Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образoвания

«Владимирский государственный университет

имени Александра Григорьевича и Николая Григорьевича Столетовых» (ВлГУ)

Кафедра **Информатики и защиты информации**

Отчет по лабораторной работе №1.

По дисциплине: «Защищенные информационные системы ».

Выполнил:

Окунев В ИСБ-119.

Преподаватель:

Мишин Д.В

Владимир 2023

Задание:

Программа должна моделировать процессы регистрации и идентификации/аутентификации пользователя с salting passwords.

Программа должна демонстрировать значения UserID, пароль, хеш-значение пароля с солью и без, соль и т.д. на различных этапах регистрации и идентификации/аутентификации.

Пояснить, как salting passwords защищает от атак полного перебора (брутфорс) или атак с помощью предварительно построенных радужных таблиц?

# Описание заданного протокола схематической записью

К - клиент, С - сервер

1. К -> С: логин, пароль
2. C -> БД: логин пароль

Цикл 1:

1. Клиент отправляет свои логин и пароль серверу.
2. Выбирает вариант дальнейших действий (вход в систему, либо регистрация нового пользователя, если права доступа позволяют)

Цикл 2:

1. Сервер отправляет запрос к базе данных на определение наличия такого пользователя с таким паролем и ролью в ней
2. Если получает подтверждение - пускает в систему этого пользователя с его ролью, если нет - не пускает
3. Если пользователь желает зарегистрировать нового пользователя и это позволяет его роль - сервер предоставляет такую возможность.
4. При регистрации новго пользователя необходимо указать его логин, пароль и роль в системе. Если все введено корректно, новый пользователь будет зарегистрирован и записан в базу данных.

# Табличное представление протокола.

Предварительный этап (идентификация, аутентификация)

|  |  |  |  |
| --- | --- | --- | --- |
| К | | С | |
| логин | -> | | Запрос в БД |
| пароль |
|  |  | |  |
|  |  | |  |