx	Доля сайтов, %	Apache	Доля сайтов, %
Application Misconfiguration	57	Information Leakage	48	Information Leakage	44
Information Leakage	43	Server Misconfiguration	22	Server Misconfiguration	36
Server Misconfiguration	43	Predictable Resource Location	13	Predictable Resource Location	24
Improper Filesystem Permissions	14	Improper Filesystem Permissions	13	Application Misconfiguration	16
Predictable Resource Location	—	Application Misconfiguration	9	Improper Filesystem Permissions	4

Самой распространенной ошибкой администрирования является разглашение важных данных (Information Leakage). Ей подвержены 45% всех исследованных информационных ресурсов. Чаще всего данная уязвимость встречается в веб-ресурсах под управлением веб-сервера Nginx.

Сравнение долей уязвимых ресурсов под управлением различных веб-серверов для каждой уязвимости администрирования приведено на диаграмме ниже.

ДОЛИ УЯЗВИМЫХ САЙТОВ НА РАЗЛИЧНЫХ ВЕБ-СЕРВЕРАХ



4.4. СТАТИСТИКА ДЛЯ РАЗЛИЧНЫЙ ОТРАСЛЕЙ ЭКОНОМИКИ

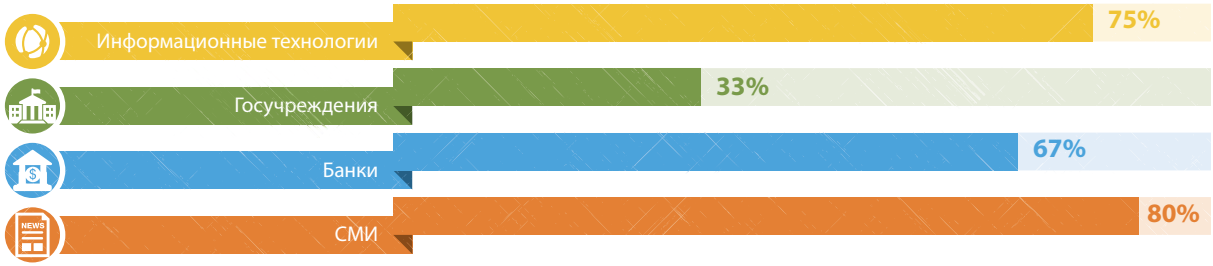
В рамках данного исследования были рассмотрены веб-приложения компаний, представляющих следующие экономические отрасли: информационные технологии, телекоммуникации, промышленность, государственные учреждения, банки, СМИ. В связи с тем, что веб-приложения, относящиеся к промышленной и телекоммуникационной отраслям, в этом году были представлены в небольшом количестве (по два приложения для каждой), далее статистика по соответствующим отраслям не приводится. Отметим лишь, что критические уязвимости были обнаружены в обоих рассмотренных веб-приложениях промышленной отрасли и в одном приложении телекоммуникационной отрасли.

Если проекты по углубленному анализу защищенности веб-приложений в двух означенных отраслях в 2013 году были немногочисленны, то в части тестирования на проникновение промышленная и телекоммуникационная сферы экономики составили более половины от рассмотренных систем (суммарно 57% от общей выборки). В рамках тестирования на проникновение оценивается, среди прочего, защищенность основных корпоративных веб-приложений (методом черного ящика). Как показывают результаты, веб-приложения все еще остаются одним из самых уязвимых компонентов корпоративных сетей. В 55% информационных систем на сетевом периметре выявлены веб-приложения, содержащие уязвимость «Внедрение операторов SQL», для такой же доли систем обнаружена критическая уязвимость «Загрузка произвольных файлов». Более подробная статистика по результатам тестирования на проникновение приведена в отчете «Статистика уязвимостей корпоративных информационных систем (2013 год)».

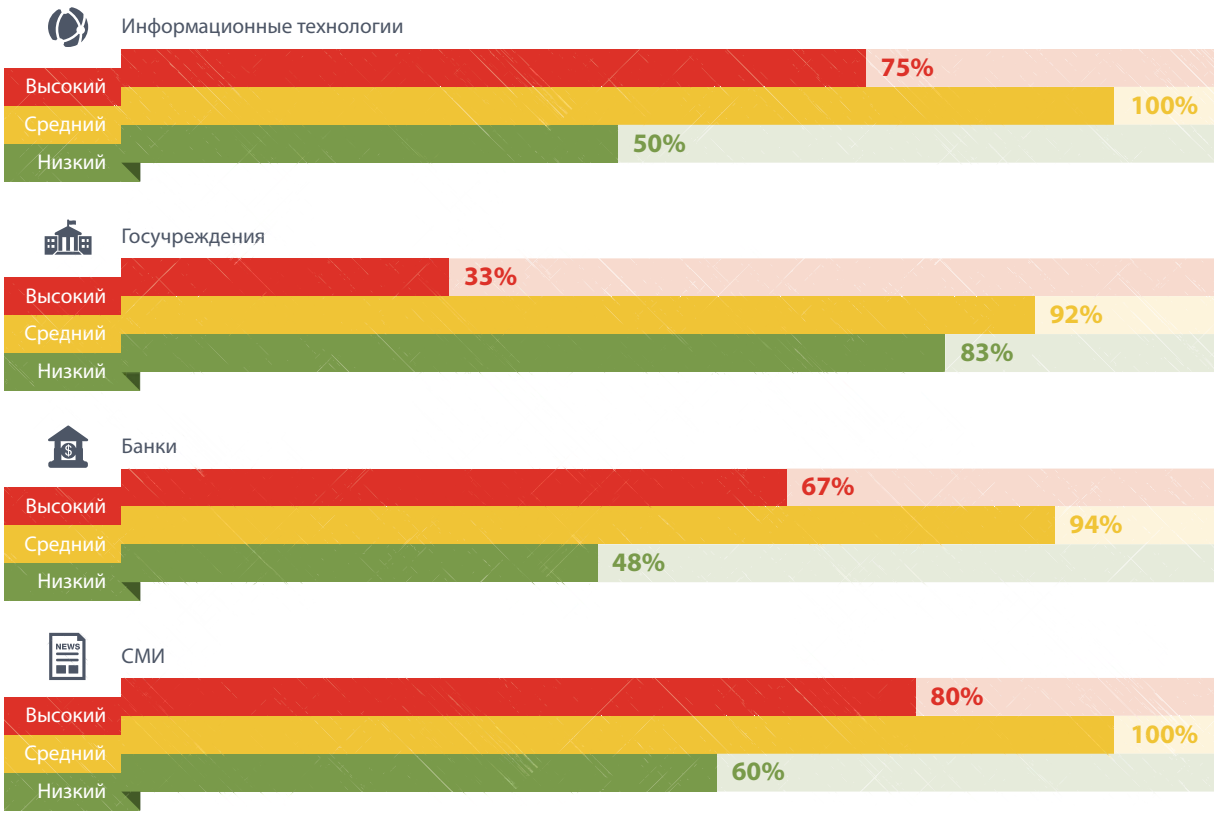
Среди прочих отраслей наиболее уязвимыми являются средства массовой информации, где 80% приложений содержат критические уязвимости. Ненамного отстает отрасль информационных технологий: 75% веб-приложений, относящихся к этой сфере, содержат уязвимости высокой степени риска. Наименьшая доля уязвимых веб-приложений (33%) наблюдается у государственных учреждений. Впрочем, оценку для рассмотренной выборки государственных организаций нельзя считать верной для отрасли в целом. Если в других сферах экономики в область оценки из года в год попадает множество различных предприятий, то среди государственных учреждений анализ защищенности проводится только для единичных крупных проектов, безопасности которых уделяется повышенное внимание. В целом же ситуация с безопасностью государственных веб-ресурсов может быть значительно хуже, поскольку для большинства государственных организаций проведение регулярных работ по анализу защищенности веб-приложений, по всей видимости, не является общепринятой практикой. Дополнительную сложность в организации работ по анализу защищенности и обе-

спечению безопасности веб-приложений государственных учреждений создает высокая бюрократизация данной сферы, в результате чего даже если проводить анализ защищенности веб-приложений, устранение уязвимостей может занимать весьма длительное время. В качестве компенсационной меры в таком случае было бы полезно использовать средства предотвращения вторжений на уровне веб-приложений (Web Application Firewall). Данная мера не отменяет необходимости своевременного обнаружения и устранения уязвимостей, но позволяет значительно снизить риски успешных атак на веб-приложения.

ДОЛИ САЙТОВ С УЯЗВИМОСТЯМИ ВЫСОКОГО УРОВНЯ РИСКА



ДОЛЯ УЯЗВИМЫХ САЙТОВ (С УКАЗАНИЕМ СТЕПЕНИ РИСКА)



В сфере информационных технологий наблюдается тенденция к ухудшению защищенности приложений: в 2012 году на 30% меньше приложений этой отрасли содержали критические уязвимости. Низкий уровень защищенности веб-приложений IT-отрасли прослеживается и при оценке среднего количества уязвимостей различных уровней риска на одну систему: одно приложение в сфере ИТ в среднем содержит 41 критическую уязвимость и 21 уязвимость среднего уровня риска, тогда как для следующих по уровню защищенности СМИ среднее количество критических уязвимостей и уязвимостей среднего уровня риска одинаково и составляет 9. Столь заметная разница в среднем количестве уязвимостей в сфере информационных технологий и в других отраслях экономики связана, среди прочего, с тем, что для IT-компаний чаще проводился анализ защищенности методом белого ящика (в 43% случаев). Эти организации, как правило, сами занимаются разработкой программного обеспечения и имеют возможность предоставить на анализ исходные коды веб-приложений, что позволяет более полно оценить защищенность систем (см. разд. 4.6).

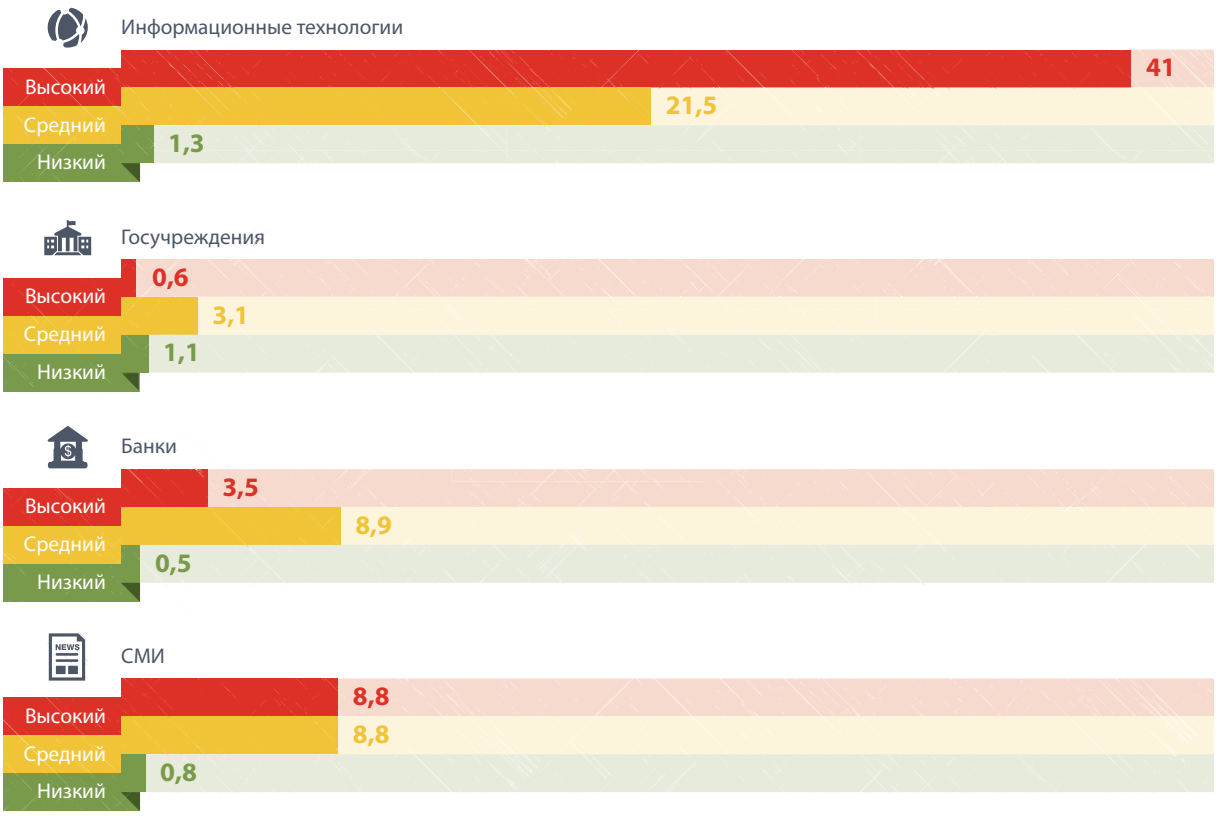
Наиболее распространенными критическими уязвимостями в 2013 году стали «Внедрение операторов SQL», «Внедрение внешних сущностей XML» и «Выполнение команд ОС». Все они

в большей степени характерны для организаций из области ИТ. Уязвимость «Внедрение операторов SQL» была обнаружена в веб-приложениях всех отраслей экономики.

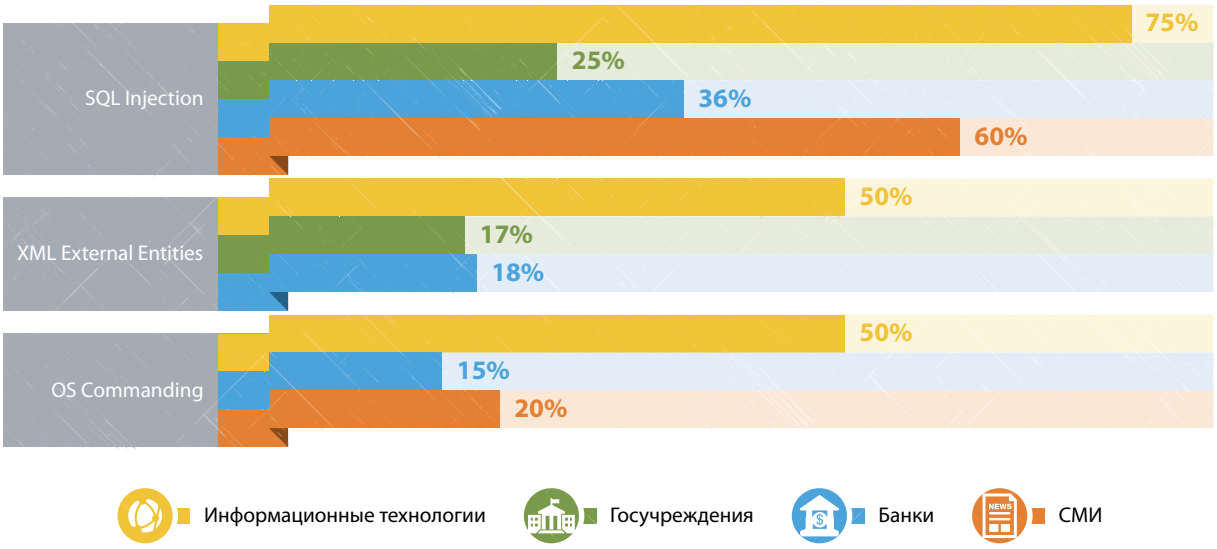
Результаты проведенного исследования показывают, что почти во всех отраслях значительная доля систем подвержена уязвимостям высокого уровня риска. Среди веб-приложений государственных и банковских организаций выявлены системы, имеющие лишь уязвимости низкой степени риска.

Таким образом, среди исследованных веб-приложений наиболее защищенными оказались ресурсы государственных учреждений. Однако, как упоминалось выше, данный показатель отчасти отражает тот факт, что все рассмотренные системы входили в рамки крупных проектов, для которых анализ защищенности осуществляется на регулярной основе.

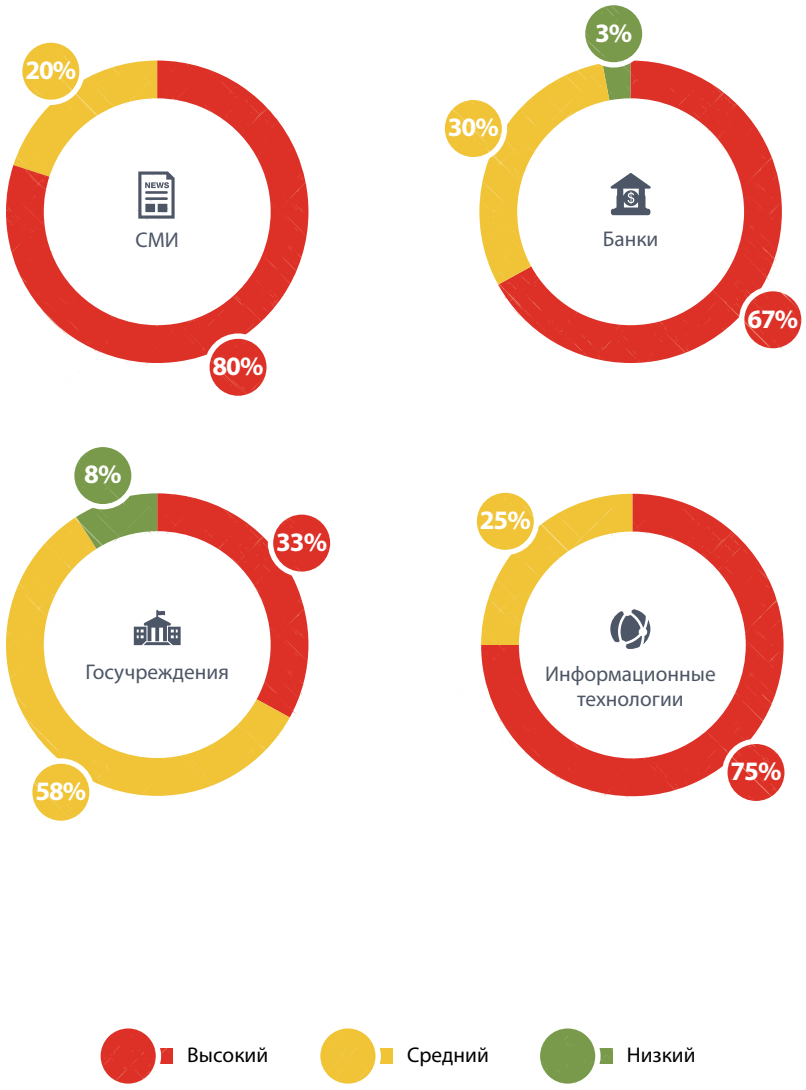
СРЕДНЕЕ ЧИСЛО УЯЗВИМОСТЕЙ В СИСТЕМЕ



ДОЛИ УЯЗВИМЫХ САЙТОВ (ПО ОТРАСЛЯМ ЭКОНОМИКИ)



ДОЛЯ УЯЗВИМЫХ САЙТОВ (С УКАЗАНИЕМ СТЕПЕНИ РИСКА)



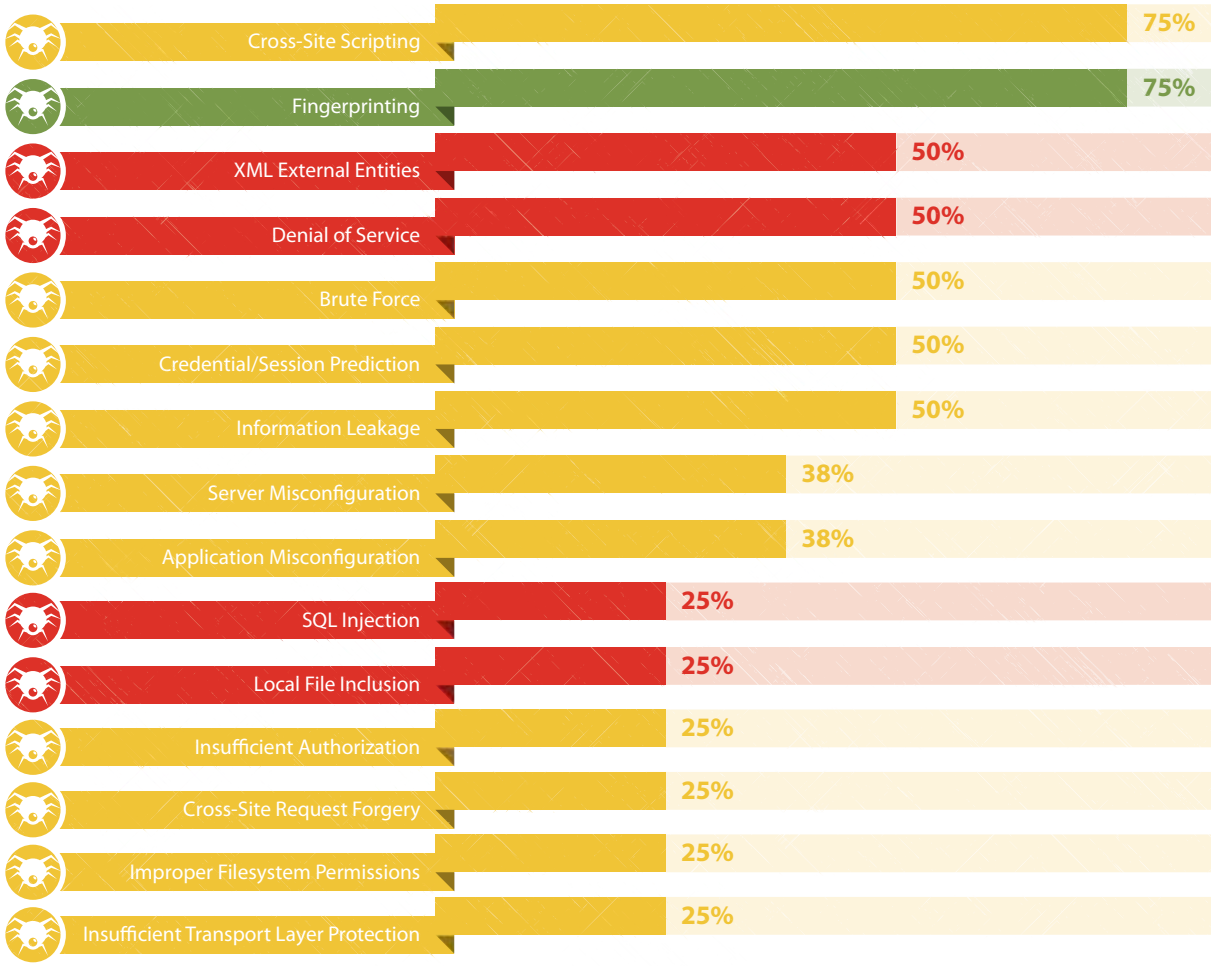
4.5. УЯЗВИМОСТИ, ХАРАКТЕРНЫЕ ДЛЯ СИСТЕМ ДБО

Среди веб-приложений, рассмотренных в 2013 году и относящихся к банковской сфере, 8 систем представляли собой системы дистанционного банковского обслуживания (ДБО). Детальный анализ уровня защищенности таких систем с рассмотрением типовых ошибок защиты транзакций будет приведен в отдельном аналитическом отчете по итогам 2013–2014 гг. В данном же разделе рассматриваются наиболее распространенные уязвимости систем ДБО в 2013 году в соответствии с классификацией угроз WASC, а также оценка соответствия систем ДБО требованиям 6.5 стандарта Payment Card Industry Data Security Standard v. 3 (PCI DSS). Отметим, что стандарт PCI DSS был выбран для проведения оценки, поскольку данный документ аккумулирует лучшие практики по защите информации, содержит развернутые технические требования к безопасности веб-приложений и широко применяется в банковской сфере. При этом рассматриваемые системы ДБО могут не обрабатывать карточные данные и не входить в область действия стандарта, но факты несоответствия систем ДБО этому стандарту позволяют судить об общем уровне их защищенности.

Наиболее распространенными недостатками систем ДБО в 2013 году оказались уязвимости «Межсайтовое выполнение сценариев» и «Идентификация приложений», каждая из которых встречается в 75% рассмотренных систем. В целом ситуация близка к картине 2011–2012 годов, при этом чаще стала встречаться уязвимость «Внедрение внешних сущностей XML» (50% систем против 27% в предыдущие два года), а лидировавшая ранее недостаточная защита от подбора учетных данных спустилась на 3-ю позицию (50% систем по сравнению с 82% в прошлом году).

В целом критические уязвимости были обнаружены в половине рассмотренных систем ДБО (показатель ниже, чем в большинстве других отраслей). Однако, как показывает практика, отсутствие уязвимостей высокой степени риска не равнозначно высокому уровню общей защищенности системы, так как комбинация нескольких уязвимостей среднего уровня риска может приводить к реализации серьезных угроз информационной безопасности, например к несанкционированному проведению транзакций.

ДОЛЯ УЯЗВИМЫХ САЙТОВ (С УКАЗАНИЕМ СТЕПЕНИ РИСКА)



Для систем ДБО была проведена оценка соответствия требованиям разд. 6.5 стандарта PCI DSS v.3. В следующей таблице перечислены требования стандарта, относящиеся к уязвимостям в веб-приложениях.

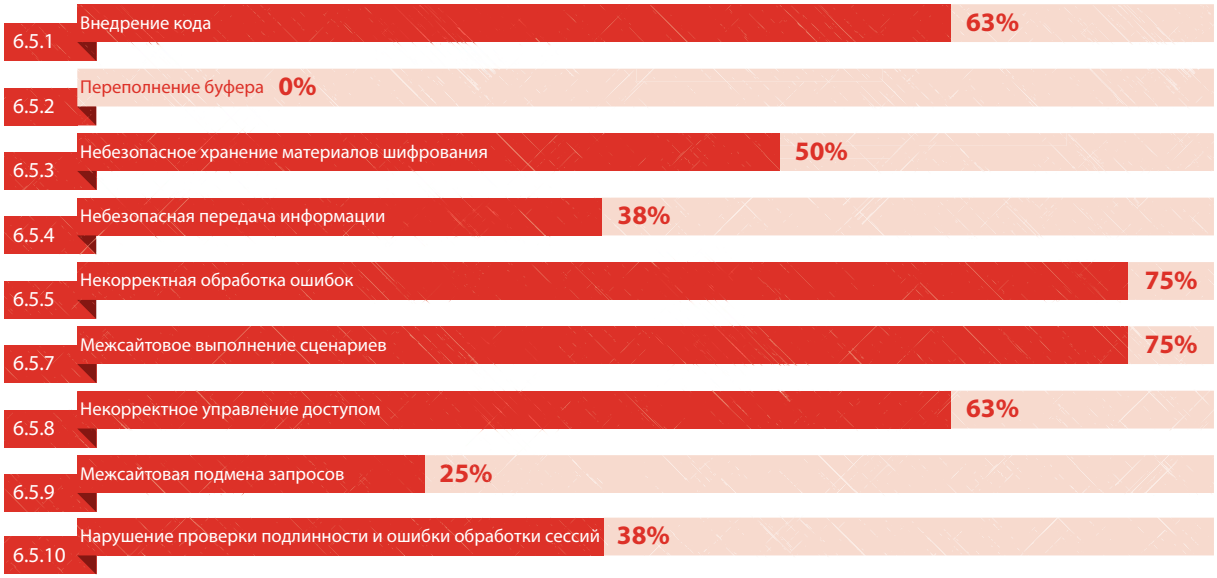
ВЫДЕРЖКА ИЗ СТАНДАРТА PCI DSS

Требование	Процедура
6.5.1. Внедрение кода, в частности SQL-инъекции. Также внедрение команд ОС, операторов LDAP и XPath	Необходимо проверять входную информацию и следить за тем, чтобы данные, вводимые пользователем, не могли влиять на значения команд, использоваться в параметризованных запросах и др.
6.5.2. Переполнение буфера	Необходимо проверять границы буфера и усекать вводимые строки
6.5.3. Небезопасное хранение материалов шифрования	Необходимо обеспечить отсутствие уязвимостей шифрования
6.5.4. Небезопасная передача информации	Необходимо реализовать надежное шифрование данных аутентификации и других важных данных при их передаче
6.5.5. Некорректная обработка ошибок	Необходимо не допускать утечки данных в сообщениях об ошибках
6.5.7. Межсайтовое выполнение сценариев	Необходимо проверять все параметры перед их включением в код, использовать контекстно-зависимое экранирование символов
6.5.8. Некорректное управление доступом, например, небезопасные прямые объектные ссылки, отсутствие ограничения доступа по URL-адресу и обход каталога	Необходимо реализовать корректную аутентификацию пользователей и очищение вводимой информации; пользователи не должны иметь доступ к ссылкам на внутренние объекты
6.5.9. Межсайтовая подмена запросов	Необходимо не допускать автоматической отправки браузером данных аутентификации и идентификаторов сессии
6.5.10. Нарушение проверки подлинности и ошибки обработки сессий	Необходимо устанавливать безопасные атрибуты идентификаторов сессий, например, свойство «secure» для cookie-файлов, скрывать идентификатор сессии в адресе, использовать ограниченное время жизни существующих сессий

63% систем оказались подвержены атакам внедрения различных элементов, среди которых наиболее распространено внедрение внешних сущностей XML. Лидером по количеству систем, не соответствующих требованиям, стали требования 6.5.5 и 6.5.7: 75% систем ДБО уязвимы к межсайтовому выполнению сценариев, в такой же доле систем происходит утечка информации в результате некорректной обработки ошибок.

Полностью требованиям PCI DSS не соответствовала ни одна из исследованных систем ДБО.

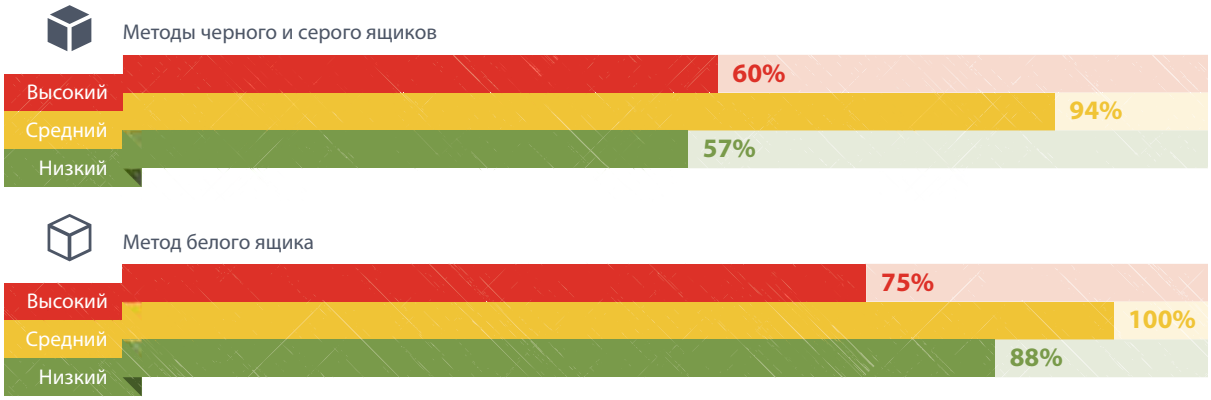
СООТВЕТСТВИЕ СИСТЕМ ДБО ТРЕБОВАНИЯМ РАЗД. 6.5 СТАНДАРТА PCI DSS (ДОЛЯ СИСТЕМ, НЕ СООТВЕТСТВУЮЩИХ ТРЕБОВАНИЯМ)



4.6. СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ТЕСТИРОВАНИЯ

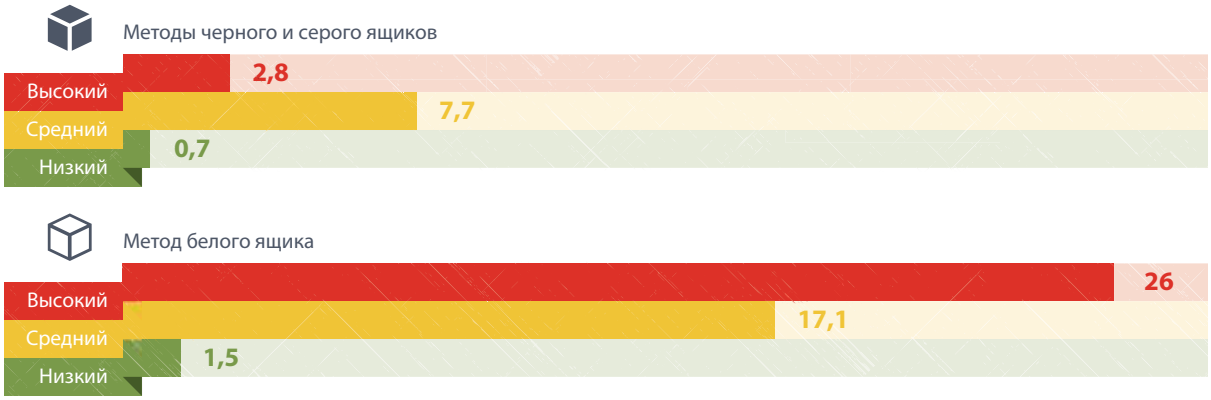
В 2013 году специалисты Positive Technologies провели сравнительный анализ методов черного, серого и белого ящиков. Среди веб-ресурсов, протестированных методами черного и серого ящиков, было выявлено 60% сайтов, содержащих критические уязвимости. Для метода белого ящика данный показатель выше — 75%. Этот метод обладает также более высокими показателями по уязвимостям среднего и низкого уровня риска.

ДОЛИ СИСТЕМ С УЯЗВИМОСТЯМИ РАЗНОЙ СТЕПЕНИ РИСКА (ПО МЕТОДУ ТЕСТИРОВАНИЯ)



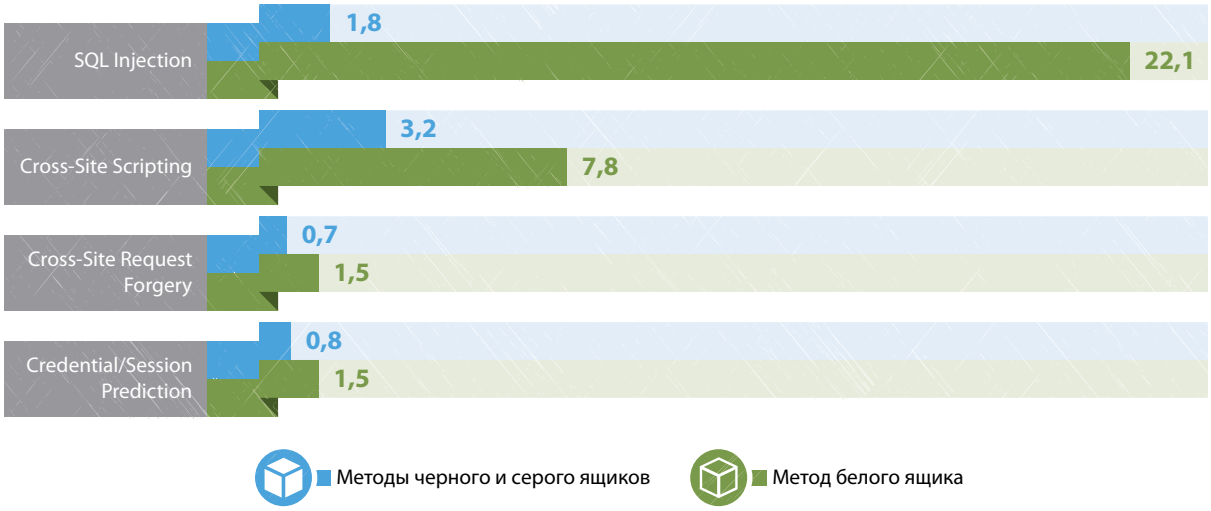
Из сравнения среднего количества уязвимостей, приходящегося на одну систему, следует, что тестирование методом белого ящика в среднем позволяет обнаружить почти в 10 раз больше критических уязвимостей, а также примерно в два раза больше уязвимостей средней и низкой степени риска, чем тестирование только методами черного и серого ящиков.

СООТНОШЕНИЕ ОБНАРУЖЕННЫХ УЯЗВИМОСТЕЙ ПО УРОВНЮ РИСКА ДЛЯ РАЗЛИЧНЫХ МЕТОДОВ ТЕСТИРОВАНИЯ



Из сравнения среднего количества уязвимостей различного типа, приходящегося на одну систему, следует, что в случае недостатков «Внедрение операторов SQL» и «Межсайтовое выполнение сценариев» дополнительный анализ исходных кодов позволяет существенно увеличить количество обнаруживаемых уязвимостей.

СРЕДНЕЕ КОЛИЧЕСТВО УЯЗВИМОСТЕЙ ОПРЕДЕЛЕННОГО ТИПА (ПО МЕТОДУ ТЕСТИРОВАНИЯ)



Таким образом, при наличии возможности предоставить для анализа исходные коды веб-приложений метод белого ящика является предпочтительным. Если при анализе методами черного и серого ящиков аудиторам не удалось обнаружить те или иные уязвимости, это не означает, что атаки со стороны злоумышленника не увенчаются успехом. В отличие от аудиторов злоумышленник может осуществлять различные атаки, связанные с высоким риском отказа в обслуживании, или может обладать исходными кодами приложения и использовать их для выявления уязвимостей (например, если злоумышленник это уволенный сотрудник компании-разработчика).

ЗАКЛЮЧЕНИЕ

Проведенное исследование показало, что на сегодняшний день уровень защищенности веб-приложений по-прежнему остается крайне низким, при этом наблюдается ухудшение среднего уровня защищенности веб-приложений по сравнению с предыдущим годом. Доля сайтов, содержащих критические уязвимости, увеличилась на 14% и составила 59%. Доля сайтов, содержащих уязвимости средней степени риска, возросла до 97%. Эти значения близки к показателям 2011 года. Уровень защищенности веб-приложений понизился практически во всех отраслях экономики.

Тестирование методом белого ящика позволяет выявить значительно больше уязвимостей, чем тестирование только методами черного и серого ящиков, однако владельцы систем прибегают к нему значительно реже: лишь 13% рассматриваемых веб-ресурсов исследовались методом белого ящика.

По-прежнему крайне редко используются средства обнаружения и предотвращения вторжений уровня приложений (Web Application Firewall): в 2013 году подобные средства защиты применялись лишь для одной исследованной системы (в прошлом году доля таких систем составляла 30%).

Положительная динамика наблюдается в отношении доли систем, в которых на момент исследования присутствовал вредоносный код: в 2013 году не было выявлено ни одной скомпрометированной системы, тогда как в 2012 году была обнаружена одна система, а в 2010–2011 годах доля подобных систем составила 10%. Необходимо отметить, что если вовремя не устранять обнаруженные уязвимости, то для многих рассмотренных веб-приложений успешное проведение атак со стороны злоумышленников является вопросом времени и будет зависеть лишь от интереса атакующего к конкретной организации.

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.

ЗАО / ПОЗИТИВ ТЕКНОЛОДЖИЗ
107061 / МОСКВА / ПРЕОБРАЖЕНСКАЯ ПЛ., Д. 8
ТЕЛ.: +7 (495) 744 01 44 / ФАКС: +7 (495) 744 01 87 / PT@PTSECURITY.COM
WWW.PTSECURITY.RU / WWW.MAXPATROL.RU / WWW.SECURITYLAB.RU