

Кибербезопасность

Advanced Bug Bounty

Поиск уязвимостей в реальных программах

Burp Suite | Caido | ffuf | subfinder | httpx

Уровень	Программа	Формат	Занятия	Язык
Продвинутый	8 модулей	Онлайн	Группа или индивидуально	Азербайджанский

О курсе

Из лаборатории – в реальные программы. Разведка, уязвимости с высоким импактом и правильные отчёты – для находок, которые принимают и оплачивают в bug bounty-программах крупных компаний.

Для кого этот курс

01 **Выпускники Red Team**
Вы решаете лабораторные машины – теперь хотите находки, которые принимают на реальных целях.

02 **Пентестеры**
У вас есть опыт работы, и вы хотите сделать bug bounty дополнительным источником дохода.

03 **Разработчики**
Вы знаете веб изнутри – это преимущество в поиске самых труднонаходимых уязвимостей.

Требования. Этот курс не для новичков. Нужно уже знать веб-уязвимости (OWASP Top 10) и уметь работать с Burp Suite – это следующий шаг после курса Red Team.

Как проходит неделя

01
Онлайн-занятие
Ментор объясняет тему в реальном времени, вопросы вы задаёте прямо на занятии.

02
Лаборатория
Ту же тему вы повторяете своими руками в лаборатории в браузере.

03
Еженедельное задание
Задание на основе реального сценария проверяет, что вы усвоили.

04
Проверка ментором
Ментор проверяет вашу работу, показывает ошибки и подсказывает следующий шаг.

Это не видеокурс: занятия проходят онлайн, вживую с ментором. В группе до 5 человек или индивидуально – ментор видит работу каждого. Обучение на азербайджанском языке.

Программа обучения

8 модулей – от основ до профессии

Каждый модуль закрепляется онлайн-занятием, лабораторией и еженедельным заданием. К следующему модулю вы переходите, когда освоили предыдущий на практике.

01

Экосистема bug bounty

Правила игры – правовые и этические рамки.

Платформы · Scope и правила · Ответственное раскрытие · Выбор целей

02

Автоматизированная разведка

Найти поверхность атаки, которую не видят другие.

Поиск поддоменов и активов · httpx · nuclei · Собственный recon-пайплайн

03

Анализ JavaScript

Скрытые эндпоинты и утёкшие ключи.

Анализ JS-файлов · Скрытые эндпоинты · Source map · Утечки ключей

04

Уязвимости API

Самое слабое место современных приложений.

IDOR / BOLA · Mass assignment · GraphQL · Rate limit

05

Аутентификация и OAuth

Сценарии захвата аккаунта.

Ошибки OAuth и SSO · JWT · Сброс пароля · Обход 2FA

06

Уязвимости с высоким импактом

Находки критического уровня.

SSRF · Request smuggling · Cache poisoning · Race condition

07

Цепочки уязвимостей

Один «critical» из двух «low».

Построение цепочки · Усиление импакта · Разбор реальных кейсов

08

Отчёты и триаж

Примут ли находку, зависит от отчёта.

Доказательство импакта · Шаги воспроизведения · Общение с триажем · Как избежать дубликатов

По итогам курса вы сможете

- Строить собственную систему автоматизированной разведки для цели
- Системно искать уязвимости API и аутентификации
- Превращать мелкие находки в цепочку с высоким импактом
- Писать ясные, подкреплённые доказательствами отчёты, которые проходят триаж
- Активно участвовать в международных bug bounty-платформах
- Работать по правилам ответственного раскрытия

Инструменты, с которыми вы будете работать

Burp Suite · Caido · ffuf · subfinder · httpx · nuclei · katana · Postman · Python · Bash

Где работают наши выпускники

Kapital Bank · Rabitəbank · birmarket · RISK COMPANY · BMU Bakı Mühəndislik Universiteti · AZTU

Следующий шаг

Приходите на бесплатный онлайн-урок – познакомьтесь с ментором, а потом решайте.

Группа или индивидуально - выбор за вами. Цену, расписание и дату старта следующей группы пришлём в WhatsApp. Обучение на азербайджанском языке.

WhatsApp и звонки	+994 70 639 33 09
Сайт	compstyle.tech/ru/kursy/advanced-bug-bounty
Instagram	@compstyle.az
Telegram	@compstylekanal
YouTube	@Compstyle



Compstyle TECHNOLOGY

Учись сам, создавай сам.

© Compstyle Technology