# Cloud-ru

# Уметалиев Алишер. Проверочное задание.

Расскажите, с какими задачами в направлении безопасной разработки вы сталкивались?

Начало моей карьеры пришлось еще на старшие классы школы, когда я начал интересоваться программированием на C++ и сразу нацелился на олимпиадную деятельность. К сожалению или к счастью, длилась она не так долго, так как я сменил фокус на изучение ОС Linux. Именно тогда я понял, что кибербезопасность – это то, что мне нужно.  
За последний год я успел стать участником ТОП-1 CTF команды Казахстана «FR13NDS TEAM», пройти стажировку и поработать сразу на нескольких должностях в сфере ИБ. Сначала я подал заявку на стажировку в Positive Technologies. Попав туда, я старался максимально быстро и качественно усвоить весь материал со стороны компании и смог перенять много полезной информации по администрированию ОС и проведению качественного пентеста внешнего контура сети. Затем, мне дали оффер на позицию Security Operation Center. Здесь я на практике узнал про принципы построения процессов мониторинга и реагирования, а также про конфигурации сети для бесперебойной отправки логов. Здесь же, мне довелось участвовать в реальных пентестах на крупные компании нашей страны, и отвечать за их организацию.

Если вам приходилось проводить security code review или моделирование угроз, расскажите, как это было?

Да, мне не раз приходилось участвовать в моделировании угроз и code review. Для моделирования угроз, чаще всего использовался всеми признанный подход, который охватывает шаги, начиная от идентификации активов и поиска потенциальных угроз, заканчивая реализацией рекомендованных мер и мониторингом эффективности. На протяжении этого цикла мне не раз было необходимо проверить код нынешней конфигурации сервиса для определения потенциальных уязвимостей.

Если у вас был опыт поиска уязвимостей, расскажите, как это было?

Поиск уязвимостей осуществлялся в формате как Black-box, так и White-Box. Здесь, я на реальных проектах оттачивал базовые аспекты и более глубокие нюансы всей цепи Kill Chain, начиная от разведки, используя разнообразные инструменты, такие как Nuclei и Acunetix, заканчивая полным получением доступа к инфраструктуре объекта через мисконфигурацию внутреннего сегмента сети. Также, в некоторых случаях клиенты предоставляли source-коды своих сервисов, для более глубокого поиска потенциальных угроз безопасности. Это помогло мне понять детали проверки source-кода для выявления слабых мест в аспектах безопасности и эффективности, используя ручное тестирование, а также прибегая и к автоматическим инструментам. К тому же я постоянно участвую в международных CTF-турнирах, где узнаю о новых трендах в сфере, и учусь эксплуатировать новые уязвимости.

Почему вы хотите участвовать в стажировке?

С давних пор хотелось вновь вернуться к более крепкой связи с программированием, а также внедрением в полученный код элементов, чтобы сделать итоговый продукт как можно более безопасным и удобным для пользователей. Поэтому, сильное желание поучаствовать в стажировке от Cloud.ru обусловлено и сменой деятельности, как нынешнего SoC аналитика на нечто более динамичное и интересное. Хочется узнать больше о безопасности контейнеров, а также о том, какие способы проверки и эксплуатации существуют. Также хочется укрепить скиллы в программировании, особенно в Go и JS-подобных языках. Было бы очень познавательно окунуться в такую профессиональную среду компании Cloud.ru, где каждый точно знает свое дело, и надеюсь, рад прийти на помощь :)