Obrana proti hackingu webových aplikácií v .NET

Kód kurzu: GOC3314

Kurz sa zaoberá zabezpečením webových aplikácií z rôznych uhlov pohľadu a je určený pre programátorov i administrátorov webových serverov na platforme Microsoft IIS, na ktorých bežia ASP.NET aplikácie. Programátorská a administrátorská časť spolu, najmä v oblasti bezpečnosti, dosť úzko súvisia, preto je tento kurz koncipovaný i ako ochutnávka tej druhej strany. Naučíme vás pozerať sa na problematiku zabezpečenia webových aplikácií komplexne: ako zabezpečiť server samotný, ako napísať aplikáciu, aby neobsahovala bezpečnostné diery, ako zabezpečiť dáta v priebehu prenosu i pri uložení na server. To všetko doplnené teoretickým základom okoreneným historkami z praxe tvorí obsah tohto kurzu.

Pre koho je kurz určený

Kurz je určený pre vývojárov webových aplikácií na platforme ASP.NET.

Požadované vstupné znalosti

- Skúsenosti s platformou .NET Framework
- Skúsenosti s objektovo orientovaným programovaním v jazyku C# alebo VB .NET
- Skúsenosti s vývojom webových aplikácií na platforme ASP.NET na úrovni kurzu GOC331

Osnova kurzu

Štyri základné zásady bezpečnosti

- Štyri základné zásady bezpečnosti

Trocha teórie na úvod

- Posudzovanie typu bezpečnostných hrozieb
- Nešťastie nechodí nikdy samo - odhalenie príbuzných problémov
- Posudzovanie závažnosti bezpečnostných hrozieb

Zabezpečenie platformy serveru

- Minimalizácia Attack Surface
- Security Configuration Wizard
- Boj proti vnútornému nepriateľovi
- Obrana do hĺbky
- Šifrovanie konfiguračných sekcií

Zabezpečenie kanálu sieťovej komunikácie

- Ako funguje protokol HTTP a prečo nie je bezpečný
- Ako funguje SSL/TLS/HTTPS
- Ako žiadať o certifikát web serveru a ako ho nainštalovať
- Rýchle vytvorenie certifikátov pomocou utilít z Platform SDK
- Prevádzka certifikačnej autority pomocou Windows Certificate Services
- Prevádzka certifikačnej autority pomocou OpenSSL (na platforme Windows a nielen tam)

Zabezpečenie aplikácie

- Identifikácia, autentizácia, autorizácia
- Bezpečnostné architektúry webových aplikácií
- Dostupné mechanizmy v IIS
- Ako napísať vlastný autentizačný modul a prečo to nerobiť

Forms Authentication v ASP.NET

- Autentizačné tickety a ich platnosť
- Doba platnosti ticketov verzus dĺžka Session
- Cookie a Cookieless autentizácia
- Login Controls
- Statické Credentials vo 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 jednej domény

Ukladanie hesiel

- Šifrovanie, hashovanie, HMAC
- Overenie e-mailovej adresy
- Riešenie zabudnutého hesla

ASP.NET Membership

- Membership Providers v ASP.NET
- Východiskové nastavenia
- ASP.NET Universal Providers
- Použitie providerov tretích strán
- Tvorba vlastných Membership providerov

ASP.NET Roles

- Role Providers v ASP.NET
- Tvorba vlastných Role Providers

Zabezpečenie dát šifrovania

- Tajomstvá, šifry a paranoja v priebehu vekov
- Symetrické a asymetrické šifrovanie, kombinácie
- Správa kľúčov
- Praktická implementácia šifrovaného ukladania dát v .NET s využitím RSA a AES algoritmov a zodpovedajúcej architektúry

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