1 Я расскажу про безопасность в Вебе. Open Web Application Security Project – некоммерческая организация которая составляет топы ошибок безопасности, в данности и OWASP Top Ten, пять открывающих пунктов из которого мы разберем.

Сразу оговорюсь что при подготовки я ставил задачу только ознакомить, и обратить на это ваше внимание. Первая ссылка в гугле по названию уязвимости приведет вас на сайт owasp.org с подробным описанием проблемы, и вариантами их решения.

2 Первоначально давайте обсудим почему появилась потребность в веб-безопасности.

- Человеческий фактор: те люди ошибались, ошибаются и будут ошибаться

- Политика разработки: шлеп шлеп и в продакшен. Быстро, дешево, много.

- Качество подготовки молодых сотрудников. Им важно уметь писать код, а не программировать и разбираться в нюансах

- Сложность Веба. Тут как и везде, есть некоторые достаточно специфичные темы, на которые никто не обращает внимание

10 Подделка запроса на стороне сервера

Всякий раз когда веб-приложение извлекает удаленный ресурс без проверки предоставленного пользователем URL-адреса, или его части. Это позволяет злоумышленнику получить доступ к сервисам(внутренним/внешним), ранее которые ему были недоступны, или могут быть нежелательны нам.

Для недопущения такой ситуации, стоит:

\* Очищать и проверять все входные данные клиента

\* Использовать порт и пункт назначения с положительным списком разрешений.

\* Не отправлять необработанные ответы клиентам.

9 Ошибки логирования и мониторинга

Например когда у нас

* Нет регистрации входа в систему, ограничений неудачных впопыток

те если ктото долго к нас стучится, то может он не знает логина, или пароля. Нам нужно ограничивать попытки входа – по количеству/или по времени. Отправлять емейл пользовотелю, что ктото пытается зайти

* Нет понятного логирования ошибок и предупреждений
* Нет предупреждений об атаках в реальном времени
* Транзакции с высокой стоимостью
* Конфиденциальные данные в логах

8 Нарушение целостности данных и программного обеспечения

* Использование ПО из ненадежный источников
* Небезопасное ПО для CI/CD открывающие возможность несанкционированного доступа
* Не отслеживаемое автоматическое обновление, через которое злоумышленники могут загружать свои пакеты

7 Ошибки идентификации и аутентификации

* Отсутствует защита от перебора – опять таки внедряем ограничения
* Возможность использовать старые/популярные пароли

Есть целые списки, 1000, 10 000 популярных паролей, мы должны даже не предоставлять возможности их использовать, также и с количеством символов.

* Слабая процедура восстановления пароля

Использовать для восстановления пароля три вопроса:

Фамилию матери, улица на которой вы выросли, номер вашей машины – НЕ НАДО

* Слабое хэширование и шифрование
* Отсутствие многофакторной аунтификации
* Нет аннулирования сеансов

6. Уязвимые и устаревшие компоненты

* Устаревшее/незащищенное ПО
* Недостаточная осведомленность о версиях компонентов
* Отсутствует проверка совместимости обновленных или исправленных библиотек
* Нет процедуры контроля внедрения изменений