CYBER SECURITY
ACADEMY

HACK IT TO DEFEND IT (L2): WEB APPLICATIONS

HACK IT TO DEFEND IT (L2): WEB APPLICATIONS

Web taikomosios programos (applications) vienos dažniausiai atakuojamų, todėl sukurta Hack IT to Defend IT (L2): web applications mokymų programa skirta padėti suprasti kas vyksta, kai atakuojami web architektūros komponentai ir nustatyti kokie pažeidžiamumai išnaudojami.

Hack IT to Defend IT (L2): web applications padės programinės įrangos inžinieriams kurti saugias taikomąsias programas ir suteiks išsamų supratimą apie logines saugumo aktualijas su orientacija į web aplikacijas.

Mokymų metu bus dirbama su realių situacijų modeliais ir laboratorijose atliekamos misijos su tam tikrais taikiniais.

Dalyvauti rekomenduojama IT vadovams, IT saugumo specialistams, tinkle administratoriams, programuotojams ir srities entuziastams.

Rekomendacijos dalyviams:

Siekiant maksimalaus rezultato mokymuose dalyvaujantiems rekomenduojama būti dalyvavus CSA Hack IT to Defend IT (L1) mokymuose. Būtini HTML ir SQL pagrindai.

Mokymų metu reikalingas nešiojamasis kompiuteris, kuriame iš USB galima įdiegti Burp Suite (reikalinga Java) arba OWASP Zed Attack Proxy.*

* Jei kompiuterio su minėtomis specifikacijomis į mokymus atsinešti nėra galimybės, informuokite CSA ir mes jį parūpinsime (bus taikomas papildomas mokestis).

TRUKMĖ: 2 dienos

DĖSTYMO KALBA: anglų (galima vesti rusų kalba)

KAINA: 750 EUR

NUOLAIDOS:

Išankstinės registracijos nuolaida – 15 %

3 ir daugiau žmonių iš vienos įmonės – 20 %

(nuolaidos nesumuojamos)

Lektorius

IT saugos ir bandomųjų įsiveržimų profesionalas, dirbantis su valstybės institucijoms bei organizacijoms įvairiose šalyse.

Jau daugiau nei 10 metų specializuojasi IT saugumo auditų, bandomųjų įsiveržimų ir IT saugumo mokymų srityse.

Cyber Security Academy
Tel.: +370 6 888 1450
mokymai@cybersecurityacademy.lt
www.cybersecurityacademy.lt

HACK IT TO DEFEND IT (L2): WEB APPLICATIONS

Programos darbotvarkė:

1. **Informacijos rinkimas ir web aplikacijų skenavimas**
    - Paieškos sistemos
    - Kaip rasti "paslėptus" resursus
    - Kaip nustatyti web aplikacijų problemas
    - Atakos nutaikytos į klientus
    - Crossite request forgery
    - Clickjacking atakos
    - Įterptinių instrukcijų atakos (XSS / Cross-site scripting), filtrų apėjimas ir kodavimas
    - Union ir Blind SQL injekcijų atakos

2. **Autentifikavimas ir sesijų tvarkymas**
    - Jungtinių autentifikavimo sprendimų saugumo pažeidžiamumai
    - Registracijų ir slaptažodžių atkūrimo funkcijų pažeidžiamumai
    - Kitos su duomenų patvirtinimu susijusios problemos
    - Unicode ir kiti nejprasti ženklai
    - Dažnos duomenų įkėlimo problemos
    - URL manipuliacija
    - Sesijų kūrimas, naikinimas ir valdymo problemos

Cyber Security Academy
Tel.: +370 6 888 1450
mokymai@cybersecurityacademy.lt
www.cybersecurityacademy.lt