ŠKOLENIA

Binary House poskytuje školenia v oblasti bezpečnosti, ktoré sú prispôsobené vývojárom, inžinierom IT a zamestnancom s prístupom k citlivým informáciám.

Tieto školenia pomáhajú pochopiť nielen rôzne bezpečnostné princípy ale aj zraniteľnosti, ich odhaľovanie a následnú prevenciu.

Školenia sa môžu uskutočniť vo Vašej spoločnosti, alebo v našich zabezpečených priestoroch. Počas úvodnej diskusie zistíme aké sú Vaše potreby a pripravíme Vám nezáväznú cenovú ponuku spolu s obsahom daného tréningu.

BEZPEČNOSŤ WEBOVÝCH APLIKÁCIÍ

Tento intenzívny technický kurz je určený pre vývojárov a testerov webových aplikácií. Študijné materiály sú založené na doterajších skúsenostiach inštruktorov a zároveň sú kompatibilné s bezpečnostným projektom OWASP Top 10. Počas kurzu analyzujeme všeobecné chyby, ktoré sa nachádzajú medzi rozličnými programovacími jazykmi. Účastníci kurzu sa oboznámia s najčastejšie sa vyskytujúcimi zraniteľnosťami vo webových aplikáciách formou názorných ukážok a praktických cvičení.

Cieľ kurzu

Hlavným cieľom je pomôcť objasniť vývojárom techniky bezpečného programovania v praxi. Po absolvovaní kurzu sú účastníci schopní bezpečnejšie vyvíjať aplikácie ale aj spätne identifikovať a odstrániť spomínané problémy.

Agenda

- Úvod do bezpečnosti webových aplikácií
- Testovacie nástroje
- Neošetrené používateľské vstupy
- Zlá implementácia autentifikácie a autorizácie (SAML, JWT, OAuth)
- Problémy v konfigurácií komponentov
- Manažment relácií
- Bezpečnosť webových služieb
- Kryptografia
- A iné..

Tento kurz umožňuje účastníkom:

- Porozumieť rizikám a hrozbám vo webových aplikáciách / API
- Získať prehľad o najčastejších zraniteľnostiach
- Zoznámiť sa s nástrojmi na testovanie bezpečnosti webových aplikácií

Trvanie kurzu: 1 až 2 dni

BEZPEČNOSŤ MOBILNÝCH APLIKÁCIÍ PRE PLATFORMU ANDROID

Na tomto odbornom školení používame príklady zraniteľného kódu v Android aplikáciách a po diskusii o danom probléme popisujeme referenčnú implementáciu, ktorá daný problém eliminuje prípadne zníži pravdepodobnosť jeho zneužitia. Počas školenia vám predstavíme bežné vektory útokov a zodpovedajúce protiopatrenia. Kladieme doraz na pochopenie typicky slabých miest v mobilných aplikáciách, tak aby boli zrejmé dôvody na implementáciu konkrétnych bezpečnostných protiopatrení a ich efektivita.

Agenda

- Úvod do platforiem Android a ich bezpečnostných pilierov
  - Úvod do počítačovej bezpečnosti
  - Sandboxing
  - Mechanizmy IPC (Content providers, intents, binders, broadcast recievers)
  - Code signing
  - Rooting
  - WebView
  - Biometrické overovanie a jeho nedostatky
  - Data storage (keystore, sharedpreferences, ..)
  - Najnovšie vylepšenia zabezpečenia Androidu
- Mobile Application Security Verification Standard (MASVS) & Mobile OWASP Top Ten
  - Metodický prístup k overovaniu bezpečnosti aplikácií
  - Bežné nástrahy pri posudzovaní aplikácií
  - Diskusia o každej požiadavke na overenie bezpečnosti opísanej v rámci MASVS
  - Príklady najčastejších zraniteľností (na základe výsledkov penetračných testov vykonaných v priebehu niekoľkých rokov v prostredí internetového bankovníctva a OWASP Mobile Top Ten)
- Statická a dynamická analýza aplikácie
  - Diskusia o platených analyzátoroch a pluginoch IDE (Checkmarx, SonarQube, Appscan)
  - find-sec-bugs
  - Príznaky kompilátora
- Overovanie - penetračné testovanie
  - Emulátory
  - Automatizovaná analýza aplikácií
  - Úvod do penetračného testovania mobilných aplikácií pomocou nástrojov (Frida, Burp Suite,..)
  - Reverzné inžinierstvo

Hlavným cieľom tohto kurzu je oboznámiť vývojárov s najlepšími bezpečnostnými postupmi pri písaní produkčného kódu.

Tento kurz umožňuje účastníkom:

- Porozumieť rizikám a hrozbám v mobilných aplikáciách
- Pochopiť bezpečnostné požiadavky na základe OWASP Mobile ASVS / OWASP Mobile T10
- Získať prehľad o najčastejších zraniteľnostiach
- Zoznámiť sa s nástrojmi statickej a dynamickej analýzy
- Dozvedieť sa o najdôležitejších bezpečnostných kontrolách, ako sú:
  - model oprávnení
  - šifrovanie a spôsob zabezpečenia uložených údajov
  - overovanie a autorizácia
  - zabezpečenie sieťových pripojení

Trvanie kurzu: 2 až 3 dni

BEZPEČNOSŤ MOBILNÝCH APLIKÁCIÍ PRE PLATFORMU IOS

Na tomto odbornom školení používame príklady zraniteľného kódu v iOS aplikáciách a po diskusii o danom probléme popisujeme referenčnú implementáciu, ktorá daný problém eliminuje prípadne zníži pravdepodobnosť jeho zneužitia. Počas školenia vám predstavíme bežné vektory útokov a zodpovedajúce protiopatrenia. Kladieme doraz na pochopenie typicky slabých miest v mobilných aplikáciách, tak aby boli zrejmé dôvody na implementáciu konkrétnych bezpečnostných protiopatrení a ich efektivita.

Agenda

- Úvod do platforiem iOS a ich bezpečnostných pilierov
  - Úvod do počítačovej bezpečnosti
  - Sandboxing
  - Mechanizmy IPC (custom URL, universal links, UIPasteboard, ..)
  - Code signing
  - Jailbreaking
  - WebView
  - Biometrické overovanie a jeho nedostatky
  - Data storage (keychain, ..)
  - Najnovšie vylepšenia zabezpečenia Androidu
- Mobile Application Security Verification Standard (MASVS) & Mobile OWASP Top Ten
  - Metodický prístup k overovaniu bezpečnosti aplikácií
  - Bežné nástrahy pri posudzovaní
  - Diskusia o každej požiadavke na overenie bezpečnosti opísanej v rámci MASVS
  - Príklady najčastejších zraniteľností (na základe výsledkov penetračných testov vykonaných v priebehu niekoľkých rokov v prostredí internetového bankovníctva a OWASP Mobile Top Ten)
- Statická a dynamická analýza aplikácie
  - Diskusia o platených analyzátoroch a pluginoch IDE (Checkmarx, SonarQube, Appscan)
  - Príznaky kompilátora
- Overovanie - penetračné testovanie
  - Emulátory
  - Automatizovaná analýza aplikácií
  - Úvod do penetračného testovania mobilných aplikácií pomocou nástrojov (Frida, Burp Suite,..)
  - Reverzné inžinierstvo

Hlavným cieľom tohto kurzu je oboznámiť vývojárov s najlepšími bezpečnostnými postupmi pri písaní produkčného kódu.

Tento kurz umožňuje účastníkom:

- Porozumieť rizikám a hrozbám v mobilných aplikáciách
- Pochopiť bezpečnostné požiadavky na základe OWASP Mobile ASVS / OWASP Mobile T10
- Získať prehľad o najčastejších zraniteľnostiach
- Získať prehľad o najčastejších zraniteľnostiach

- Dozvedieť sa o najdôležitejších bezpečnostných kontrolách, ako sú:
  - model oprávnení
  - šifrovanie a spôsob zabezpečenia uložených údajov
  - overovanie a autorizácia
  - zabezpečenie sieťových pripojení

Trvanie kurzu: 2 až 3 dni

ŠKOLENIE NA MIERU

Naši zamestnanci majú niekoľkoročné skúsenosti v mnohých oblastiach týkajúcich sa IT bezpečnosti. Nižšie uvedené oblasti nie sú kompletným zoznamom a v prípade záujmu o ďalšie témy v oblasti IT bezpečnosti nás kontaktujte.

Stručný prehľad preberaných tém:

- Penetračné testovanie
- Bezpečnostné povedomie pre zamestnancov
- Kryptografia

Trvanie kurzu: Dohodou