



МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное образовательное учреждение
высшего образования**

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт комплексной безопасности и специального приборостроения

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

ОТЧЕТ

по лабораторным работам № 8

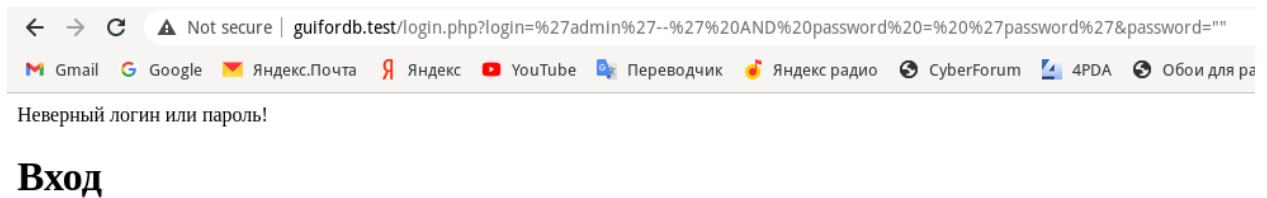
по теме: «SQL-инъекции в созданную базу данных»

по дисциплине: «Управление данными»

Выполнили: студенты 3 курса,
группы БСБО-04-18,
Канаев М.А., Ковырев А.Р.,
Одинцов А.Н., Мусаев А.М.
Проверил: преп. Котилевец И. Д.

Москва – 2020 год

1. Классическая SQL-инъекция.



← → ↻ Not secure | guifordb.test/login.php?login=%27admin%27--%27%20AND%20password%20=%20%27password%27&password=""

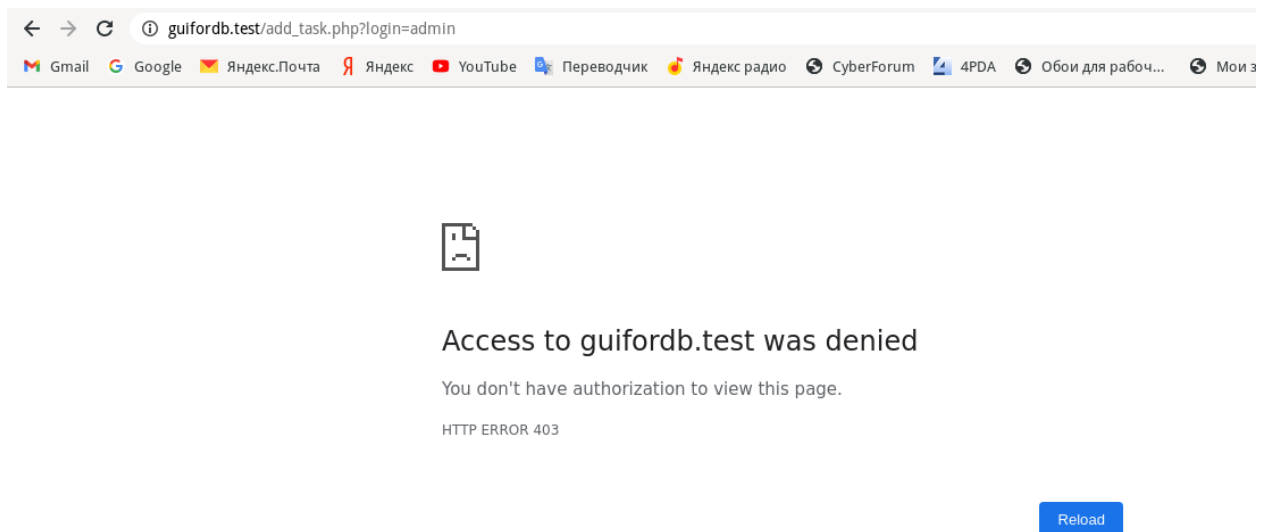
Gmail Google Яндекс.Почта Яндекс YouTube Переводчик Яндекс радио CyberForum 4PDA Обои для ра

Неверный логин или пароль!

Вход

Попытка SQL-инъекции с подменой логина на admin и отсечением пароля методом вставки комментария в поле ввода.

2. Классическая SQL-инъекция.



Попытка рядового пользователя/злоумышленника войти в раздел добавления задач, который доступен только для менеджеров. Передача данных осуществляется с помощью GET-запроса в адресной строке. Акт взлома предотвращается системой безопасности сервера. Сервер возвращает ошибку 403.

3. Error-based (получить информацию о базе, таблицах и данных на основе выводимого текста ошибки СУБД).

Неверный логин или пароль!

Вход

""#\$%asdf□□qw123412`4"\t\n\
.....
<input type="button" value="Войти"/>

Попытка создания ошибки на стороне сервера путем ввода недопустимых символов, в частности кавычек, двойных кавычек, знака решетки, знака доллара, знака процентов, символов utf-16, \t, \n и других.

Вывод: все попытки взлома обернулись неудачей. Благодаря хорошо построенной архитектуре приложения ни одна SQL-инъекция не прошла.