Skillbox

Меры защиты веб-приложений

Общая тенденция

Уровень защищенности большинства веб-приложений продолжает оставаться низким. В каждом втором сайте присутствуют уязвимости высокого уровня риска.

Однако с каждым годом постепенно снижается доля веб-приложений, содержащих критически опасные уязвимости. Снижается число уязвимостей, которое в среднем приходится на одно приложение.

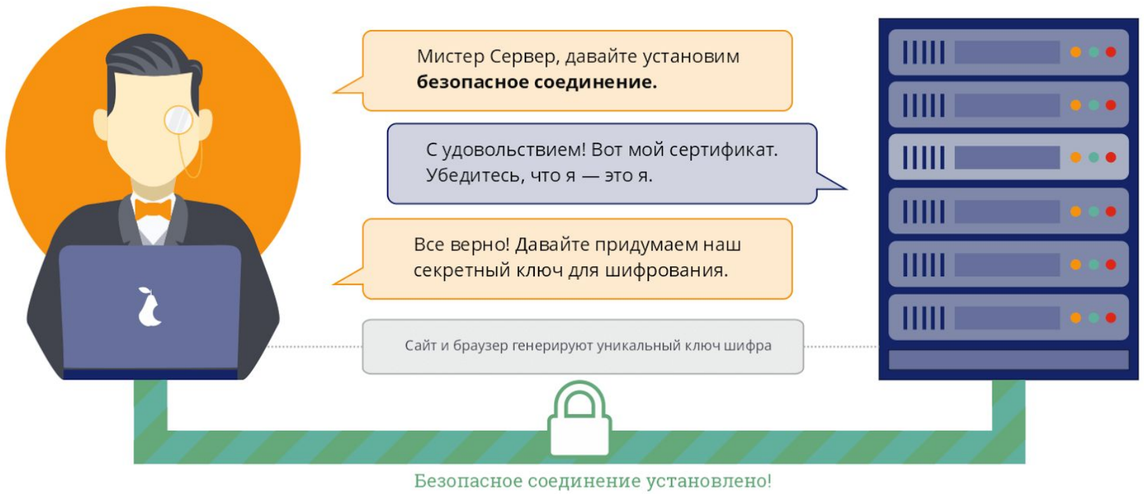
Компании начинают серьезней относиться к защите веб-приложений, причем не только публичных, но и используемых для внутренних нужд.

2 основных правила .для достижения и поддержания высокого уровня защищенности веб-приложений:

- исправлять выявленные уязвимости как можно раньше
- автоматизировать процессы, где это возможно

Использование HTTPS

HTTPS (secure) – расширение HTTP, которое поддерживает шифрование и защищает данные пользователей при передаче в Интернете.



Своевременное обновление ПО

Обновление операционной системы

Обновление инфраструктуры передачи данных

Обновление библиотек

Защита от SQL-инъекций

1. Не помещать данные в БД без обработки
   - все числовые параметры должны быть приведены к нужному типу
   - все остальные параметры должны быть обработаны функцией mysql_real_escape_string() и заключены в кавычки.
2. Не помещать в запрос управляющие структуры и идентификаторы, введенные пользователем, а заранее прописывать в скрипте список возможных вариантов, и выбирать только из них.

CSP – политика безопасности содержимого

1. Обращать внимание на функции ввода данных пользователем и их обработку
    - element.setAttribute и element.textContent
    - шаблонизаторы
2. Хеширование паролей
3. Валидация: ограничение на минимальную длину пароля, проверка совпадения вводных данных
4. Контроль процесса загрузки файлов
    - запретить исполнение загружаемых файлов пользователей
    - изменять разрешения (0666)

Спасибо за внимание!