Тема: «Создание системы анализа защищённости веб-приложений на основе моделирования сетевых атак (без DoS и DDoS)»

Как заказчик проекта, я хочу получить инструмент, который поможет выявлять уязвимости в веб-приложениях до того, как это сделают злоумышленники. Мне нужна система, которая автоматически проверяет безопасность кода и инфраструктуры, но при этом не воздействует на реальные рабочие сервисы.

Что именно я хочу от системы:

Чтобы она могла самостоятельно анализировать мои веб-приложения и сообщать о найденных проблемах. Я хочу, чтобы система умела:

- моделировать типовые сетевые атаки (например, SQL-инъекции, XSS, CSRF, brute-force, перехват сессий, ошибки конфигурации);
- выполнять все проверки в безопасной тестовой среде, без риска для продуктивных систем;
- проводить анализ кода, логов и сетевого трафика, чтобы находить потенциальные угрозы на разных уровнях.

Мне важно, чтобы она не просто показывала найденные уязвимости, а формировала понятные отчёты — с описанием проблемы, уровнем её опасности и рекомендациями, как исправить.
Хочу, чтобы отчёты можно было получать в разных форматах — PDF, HTML или JSON, чтобы было удобно и смотреть, и интегрировать в другие системы безопасности.

Хочу видеть всё в единой веб-панели с разделением ролей:

- **Администратор** управляет пользователями и настройками системы;
- **Аналитик** запускает проверки и формирует отчёты;
- **Разработчик** использует результаты для исправления уязвимостей.

Также нужно, чтобы была база данных уязвимостей и сценариев атак — с поиском, фильтрацией и регулярным обновлением.

Чтобы решение было надёжным и современным

Для меня важно, чтобы система:

- работала под Windows и Linux;
- могла интегрироваться с GitLab;
- использовала современные технологии (Python для сервера, React для клиента, PostgreSQL или SQLite для хранения данных);

- взаимодействовала через REST API.

Система должна сохранять данные при сбоях, вести журнал действий, делать резервные копии и продолжать работать даже при ошибках моделирования. Она не должна перегружать сеть или как-то влиять на внешние ресурсы — всё должно быть полностью изолировано.

Хочу, чтобы система включала встроенный краулер — автоматический сканер веб-страниц, который безопасно обходит ссылки веб-приложения и собирает информацию о структуре сайта для обнаружения потенциальных точек входа и уязвимостей.

Требования к краулеру:

• Настраиваемая глубина обхода и скорость для предотвращения перегрузки среды.

• Поддержка аутентификации, возможность работы с защищёнными частями приложения при наличии тестовых учётных данных.

• Сохранение результатов обхода (карта сайта, список конечных точек, обнаруженные формы и параметры) в базе данных уязвимостей.

• Возможность повторного запуска с учётом изменений и история сканов для аудита.

Я хочу получить безопасный, надёжный и понятный инструмент, который будет автоматически искать уязвимости, моделировать сетевые атаки и помогать повышать уровень информационной безопасности моих веб-приложений.