**IT-Колледж “Сириус”**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**ДОКЛАД**

по дисциплине “Введение в специальность”

на тему “Информационная безопасность веб-приложений”

Выполнил:  
Студент группы

1.9.7.2  
Колкарева Даяна Андреевна

Принял:

Старший преподаватель  
Тенигин Альберт Андреевич

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IT-Колледж “Сириус”  
2022

# Оглавление

1. Введение
   1. Что такое информационная безопасность
   2. Что такое веб-приложения и как они работают
2. Безопасность приложений
   1. Методы взлома
   2. Методы защиты
3. Вывод
4. Список используемой литературы

# 1. Введение:

Понятия информационная безопасность и веб-приложения очень обширны сами по себе и для того, чтобы рассмотреть их вместе, для начала необходимо углубиться в каждый из них.

## A. Что такое информационная безопасность?

**Информационная безопасность** — совокупность способов предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты данных и информационной системы.

**Цель обеспечения информационной безопасности** – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения.

**Угрозы информационной безопасности** можно разделить на следующие:

* Естественные (катаклизмы, независящие от человека: пожары, ураганы, наводнение, удары молнии и т.д.).
* Искусственные, которые также делятся на:
  + непреднамеренные (совершаются людьми по неосторожности или незнанию);
  + преднамеренные (хакерские атаки, противоправные действия конкурентов, месть сотрудников и.т.п.).
* Внутренние (источники угрозы, которые находятся внутри системы).
* Внешние (источники угроз за пределами системы)

Так как угрозы могут по-разному воздействовать на систему, их делят на пассивные (те, которые не изменяют структуру и содержание информации) и активные (те, которые меняют структуру и содержание системы, например, применение специальных программ).

Наиболее опасны преднамеренные угрозы, которые все чаще пополняются новыми разновидностями, что связано, в первую очередь, с распространением электронных платежей.

Злоумышленники не стоят на месте, а ищут новые пути добраться до данных пользователей и компаний.

Чтобы обезопасить компанию от потери денежных средств и интеллектуальной собственности, необходимо уделять больше внимания информационной безопасности. Это возможно благодаря средствам защиты информации в лице передовых технологий.

## B. Что такое веб-приложения.

**Веб-приложение** — это программа, доступ к которой пользователь получает через интернет, то есть она не требует установки на устройство. Веб-приложение интерактивно и позволяет пользователям взаимодействовать с разными элементами: например, оставить заявку на покупку товара или прокомментировать пост друга.

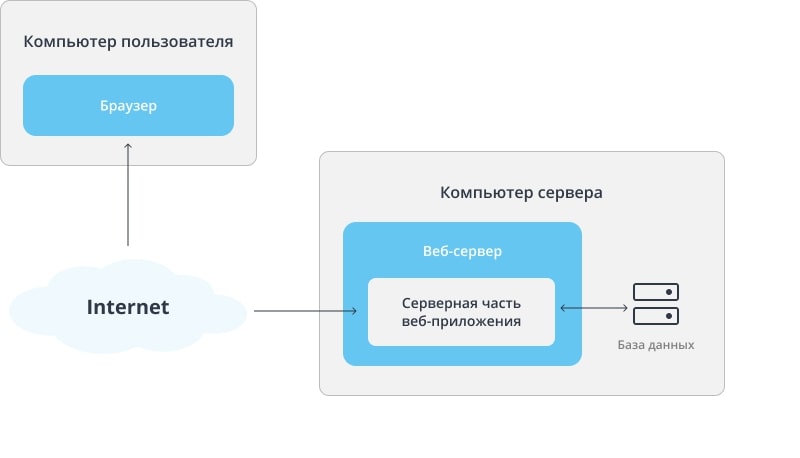
Веб-приложения можно классифицировать по-разному: в зависимости от их функционала и назначения.

Есть три основных шаблона построения сайтов:

* **MPA** (multi-page application): многостраничное приложение, которое отправляет запрос на сервер и полностью обновляет страницу, когда с ней совершается действие;
* **SPA** (single-page application): одностраничное приложение, содержащее HTML-страницу, которая динамически обновляется в зависимости от действий пользователя — без полной перезагрузки;
* **PWA** (progressive web application): приложение, которое пользователь устанавливает и может использовать в режиме офлайн.

Веб-приложения работают по принципу “клиент-сервер”. В данном случае клиент-браузер связывается с веб-сервером. Содержание приложения у пользователя формируется, когда он отправляет определенный запрос.

В зависимости от типа веб-приложения принципы их работы могут отличаться:

* Статические страницы. Пользователь делает запрос в браузере, а веб-сервер обрабатывает его и отправляет в ответ заранее созданную веб-страницу.
* Динамические страницы, напротив, не отправляются напрямую от веб-сервера браузеру. 

Сначала они направляются на сервер приложений, где считывается код и подбираются данные для формирования страницы. Только после этого страница отправляется на веб-сервер, а затем в браузер.

# 2. Безопасность веб-приложений

Как и несколько лет назад, веб-приложения по-прежнему остаются наиболее привлекательной мишенью для хакеров. Веб-приложения были и остаются первоочередной мишенью при взломе внешнего периметра компаний, как в тестированиях, так и в жизни.

Низкая безопасность веб-приложений обусловлена множеством факторов: от качества кода и выбранного языка программирования, до используемых настроек на стороне сервера. Большой проблемой является еще и то, что безопасность веб-приложений держится особняком относительно общей информационной безопасности. И к сожалению, больше половины ИБ подразделений в российских компаниях даже не подозревают, кто ответственен за внешний, официальный сайт компании, не говоря уже о том, кто занимается его безопасностью. Поэтому веб-приложения и становятся жертвами взлома так часто.

Проводимые в последнее время пентесты(тесты моделирующие атаки) подтверждают эти доводы. Так группы пентестеров используя уязвимости веб-приложений могли выполнять команды внутри операционной системы.

Большинство уязвимостей в веб-приложениях обнаруживаются в собственном коде, их называют уязвимостями нулевого дня (Так как у разработчиков было 0 дней на исправление). Это все потому, что уязвимости являются специфическими для каждого приложения и никогда не были известны ранее. Лучшая защита против этих атак — создание приложений с продуманной безопасностью. Разработчики должны понимать как работают те или иные виды атак и уметь продумывать защиту от них.

## A. Методы взлома

Обучение и информирование разработчиков об уязвимостях приложений является основной целью проекта Open Web Application Security Project (OWASP). Организация публикует списки десяти самых распространенных атак. Данный список обновляется каждые три года и последний раз обновлялся в 2021 году.

Команда IBM выделила самые распространенные виды атак основываясь на отчёты OWASP:

1. Инъекции

Инъекции позволяют атакующим изменить запрос бэкэнда команды через несанкционированный ввод данных пользователем. Проще говоря SQL инъекция - изменение SQL команды и использование её в произвольных целях.

2. Повреждение аутентификации и управление сеансами

Повреждение аутентификации - взлом системы входа на сайт. Может быть произведен как грубым брутфорсом (простым перебором паролей), так и более хитрыми методами.

3. Межсайтовый скриптинг

Межсайтовый скриптинг тип уязвимости, позволяющий злоумышленникам вставить JavaScript на страницах реальных сайтов. Поступая таким образом, они могут полностью изменить содержимое сайта, чтобы получить возможность отправить учетные данные пользователя на любой другой сервере.

4. Незащищенные прямые ссылки на объект

Изменяя имя файла в ссылке можно получить доступ к базе данных. Так при загрузке файла на сайт можно его взломать.

5. Неправильная настройка безопасности

Просто неверная настройка сервера.

6. Чувствительная экспозиция данных

Отсутствие шифрования данных во время перемещения и в состоянии покоя. Если веб-приложения, которые вы используете неправильно защищают конфиденциальные данные, такие как кредитные карты или данные аутентификации, злоумышленники могут украсть или изменить данные.

7. Отсутствие функции контроля уровня доступа

Вместо разделения уровня доступа пользователей (на простых юзеров и администраторов) стоит простая заглушка которая “прячет” информацию для админов.

8. Межсайтовая подделка запроса

Этот тип атаки используется в сочетании с социальными проектами. Атака направлена на посетителей веб-сайтов, использует недостатки протокола HTTP(протокол прикладного уровня передачи данных). Если жертва заходит на сайт, созданный злоумышленником, от её лица тайно отправляется запрос на другой сервер, осуществляющий некую вредоносную операцию.

9. Использования компонентов с уже известными уязвимостями

Эта категория включает в себя различные приложения, которые продолжают использовать компоненты даже после обнаружения уязвимости в них. Злоумышленники с легкостью могут использовать уязвимости устаревших компонентов на приложения, которые их используют, так как эти уязвимости были уже давно доказаны и опубликованы. Любой скрипт-кидди (взломщик пользующийся инструментами находящимися в общем доступе, не понимающий при этом механизм их действия) может произвести такой взлом.

10. Непроверенный переход и редирект

Эта категория уязвимостей используется в фишинговых атаках, в которых жертв обманом перенаправляют на вредоносный сайт. Злоумышленники могут манипулировать URL-ми реального сайта, чтобы перенаправить пользователя на нужную им страницу.

## B. Методы защиты

**Прямой способ защиты приложений** — межсетевой экран или брандмауэр. Для большего числа веб-приложений применяется сетевой экран **Web Application Firewall** (WAF).

Можно использовать приложения и фреймворки для автоматического обнаружения брешей в системе (такими пользуются белые хакеры):

* OpenVAS сканирует узлы сети на наличие уязвимостей и позволяет управлять уязвимостями.
* OWASP Xenotix XSS Exploit Framework сканирует ресурс на возможность эксплуатации XSS-уязвимостей.
* Approof от Positive Technologies проверяет конфигурацию веб-приложения, сканирует на наличие уязвимых компонентов и вредоносного кода.

Также можно (а на сегодняшний день обязательно) использовать **HTTPS** (HyperText Transfer Protocol Secure) - расширение к уже упомянутому HTTP для шифрования данных пользователей при их передаче в Интернете. HTTPS гарантирует целостность и конфиденциальность взаимодействия с сервером.

Обязательным при обеспечении безопасности является - **обновление ПО.** Так как с новыми обновлениями всегда приходят правки безопасности. А долгое использование одной и той же версии программного обеспечения является большим риском.

Ну и нельзя не упомянуть такие методы как: защита от SQL инъекций, нежелательного редиректа, шифрование паролей, контроль вводимых сообщений и загружаемых файлов, а также распределение прав доступа к тому или иному функционалу.

# 

# 3. Вывод

Таким образом - основным параметром обеспечения безопасности web-приложения является простая внимательность к деталям. При ответственном подходе к вопросу, своевременном обновлении ПО и регулярном проведении пентестов уровня защиты будет достаточно для отражения большей части атак.

# 4. Список используемой литературы

1.A.: <https://pirit.biz/reshenija/informacionnaja-bezopasnost>

1.B.: <https://www.azoft.ru/blog/web-apps/>

2.A.: <https://habr.com/ru/company/ua-hosting/blog/272205/>

2.B.: <https://tproger.ru/translations/webapp-security/>

Дополнительные источники:

* <https://habr.com/ru/post/128943/>
* <https://habr.com/ru/amp/post/654783/>
* <https://gardatech.ru/articles/smi/informatsionnaya-bezopasnost-web-prilozheniy-sovremennye-resheniya/>