г. Нур-Султан, пр. Мангилик ел 19/2-93
+7 (7172) 47-84-13, 87076028997
info@cybersec.kz

КОММЕРЧЕСКОЕ ПРЕДЛОЖЕНИЕ

ОЮЛ «Центр анализа и расследования кибер атак» (далее - ЦАРКА) - одна из ведущих организаций в области информационной безопасности в Центральной Азии. Организация была образована в 2015 году и за время своего существования завоевала признание специалистов по информационной безопасности по всему миру. Первый частный CERT в Казахстане.

Организация предоставляет широкий спектр услуг в области оценки защищенности, в том числе проведение аудитов ИБ и тестирований на проникновение, анализ защищенности банковских систем и бизнес-приложений, веб приложений, информационных инфраструктур.

Более 50 экспертов. Эксперты ЦАРКА обладают сертификатами OSCP, OSWP, CHFI, CISA, CCNA Security, ISO/IEC 27001—2015, OSCE и CEH и регулярно принимают участие в международных конференциях, таких как PHDays, ZeroNights, Инфофорум, КодИБ.

Эксперты организации являются авторами публикаций на таких ресурсах как журнал Хакер, HabraHabr, DigitalReport, ProfIT.kz и др.

Команда ЦАРКА занимала 1 и 2 места в соревновании The Standoff на международной конференции по информационной безопасности PositiveHackDays с 2017 по 2019 года.

СПЕЦИФИКАЦИЯ

Курс: «Безопасность веб-приложений»

№	Наименование курса	Примечание	Цена за одного чел., тенге с НДС
1	Безопасность веб-приложений	За одного слушателя	**300 000**
2	Безопасность веб-приложений	При наборе группы от 2 до 4 человек от организации	**250 000**
3	Безопасность веб-приложений	При наборе группы от 5 человек от организации	**200 000**

Главный тренер: Александр Пушкин (Twost) - Security Expert, обладатель сертификатов OSCP (Offensive Security Certified Proffesional), победитель и двухкратный призер PHDays Standoff. Имеет опыт в проведении более 100 пентестов за время своей карьеры от стартапов до банков, пентестер с опытом более 15 лет. Спикер KazHackStan.

Ведущий известного в СНГ YouTube канала [NO OFFENCE] про практическую безопасность.

Целевая аудитория: курс предназначен для разработчиков, специалистов по тестированию на проникновение, DevOps-инженеров.

Предварительный уровень подготовки: понимание основ ИТ и ИБ, а также основ программирования.

Цель курса: научить разработчиков приложений выявлять уязвимости, оценивать их риск для проекта и устранять их различными способами.

Результат обучения: по итогам курса учащиеся овладеют навыками

- использовать средства анализа защищенности кода;
- внедрять практики безопасной разработки (Secure SDLC);
- выявлять уязвимости белым и черным ящиком;
- эксплутировать уязвимости OWASP Top-10.

Форма обучения: онлайн курс.

Периодичность проведения занятий: 2 занятия в неделю.

Продолжительность: 38 академ.часов.

Дополнительная информация: в ходе курса у каждого учащегося будет домашняя задача и по завершению курса - индивидуальный проект.

По результатам защиты проекта учащиеся получат соответствующий документ об окончании курса.

Документ об окончании курса: Сертификат о прохождении курса «Безопасность веб-приложений», Сертификат об успешной защите проекта в рамках курса «Безопасность веб-приложений».

Договор на оказание услуг будет заключен с одной из компаний, входящих в состав ОЮЛ «ЦАРКА».

С уважением,
Президент ОЮЛ «ЦАРКА» **О. Сатиев**

ПРОГРАММА КУРСА: **«Безопасность веб-приложений»**

Модуль 1. Знакомство со структурой курса и используемым программным обеспечением.

Модуль 2. Классификация OWASP top 10.

Модуль 3. ClientSide: Open Redirect, CSRF, HTML Injection and Content Spoofing, Cross-Site Scripting.

Модуль 4. ServerSide: HTTP Parameter Pollution, CRLF Injection, ServerSide Request Forgery, Subdomain Takeover.

Модуль 5. ServerSide: SQL Injection.

Модуль 6. ServerSide: RCE, LFI, Deserialization.

Модуль 7. ServerSide: XXE, Template Injections.

Модуль 8. ServerSide: Race condition, IDOR.

Модуль 9. Сбор информации (разведка) о веб-приложении и его компонентах.

Модуль 10. Статические анализаторы кода и ручной анализ.

Модуль 11. Fuzzing.

Модуль 12. Инструменты для автоматического поиска и эксплуатации уязвимостей.

Модуль 13. Самописные инструменты для автоматизации поиска и эксплуатации уязвимостей.

Модуль 14. Web-shells и постэксплуатация.

Модуль 15. Права доступа и повышение привилегий.

Модуль 16. Методологии анализа защищенности и написание отчёта по аудиту.

Модуль 17. Выбор темы и организация проектной работы.

Модуль 18. Консультации по проектной работе.

Модуль 19. Защита проектных работ.

За дополнительной информацией обращаться:

Баян Оразгалиева

87076028997

bo@cybersec.kz