

# АВТОМАТИЗИРОВАННЫЙ АНАЛИЗ КОДА

## СТАТИСТИКА УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ ЗА 2017 ГОД

## СОДЕРЖАНИЕ

Введение.....	3
Методика исследования.....	3
1. Резюме.....	4
2. Особенности работы PT AI.....	4
2.1. Верификация уязвимостей.....	5
2.2. Диаграммы потоков данных.....	6
2.3. Схема уязвимости.....	7
3. Результаты исследования.....	7
3.1. Портрет участников.....	7
3.2. Общая статистика.....	8
3.3. Наиболее распространенные уязвимости.....	8
3.4. Анализ актуальных угроз безопасности.....	9
3.5. Статистика для различных отраслей экономики.....	11
3.5.1. Финансовые организации.....	11
3.5.2. Государственные учреждения.....	12
3.5.3. Интернет-магазины.....	15
Заключение.....	16

## ВВЕДЕНИЕ

Специалисты Positive Technologies регулярно проводят множество исследований, связанных с анализом защищенности веб-приложений. Важно отметить основные результаты некоторых из этих исследований, которые характеризуют уровень безопасности веб-приложений сегодня:

- + в 77% случаев при работах по внешнему тестированию на проникновение была выявлена возможность проведения атак для получения доступа к внутренним корпоративным ресурсам через эксплуатацию уязвимостей веб-приложений<sup>1</sup>;
- + 26% киберинцидентов в III квартале 2017 года связаны с атаками на веб-ресурсы<sup>2</sup>.

Все эти данные свидетельствуют о том, что веб-приложения являются одной из основных мишеней для злоумышленников, потому что большое число неисправленных уязвимостей и простота их эксплуатации помогают атакующим успешно достигать своих целей — от кражи чувствительной информации до доступа к внутренним ресурсам локальной вычислительной сети.

Важно понимать, что большинство уязвимостей можно выявить задолго до атаки, а анализ исходного кода веб-приложений позволяет обнаружить в несколько раз больше критически опасных уязвимостей, чем тестирование систем без исследования кода.

Представленный отчет содержит статистику по уязвимостям 33 веб-приложений, которые были исследованы в рамках работ по автоматизированному анализу защищенности с применением PT Application Inspector (PT AI) в 2017 году.

## МЕТОДИКА ИССЛЕДОВАНИЯ

Оценка защищенности проводилась методом белого ящика в автоматизированном режиме с применением анализатора исходных кодов PT AI. Метод заключается в том, что для оценки защищенности информационной системы используются все необходимые данные о ней, включая исходный код приложений.

В данном исследовании используется классификация уязвимостей, которая применяется в автоматизированном сканере защищенности. Эта классификация отличается от предложенной Web Application Security Consortium (WASC TC v. 2), в частности, более детальной проработкой недостатков, которые в классификации WASC объединены в категории общих недостатков конфигурации приложения, параметров доступа к файловой системе и др.

В статистику вошли не только внешние веб-приложения, доступные из сети Интернет, но и предназначенные для внутреннего пользования организаций.

В настоящей статистике 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.

Степень риска уязвимостей определялась с помощью встроенных механизмов PT AI.

<sup>1</sup> «Уязвимости корпоративных информационных систем (2017)».

<sup>2</sup> «Актуальные киберугрозы: III квартал 2017 года».

## 1. РЕЗЮМЕ

Основные результаты исследования:

### Все веб-приложения уязвимы

По результатам автоматизированного анализа исходного кода было установлено, что все веб-приложения имеют уязвимости, причем всего лишь в 6% исследованных систем отсутствуют уязвимости высокой степени риска.

### Пользователи веб-приложений — основная мишень

В 85% протестированных веб-приложений присутствуют уязвимости, которые позволяют проводить атаки на пользователей. Используя данные уязвимости, злоумышленник может похищать cookie пользователей, проводить фишинговые атаки или заражать их рабочие станции вредоносным программным обеспечением.

### Веб-приложения финансовых организаций наиболее уязвимы

Во всех протестированных приложениях банков и других финансовых организаций найдены уязвимости высокой степени риска. Подобные результаты связаны с тем, что приложения банков имеют более сложную логику работы по сравнению с информационными веб-ресурсами других организаций, и этот фактор создает предпосылки для появления большего числа уязвимостей высокой степени риска. В результате эксплуатации данных уязвимостей злоумышленник может попытаться нарушить работоспособность приложения или выполнить произвольный код на целевой системе, что может привести к полному контролю над сервером с веб-приложением.

### Все протестированные веб-приложения государственных учреждений могут использоваться для атак на пользователей

Во всех исследованных веб-приложениях государственных учреждений присутствуют уязвимости, позволяющие проводить атаки на пользователей. При этом важно отметить, что подавляющее большинство пользователей таких веб-ресурсов очень плохо осведомлены в вопросах информационной безопасности и легко могут стать жертвами злоумышленников.

### Отказ в обслуживании — самая распространенная угроза для интернет-магазинов

В 75% исследованных веб-приложений, связанных с электронной торговлей, выявлены уязвимости, потенциально приводящие к отказу в обслуживании. Реализация данной угрозы может привести к значительным финансовым потерям для владельцев.

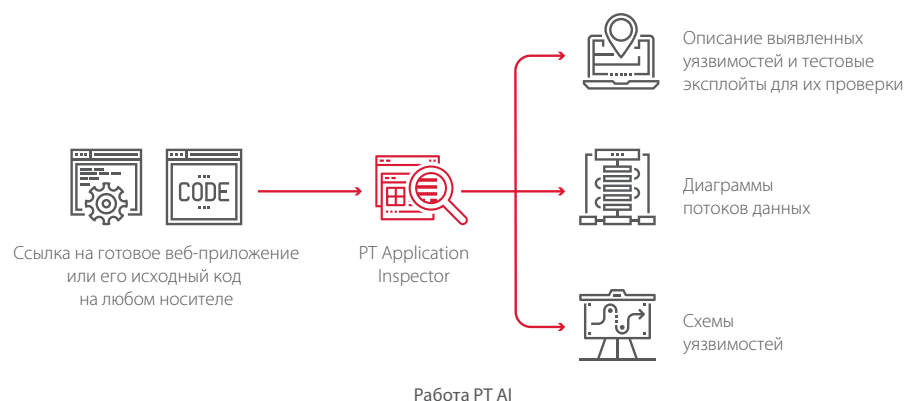
## 2. ОСОБЕННОСТИ РАБОТЫ PT AI

PT AI анализирует исходный код или скомпилированное веб-приложение при помощи метода, называемого абстрактной интерпретацией, который применяется в дополнение к классическому методу статического анализа (SAST) для уточнения полученных результатов. С помощью абстрактной интерпретации для каждой найденной уязвимости возможно строить вектор атаки, определять конкретные рекомендации по ее устранению, генерировать тестовые запросы для ее проверки и определять дополнительные условия эксплуатации. Уже развернутое и функционирующее веб-приложение PT AI может проанализировать при помощи модуля динамического анализа (DAST).

По итогам анализа PT AI предоставляет следующие основные данные об уязвимости:

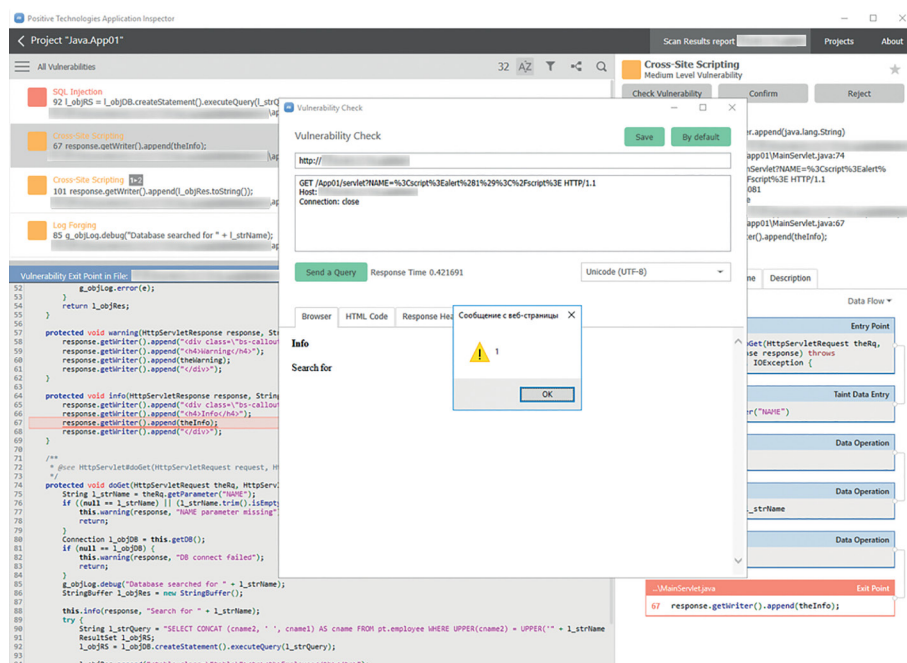
- + тип уязвимости, номер строки и фрагмент исходного кода, где она выявлена, ее описание и общие рекомендации по устранению уязвимостей данного типа;
- + тестовый эксплойт, который позволяет подтвердить или опровергнуть наличие выявленной уязвимости;
- + диаграмму потоков данных (data flow diagram);
- + схему уязвимости.

Особенности работы PT AI, связанные с генерацией тестовых эксплойтов, диаграмм потоков данных и схем уязвимостей, позволяют получать полную информацию о выявленных уязвимостях и корректно вносить изменения в исходный код веб-приложения для их устранения.



## 2.1. Верификация уязвимостей

Использование методов абстрактной интерпретации делает возможной верификацию выявленных уязвимостей при помощи функций PT AI. Верификация выполняется с помощью специальных тестовых HTTP-запросов (эксплойтов), которые производят эксплуатацию уязвимостей на стенде с развернутым приложением. Проверять уязвимости можно не только вручную, но и в автоматическом режиме (функция Autocheck). При необходимости на основе сгенерированного эксплойта можно подготовить виртуальный патч и загрузить его в межсетевой экран уровня веб-приложений PT Application Firewall, который применяет правила для блокировки атак на уже функционирующий веб-ресурс до момента исправления исходного кода приложения.



Верификация уязвимости с помощью тестового эксплойта

Генерация тестовых эксплойтов возможна и в тех случаях, когда для проверки уязвимости требуется выполнить дополнительные условия, например авторизоваться в системе. Для этого строится частичный эксплойт и с помощью абстрактной интерпретации определяют дополнительные условия эксплуатации уязвимости. В дальнейшем при выполнении этих условий возможно успешно верифицировать уязвимость. Такой метод позволяет находить и проверять уязвимости второго порядка.



Условия эксплуатации уязвимости

## 2.2. Диаграммы потоков данных

На основе результатов сканирования PT AI строит диаграммы потоков данных, которые отображают последовательность преобразований над данными, контролируемыми пользователем, от точки их возникновения в программе до точки выхода уязвимости (потенциально опасной операции). Каждая диаграмма показывает один конкретный путь от точки входа до точки выхода, что соответствует варианту эксплуатации уязвимости.

Диаграммы потоков данных имеют одинаковое представление и состоят из следующих блоков:

- + точка входа приложения (entry point) — начальная точка потока выполнения;
- + точка входа данных (taint data entry) — файл и строка кода с координатами входа данных, контролируемых пользователем;
- + операция над данными (data operation) — описание одной или нескольких функций, которые изменяют потенциально опасные входные данные;
- + точка выхода (exit point) — строка выполнения потенциально уязвимой функции.

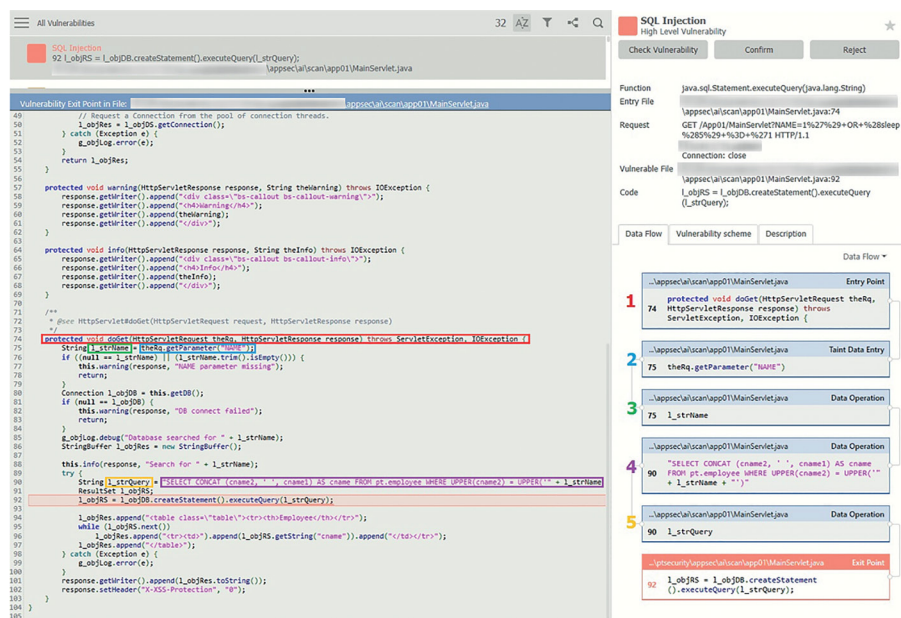
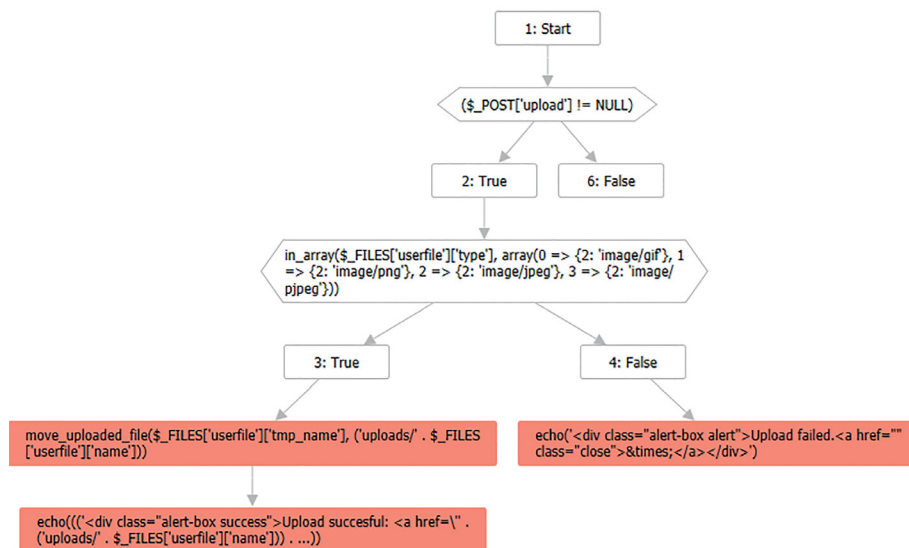


Диаграмма потоков данных

Задача диаграмм потоков данных — продемонстрировать наглядное отображение потока данных от точки входа до точки выхода уязвимости для облегчения ее верификации.

### 2.3. Схема уязвимости

Схема уязвимости — ориентированный граф, соответствующий потоку управления программы, содержит операции ветвления и потенциально опасные операции (выделяются красным цветом). В качестве примера на рисунке ниже приведена простая схема уязвимости, однако часто схемы выглядят значительно сложнее и имеют большее число блоков и операций ветвления.

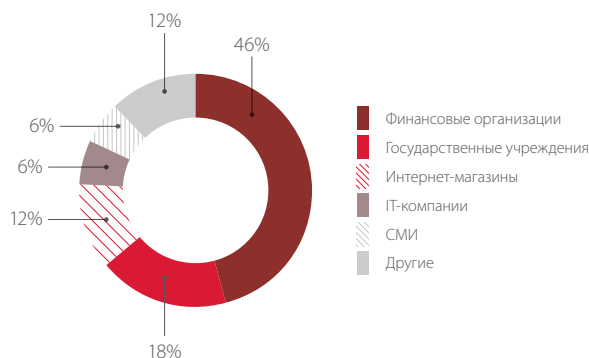


Простая схема уязвимости

## 3. РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

### 3.1. Портрет участников

Веб-приложения, исследованные с применением РТ AI, принадлежат организациям, относящимся к различным отраслям экономики. Наиболее заинтересованы в анализе исходного кода банки и другие финансовые организации, а также государственные учреждения.



Распределение исследованных веб-приложений по отраслям экономики

Стоит отметить, что данная статистика подтверждает результаты исследования SANS Institute<sup>3</sup>, и именно для банков и правительственных организаций безопасность приложений является одной из ключевых задач, так как их веб-ресурсы являются приоритетными целями для злоумышленников. Это же подтверждается в наших ежеквартальных исследованиях со статистикой атак на веб-приложения<sup>4</sup>.

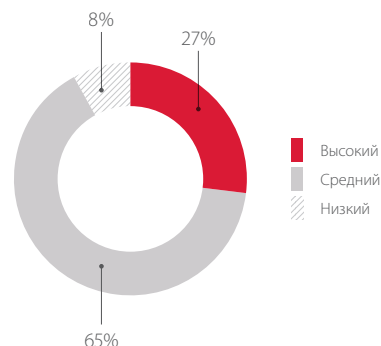
<sup>3</sup> «State of Application Security: Closing the Gap».

<sup>4</sup> Ежеквартальные статистики по атакам на веб-приложения доступны по адресу [ptsecurity.com/ru-ru/research/analytics/](https://ptsecurity.com/ru-ru/research/analytics/)



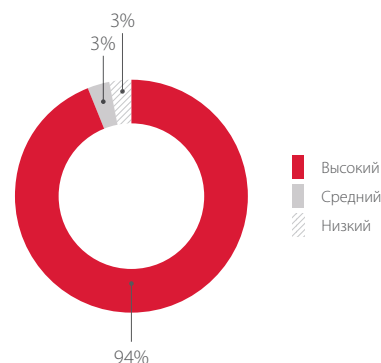
### 3.2. Общая статистика

Автоматизированный анализ защищенности с применением PT AI показал, что все протестированные веб-приложения содержат уязвимости различной степени риска. При классификации уязвимостей по степени риска было установлено, что большая их часть (65%) относится к среднему уровню опасности.



Распределение уязвимостей по уровню риска

При оценке систем по максимальному уровню риска обнаруженных уязвимостей было установлено, что всего лишь в 6% исследованных веб-приложений отсутствуют уязвимости высокой степени риска. Следует учитывать, что исследуемые приложения не являются типовыми CMS-платформами и содержат большое количество кода, написанного их владельцами. Но при этом не нужно забывать, что успешная эксплуатация даже одной критически опасной уязвимости на практике может привести к полной компрометации приложения или даже сервера.



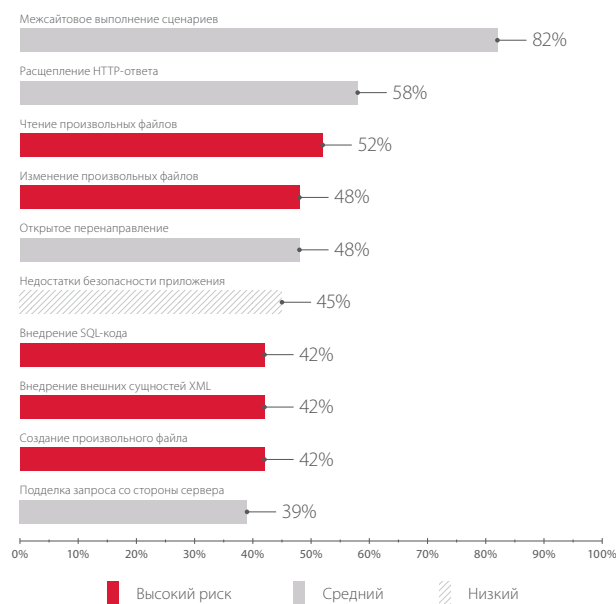
Распределение систем по максимальному уровню риска обнаруженных уязвимостей

### 3.3. Наиболее распространенные уязвимости

Самая распространенная уязвимость, выявляемая при автоматизированном анализе исходного кода приложений, — «Межсайтовое выполнение сценариев», с помощью которой злоумышленник может проводить фишинговые атаки на клиентов веб-приложения или заражать их рабочие станции вредоносным программным обеспечением. Данная уязвимость также лидирует и в аналогичном рейтинге, основанном на результатах ручного тестирования веб-приложений<sup>5</sup>. Вторая по распространенности уязвимость — «Расщепление HTTP-ответа», при успешной эксплуатации которой злоумышленник может проводить атаки на клиентов веб-приложения, основанные на отправке браузеру атакуемого двойного HTTP-ответа, содержимое заголовков и полей которого частично контролируется нарушителем. И замыкает тройку лидеров уязвимость высокого уровня риска «Чтение произвольных файлов», с помощью которой злоумышленник может получить несанкционированный доступ к содержимому произвольного файла на сервере. Таким образом нарушитель может получить исходный код веб-приложения, учетные данные и иную чувствительную информацию, обрабатываемую в системе.

<sup>5</sup> «Уязвимости веб-приложений (2017)».



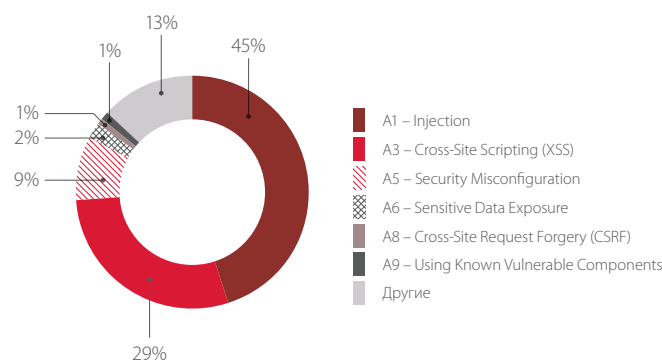


Наиболее распространенные уязвимости (доля систем)

Из десяти наиболее распространенных уязвимостей пять имеют высокую степень риска, и их эксплуатация может привести к серьезным последствиям. Например, в некоторых случаях в результате эксплуатации уязвимости «Создание произвольного файла» злоумышленник может выполнить произвольный код на целевой системе и в дальнейшем полностью скомпрометировать атакуемый сервер.

К недостаткам безопасности приложения относятся неустановленные или некорректно настроенные значения различных свойств и директив. Например, в некоторых приложениях не было установлено свойство `requireSSL`, отвечающее за установку флага `secure` для HTTP-заголовка `Set-Cookie`, который определяет необходимость передачи cookie только по защищенному соединению (HTTPS). Недостатки такого рода в соответствии с классификацией уязвимостей OWASP<sup>6</sup> относятся к категории A5 — Security Misconfiguration.

Распределение обнаруженных уязвимостей в соответствии с классификацией OWASP Top 10 (2017) приведено на диаграмме ниже. Все уязвимости, которые не входят в список 10 самых опасных, были помещены в категорию «Другие».

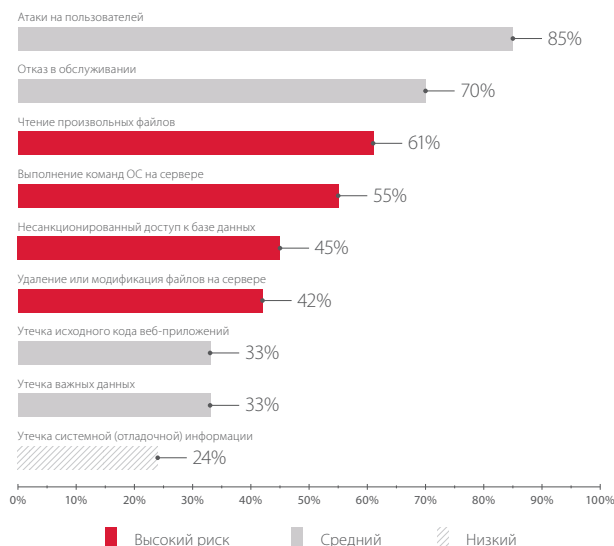


Типы уязвимостей по системе OWASP Top 10

### 3.4. Анализ актуальных угроз безопасности

На основании анализа последствий от эксплуатации выявленных в веб-приложениях уязвимостей был составлен рейтинг угроз безопасности. Самой распространенной угрозой является возможность проведения атак на клиентов веб-приложения.

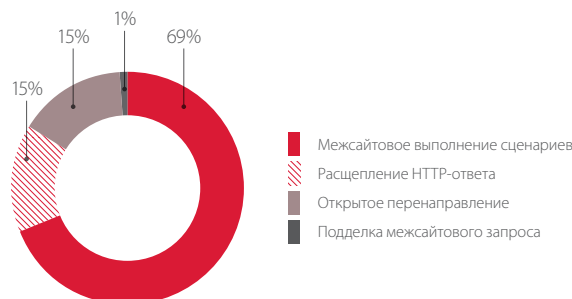
<sup>6</sup> [owasp.org/index.php/Top\\_10\\_2017-Top\\_10](https://owasp.org/index.php/Top_10_2017-Top_10)



Рейтинг наиболее распространенных угроз (доля систем)

Четыре из девяти угроз имеют высокий уровень риска. В случае их реализации злоумышленник может получить несанкционированный доступ к чувствительной информации, хранящейся либо в файлах на сервере (61%), либо в базе данных (45%), выполнять произвольные команды ОС на атакуемом сервере (55%) или удалять или модифицировать файлы (42%). Для доступа к содержимому произвольных файлов на сервере злоумышленник должен успешно провести атаку, направленную на эксплуатацию таких уязвимостей, как «Чтение произвольных файлов» и «Внедрение внешних сущностей XML». Кража информации из базы данных, а также модификация данных, вплоть до удаления всей базы, возможны в результате эксплуатации уязвимостей «Внедрение SQL-кода». Наиболее опасная угроза связана с возможностью выполнения произвольных команд ОС. В результате ее реализации злоумышленник может получить полный контроль над сервером и выполнять команды ОС с привилегиями веб-приложения. При обнаружении на данном сервере интерфейса внутренней сети возможно развитие атаки на ресурсы внутренней сети владельца веб-приложения вплоть до полной компрометации всей корпоративной инфраструктуры. Такие примеры атак нередко демонстрируются в рамках работ по тестированию на проникновение, проводимых нашей компанией<sup>7</sup>.

Уязвимости, эксплуатация которых позволяет проводить атаки на клиентов, выявлены в 85% веб-приложений. В основном совершать атаки на пользователей возможно из-за эксплуатации самой распространенной уязвимости «Межсайтовое выполнение сценариев». Однако во многих протестированных приложениях также возможно проводить подобные атаки из-за наличия уязвимостей «Расщепление HTTP-ответа», «Открытое перенаправление» и «Подделка межсайтового запроса».



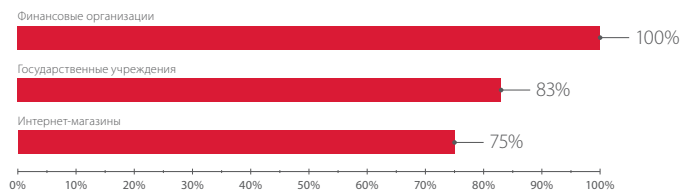
Уязвимости, приводящие к атакам на клиентов

Полученные результаты наглядно демонстрируют необходимость проводить поиск уязвимостей в исходном коде веб-приложения как перед его запуском в эксплуатацию, так и в процессе функционирования.

<sup>7</sup> «Корпоративные информационные системы: тестирование на проникновение (сценарии атак)».

### 3.5. Статистика для различных отраслей экономики

В данном разделе приведена статистика с результатами анализа исходного кода веб-приложений финансовых организаций, государственных учреждений и интернет-магазинов. Веб-приложения IT-компаний и СМИ рассматриваться не будут, поскольку их выборка в настоящем исследовании недостаточна для получения объективной оценки.

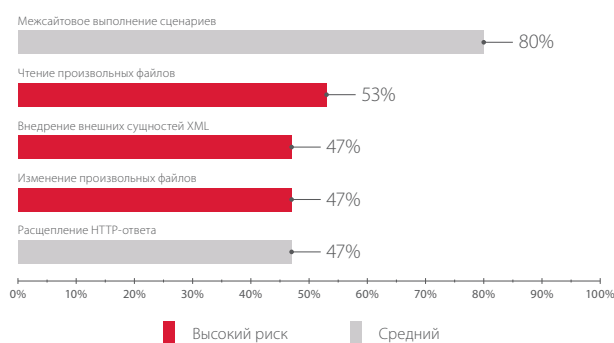


Доля веб-приложений с уязвимостями высокой степени риска

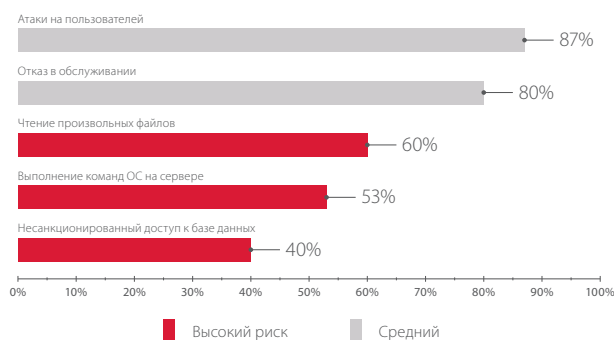
Для каждой отрасли экономики были определены наиболее распространенные уязвимости в веб-приложениях и актуальные угрозы.

#### 3.5.1. Финансовые организации

В 80% исследованных приложений финансовых организаций выявлена уязвимость «Межсайтовое выполнение сценариев», и почти в половине — уязвимость «Расщепление HTTP-ответа». Именно из-за этих уязвимостей в 87% приложений возможно проведение атак на пользователей веб-приложений. Угроза отказа в обслуживании связана с возможностью успешной эксплуатации уязвимостей высокой степени риска «Внедрение внешних сущностей XML» и «Изменение произвольных файлов». Кроме того, с помощью уязвимости «Изменение произвольных файлов» злоумышленник может попытаться выполнить произвольный код на целевой системе, что даст ему полный контроль над сервером с веб-приложением. Если атакуемый ресурс является системой ДБО или если на скомпрометированном сервере расположены приложения, позволяющие проводить финансовые транзакции, — злоумышленник может похитить крупные суммы денежных средств в результате успешного проведения мошеннических операций.



Наиболее распространенные уязвимости финансовых организаций (доля систем)



Наиболее распространенные угрозы для финансовых организаций (доля систем)

**Пример:** при анализе защищенности веб-приложения одного из банков установлено, что в результате ошибки, допущенной при разворачивании ПО, в состав используемых фреймворков была произведена загрузка тестовых и демонстрационных файлов. Данная ошибка привела к множественным уязвимостям. Например, в модуле `index.php` выявлена уязвимость «Межсайтовое выполнение сценариев», позволяющая злоумышленнику особым образом сформировать ссылку на указанную веб-страницу и инициировать выполнение вредоносного JavaScript-кода. Посредством этого кода можно сформировать HTTP-запрос типа GET от имени легитимного пользователя к модулю `cookies.php` и таким образом получить cookie пользователя.

Medium	Cross-Site Scripting
✓	<p>Vulnerable Code: <b>26</b> <code>&lt;?php print_r(\$_POST); ?&gt;</code></p> <p>Function: <b>print_r</b></p> <p>Vulnerable File: <code>... \vendor\codeception\codeception\tests\data/app\view\index.php</code></p> <p>Entry File: <code>... \vendor\codeception\codeception\tests\data/app\view\index.php : 1</code></p> <p>Exploit: <code>POST /vendor/codeception/codeception/tests/data/app/view/index.php HTTP/1.1</code>  Host: <code>...</code>  Accept-Encoding: identity  Connection: close  Content-Length: 49  Content-Type: application/x-www-form-urlencoded</p> <p><code>someparam=3Cscript3Ealert12814293C42Fscript3E</code></p> <p>OWASP - A3 <a href="#">CWE-79</a></p> <p><a href="#">Show Data Flow</a></p>

### Выявленная уязвимость «Межсайтовое выполнение сценариев»

Кроме того, было установлено, что комплекс модулей в каталоге `\filebrowser` содержит демонстрационное приложение, обеспечивающее базовую функциональность по управлению файлами в каталоге `\root` с помощью веб-интерфейса. При анализе исходного кода были выявлены множественные уязвимости «Создание произвольного файла» и «Изменение произвольных файлов», эксплуатация которых позволяет беспрепятственно копировать и переименовывать файлы в каталоге `\filebrowser`. С помощью этих уязвимостей злоумышленник может провести атаку, ориентированную на исчерпание свободного места на локальном диске веб-сервера, и вызвать отказ в обслуживании приложения.

[illegible]

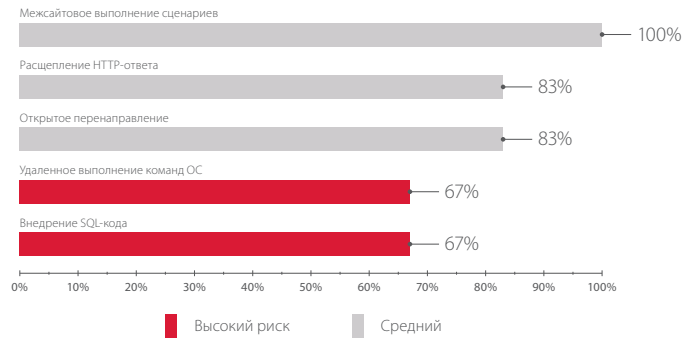
### Выявленная уязвимость «Изменение произвольных файлов»

[illegible]

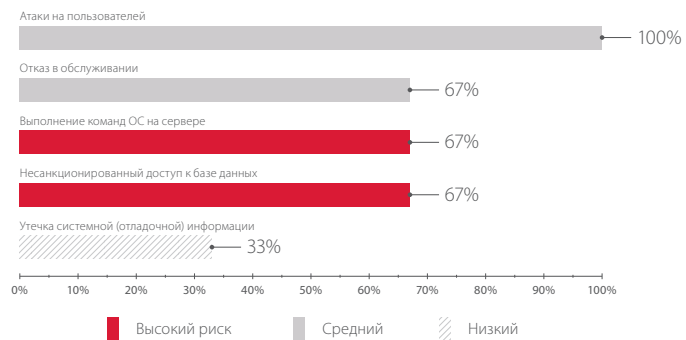
### Выявленная уязвимость «Создание произвольного файла»

### 3.5.2. Государственные учреждения

Во всех исследованных веб-приложениях государственных учреждений присутствуют уязвимости, позволяющие проводить атаки на пользователей. При этом важно отметить, что большинство пользователей таких веб-ресурсов очень плохо осведомлены в вопросах информационной безопасности и легко могут стать жертвами злоумышленников.



Наиболее распространенные уязвимости государственных учреждений (доля систем)



Наиболее распространенные угрозы для государственных учреждений (доля систем)

**Пример:** при исследовании веб-приложения администрации одного из муниципальных образований была обнаружена уязвимость высокой степени риска «Внедрение SQL-кода», с помощью эксплуатации которой возможно получить чувствительную информацию из базы данных.

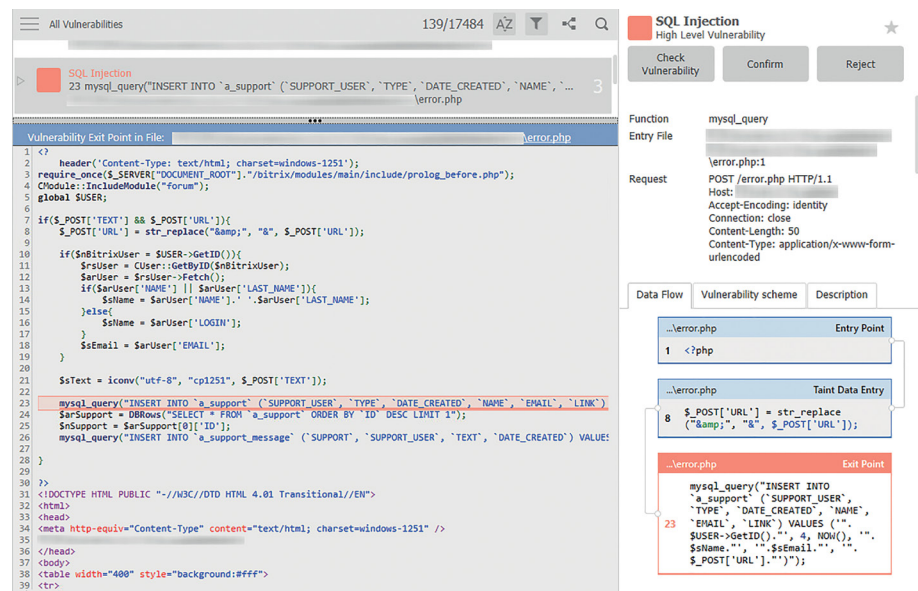


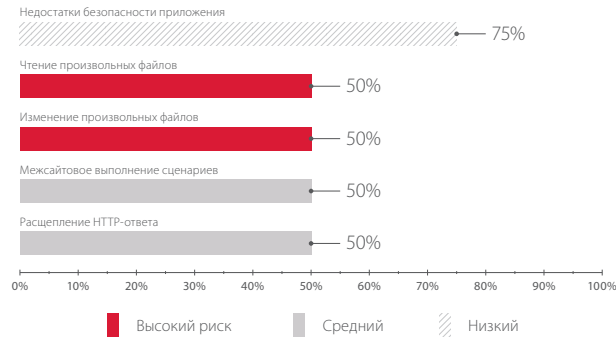
Диаграмма потоков данных для уязвимости «Внедрение SQL-кода»

Кроме того, в ходе дальнейшего анализа исходного кода было установлено, что любому внешнему нарушителю доступен файл `info.php` с конфигурационной информацией о системе. В ходе дальнейших работ была проведена ручная верификация уязвимости и получен доступ к содержимому данного файла. Полученная информация может быть использована злоумышленником при планировании дальнейших атак на приложение.

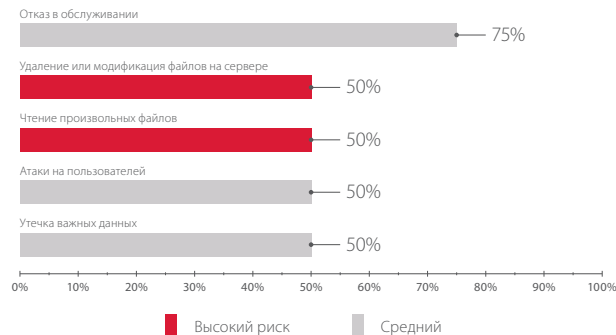


### 3.5.3. Интернет-магазины

Уязвимости, проводящие к отказу в обслуживании, представляют наибольшую проблему для интернет-магазинов, так как сбой в работе веб-приложения для организации, занимающейся электронной торговлей, напрямую связан с финансовыми потерями. Кроме того, чем популярнее интернет-магазин, тем больше клиентов посещают его каждый день и тем вероятней, что злоумышленник попытается использовать уязвимости данного веб-ресурса для атак на его пользователей.



Наиболее распространенные уязвимости интернет-магазинов (доля систем)



Наиболее распространенные угрозы для интернет-магазинов (доля систем)

**Пример:** в ходе исследования CMS-платформы, применяемой для управления контентом интернет-магазинов, была выявлена уязвимость высокой степени риска «Чтение произвольных файлов». Использовать тестовый HTTP-запрос для верификации уязвимости не удалось, так как для ее эксплуатации необходимо, чтобы пользователь авторизовался в системе. При этом в графе «Условия эксплуатации уязвимости» указана MD5-хеш-сумма требуемого пароля, найденная при анализе исходного кода. По этой хеш-сумме можно осуществить подбор пароля, авторизоваться в системе и успешно провести эксплуатацию уязвимости. Это типичный случай выявления недеklarированных возможностей, заложенных в веб-приложение его разработчиком.

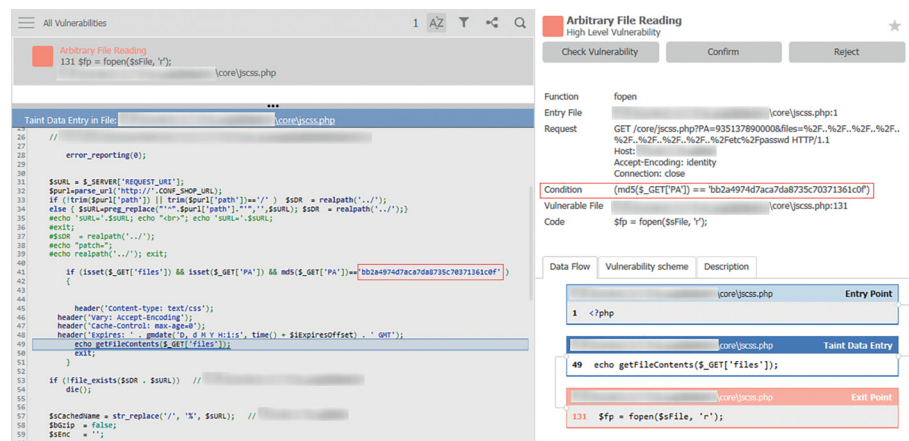


Диаграмма потоков данных для уязвимости «Чтение произвольных файлов»



## ЗАКЛЮЧЕНИЕ

Результаты исследования показывают, что анализ исходного кода веб-приложений позволяет найти большое количество уязвимостей различной степени риска и в процессе разработки веб-приложений значительно повысить защищенность конечного продукта. При этом независимо от стадии разработки целесообразно применять автоматизированные средства, поскольку скорость работы анализатора превосходит возможности ручного анализа.

Также важно отметить, что после выявления уязвимостей в коде веб-приложения может потребоваться значительное время для их устранения. В этот период продуктивные системы остаются уязвимыми. Поэтому для их эффективной защиты важно не только регулярно проводить анализ защищенности веб-приложений методом белого ящика, в том числе с использованием автоматизированных средств, но и использовать превентивные средства защиты, такие как межсетевой экран уровня приложений, для обнаружения и предотвращения атак на веб-ресурсы.

---

### О компании

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.