

XSS:

1. Установил заголовок Content-Type
2. Добавил HTTP-заголовки безопасности Information

Disclosure:

1. Отключил вывод ошибок в production
2. Унифицированные сообщения об ошибках

SQL Injection:

1. Валидация входных данных
2. Использование подготовленных выражений

CSRF:

1. Добавил CSRF-токена
2. Проверка этого токена

Include и Upload:

1. Валидация MIME-типов входящих файлов
2. Ограничение размера входящих файлов