УДК 28.27.27

ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ

© 2024 М. А. Лапина[1], А. Р. Багаутдинова[2], Н. Загнетов[3]

[1]доцент кафедры «Информационная безопасность автоматизированных систем»
e-mail: m.lapina@ncfu.ru

[2]студент по направлению подготовки «Информационная безопасность автоматизированных систем»
e-mail: bagautdinova@mail.ru
[3] аспирант по направлению подготовки «Математическое и программное обеспечение вычислительных систем, комплектов и компьютерных сетей»
e-mail: zagnetov@gmail.ru

[1]Северо-Кавказский федеральный университет
[2] Московская финансово-юридическая академия

В статье рассмотрены основные проблемы безопасности веб-приложений и приведены методы их решения. Проведён анализ всех проблем и составлен рейтинг самых опасных, но распространенных проблем с безопасностью веб-приложений.

Ключевые слова: уязвимости веб-сервисов, информационная безопасность, анализ угроз веб-приложений, архитектура приложений, шифрование.

RESEARCHING WEB APPLICATION SECURITY VULNERABILITIES

© 2024 M. A. Lapina[1], A. R. Bagautdinova[2], N. Zagnetov[3]

[1] Associate Professor, Department of Information Security of Automated Systems
e-mail: m.lapina@ncfu.ru
[2] Student in the field of training “Information security of automated systems”
e-mail: bagautdinova@mail.ru
[3] Postgraduate student in the field of training "Mathematical and software of computer systems, kits and computer networks"
e-mail: zagnetov@gmail.ru

[1]North Caucasus Federal University
[2] Moscow Financial and Legal Academy

The article discusses the main security problems of web applications and provides methods for solving them. An analysis of all the problems was carried out and a rating of the most dangerous but common problems with web application security was compiled.

Keywords: web service vulnerabilities, information security, web application threat analysis, application architecture, encryption.

На сегодняшний день веб-сервисы пользуются популярностью как у обычных пользователей, так и у ученых. Веб-сервисы, основанные на существующих интернет-

протоколах и открытых стандартах, могут обеспечить гибкое решение проблемы интеграции приложений. С помощью WSDL, SOAP и UDDI веб-сервисы становятся популярными в веб-приложениях. Стоит отметить, что архитектуры веб-сервисов сталкиваются с несколькими значительными проблемами с безопасностью. В данной статье мы проведем обзор данных проблем и их решение. Решение этих проблем является ключевым фактором успеха веб-сервисов. Мы прогнозируем явный прогресс в области семантических грид-сервисов. Одна из самых популярных угроз безопасности web-приложений – эксплуатация уязвимостей и DDos-атаки.

Интернет стал частью нашей рутины, мы пользуемся им на постоянной основе и не только в развлекательных целях, но и в профессиональной и иной деятельности. Именно поэтому необходимо продумывать архитектуру сервисов так, чтобы не происходило утечек данных. Этот вид незаконных действий получил название киберпреступность. Угрозы возрастают быстрее, чем происходит развитие информационных технологий. Стоит отметить, что большинство атак на веб-сервисы всё еще происходят с помощью самых распространенных уязвимостей. К основным относятся отсутствие фильтрации обрабатываемых данных, уязвимости в программном обеспечении.

Области и спецификации веб-сервисов. Веб-сервисы – это новая ступень развития информационных технологий. Это модульные приложения, которые могут быть опубликованы на площадках или быть использованы с помощью поисковой системы в сети Интернет. Веб-службы способны выполнять самые разные функции от примитивных к сложным, например выполнение бизнес-процессов.

Главной особенностью использования веб-приложений является возможность создавать собственные приложения «на лету» благодаря использованию слабосвязанных многоразовых программных компонентов. Программное обеспечение может быть доставлено и оплачено как текучий поток услуг, в отличие от упакованных продуктов. Также можно с легкостью добиться автоматической и динамической интероперабельности между системами для выполнения процессов. Бизнес-услуги могут быть полностью децентрализованы и распределены через Интернет, а доступ осуществляется с помощью различных устройств связи. Это помогает программистам отказаться от плохих условий, то есть от сложной, низкой и дорогой интеграции программного обеспечения, и вместо этого скорректировать свое внимание на ценности своих предложений и важных задачах. При таком подходе Интернет станет глобальной общей платформой, на которой организации и отдельные лица строят дружеские отношения, общаясь друг с другом и понимая свои потребности, для осуществления различной деятельности и удовлетворения потребностей потребителей. Сложности с предоставлением новых предложений и выходом на новые рынки будут значительно снижены, чтобы обеспечить доступ малому бизнесу. Динамичные предприятия и цепочки создания стоимости становятся крайне обязательными для получения конкурентных преимуществ.

Причинами производительности являются, с одной стороны, связь по протоколу, который генерирует значительный сетевой, а с другой стороны, генерация и анализ сообщений может занимать много памяти. Хотя шифрование XML не обеспечивает безопасность в этих веб-сервисах, но может использоваться для обеспечения безопасности веб-сервисов.

Для веб-сервисов существуют свои требования, которые определяют уровень безопасности.

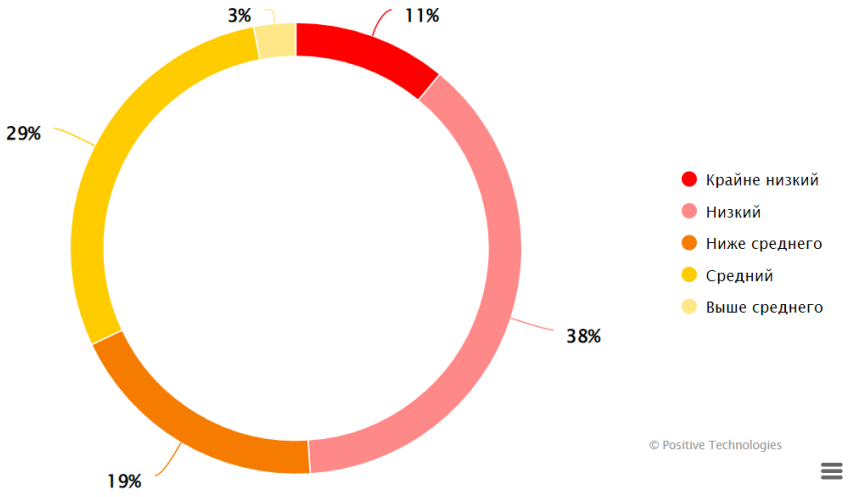

Рис. 1. Уровень защищенности веб-приложений((Positive Technologies)

Во-первых, конфиденциальность – свойство информации, благодаря которому она не разглашается лицам без санкционированного доступа и гарантирует полную безопасность ваших данных. Во-вторых, разрешение – полномочие на доступ к данным или информации. Для ее получения необходимо, чтобы отправитель был сертифицирован для отправки сообщения. В-третьих, целостность данных – также является свойством информации, согласно которому данные не подлежат изменению, малейшему редактированию, уничтожению, тем самым убеждаясь, что данные не изменялись никаким из доступных способов. В-четвертых, доказательство происхождения – это доказательство, идентифицирующее создателя данных. Это показатель, что сообщение было отправлено разрешенным лицом (автором) и не является массовой пересылкой с целью введения в заблуждения.

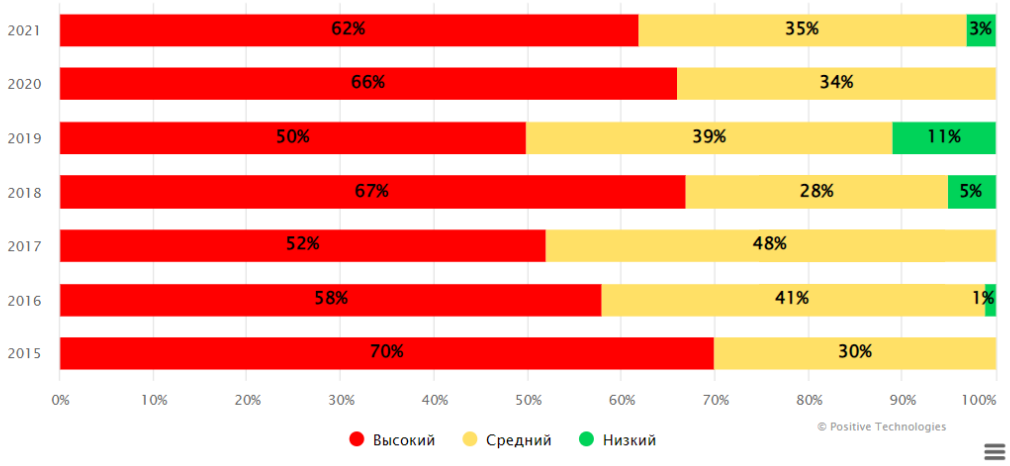

Рис. 2. Процентное соотношение уязвимостей веб-приложений за 2015–2021 г (Positive Technologies)

Злоумышленники могут получить конфиденциальную информацию людей, если у сайта есть проблемы с безопасностью, а по данным «Positive technologies» 81% веб-страниц имеют уязвимости. Чтобы заблаговременно урегулировать такие проблемы, необходимо на стадии архитектуры страниц программисту взаимодействовать со специалистом по информационной безопасности.

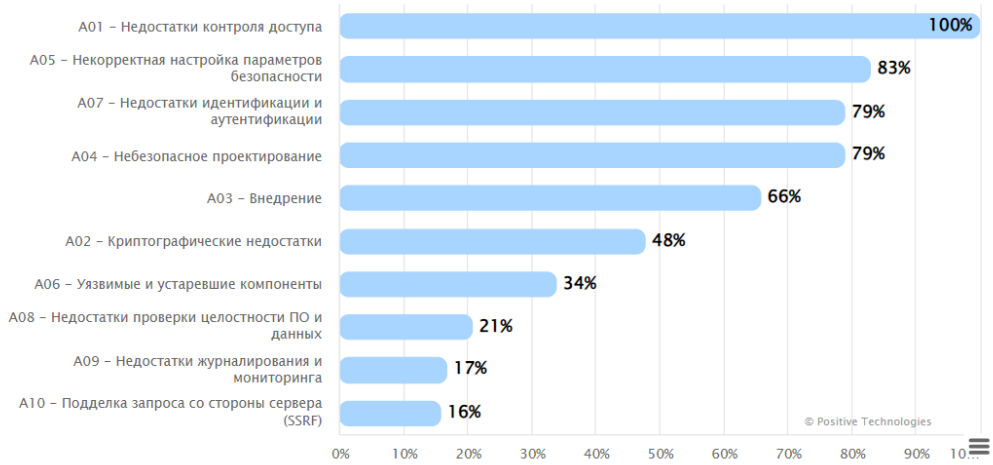

Рис. 3. Рейтинг уязвимостей (Positive Technologies)

Создание безопасного веб-сайта – трудоемкая, дорогостоящая и сложная задача для веб-разработчиков. Исследователи для выявления поглотителей веб-страниц для решения проблем безопасности, поскольку это помогает сократить время и деньги на защиту веб-приложений, внедряют различные модели прогнозирования веб-уязвимостей. Некоторые из хорошо известных веб-уязвимостей – SQL-инъекция, межсайтовый скриптинг (XSS) и подделка межсайтовых запросов (CSRF). Существующие модели прогнозирования уязвимостей используют различные методы машинного обучения для предотвращения уязвимых компонентов в веб-приложениях. Однако большинство из этих методов не могут противостоять всем веб-уязвимостям. Ежедневно появляется множество уязвимостей, поэтому на рынок выпускается множество инструментов для обнаружения этих уязвимостей. Пользователям необходимо знать об распространенных уязвимостях и возможных способах их использования, чтобы идентифицировать их и защитить себя от угроз и атак.

Библиографический список

1. *Золотарев, В. В.* Модель и алгоритм управления информационной безопасностью образовательной организации высшего образования с учетом требований управления на основе данных / В. В. Золотарев, М. А. Лапина // Прикаспийский журнал: управление и высокие технологии. – 2022. – №. 4 (60). – С. 107–118.

2. *Котляров, Д. В.* Исследование состязательных атак на нейронные сети распознавания образов / Д. В. Котляров, М. А. Лапина и др. // Труды Института системного программирования РАН. – 2023. – Том 35. – №. 2. – С. 35–48.

3. *Кудратиллоев, Н. А.* Взаимодействие web-сервера и web-приложение через web-socket / Н. А. Кудратиллоев, Б. А. Ахмедов // Экономика и социум. – 2021

4. *Лапина, М. А.* Особенности обеспечения безопасности персональных данных в сети Интернет / М. А. Лапина, А. П. Львова, В. А. Калашникова // Проблемы информационной безопасности. – 2016. – С. 57–62.

5. *Наскидашвили, К. А.* Информационная безопасность. Виды угроз информационной безопасности / К. А. Наскидашвили // Вестник студенческого научного общества ГОУ ВПО «Донецкий национальный университет». – 2020. – Том 1. – № 12. – С. 187–189.

6. *Низамутдинов, М. Ф.* Тактика защиты и нападения на web-приложения / М. Ф. Низамутдинов. – Санкт-Петербург, 2005.

7. *Николаева, М. О.* Информационная безопасность: современная картина проблемы информационной безопасности и защиты / М. О. Николаева // Мониторинг. Образование. Безопасность. – 2023. – Том 1. – № 1. – С. 51–57.

8. *Тузовский, А. Ф.* Проектирование и разработка web-приложений: учебное пособие для академического бакалавриата / А. Ф. Тузовский. – Москва, 2016

9. *Тузовский, А. Ф.* Проектирование и разработка web-приложений: учебное пособие / А. Ф. Тузовский. – 1-е изд. – Сер. 11 Университеты России

10. *Чипига, А. Ф.* Организационное обеспечение информационной безопасности / А. Ф. Чипига, М. А. Лапина. – 2009.

11. *Шерстюк, В. П.* Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения информационной / В. П. Шерстюк // Информационное общество. – 1999. – № 5. – С. 3–5.