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

Начиная свой путь в сфере информационной безопасности и программирования, я сталкивался с различными задачами безопасной разработки, даже не осознавая этого на начальных этапах. Развивая свои навыки в программировании еще будучи школьником, я косвенно затронул тему **SAST (Static Application Security Testing)**, когда задавался вопросом о том, как злоумышленник может атаковать мой сервис и неправомерно получить доступ к информации. Это подвигло меня на изучение актуальных угроз хотя бы на уровне **OWASP Top 10** для более надежного санитайзинга ввода пользователя. В ходе обучения я познакомился с различными тактиками и подходами, что позволило мне **научиться выявлять слабые места в фильтрациях и способы их обхода** для выполнения различных атак, таких как **инъекции, скриптинг (XSS), брутфорс, IDOR, XXE** и так далее. Эти знания существенно повысили уровень безопасности моего кода и дали возможность анализировать код моих друзей и сокомандников, а также смотреть на код других разработчиков для выявления потенциальных угроз или наоборот, вдохновляться подходами более опытных специалистов. Кроме того, опыт в разработке помог мне изучить **паттерны проектирования и ООП**, что также играет большую роль в написании и идентификации **качественного и безопасного** кода.

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

В процессе обучения в университете на факультете кибербезопасности и участия в CTF-олимпиадах я столкнулся с **DAST (Dynamic Application Security Testing)**, особенно во время **имитации пентестов в контексте олимпиад**. Этот опыт очень сильно помог **при участии в боевых проектах**, уже работая в компании. Не менее важно, подготовка к сертификации (OSED) побудила меня углубиться в архитектуру компьютеров, устройство памяти и **reverse engineering**, что дало **понимание на уровне процессов и техник бинарной эксплуатации**. Этот опыт не только расширил мои знания в области безопасной разработки, но и научил меня важности комплексного подхода к анализу безопасности, включая **security code review и моделирование угроз**, что позволяет выявлять и устранять потенциальные уязвимости на ранних этапах разработки. Также хочу отметить увлеченность **криптографией**, что нередко помогает обнаружить уязвимые алгоритмы, которые интересно разгадывать и подходить к задаче под другим углом, чтобы достичь успеха при тестировании на защищенность :).

Если у вас был опыт поиска уязвимостей, расскажите, как это было?  
 Мой опыт поиска уязвимостей, что неудивительно, начался с CTF-олимпиад, где приходилось тестировать разные сервисы, как клиентские, так и веб, перебирая различные вводные данные (если есть куда вводить) и проверять базовые пейлоуды, чтобы разобраться, как что работает. Поначалу это было сложно делать всё руками, но позже это дало свои плоды. Также особое внимание хочу обратить на категорию reverse, которая привязала привычку углублённо разбираться в ходе компиляции и логике кода, что дало хорошую базу для полноценного пентеста. Со временем, переходя к боевым проектам, я перешёл к более систематизированному подходу, используя подход Cyber Kill Chain и различные инструменты по типу Nessus и Acunetix, а также Burp Suite для поиска базовых уязвимостей. Несмотря на очевидную иррациональность полной ручной проверки в аудите крупных проектов, на личном опыте убедился, что начиная с самых азов и проделывая процесс вручную, можно не только глубже понять уязвимости и техники их эксплуатации, но и разрабатывать персонализированные рекомендации, так как даже передовые сканеры пока что не способны составить точное решение существующей уязвимости для клиента :).

Почему вы хотите участвовать в стажировке?

Огромное желание пройти стажировку от Cloud.ru обусловлено рвением использовать свои навыки и специализацию вне нынешнего контекста (как SOC аналитика) на нечто более динамичное и интересное, а именно в безопасной разработке, так как я начиная со школы очень увлекался программированием, а позже кибербезопасностью. Хочется узнать больше о безопасности контейнеров, виртуализации, а также о том, какие ещё способы проверки и эксплуатации существуют. Также хочется укрепить скиллы в программировании, особенно в Go и JS подобных языках. Более того, очень хотелось бы поучиться у специалистов своего дела и внести вклад в международную компанию, параллельно развиваясь и изучая данное направление всё глубже и глубже. Также, буду очень рад потенциальной релокации при необходимости. Заряжен на успех и работу в супер-команде Cloud․ru!