دانشکده مهندسی برق

Core Software Security

نگارش

فاطمه پیرمرادیان

شماره دانشجویی:

۹۵۰۲۱۶۵

مقطع: دکترا

استاد:

دکتر فانیان

ده سوال پروژه امنیت شبکه

در رشته مهندسی برق مخابرات (سیستم)

خردادماه ۱۳۹۶

سوال یک:

وظایف کلیدی در طول جلسه Discovery در توسعه امنیت چرخه‌ی حیات کدام‌اند؟

پاسخ:

- شناسایی منابع جهت نیازهای امنیتی شامل قوانین مربوطه، استانداردها، مقررات و نیازهای مشتریان.
- شناسایی هر گواهینامه و یا مجوز رسمی موردنیاز.
- شناسایی هر شخص ثالث یا نرم‌افزار منبع باز.
- شناسایی کنترل‌های امنیتی رایج مورد استفاده جهت توسعه.
- شناسایی و تعریف معیارهای امنیتی در هر دو شرایط تاکتیکی واستراتژیک.
- توسعه یک چارچوب اولیه از نقاط عطف امنیت کلیدی، از جمله چارچوب‌های زمانی.
- تعریف مسئولیت‌های امنیتی تیم امنیت نرم‌افزار، قهرمانان امنیت نرم افزار،توسعه دهندگان، تیم حریم خصوصی و هر سهام دار دیگر موردنیاز جهت برقراری امنیت در طول فرایندSDL/SDLC .
- شناسایی و مستندسازی طرح امنیتی نرم افزار، معماری و امنیت شیوه‌های برنامه نویسی مورد استفاده
- تست امنیت و ارزیابی تکنیک‌هایی که استفاده خواهد شد.
- پخش کردن یک فرایند ارزیابی اثرات پیش حفظ حریم خصوصی ازجمله طبقه‌بندی اطلاعات، شناسایی شرایط خاص جهت انتقال، نگه داری یا ایجاد اطلاعات شناسایی شخصی و شناسایی مقدماتی هرگونه نیازهای امنیتی.
- در صورت امکان، محصول مصنوعی پروژه مانند صورت جلسه، مختصرسازی و هویت نقش باید استاندارد شود و به توسعه دهندگان برای برنامه‌ریزی مناسب داده شود. این باید یک فرایند مداوم در SDL باشد.

سوال دو:

تاثیر حریم خصوصی شامل چند دسته است؟

پاسخ:

- خطر حریم خصوصی بالا (P1)
- خطر حریم خصوصی متوسط (P2)
- خطر حریم خصوصی پایین(P3)

سوال سه:

عوامل و استانداردهای کلیدی ارزیابی امنیت موفقیت(A1) چیست؟

پاسخ:

- عامل اول موفقیت: دقت فعالیت‌های برنامه‌ریزی‌شده SDL
- عامل دوم موفقیت: مشخصات خطر محصول
- عامل سوم موفقیت: دقت پروفایل تهدید
- عامل چهارم موفقیت: پوشش مقررات مربوطه و گواهینامه‌های پذیرش
- عامل پنجم موفقیت: گستره اهداف امنیتی موردنیاز برای نرم افزار

سوال چهار:

پنج گام فرایند مدل‌سازی خطر تهدید را نام ببرید؟

پاسخ:

۱- شناسایی اهداف امنیتی
۲- بررسی نرم افزار
۳- تجزیه آن
۴- شناسایی تهدیدها
۵- شناسایی آسیب پذیری ها

سوال پنج:

هر حرف در TRIDE به عنوان یک روش طبقه‌بندی تهدید نشان‌دهنده کدام یک ز اهداف حمله است؟

پاسخ:

- حقه‌بازی
- دستکاری
- انکار
- افشای اطلاعات
- خودداری ازخدمات (منع خدمات)
- ترفیع امتیاز

سوال شش:

PASTA چیست؟

پاسخ:

PASTA فرایند هفت مرحله‌ای است که در بسیاری از روش‌های توسعه برنامه کاربردی قابل کاربرد موجود است و از نوع Platform - agnostic است. این نه تنها اهداف کسب وکار را با الزامات فنی هم‌تراز می‌کند، هم‌چنین ازالزامات قابل قبول account ، تجزیه‌وتحلیل کسب‌وکار و یک رویکرد پویا جهت مدیریت تهدید پیروی می‌کند **که** این فرایند در سال ۲۰۱۱ به عنوان یک روش مدل‌سازی تهدید برنامه‌های جدید توسعه یافته با مارکو و مورانا وTony uceda velez ارائه شد.

سوال هفت:

هفت گام روش مدل‌سازی تهدید PASTA را نام ببرید؟

پاسخ:

۱- تعریف اهداف
۲- تعریف قلمرو فنی
۳- نرم‌افزار تجزیه
۴- تجزیه وتحلیل تهدید
۵- تجزیه وتحلیل ضعف و آسیب‌پذیری
۶- مدل‌سازی حمله
۷- ریسک و تحلیل اثرات

سوال هشت:

CVSS چیست؟

پاسخ:

یکی دیگر از روش‌های ارزیابی بسیار رایج که به طور گسترده توسط تیم‌های واکنش حادثه (PSIRT) و گروه‌های امنیتی نرم افزار داخلی جهت طبقه‌بندی آسیب‌پذیری‌های نرم افزار کشف شده خارجی ایجاد شده است، سیستم امتیازدهی آسیب‌پذیری مشترک دولت (VSS) است. شورای مشورتی زیرساخت ملی (NIAC)، CVSS را ماموریت داد که چارچوب افشای آسیب‌پذیری جهانی را حمایت کند. CVSS در حال حاضر توسط انجمن جوابگویی حادثه‌ها و تیم‌های امنیتی (FIRST) حفظ شده است و این یک تلاش مشترک با شرکت‌های زیادی، از جمله CERT/CC، سیستم‌های Cisco، eBay DHS/MITRE، سیستم‌های امنیتی اینترنت، مایکروسافت، Qulays و سیمانتیک است.

سوال نه:

OCTAVE چیست و چند روش دارد؟

پاسخ:

OCTAVE (عملیات تهدید بحرانی، دارایی و ارزیابی آسیب‌پذیری) یک روش خطر بسیار پیچیده نشات گرفته از موسسه مهندسی نرم افزار دانشگاه Carnegime (SEI) است که در همکاری با تیم واکنش اضطراری کامپیوتر SEI می‌باشد. OCTAVE روی خطر سازمانی تمرکز می‌کند و نه خطر فنی. این شامل مجموعه‌ای از ابزارها، تکنیک‌ها و روش‌ها برای ارزیابی استراتژی امنیت اطلاعات مبتنی بر ریسک است.

سه روش OCTAVE وجود دارد:

۱- روش OCTAVE اصلی، که به شکل پایه‌ای برای OCTAVE بدون دانش است.
۲- OCTAVE-S، برای سازمان‌های کوچک‌تر.
۳- OCTAVE-Allegro، یک رویکرد کارآمد برای ارزیابی امنیت اطلاعات است.

سوال ده

چهار روش جهت بیان تهدیدات و برنامه ریزی در جهت کاهش خطرها کدام اند؟

پاسخ:

- ✓ طراحی مجدد فرایندها برای از بین بردن تهدید.
- ✓ اعمال یک کاهش استاندارد به عنوان توصیه‌های کلی.
- ✓ اختراع یک استراتژی جدید کاهش (مخاطره‌آمیز و وقت‌گیر).
- ✓ قبول آسیبب پذیری‌ها با خطر کم و تلاش بالا برای تعمیر آن‌ها.