

Аудит безопасности (Кривошей)

1. **Защита от xss** — формат .jsp совместно со вставками java обеспечивает встроенное экранирование вставляемых данных, поэтому xss-уязвимости отсутствуют
2. **Защита от Information Disclosure** — пользователям отображаются только ошибки, которые заранее подготовлены, без уточнения каких-либо персональных данных
3. **Защита от SQL Injection** — hibernate при создании SQL запросов всегда использует Prepared Statements, которые созданы для защиты от sql-инъекций
4. **Защита от CSRF** — во все формы для post/put запросов сделаны вставки специальных csrf-токенов. За их работу отвечает класс CSRFTokenUtil
5. **Защита от Include и Upload** уязвимости — нет работы с файлами, поэтому такие уязвимости в целом отсутствуют
6. Для хеширования паролей используется алгоритм **SHA-256**