Отчет 27 января

1. **XSS (Cross-Site Scripting)**
   - **Код:** Вывод `$_GET['username']` без экранирования
   - **Категория OWASP:** A7:2017 (Cross-Site Scripting)
   - **Описание:** Возможно внедрение жс кода через параметр `username`, что приведет к выполнению стороннего скрипта в браузере
2. **SQL-инъекция**
   - **Код:** Прямая подстановка `$_POST['username']` и `$_POST['password']` в SQL-запрос
   - **Категория OWASP:** A1:2017 (Injection)
   - **Описание:** Возможна подстановка скл скрипта вместо этих значений, которое может выполнить недопустимые для изначального запроса действия (вывести чувствительные данные, снести базу и прочее)
3. **Выполнение команд**
   - **Код:** Использование `shell_exec($_GET['cmd'])`
   - **Категория OWASP:** A1:2017 (Injection)
   - **Описание:** Позволяет выполнить любую команду на сервере через параметр `cmd`
4. **Небезопасные куки**
   - **Код:** Фиксированное значение `session_id` без флагов `HttpOnly` и `Secure`
   - **Категория OWASP:** A3:2017 (Sensitive Data Exposure)
   - **Описание:** Куки могут быть перехвачены или изменены из-за чего может быть слиты токены сессии и тд
5. **Небезопасная загрузка файлов**
   - **Код:** Использование оригинального имени файла и отсутствие проверок
   - **Категория OWASP:** A6:2017 (Security Misconfiguration)

- **Описание:** Возможна загрузка вредоносных файлов (например, .php) на сервер