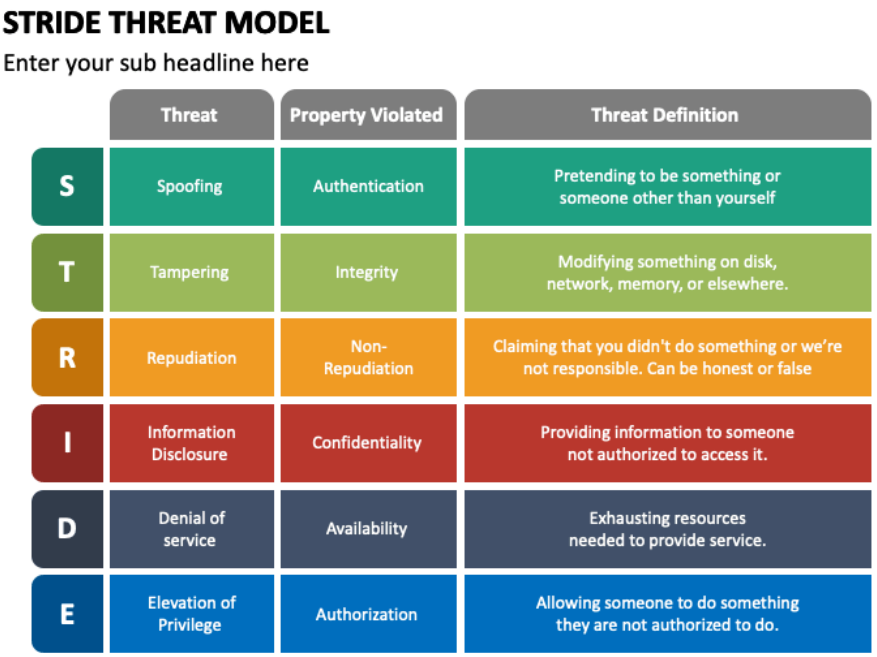
Форма входа и регистрации

Участники **Команды 1**:

1. Козак Борис P3421
2. Круглов Егор P3424
3. Крохин Роман P3424
4. Колмаков Дмитрий P3431
5. Барсуков Максим P3415
6. Суворова Елизавета P3423
7. Бушмелев Костя P3318

Угрозы

1. Подбор пароля от admin - Elevation of Privilege
2. SQL-инъекция в поле логина/пароля, чтобы получить всю таблицу пользователей - Elevation Of Privilege
3. Перехват кредов по незащищенному соединению - Information Disclosure
4. Отказ в обслуживании (Denial of Service) - Массовая отправка запросов на вход/регистрацию перегружает систему / Злоумышленник запускает бота, который массово регистрирует фейковые аккаунты, перегружая сервер и БД, что мешает легитимным пользователям
5. **Подмена пользователя (Spoofing) - Злоумышленник регистрируется в системе под чужим именем (например, используя почту или данные другого человека), чтобы в дальнейшем действовать от его лица, нанося репутационный вред или получая несанкционированный доступ к ресурсам, привязанным к email (например, сброс пароля на других сайтах).**



DREAD

Критерий	Оценка (1-3)	Обоснование
Damage	3	identity theft с серьёзными последствиями
Reproducibility	2	Атака несложна в повторении при типовых настройках регистрации, но требует дополнительных умений от злоумышленника
Exploitability	3	Достаточно знать только базовую информацию о жертве при хороших навыках СИ
Affected Users	2	Риск затрагивает значимую долю пользователей и сервисов
Discoverability	3	Точки входа публичны, а векторы широко опубликованы и обсуждаются в индустрии

(3 + 2 + 3 + 2 + 3) / 5 = 13 / 5 = 2.6 -> Высокий риск

Меры защиты

1. Мониторинг подозрительной активности. Отслеживание массовых регистраций. Система предупреждений при попытке использовать «одноразовые почты».
2. Ввести проверку биометрии (документов) пользователя при регистрации