Obrana proti hackingu webových aplikací v .NET

Kód kurzu: GOC3314

Kurz se zabývá zabezpečením webových aplikací z různých úhlů pohledu a je určen pro programátory i administrátory webových serverů na platformě Microsoft IIS, na nichž běží ASP.NET aplikace. Část „programátorská" a „administrátorská" spolu zejména v oblasti bezpečnosti dost těsně souvisí. Proto je kurz koncipován i jako „ochutnávka" té druhé strany. Naučíme vás nahlížet komplexně na problematiku zabezpečení webových aplikací: jak zabezpečit server samotný, jak napsat aplikaci, aby neobsahovala bezpečnostní díry, jak zabezpečit data v průběhu přenosu i při uložení na serveru. To vše doplněno teoretickým základem, okořeněným historkami z praxe.

Pro koho je kurz určen

- Kurz je určen pro vývojáře, administrátory a architekty webových aplikací na platformě ASP.NET

Požadované vstupní znalosti

- Zkušenosti s platformou .NET Framework
- Základní zkušenosti s objektově orientovaným programováním v jazyce C# nebo VB .NET
- Základní zkušenosti s vývojem webových aplikací na platformě ASP.NET

Osnova kurzu

Čtyři základní zásady bezpečnosti

- Čtyři základní zásady bezpečnosti

Trocha teorie na úvod

- Posuzování typu bezpečnostních hrozeb
- Neštěstí nechodí nikdy samo - odhalení příbuzných problémů
- Posuzování závažnosti bezpečnostních hrozeb

Zabezpečení platformy serveru

- Minimalizace attack surface
- Security Configuration Wizard
- Boj proti vnitřnímu nepříteli
- Obrana do hloubky
- Šifrování konfiguračních sekcí

Zabezpečení kanálu síťové komunikace

- Jak funguje protokol HTTP a proč není bezpečný
- Jak funguje SSL/TLS/HTTPS
- Jak žádat o certifikát web serveru a jak ho nainstalovat
- Rychlé vytvoření certifikátů pomocí utilit z Platform SDK
- Provoz certifikační autority pomocí Windows Certificate Services
- Provoz certifikační autority pomocí OpenSSL (na platformě Windows a nejen tam)

Zabezpečení aplikace

- Identifikace, autentizace, autorizace
- Bezpečnostní architektury webových aplikací
- Dostupné mechanismy v IIS
- Jak napsat vlastní autentizační modul a proč to nedělat

Forms Authentication v ASPNET

- Autentizační tickety a jejich platnost
- Doba platnosti ticketů versus délka session
- Cookie a Cookieless autentizace
- Login Controls
- Statické credentials ve web.config

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk

- Single sign-on v rámci jedné domény

Ukládání hesel

- Šifrování, hashování, HMAC
- Ověření e-mailové adresy
- Řešení zapomenutého hesla

ASPNET Membership

- Membership providers v ASP.NET
- Výchozí nastavení
- ASP.NET Universal Providers
- Použití providerů třetích stran
- Tvorba vlastních membership providerů

ASPNET Roles

- Role providers v ASP.NET
- Tvorba vlastních role providerů

Zabezpečení dat šifrování

- Tajemství, šifry a paranoia v průběhu věků
- Symetrické a asymetrické šifrování, kombinace
- Nakládání s klíči
- Praktická implementace šifrovaného ukládání dat v .NET, s využitím RSA a AES algoritmů a odpovídající architektury

GOPAS Praha
Kodaňská 1441/46
101 00 Praha 10
Tel.: +420 234 064 900-3
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 542 422 111
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 248 282 701-2
info@gopas.sk