Основные типы атак на web-приложения и системы электронной комерции

Рейтинги уязвимости:

* Owasp top-10
* Cwe.mitre.org top-25

SQL-инъекция

where Passport = ‘passport’ OR ‘1’=’1’

union

Межсайтовый скриптинг (XSS)

Небезопасные ссылки на объекты

Файл, ключ из БД (download.php?file=file.txt заменяем на download.php?file=database.db)

Небезопасная конфигурация

Пароль по умолчанию, не отключенные детализированные логи в «продакшен», вывод стека сообщений ошибки.

Незащищённость критичных данных

Хранение не шифрованных паролей, не используется шифрованное соединение, отсутствие шифрования критичной информации, открытая передача сессионных данных, ключи шифрования хранятся с данными.

Отсутствия функций контроля доступа

Межсайтовая подделка запросов (CSFR)

Подмена строки на новостном ресурсе. При одновременной авторизации в банковском аккаунте возможен перевод на счёт злоумышленника. (Не использовать get метод, а использовать post)

Использование компонентов с известными уязвимостями.

OpenSSL Heartbeels (?)

Непроверенные переадресации и пересылки

Манипулирование входными данными

Проверяйте данные от внешних сервисов (подмена сумма оплаты). Проверка подписи, от внешней системы.

Какая защита?

* Технические решения (web application firewall)
* Сканеры уязвимости (AppScan. Nessus, OpenVAS)
* Подписка на тематические рассылки. Например, www.cvedetails.com

Прогон решения через организацию или эксперта для определения «взломоустойчивости» системы.