



مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی

و برگزار کننده دوره های آموزشی

ECSP .NET

EC-Council Certified Secure Programmer(ECSP) .NET

اعتبار دهنده: EC-Council

پیش نیاز: آشنایی با برنامه نویسی

مدت (ساعت): ۳۵

کاریار ارقام نماینده رسمی شرکت بین المللی EC-Council در ایران

معرفی دوره :

فریم ورک NET، به صورت گسترده ای در سازمان ها به عنوان یکی از تکنولوژی های پیشرو در زمینه توسعه نرم افزارهای تحت وب بکار گرفته شده است. این دوره آموزشی برای برنامه نویسان و توسعه دهندگان نرم افزار که به دنبال طراحی و تولید نرم افزارهای امن در بستر NET هستند، بسیار با ارزش و موثر خواهد بود.

این دوره به فراگیر آموزش می دهد که چگونه ایرادات امنیتی را شناسایی کرده و مکانیزم های مقابله لازم با آنها را در طول چرخه عمر نرم افزار پیاده سازی نماید تا کیفیت و امنیت رو در محصولات نرم افزار ارتقا بخشد.

دوره ECSP.NET زیربنای مورد نیاز برای تمامی توسعه دهندگان و سازمان های تولیدکننده نرم افزار را برای تولید نرم افزارهای پایدارتر و با مشکلات امنیتی کمتر پایه ریزی می کند. با استانداردسازی دانش مورد نیاز توسعه دهندگان و سایر نقش های درگیر در تولید نرم افزار امن در قالب اصول امنیتی استخراج شده از بهروش ها و رهنمودهای امنیتی، فراگیر به تجربیات باارزش متخصصین این حوزه دست خواهد یافت.

این دوره با فعالیت های کارگاهی متعددی در طول برگزاری آن همراه خواهد بود و اصول نوین و موثری در زمینه تکنیک ها و استراتژی های برنامه نویسی امن را ارایه می نماید.
کد Exam این دوره:

Exam Prefix: 312-93

مخاطبان دوره :

این دوره ویژه توسعه دهندگانی است که مسئولیت طراحی و تولید نرم افزارهای امن و قابل اطمینان را بر پایه فریم ورک NET در وب یا ویندوز بر عهده دارند و شرکت در این دوره مستلزم دارا بودن تجربه کاری مفید با این فناوری می باشد.

امتیازات دوره :

- اعطای مدرک فارسی و انگلیسی با مجوز رسمی از :
- سازمان مدیریت و برنامه ریزی کشور (معاونت توسعه مدیریت و سرمایه انسانی رئیس جمهوری سابق)
- مجوز از اداره کل نظام مدیریت امنیت اطلاعات (نما)
- شورای عالی انفورماتیک
- قابلیت ترجمه و تایید قوه قضاییه و امور خارجه
- بهره گیری از لابراتوار سخت افزاری و نرم افزاری مجهز
- بهره گیری از اساتید مجرب و تأیید شده با سابقه حضور در پروژه های ملی

اهداف دوره :

- ایجاد آشنایی با مفاهیم و اصول پایه امنیتی در NET، معماری امنیتی در ASP.NET و کمک به فراگیر جهت درک مفاهیم امنیت نرم افزار و تهدیدات عمومی برنامه های مبتنی بر NET.
- بحث در مورد حملات امنیتی بر بستر فریم ورک NET، و تشریح چرخه عمر توسعه نرم افزار امن
- کمک به فراگیر جهت آشنایی با تهدیدات رایج علیه Net Assemblies و آشنایی با Stack Walking
- اعتبارسنجی ورودی ها و رویکردهای مختلف آن، حملات رایج بر علیه اعتبارسنجی ورودی ها، آسیب پذیری های موجود در کنترل های اعتبارسنجی و بهروش های موجود در این زمینه
- آشنایی با مفاهیم احراز هویت (Authentication) و مجازشماری (Authorization) و تهدیدات رایج در این زمینه
- بررسی اصول امنیتی مرتبط با توکن های مدیریت نشست (Session Management)، تهدیدات رایج در این زمینه و تکنیک های مدیریت نشست در ASP.NET و حملات در این بخش
- اهمیت رمزنگاری در NET، انواع حملات رمزنگاری در NET، و فضاهای نام (Namespaces) مربوط به رمزنگاری
- رمزنگاری متقارن (Symmetric) و نامتقارن (Asymmetric)، مفاهیم درهم سازی (Hashing)، گواهینامه دیجیتال، امضای دیجیتال و XML
- تشریح اصول مدیریت خطای امن، سطوح مختلف در مدیریت استثنائات (Exception Handling) و ابزارهای رویدادنکاری (Logging) در NET.
- مفاهیم مدیریت فایل، مدیریت تهدیدات در این بخش، حملات Path Traversal و تکنیک های مقابله با این دسته از حملات

www.Cdigit.com



« مالکیت مادی و معنوی این مستند منحصراً متعلق به کاریار ارقام است »

لطفاً در باز نشر این مستند نام پدیدآورنده لحاظ گردد.

تهران : خیابان ملاصدرا، بعد از خیابان شیخ بهائی، ساختمان فردوس، پلاک ۲۴۲ تلفن مستقیم آموزش: ۸۸۰۶۲۲۰۳، فاکس: ۸۸۰۶۵۲۲۲





مشاوره، تحقیقات، طرح و اجرای شبکه های ارتباطی
و برگزار کننده دوره های آموزشی

Course Outline :	محتوای دوره :
1 - Introduction to .NET Application Security • Microsoft .NET Application Security • Common Security Threats on .NET • Secure Development Lifecycle (SDL) • Secure Coding Principles • Guidelines for Developing Secure Codes 2 - .NET Framework Security • Introduction to .NET Framework • .Net Runtime Security • .NET Class Libraries Security • .NET Assembly Security • .NET Security Tools • Best Practices for .NET Framework Security 3 - Input Validation and Output Encoding • Input Validation • Input Validation Attacks • Defensive Techniques against XSS Attacks • Defensive Techniques against SQL Injection Attacks • Output Encoding • Sandboxing • Best Practices 4 - .NET Authorization and Authentication • Introduction to Authentication and Authorization • Authentication • Authorization • Authentication and Authorization Vulnerabilities • Authentication and Authorization Best Practices • Secure Communication 5 - Secure Session and State Management • Session Management • Session Management Techniques in ASP.NET • Session Attacks and Its Defensive Techniques • Securing Cookie Based Session Management	• ViewState Security • Guidelines for Secure Session Management 6 - .NET Cryptography • Introduction to Cryptography • Symmetric Encryption • Asymmetric Encryption • Hashing • Digital Signatures • Digital Certificates • XML Signatures 7 - .NET Error Handling, Auditing, and Logging • Error Handling • Exception Handling in ASP.NET • Exception Handling Best Practices • Auditing and Logging • Auditing and Logging Best Practices • .NET Logging Tools 8 - .NET Secure File Handling • File Handling • Attacks on File and Its Defensive Techniques • Securing Files • File Extension Handling • Isolated Storage • File Access Control Lists (ACLs) • Checklist for Securely Accessing Files 9 - .NET Configuration Management and Secure Code Review • Configuration Management • Machine Configuration File • Application Configuration Files • Code Access Security Configuration Files • Configuration Management Best Practices • Secure Code Review • Static Code Analysis Tools

www.Cdigit.com