Безопасность интернет-проекта
Основные угрозы
Инструменты безопасности в платформе

Сайты сегодня – набор запчастей

Большая часть современных сайтов - набор запчастей.

- **низкий уровень стандартной разработки**
- **отсутствие единой концепции безопасности**
- **несколько аккаунтов для одного пользователя**
- **не обновляемое ПО, особенно после модификации**

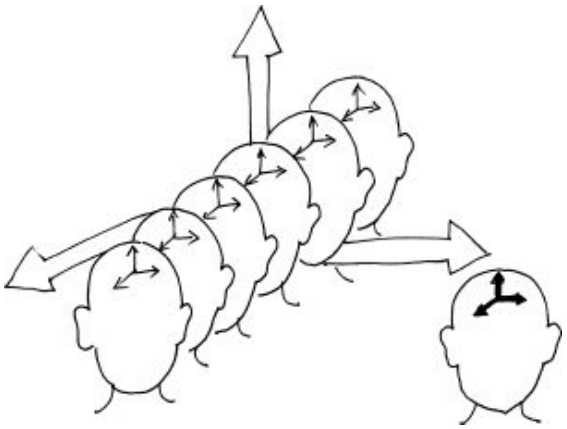
Разработчики интернет-приложений зачастую не задумываются о безопасности.

О безопасности сайта думают в последнюю очередь!

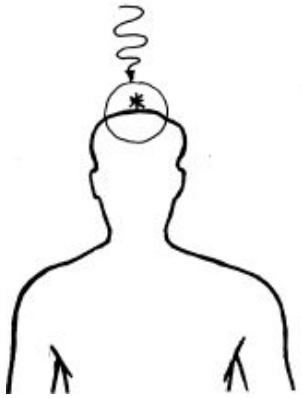
- индивидуальные разработчики думают о безопасности сайтов в самую последнюю очередь
- клиенты не готовы платить за безопасность интернет-проектов
- подразумевается, что разработчик должен этим заниматься, но у него не остается ни времени, ни бюджета

Психология хакера и разработчика

Психология хакера и разработчика принципиально отличаются:



Как мыслит разработчик…



… и как мыслит хакер

Ошибки бывают у всех, даже у профессиональных разработчиков.

Хостинг часто не защищен

- зачастую уровень администрирования серверов и хостинга *критически низкий*
- редко используются системы автоматического мониторинга

Категории хакеров

Студенты, ИТ специалисты начального уровня

- пробуют силы на первых попавшихся сайтах
- нет понимания последствий для жертвы
- нет осознания юридической личной ответственности
- редко зарабатывают на хакерстве как на бизнесе

Профессиональные специалисты

- прекрасный технический багаж
- никогда не светятся в тусовках, не кривляются
- делают только на заказ и только за деньги
- активно работают на службы безопасности крупных компаний

Обычный студент может пользоваться самыми банальными методами.

Комплекс проактивной защиты сайта

Проактивная защита – это комплекс технических и организационных мер, которые объединены общей концепцией безопасности и позволяют значительно расширить понятие защищенности и реакции веб-приложения на угрозы.

- **Аутентификация и система составных паролей**
- **Технология защиты сессии пользователя**
- **Проактивный фильтр защиты от атак**
- **Активная реакция на вторжение**
- **Контроль целостности системы**
- **Защита от фишинга**
- **Шифрование данных**

Web Application Fire Wall

Основан на анализе и фильтрации всех данных, поступающих от пользователей через переменные и куки.

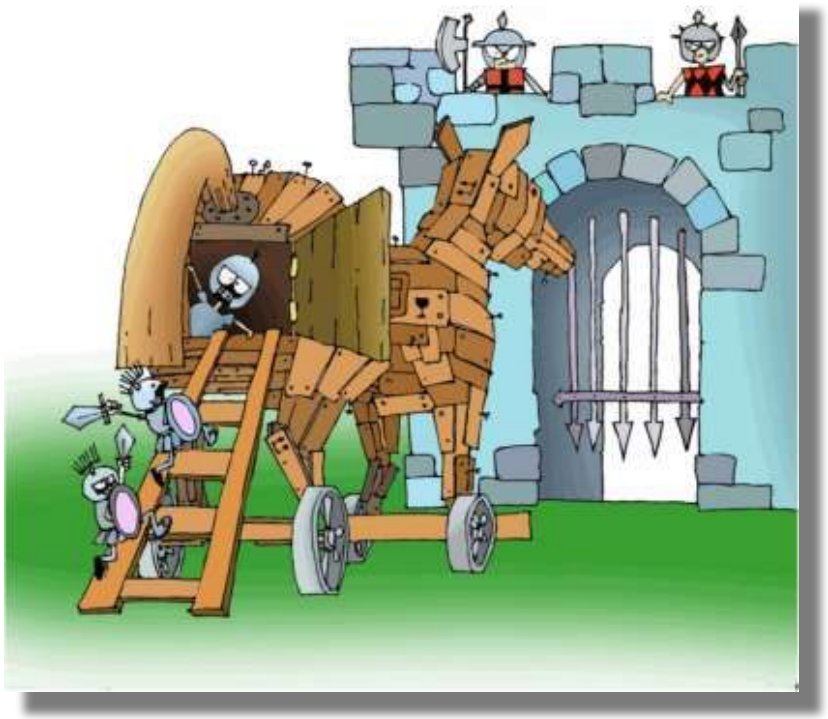
- XSS - cross site scripting (CSS)
- SQL инъекции
- часть атак, связанных с обходом каталогов (в том числе PHP source code injection)

- Экранирует приложение от наиболее активно используемых атак
- Фиксирует попытки атаки в журнале
- Информирует администратора о случаях вторжения

Способы взлома веб-приложений

Атаки непосредственно на веб-приложения:

- SQL инъекция
- Внедрение в имя файла
- Внедрение в system и т.п.
- Подбор реквизитов доступа
- Логические ошибки



Атаки на клиентов веб-приложения:

- XSS
- CSRF
- Социальная инженерия
- Фишинг

Обычные ДОС атаки, ДДОС атаки

Сайты – основной способ распространения вирусов

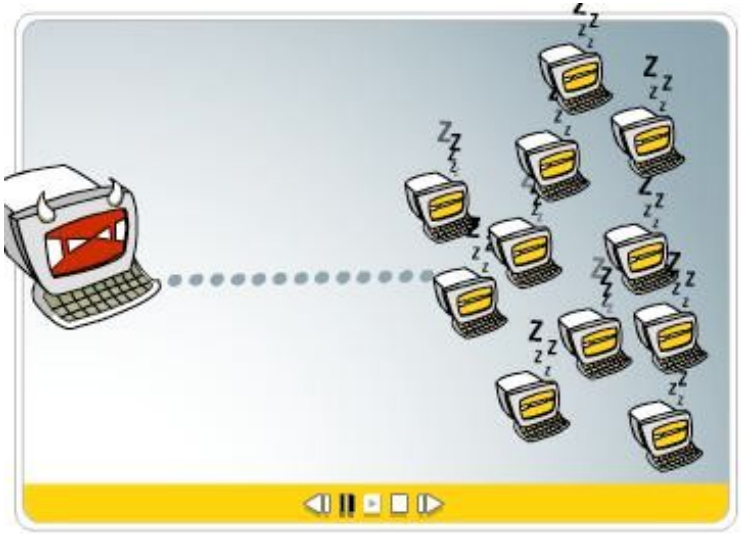
Способы распространения вирусов через веб:

iframe и JavaScript

На самом деле, способ даже один, так как все JavaScript, как правило в конце концов «рисуют» iframe.

Бот-сети и трояны

Ботнет (бот-сеть) — это некоторое количество компьютеров (100 - 100000 >) - ботов - подключенных к сети интернет, и подчиняющихся командам центра управления.



Бот (или компьютер-зомби) — это компьютер, на котором установлено вредоносное программное обеспечение — троян, имеющий функционал БОТ-клиента.

Строго говоря, троян может быть и просто «трояном», не делающим компьютер частью зомби сети. Тем не менее, и способы заражения и опасность от заражения обычных троянов, и троянов-бот-клиентов совершенно одинаковые.

Варианты установки троянов на компьютер

- уязвимости в системном ПО
- через веб-сайты
- запуск исполняемого файла с вирусом
- санкционированный доступ к компьютеру (крайне редко)
- подбор слабого административного пароля (редко)
- ручной взлом

Механизмы защиты от троянов

- регулярно обновлять системное ПО
- регулярно обновлять все прикладное ПО
- с подозрением относится ко всем исполняемым файлам
- не предоставлять никому доступа к компьютеру
- использовать сложные пароли для все аккаунтов удаленного доступа
- уделять внимание защите всех компонентов системы

Веб-антивирус

В платформу «1С-Битрикс» встроена система противодействия заражениям сайтов, которая:

- выявляет в html-коде потенциально опасные участки
- определяет 90% заражений сайта
- «белый список» для отсечения ложно положительных срабатываний

Веб-антивирус ни в коем случае не является заменой персонального антивируса!

Аутентификация и система одноразовых паролей OTP

Надежная аутентификация пользователя с использованием одноразовых паролей (OTP)

Система одноразовых паролей дополняет стандартную систему авторизации и позволяет значительно усилить систему безопасности интернет-проекта.

При авторизации на сайте пользователь в дополнение к паролю дописывает одноразовый пароль.

eToken
YOUR KEY TO eSECURITY

Инструменты безопасности в «1С-Битрикс»

- Аутентификация и система составных паролей
- Технология защиты сессии пользователя
- Проактивный фильтр защиты от атак
- Активная реакция на вторжение
- Контроль целостности системы
- Защита от фишинга
- Шифрование данных
- Групповые политики безопасности
- Защита при регистрации и авторизации
- Журнал событий
- Веб-антивирус