

Kibertəhlükəsizlik

Advanced Bug Bounty

Real proqramlarda zəiflik ovçuluğu

Burp Suite | Caido | ffuf | subfinder | httpx

Səviyyə	Proqram	Format	Dərs növü
İrəli səviyyə	8 modul	Onlayn	Qrup və ya fərdi

Kurs haqqında

Laboratoriyadan real proqramlara. Böyük şirkətlərin bug bounty proqramlarında qəbul olunan, ödənilən tapıntılar üçün recon, yüksək təsirli zəifliklər və düzgün hesabat yazımı.

Bu kurs kimin üçündür

01 **Red Team məzunları**
Laboratoriya maşınlarını həll edirsən, indi real hədəflərdə qəbul olunan tapıntı istəyirsən.

02 **Pentesterlər**
İş təcrübən var – bug bounty-ni əlavə gəlir mənbəyinə çevirmək istəyirsən.

03 **Developerlər**
Web-i içəridən tanıyırsan – bu bilik ən çətin tapılan zəifliklərdə üstünlükdür.

İlkin tələb. Bu kurs sıfırdan deyil. Web zəifliklərini (OWASP Top 10) və Burp Suite ilə işi bilməlisən – Red Team kursunu bitirənlər üçün növbəti addımdır.

Bir həftə necə keçir

01
Onlayn dərs
Mentor mövzunu real vaxtda izah edir, sualını dərsdəcə verirsən.

02
Laboratoriya
Eyni mövzunu brauzerdə açılan laboratoriyada öz əlinlə təkrarlayırsan.

03
Həftəlik tapşırıq
Real ssenariyə əsaslanan tapşırıqla bildiyini yoxlayırsan.

04
Mentor rəyi
Mentor işini yoxlayır, səhvini göstərir, növbəti addımı deyir.

Bu, video kurs deyil: dərslər onlayndır, mentorla real vaxtda. Qrupda maksimum 5 nəfər və ya fərdi: mentor hər kəsin işini görür.

Tədris proqramı

8 modul – təməldən peşəyə

Hər modul onlayn dərs, laboratoriya və həftəlik tapşırıqla bağlanır. Növbəti modula əvvəlkini praktikada mənimsədikdən sonra keçirsən.

01

Bug bounty ekosistemi

Oyunun qaydaları – qanuni və etik çərçivə.

Platformalar · Scope və qaydalar · Məsuliyyətli açıqlama · Hədəf seçimi

02

Avtomatlaşdırılmış recon

Başqalarının görmədiyi səthi tapmaq.

Subdomain və asset kəşfi · httpx · nuclei · Öz recon pipeline-ın

03

JavaScript analizi

Gizli endpointlər və sızan açarlar.

JS faylların təhlili · Gizli endpointlər · Source map · Açar sızmaları

04

API zəifliklər

Müasir tətbiqlərin ən zəif yeri.

IDOR / BOLA · Mass assignment · GraphQL · Rate limit

05

Autentifikasiya və OAuth

Hesab ələ keçirmə ssenariləri.

OAuth və SSO xətaları · JWT · Parol sıfırlama · 2FA bypass

06

Yüksək təsirli zəifliklər

Kritik səviyyəli tapıntılar.

SSRF · Request smuggling · Cache poisoning · Race condition

07

Zəncirvari zəifliklər

İki «low»-dan bir «critical».

Zəncir qurmaq · Təsirin artırılması · Real keys analizləri

08

Hesabat və triaj

Tapıntının qəbul olunması hesabatdan asılıdır.

Təsir sübutu · Reproduksiya addımları · Triaj ilə ünsiyyət · Dublikatdan qaçmaq

Kursun sonunda bacaracaqsan

- Hədəf üçün öz avtomatlaşdırılmış recon sistemini qurmaq
- API və autentifikasiya zəifliklərini sistemli şəkildə axtarmaq
- Kiçik tapıntıları yüksək təsirli zəncirə çevirmək
- Triajdan keçən, aydın və sübutlu hesabat yazmaq
- Beynəlxalq bug bounty platformalarında aktiv iştirak etmək
- Məsuliyyətli açıqlama qaydalarına uyğun işləmək

İşlədəcəyin alətlər

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

Məzunlarımızın çalışdığı qurumlar

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

Növbəti addım

Pulsuz onlayn sınaq dərsinə qoşul – mentorla tanış ol, sonra qərar ver.

Qrup və ya fərdi format – seçim sənindir. Qiymət, cədvəl və növbəti qrupun başlama tarixini WhatsApp-da yazırıq.

WhatsApp və zəng	+994 70 639 33 09
Sayt	compstyle.tech/kurslar/advanced-bug-bounty
Instagram	@compstyle.az
Telegram	@compstylekanal
YouTube	@Compstyle



Compstyle TECHNOLOGY

Özün öyrən, özün yarat.

© Compstyle Technology