



POSITIVE TECHNOLOGIES

Уязвимости веб-приложений

2019

Содержание

Введение.....	2
Резюме.....	2
Тенденции.....	3
Анализ защищенности веб-приложений	4
Наиболее распространенные уязвимости	4
Анализ угроз и уровень защищенности	6
Сравнение тестовых и продуктивных систем	8
Сравнение методов тестирования.....	8
Выводы	10
Портрет участников.....	11
Методика	12

Введение

Современную компанию из сегмента малого бизнеса, не говоря уже о крупных финансовых или промышленных предприятиях, сложно представить без веб-приложения. Желая получить услугу или приобрести продукт, мы все чаще предпочитаем сделать это онлайн, ознакомившись с ассортиментом компании на ее сайте. Благодаря развитию веб-технологий в последние годы существенно повысились доступность и качество государственных услуг. Сайт стал визитной карточкой не только для бизнеса, но и для государственных структур, оказывая существенное влияние на репутацию. Это обстоятельство мотивирует владельцев веб-приложений поддерживать их на высоком технологическом уровне, который невозможен без должного внимания к защите от кибератак.

Для обеспечения высокой степени защищенности веб-приложения необходим его регулярный анализ на наличие уязвимостей. В данном отчете представлена статистика, полученная экспертами Positive Technologies в ходе работ по анализу защищенности веб-приложений в 2018 году, а также ее сравнение с результатами предыдущих лет.

Резюме

В 19% веб-приложений есть уязвимости, позволяющие злоумышленнику получить контроль как над самим приложением, так и над ОС сервера. Если сервер находится на периметре сети организации, злоумышленник может проникнуть во внутреннюю сеть компании. Как показывают результаты нашего исследования уязвимостей корпоративных информационных систем, 75% векторов проникновения в ЛВС связаны с недостатками защиты веб-приложений.

В большинстве случаев веб-приложения уязвимы из-за ошибок в коде. Изменениями в конфигурации могут быть устранены только 17% уязвимостей, причем большинство из них имеют низкий уровень риска. Для устранения критически опасных уязвимостей, как правило, потребуется внести исправления в код.

Каждая вторая утечка может привести к разглашению учетных данных, в том числе для доступа к сторонним ресурсам. В качестве примера можно привести доступные всем пользователям конфигурационные файлы с хранящимися в них паролями.

Злоумышленник может похитить персональные данные пользователей в 18% веб-приложений, где осуществляется их обработка. При этом важно отметить, что персональные данные хранятся и обрабатываются почти в каждом исследованном нами веб-приложении (91%).

В среднем на одно веб-приложение приходится 33 уязвимости, шесть из которых имеют высокий уровень риска. Число критически опасных уязвимостей, которое приходится на одно веб-приложение, по сравнению с 2017 годом выросло в 3 раза.

Продуктивные системы содержат меньше уязвимостей, чем тестовые, но это не делает их более защищенными. Доля продуктивных систем, содержащих хотя бы одну уязвимость высокого уровня риска, больше, чем тестовых. Как показывает практика, для успешного взлома веб-приложения часто достаточно одной критически опасной уязвимости.

Анализ исходного кода повышает эффективность проверки. При наличии у экспертов доступа к исходному коду среднее число выявленных уязвимостей высокого уровня риска, по нашей статистике, возрастает более чем в два раза.

Тенденции

Количество веб-приложений с критически опасными уязвимостями растет.

После двухгодичного курса на снижение доли веб-приложений, содержащих уязвимости высокого уровня риска, она вновь выросла и достигла 67%. Наиболее распространены уязвимости, связанные с недостаточной авторизацией, возможностью загрузки или чтения произвольных файлов, а также с возможностью внедрения SQL-кода.

Несанкционированный доступ — угроза, которая не отступает.

После снижения в 2017 году доли веб-приложений с уязвимостями, создающими угрозу несанкционированного доступа, их доля выросла до 72% и практически достигла уровня 2016 года (75%).

Версии используемого ПО стали раскрываться реже.

В 2018 году доля веб-приложений, в которых раскрываются версии используемого ПО, составила лишь 42%, что существенно меньше, чем в 2017 году (61%). Вероятно, такая тенденция объясняется широким освещением данной уязвимости и сравнительной простотой ее устранения.

Доля систем, в которых возможна утечка данных, продолжает расти.

Утечка конфигурационной и отладочной информации, исходных кодов, идентификаторов сессий, а также другой чувствительной информации, возможна в 79% веб-приложений. Для сравнения: аналогичный показатель в 2016 году составил 60%, в 2017 году — 70%.

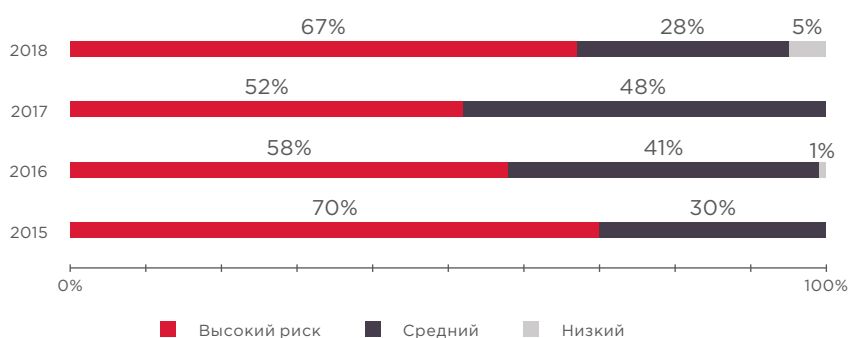


Рисунок 1. Доля уязвимых сайтов в зависимости от максимальной степени риска уязвимостей

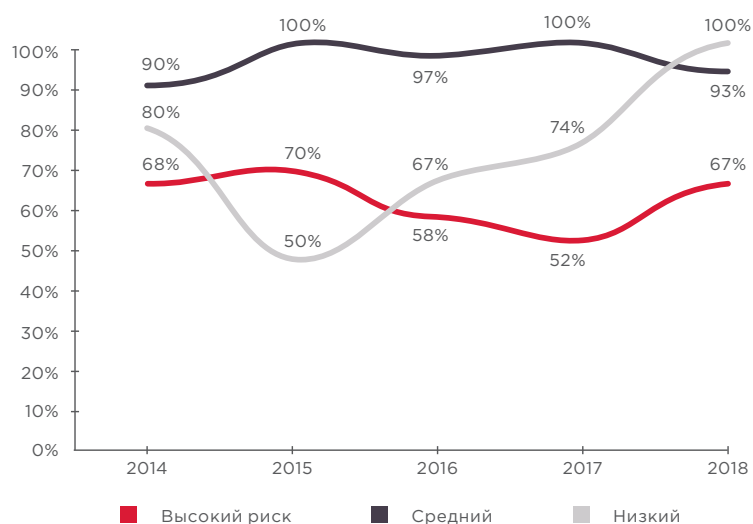
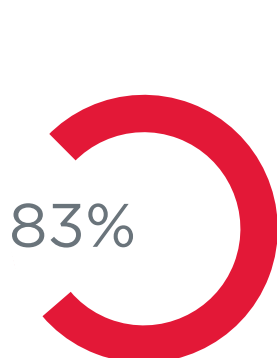


Рисунок 2. Доля сайтов с уязвимостями различной степени риска

Анализ защищенности веб-приложений



Доля уязвимостей
кода в исследованных
веб-приложениях

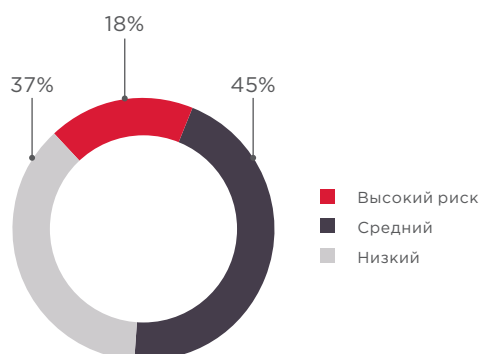


Рисунок 3. Доля уязвимостей
различной степени риска

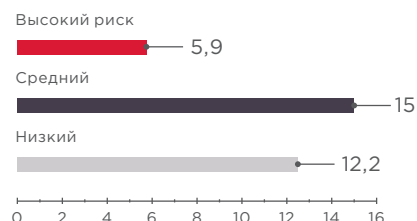


Рисунок 4. Среднее число уязвимостей
на одну систему



Грамотно конфигурируйте
компоненты веб-
приложения, веб-сервер
и сервер базы данных.
Не оставляйте параметры
по умолчанию и пароли,
предусмотренные
производителем



Отключите поддержку
внешних сущностей и DTD
в XML-парсерах, если они
не предусмотрены логикой
веб-приложения

Наиболее распространенные уязвимости

В этом году наши специалисты находили около 70 различных видов недостатков в веб-приложениях. Как всегда, высока доля веб-приложений с уязвимостями «Межсайтовое выполнение сценариев» (Cross-Site Scripting, XSS). В четырех из каждых пяти веб-приложений отмечены ошибки конфигурации: параметры по умолчанию, стандартные пароли, сообщения об ошибках, в которых раскрываются версии используемого ПО, установочные пути и другие данные, представляющие ценность для злоумышленника на этапе сбора информации о системе и при планировании атаки.

В 2018 году мы отмечаем снижение доли веб-приложений, подверженных уязвимости «Внедрение внешних сущностей XML» (XML External Entities, XXE). В то же время мы не спешим утверждать, что это тренд, скорее это особенность выборки веб-приложений. Напротив, если говорить о веб-уязвимостях в целом, то XXE по-прежнему актуальна. В 2017 году она впервые вошла в рейтинг OWASP Top 10 и сразу заняла четвертую позицию.

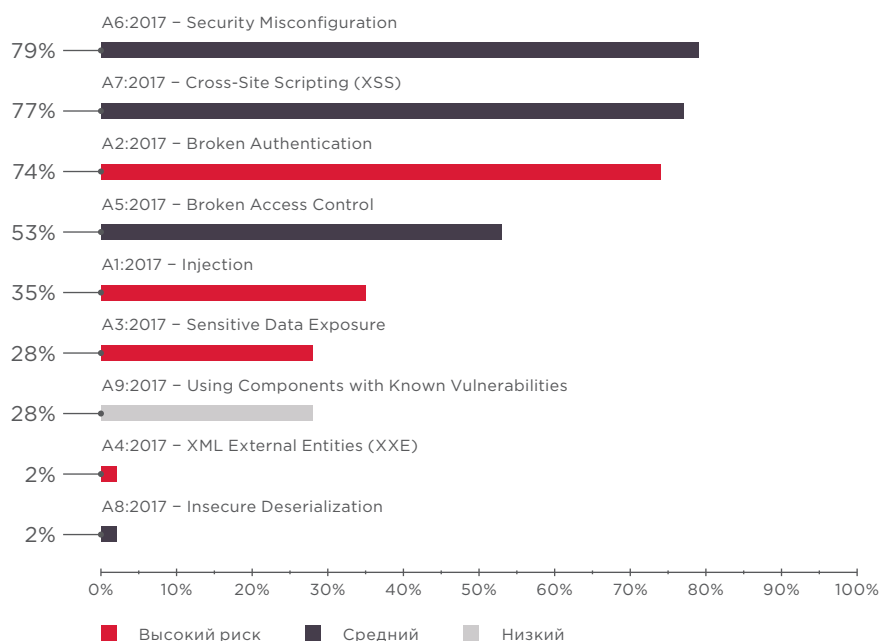


Рисунок 5. Уязвимости из списка OWASP Top 10–2017 (доля приложений)*

*Уровень риска указан в соответствии с методикой [OWASP Top 10](#)

В апреле 2018 года стало известно, что на сайте американской сети кафе Panera Bread в открытом доступе хранились персональные данные 37 млн клиентов и данные их платежных карт

Чувствительные данные не должны храниться в открытом виде.

Используйте надежные криптографические алгоритмы для их защиты. Настройте эффективную политику разграничения доступа к чувствительным данным

Тренд утечки важной информации наблюдается в 2018 году во всем мире. Причиной многих громких инцидентов становятся недостатки администрирования и разграничения доступа к различным ресурсам, при этом наше исследование демонстрирует проблемы безопасного хранения важных данных в веб-приложениях. Так, в 46% утечек под угрозу попадают учетные данные. Персональные данные обрабатываются в 91% исследованных нами веб-приложений, при этом в 18% этих систем возможна их утечка (19% всех утечек).

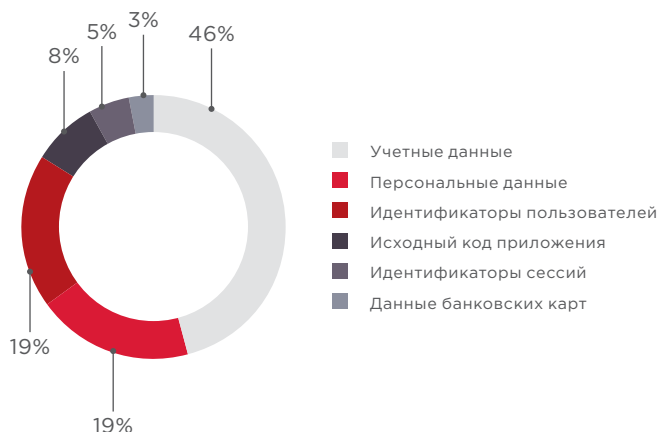


Рисунок 6. Разглашенные чувствительные данные

Утечка данных 21 млн пользователей сервиса Timehop произошла по вине злоумышленника, который завладел учетными данными администратора. Дальнейшие действия злоумышленника оказались успешны из-за отсутствия двухфакторной аутентификации

Уязвимости, связанные с недостатками механизмов аутентификации и управления сессиями, могут стать причиной несанкционированного доступа к функциональным возможностям веб-приложения или его контенту.

Используйте многофакторную аутентификацию для противодействия атакам с украденными учетными данными (credential stuffing)

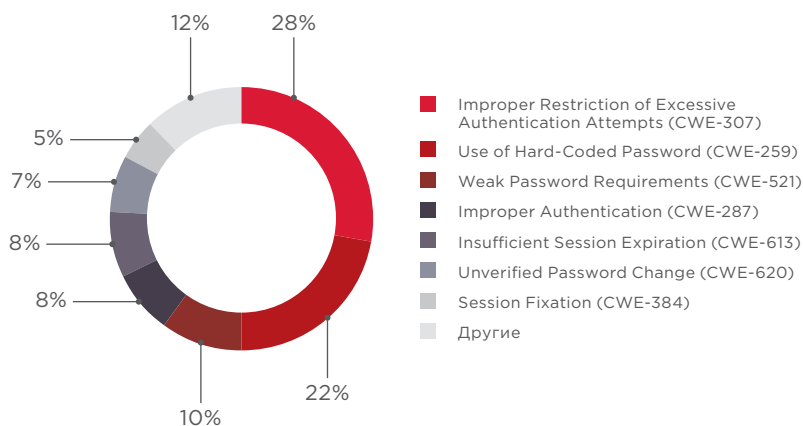


Рисунок 7. Уязвимости механизмов аутентификации и управления сессиями (Broken Authentication)

В 2018 году в СМИ появлялись сообщения о штрафах (на общую сумму более 149 млн долл. США) компании Uber, допустившей утечку персональных данных 50 млн пассажиров и 7 млн водителей. Как следует из официального заявления, злоумышленник обнаружил учетные данные для доступа к базе в исходном коде, хранившемся в корпоративном репозитории на GitHub

При автоматизированном анализе веб-приложений наши специалисты часто сталкиваются с жестко заданными в коде паролями, например для доступа к СУБД или к API сторонних систем. Злоумышленник, получивший доступ к исходному коду, может воспользоваться этими учетными данными для несанкционированного доступа к соответствующим системам и кражи информации. Кроме того, в ряде случаев обнаруженные нами жестко заданные пароли не отвечают минимальным требованиям к стойкости, а значит — могут быть успешно подобраны в результате брутфорс-атак. В свою очередь, смена скомпрометированного пароля потребует внесения изменений в код.



Откажитесь от жестко заданных паролей в коде. В качестве паролей выбирайте стойкие к подбору комбинации символов

```
4 "PASSWORD"=>'123456'
.../application/.../reset.php
CWE-259
```

Рисунок 8. Пример жестко заданного пароля, обнаруженного в ходе автоматизированного тестирования веб-приложения

Сообщество OWASP выделяет ряд уязвимостей, не вошедших ни в одну из категорий Top 10—2017, наличие которых рекомендуется проверять. В этом списке есть возможность загрузки произвольных файлов — критически опасная уязвимость, которая позволяет злоумышленнику загружать на сервер исполняемые файлы и выполнять код, что может привести к получению им полного контроля над веб-приложением и сервером.

Каждое четвертое

исследованное веб-приложение допускает загрузку произвольных файлов



Фильтруйте расширения загружаемых файлов по белому списку. Настройте политику разграничения доступа к каталогам, где хранятся исполняемые файлы

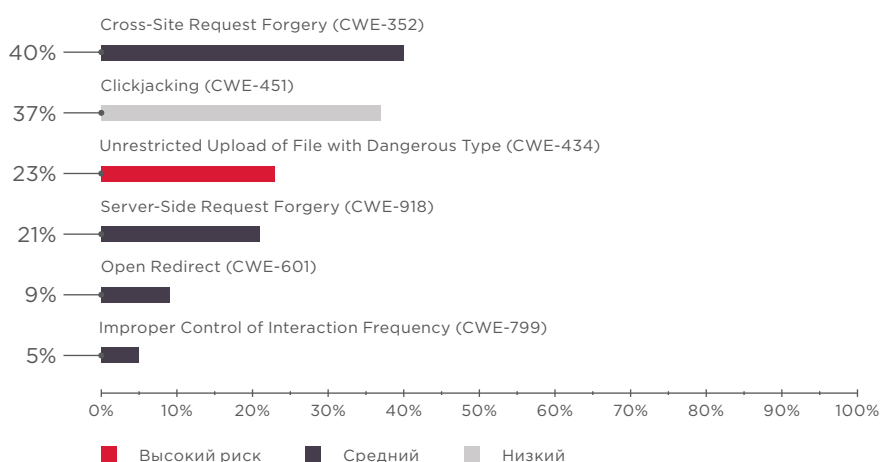


Рисунок 9. Распространенные уязвимости, не вошедшие в OWASP Top 10—2017 (доля приложений)

Анализ угроз и уровень защищенности

Каждое третье веб-приложение

имеет крайне низкий уровень защиты. Это на 15% больше, чем в 2017 году

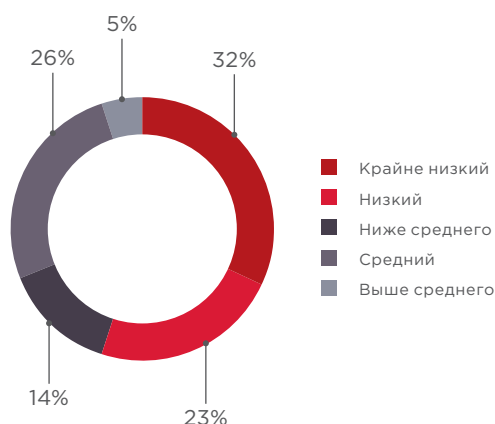


Рисунок 10. Уровень защищенности (доля веб-приложений)

Помимо хищения информации,

несанкционированный доступ к веб-приложению может отрицательно сказаться на репутации его владельца

Г Хакер, взломавший сервис Ticketfly, похитил базу данных клиентов, включающую 27 млн записей, но кроме этого, он оставил на главной странице послание, так что любой посетитель сайта незамедлительно узнавал о проблеме в безопасности сервиса

Г Данные платежных карт 380 тысяч пользователей приложения авиакомпании British Airways были похищены в результате внедрения вредоносного сценария на языке JavaScript. В результате инцидента акции авиаперевозчика упали на 3,8%, а самой компании грозит штраф в размере до 500 млн фунтов стерлингов

Экранируйте входные данные, для этого предпочтительно использовать встроенные функции языка программирования.

Рекомендуется придерживаться принципов стандарта Content Security Policy и использовать механизм Subresource Integrity (SRI) для защиты от вредоносного JavaScript-кода

В 2017 году каждое второе веб-приложение (48%) было под угрозой несанкционированного доступа, однако в 2018 году доля таких приложений выросла до 72%. В 19% веб-приложений были найдены критически опасные уязвимости, позволяющие получить контроль не только над приложением, но и над ОС сервера. Если при этом сервер находится на сетевом периметре организации, то его компрометация позволяет проводить атаки на корпоративные ресурсы. Однако атаки на ЛВС возможны и без полного контроля над сервером веб-приложения. Например, уязвимость «Подделка запроса со стороны сервера» (Server-Side Request Forgery, SSRF) позволяет сканировать ЛВС и обращаться к внутренним ресурсам.

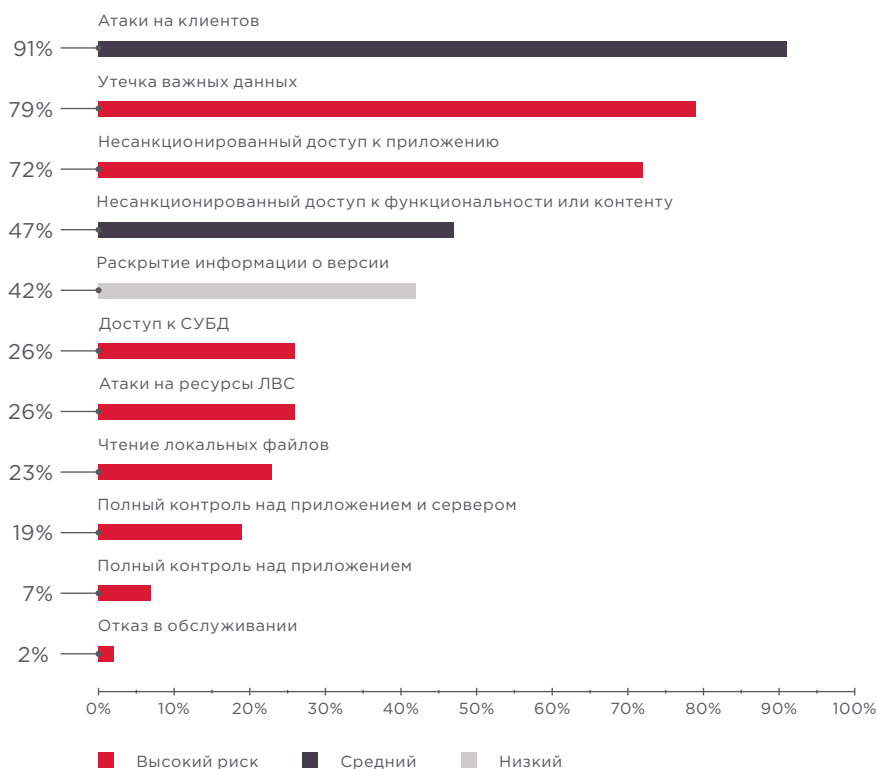


Рисунок 11. Наиболее распространенные угрозы (доля систем)

По-прежнему почти каждое веб-приложение содержит уязвимости, которые позволяют совершать атаки на пользователей. В большинстве случаев, как и прежде, это «Межсайтовое выполнение сценариев» (Cross-Site Scripting, XSS). Однако в этом году доля этой уязвимости стала еще внушительней (88,5% против 77,9% в прошлом году). Одна такая уязвимость может привести к серьезным последствиям, что подтверждается прогремевшими на весь мир утечками.

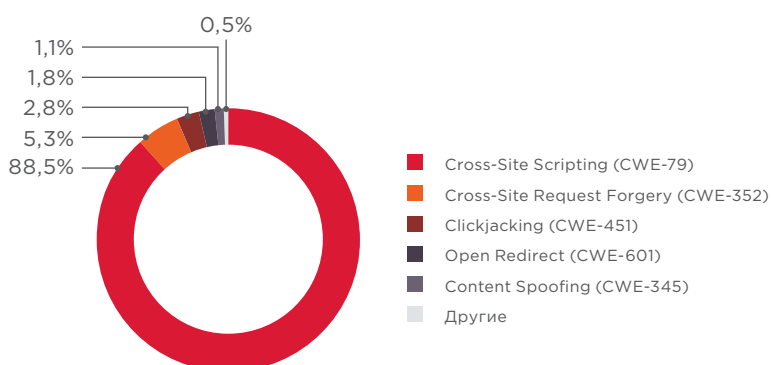


Рисунок 12. Уязвимости, позволяющие проводить атаки на пользователей

Сравнение тестовых и продуктивных систем

Мы наблюдаем увеличение доли продуктивных систем, содержащих уязвимости высокого уровня риска, почти в три раза (с 25% в 2017 году до 71% в 2018-м). Кроме того, в несколько раз выросло и среднее число уязвимостей в одном веб-приложении; это относится как к тестовым, так и к продуктивным системам.

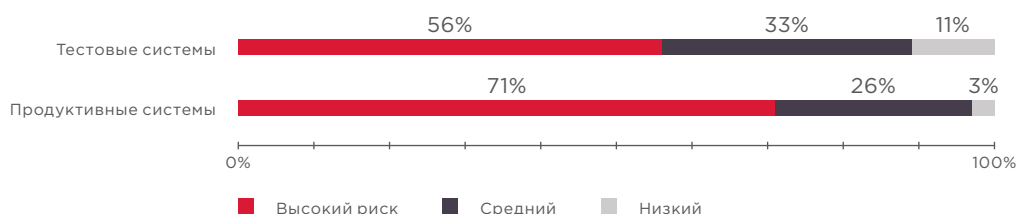


Рисунок 13. Доля систем по максимальному уровню риска

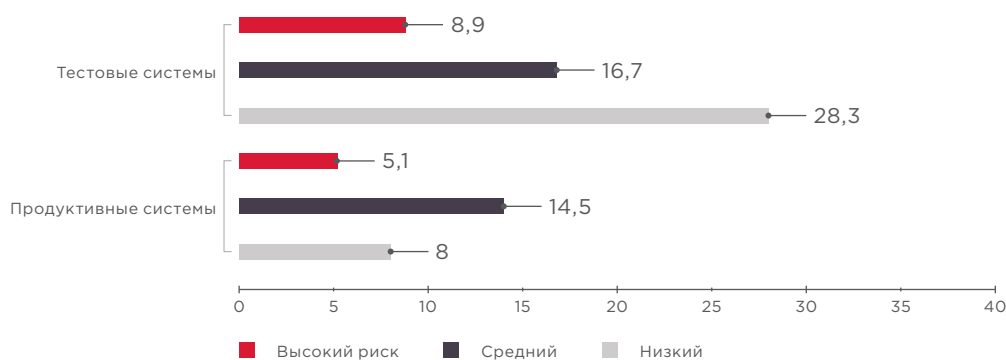


Рисунок 14. Среднее число уязвимостей на одну систему

Сравнение методов тестирования

Сравнение методов тестирования ежегодно подтверждает более высокую эффективность анализа веб-приложений методом белого ящика. Например, при наличии доступа исследователей к исходному коду число критически опасных уязвимостей, выявленных в одной системе, существенно больше, чем при тестировании методами серого и черного ящика. В частности, число выявленных уязвимостей внедрения кода (A1 – Injection) при тестировании методом белого ящика возрастает в 3 раза.

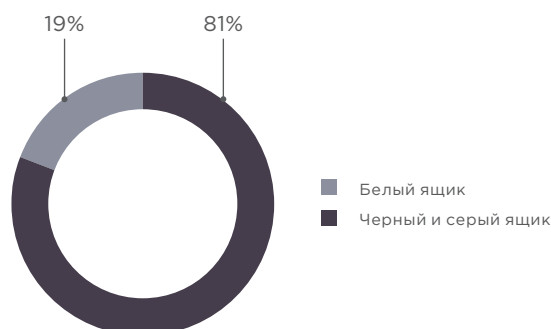


Рисунок 15. Методы тестирования (доля приложений)

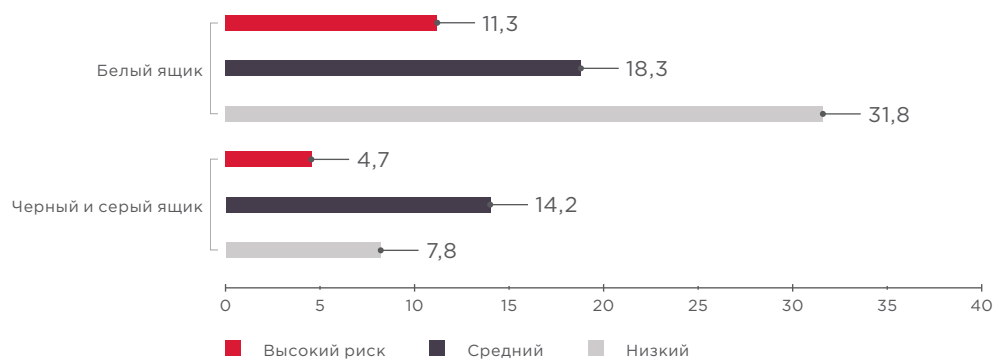


Рисунок 16. Число обнаруженных уязвимостей на одну систему

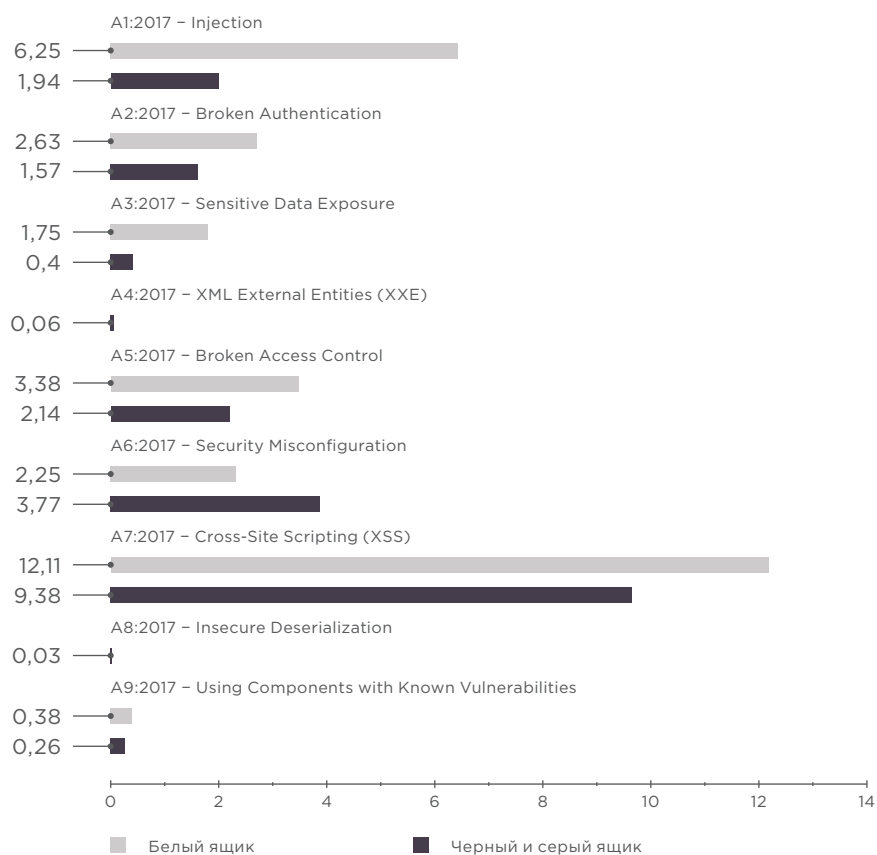


Рисунок 17. Число выявленных уязвимостей из списка OWASP Top 10-2017 на одну систему

Выводы

По результатам исследования мы приходим к выводу, что большинство веб-приложений имеют низкий уровень защищенности. При этом доля веб-приложений с крайне низким уровнем защищенности выросла по сравнению с прошлым годом почти в два раза, а среднее число уязвимостей в одной системе для отдельных категорий уязвимостей увеличилось многократно.

Регистрируясь на сайте, пользователь вынужден доверять владельцам ресурса свои данные, в то время как в 18% веб-приложений, где обрабатываются персональные данные, существует риск их утечки.

Для эффективного обеспечения безопасности веб-приложений мы рекомендуем проводить анализ их защищенности. Наличие исходного кода (тестирование методом белого ящика) делает анализ более эффективным, позволяя выявить и в дальнейшем устранить уязвимости, не дожидаясь кибератак. При этом необходимо подчеркнуть: важна регулярность такого анализа, ведь только систематический подход позволяет минимизировать число уязвимостей в системе и оптимизировать ресурсы на их устранение.

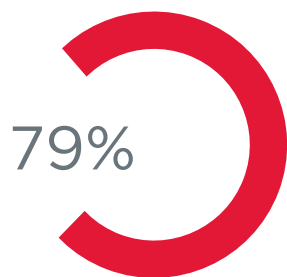
Результаты нашего исследования говорят о том, что уязвимости высокого уровня риска содержатся и в тестовых, и в продуктивных системах. Анализ защищенности веб-приложения начиная с самых ранних этапов его разработки не только снижает затраты на устранение выявленных уязвимостей, но и повышает его эффективность.

Для исправления 83% уязвимостей, включая большинство критически опасных, разработчику веб-приложения придется внести изменения в программный код. Не секрет, что даже частичная переработка веб-приложения может потребовать от компании значительных ресурсов. Чтобы снизить риск нарушения бизнес-процессов в течение времени, которое потребуется на выпуск нового релиза веб-приложения, мы рекомендуем использовать специализированные решения, в частности межсетевые экраны уровня приложений (web application firewalls, WAF). Только комплексный подход к защите веб-приложений сводит риск успешных кибератак к минимуму, позволяя тем самым сохранить деньги и доверие клиентов.

Портрет участников

43 веб-приложения

проанализированы в 2018 году



Доля продуктивных систем

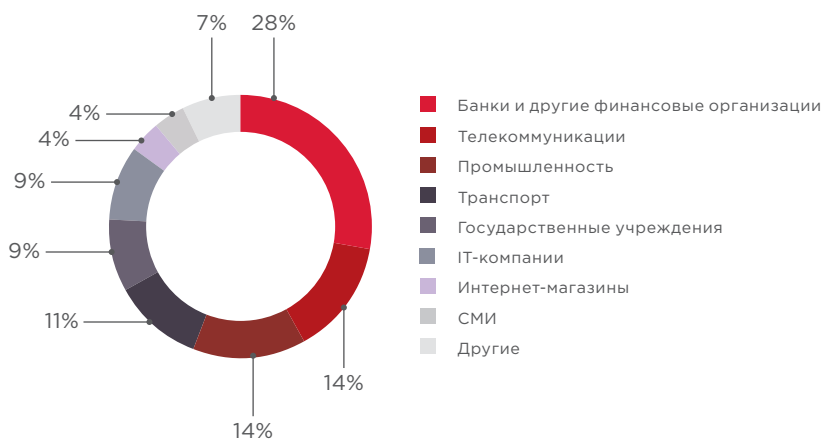


Рисунок 18. Портрет участников исследования

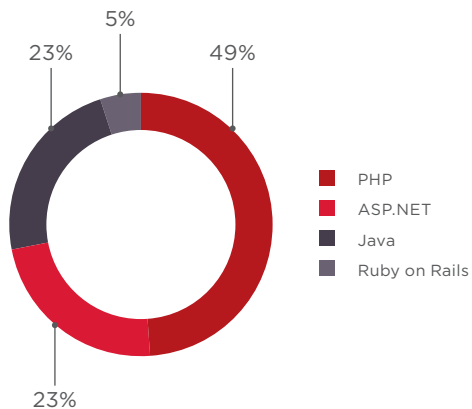


Рисунок 19. Средства разработки (доля веб-приложений)

Методика

Отчет содержит результаты исследования 43 полнофункциональных веб-приложений, для которых в 2018 году проводился углубленный анализ с наиболее полным покрытием проверок. Результаты проектов по тестированию на проникновение, инструментальному сканированию и исследованию систем ДБО не вошли в статистику: эта информация представлена в других аналитических отчетах. Кроме того, в выборке не представлены системы, владельцы которых не дали своего согласия на использование результатов анализа защищенности в исследовательских целях.

Оценка защищенности проводилась методами черного, серого и белого ящика с использованием вспомогательных автоматизированных средств. Метод черного ящика заключается в проведении работ по оценке защищенности информационной системы со стороны внешнего атакующего без предварительного получения какой-либо дополнительной информации о ней от владельца. Метод серого ящика аналогичен, но в качестве нарушителя рассматривается пользователь, имеющий определенные привилегии в системе. При анализе методом белого ящика для оценки защищенности информационной системы используются все имеющиеся данные о ней, включая исходный код приложений.

Обнаруженные уязвимости классифицированы по системе Common Weakness Enumeration (CWE). Ввиду высокой степени дифференциации уязвимостей для удобства читателя мы выделили из них те, которые входят в рейтинг OWASP Top 10–2017, и проанализировали, как часто они встречались в исследованных нами веб-приложениях.

В настоящем документе приведены только уязвимости, связанные с ошибками в коде и конфигурации веб-приложений. Другие распространенные проблемы информационной безопасности (к примеру, недостатки процесса управления обновлениями ПО) не рассматриваются. В статистике также не учтены уязвимости из категории A10 – Insufficient Logging & Monitoring рейтинга OWASP Top 10–2017, так как в рамках границ проведения работ по анализу защищенности веб-приложений мы не оценивали достаточность журналирования и мониторинга. Степень риска уязвимостей оценивалась согласно системе Common Vulnerability Scoring System (CVSS v. 3); на основе этой оценки выделялись качественные оценки высокого, среднего и низкого уровней риска.

О компании

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.