



PT

# Взлом на заказ

[ptsecurity.com](http://ptsecurity.com)

## Содержание

Об исследовании	3
Зачем взламывают сайты	4
Кто-то ломает, а кто-то покупает	7
Базы пользователей	10
Сложно ли взломать сайт?	11
Выводы	12

С помощью корпоративных сайтов, интернет-магазинов, веб-сервисов бизнес решает множество своих задач. Клиенты регистрируются на этих площадках, оставляя свои персональные данные, совершают покупки, вводя данные банковских карт, а также используют предоставленные ресурсы для хранения или отправки конфиденциальной информации. Очевидно, что к такому объему данных захотят получить доступ не только конкуренты, но и киберпреступники, поэтому сегодня никого не удивишь новостями об очередной утечке персональных данных клиентов крупной компании. Зачастую эти события связаны с успешной атакой на веб-приложения организации, в результате которой злоумышленники получили доступ к базе данных пользователей этого ресурса или похитили другую информацию. Например, в сентябре 2020 года хакеры взломали более 2800 интернет-магазинов на платформе Magento и внедрили вредоносный скрипт, который собирал личную информацию и данные платежных карт клиентов.

В результате взлома сайта могут пострадать и пользователи, и сама компания. Анализ защищенности веб-приложений, проведенный специалистами Positive Technologies, показывает, что в 92% веб-приложений злоумышленник может проводить атаки на клиентов, в 68% случаев возможна утечка важных данных, а в 16% злоумышленник смог бы получить контроль над приложением и ОС сервера.

В данной статье мы расскажем о том, зачем хакеры взламывают сайты, и к каким последствиям для владельца и пользователей ресурса это может привести.

## Об исследовании

Мы выбрали десять наиболее активных форумов в дарквебе, на которых представлены услуги по взлому сайтов, покупке и продаже баз данных и доступов к веб-ресурсам. Всего на этих форумах зарегистрировано более 8 млн пользователей, создано более 7 млн тем, в которых опубликовано более 80 млн сообщений.

Отметим, что в статье не рассматриваются объявления, связанные с услугами по организации DDoS-атак на веб-ресурсы, так как мотивы, цели и инструменты атакующих или тех, кто их нанял, в этом случае отличаются кардинально и выходят за рамки данного исследования.

## Зачем взламывают сайты

В 90% случаев в дарквебе на форумах, посвященных взлому сайтов, ищут исполнителя-хакера, который сможет предоставить заказчику доступ к ресурсу или выгрузит базу пользователей. В 7% записей фигурируют предложения услуг по взлому сайтов. Остальные сообщения направлены на продвижение сервисов и программ для взлома сайтов и поиск единомышленников по взлому.

Под предложениями услуг подразумеваются объявления, опубликованные владельцами сервисов и хакерскими группировками. Они не могут выступать в качестве показателей спроса и предложения, так как зачастую размещаются единожды. О величине спроса на вышеперечисленные услуги можно приблизительно судить только по единичным запросам пользователей, которые по различным причинам не воспользовались информацией о предложениях услуг.

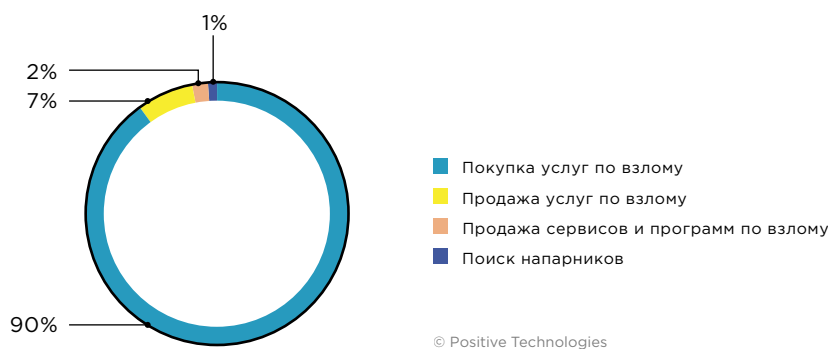


Рисунок 1. Категории запросов, связанных со взломом сайтов

Начиная с марта 2020 года мы наблюдаем укрепление интереса к теме взлома сайтов. К этой тенденции могло привести увеличение количества компаний, представленных в интернете, которое спровоцировала пандемия коронавируса. Организации, ранее работавшие на офлайн-площадках, были вынуждены перейти в онлайн-формат для того, чтобы не потерять клиентов и прибыль, а киберпреступники не могли не воспользоваться этой ситуацией.

На графике ниже приведены данные о количестве новых объявлений на форумах в дарквебе. Объявления размещаются не только новыми участниками, но и хакерами с репутацией. Последние делают это, чтобы напомнить о себе. Узнать, какие объявления дублируются или потеряли актуальность на определенный момент времени, сложно, поэтому мы не приводим количество хакеров или группировок, которые активно предоставляли услуги по взлому в начале 2019 года или занимаются этим сегодня.

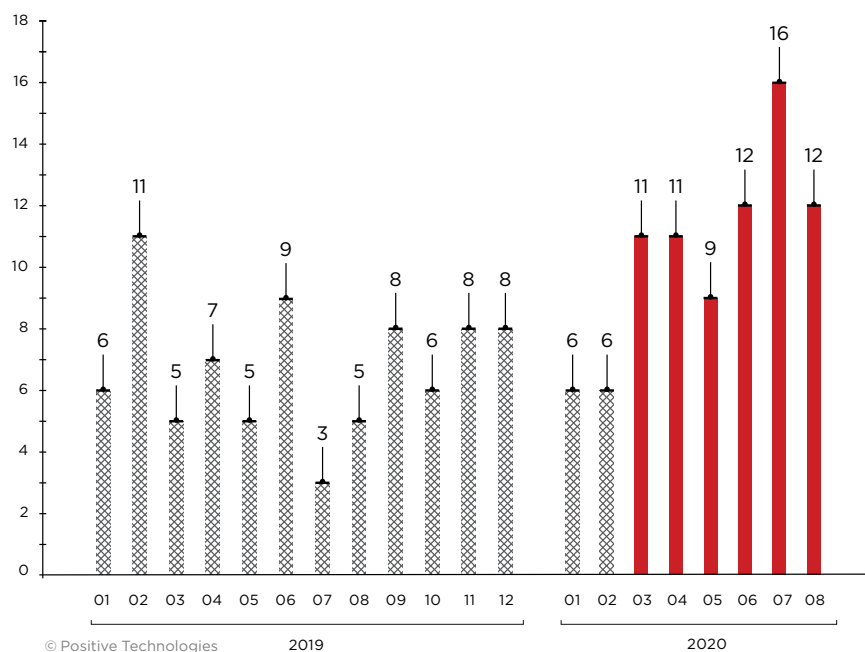


Рисунок 2. Количество новых объявлений про взлом веб-ресурсов на форумах в 2019–2020 гг.

Примерно в семи из десяти запросов, касающихся взлома сайтов, основной целью является получение доступа к веб-ресурсу. Злоумышленники могут не только похитить конфиденциальную информацию, но и продать доступ к веб-приложению так называемым скупщикам.

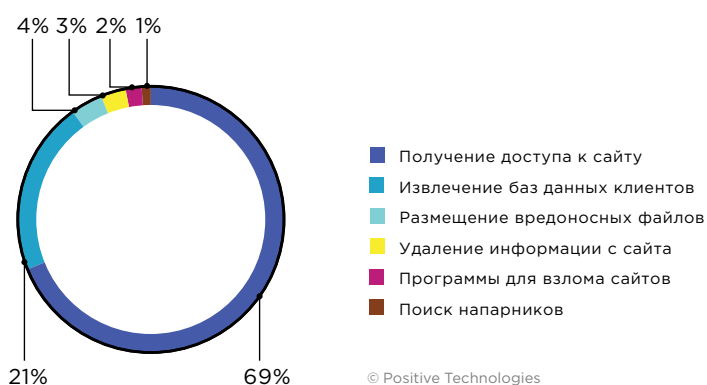


Рисунок 3. Распределение запросов по тематикам

Запросы, направленные на получение баз данных пользователей или клиентов атакуемого ресурса, составляют 21% от всех объявлений. В приобретении такой информации в первую очередь заинтересованы конкуренты и спамеры, которые собирают списки адресов для целевой тематической рассылки, ориентированной на определенную аудиторию.



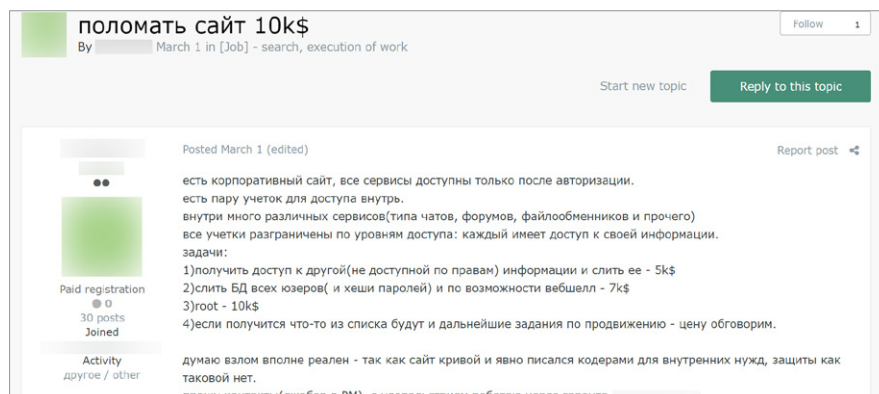


Рисунок 4. Заказной взлом сайта

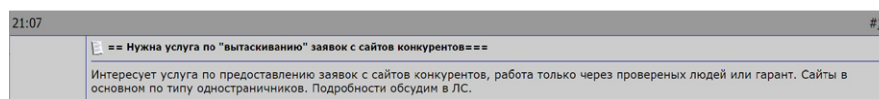


Рисунок 5. Сбор сведений с сайтов конкурентов

В 4% запросов основной целью злоумышленников является не взлом сайта, а размещение на нем вредоносных программ, например для проведения атаки типа watering hole или размещения веб-скиммеров. Так, в августе 2020 года АРТ-группировка Charming Kitten в ходе одной из своих кампаний, направленной на ученых из университетов Хайфы и Тель-Авива, взломила сайт Deutsche Welle для размещения на нем вредоносной ссылки. При переходе по этой ссылке жертве предлагалось пройти процедуру авторизации, а введенные учетные данные отправлялись злоумышленникам.

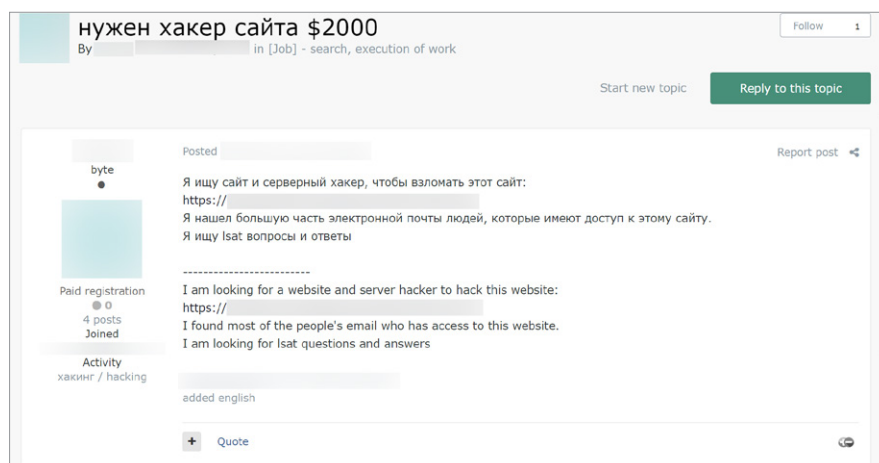


Рисунок 6. Поиск исполнителя для взлома сайта

На поиск хакера, который сможет взломать сайт и удалить определенные заказчиком данные, направлены 3% объявлений. Например, эта услуга может быть востребована среди тех, кто хочет удалить негативные отзывы о компании, размещенные на неподконтрольных этой компании ресурсах.

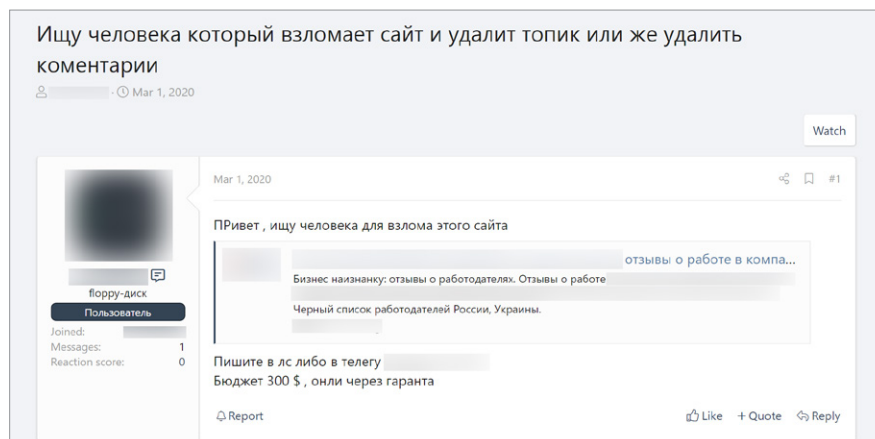


Рисунок 7. Объявление о поиске злоумышленника-исполнителя

Предложения о продаже готовых программ и скриптов для взлома встречаются в 2% от общего числа проанализированных запросов.

## Кто-то ломает, а кто-то покупает

Ранее мы уже рассказывали о том, что в дарквебе появились «скупщики» доступов к сайтам. Теперь, когда это явление укрепилось, оказалось, что их можно разделить по направлениям. Одни покупают веб-шеллы, другие — доступ к интерфейсам администрирования различных сайтов, а третьи приобретают готовые эксплойты для внедрения SQL-кода применительно к конкретным ресурсам.

Г

### Что такое веб-шелл

Веб-шелл — это загруженный на сервер файл, с помощью которого злоумышленник может выполнить команды ОС на сервере через веб-интерфейс и получить доступ к другим файлам.

Веб-шеллы стоят не так дорого, как, например, базы данных, о которых мы расскажем далее, — цены на них варьируются от нескольких центов до тысячи долларов США. В основном это связано с тем, что полученные в результате загрузки веб-шелла привилегии в файловой системе сильно ограничены. Продажа веб-шелла заключается в передаче ссылки на путь к файлу и, возможно, данным для авторизации. Наиболее распространены веб-шеллы на сайтах в доменной зоне .com — 54,3% предложений о продаже.

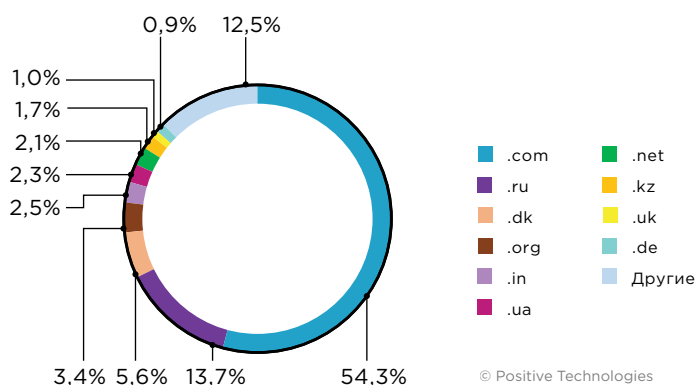


Рисунок 8. Распределение доменов первого уровня, в которых зарегистрированы сайты с веб-шеллами

Скупщикам в первую очередь приходится следить за тем, что интересно рынку потребителей. Явную отраслевую специфику по продаваемым или покупаемым доступам проследить сложно, однако можно смело утверждать, что доступы к интернет-магазинам («шопам») стоят особняком. Спрос на них стабильно высокий: это обусловлено тем, что при оплате товаров пользователь вносит данные своей банковской карты. Таким образом, хакеру достаточно внедрить на сайте вредоносный код на языке JavaScript, который будет перехватывать вводимую покупателем информацию, и использовать полученные сведения в корыстных целях. Еще один способ нажиться на пользователях это получить привилегированный доступ к интернет-магазину, чтобы оформлять заказы, используя данные чужих банковских карт или вовсе не оплачивая их. Цены на доступы к интернет-магазинам варьируются в диапазоне от 50 до 2000 долл. США.



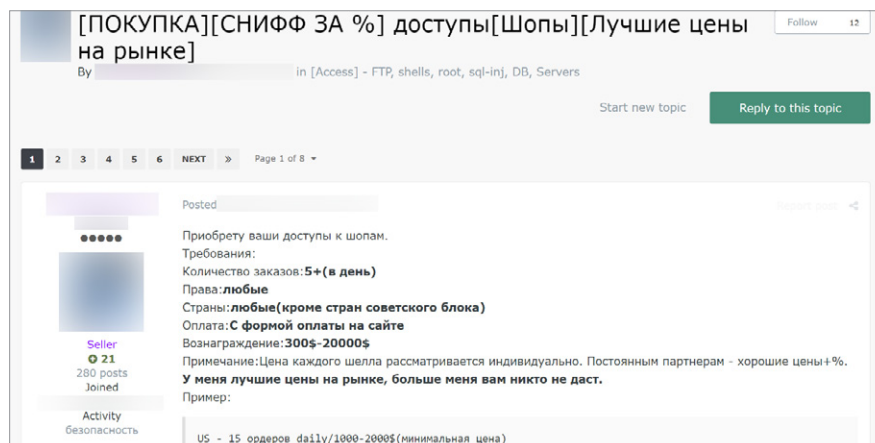


Рисунок 9. Объявление о покупке доступов к интернет-магазинам

Если веб-сервис размещается на сервере, подключенном к внутренней сети компании, то главный риск для организации заключается в том, что атакующий (или тот, кто купит доступ к серверу через веб-шелл) сможет развить атаку и проникнуть в инфраструктуру компании. Результаты внешних пентестов, проведенных экспертами Positive Technologies в 2019 году, показывают, что в 86% компаний существует хотя бы один вектор проникновения в локальную сеть, который связан с недостаточной защитой веб-приложений. В каждой шестой компании были обнаружены следы атак злоумышленников — выявлены веб-шеллы на ресурсах сетевого периметра, вредоносные ссылки на официальных сайтах или валидные учетные записи в публичных базах утечек.

Доступы к веб-интерфейсам администрирования популярных CMS злоумышленники используют для того, чтобы размещать на них веб-шеллы, вредоносное ПО и использовать их в незаконных рекламных схемах. К примеру, в августе и сентябре 2020 года была замечена серия атак, направленных на сайты ЮНЕСКО, ВОЗ, правительственных организаций, Национального института здравоохранения и крупных образовательных учреждений. На этих ресурсах хакеры разместили фишинговую рекламу инструментов для взлома аккаунтов в известных социальных сетях и читерства в онлайн-играх. Они преследовали две цели: кражу данных платежных карт и распространение вредоносного ПО. Часть пользователей перенаправлялась на страницу оплаты, где нужно было ввести реквизиты карты, а другие сразу загружали вредоносы на свои устройства.

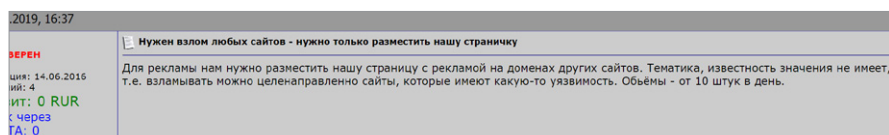


Рисунок 10. Поиск взломщика с целью размещения рекламы

Стоит отметить, что участие сайта в незаконных рекламных кампаниях может негативно сказаться на его позиции в списке выдачи в популярных поисковых системах.

## Базы пользователей

Дампы или базы данных со взломанных сайтов могут покупать конкуренты или злоумышленники, которые планируют целевые фишинговые рассылки.

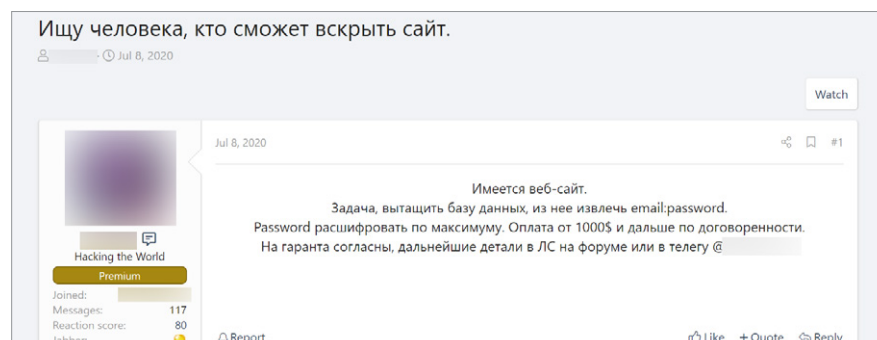


Рисунок 11. Объявление о поиске взломщика сайта

Базы, которые добывают на заказ, стоят от 100 до 20 000 долл. США или от 5 до 50 долл. за 1000 записей о пользователях.

<b>SELLING</b>	2020 DB & Combos 110 Million Lines II	4	805	August 04, 2020 at 11:48 AM	Last Post
<b>BUYING</b>	FB Database	1	336	August 04, 2020 at 09:22 AM	Last Post
<b>BUYING</b>	Buying Japanese Gaming databases	2	398	August 04, 2020 at 07:19 AM	Last Post
<b>SELLING</b>	AT&T 63K PHISHED ACCOUNTS FRESH	7	678	August 04, 2020 at 06:45 AM	Last Post
<b>BUYING</b>	Buying high quality data and combos. Can pay high looking for long term business!	0	256	August 04, 2020 at 12:21 AM	Last Post
<b>SELLING</b>	Big DB Collection	7	1,638	August 03, 2020 at 06:11 PM	Last Post
<b>BUYING</b>	Fresh, hq antipublic @	0	445	August 03, 2020 at 04:17 PM	Last Post
<b>TRADING</b>	Couple of dbs for trade	11	732	August 03, 2020 at 09:45 AM	Last Post
<b>BUYING</b>	Spotify Log/Combo	0	258	August 03, 2020 at 07:02 AM	Last Post
<b>SELLING</b>	Sale of the account of the representative of Asiatek and Sabadita telecommunication	0	422	August 03, 2020 at 04:03 AM	Last Post
<b>BUYING</b>	mail-pass of @	2	348	August 03, 2020 at 03:22 AM	Last Post

Рисунок 12. Объявления о продаже учетных записей, полученных с помощью фишинга

Записи о пользователях, к примеру, содержат следующую информацию: логин, email, ФИО, номер телефона, адрес проживания, номер социального страхования и дату рождения. Эти сведения могут использоваться для проведения атак с использованием методов социальной инженерии.

## Сложно ли взломать сайт?

По результатам анализа защищенности веб-приложений было выявлено, что в среднем в одном веб-приложении имеется 4 уязвимости высокой степени риска и 12 — средней. Даже если не принимать во внимание большое количество уязвимостей, злоумышленники могут воспользоваться методами социальной инженерии и, например, провести целенаправленную фишинговую атаку на администратора ресурса с целью получения учетных данных — логина и пароля. Эти данные позволяют получить доступ к сайту компании.



Рисунок 13. Объявление о взломе сайта на заказ

Основываясь на данных наших исследований, можно сделать вывод о том, что большинство веб-ресурсов недостаточно защищены от воздействия злоумышленников. Также стоит учитывать количество объявлений в дарк-вебе, в которых предлагаются услуги по взлому веб-сервисов. При желании преступники могут без особых сложностей найти опытного исполнителя или уже готовый инструмент для взлома, например, у скупщика.

## Выводы

Услуги по взлому веб-приложений пользуются большим спросом. Объявления о взломе сайтов на заказ не имеют привязки к определенной отрасли, но больше всего клиентов злоумышленников, предоставляющих такие услуги, интересуют интернет-магазины. В первую очередь это связано с тем, что пользователи этих ресурсов оставляют там личные данные и реквизиты банковских карт. Мы считаем, что наметилась определенная тенденция на дальнейшее увеличение спроса, так как все больше компаний переходят в онлайн — этому тренду поспособствовала пандемия COVID-19.

Взлом веб-приложений компании может повлечь за собой глобальные последствия: от утечек данных и санкций за нарушение действующего законодательства (например, GDPR) до проникновения в локальную сеть компании, использования ее ресурсов в последующих атаках — в виде платформы для распространения ВПО или хранения инструментов, которые будут загружены в ходе атаки. При построении системы защиты мы советуем руководствоваться принципами риск-ориентированного подхода, основанного на понимании уровня допустимого для компании негативного эффекта. Проще и дешевле будет превентивно защитить уязвимую часть сети компании, чем оплачивать огромные штрафы и терять свою репутацию.

Чтобы защитить свою компанию, следует придерживаться принципов безопасной разработки и использовать средства автоматизированного анализа исходного кода на предмет ошибок и уязвимостей, так как по результатам анализа защищенности веб-приложений за 2019 год было выявлено, что 82% от числа всех уязвимостей сосредоточены именно в коде веб-приложения. Необходимо регулярно проводить анализ защищенности веб-приложений, а также использовать в качестве превентивной защиты межсетевой экран уровня приложений — web application firewall, WAF.

---

### О компании

ptsecurity.com  
pt@ptsecurity.com  
facebook.com/  
PositiveTechnologies  
facebook.com/PHDays

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «Новости» на сайте [ptsecurity.com](#).