۱-SDL (چرخه ی توسعه ی امنیت ) چیست؟

از مراحل کلیدی در توسعه ی امنیت نرم افزار است.و فرآیندی است که برای کاهش هزینه های تعمیر و نگهداری و افزایش قابلیت اطمینان نرم افزار درباره ی امنیت وابسته به bugها مورد استفاده قرار می گیرد.

۲- fuzzing را مختصرا شرح دهید؟

یک تکنیک تست نرم افزار است که از طریق تولید و تزریق داده های ناقص و نیمه ناقص به نرم افزار، اشکال های زمان اجرا و نقص های امنیتی را به طور اتوماتیک پیدا می کند.مزیت عمده ی این روش نسبت به سایر روش ها این است که بسیار ساده است و عاری از تعصبات رفتاری سیستم عمل می کند.

۳- منظور از تحلیل استاتیکی نرم افزار چیست؟

تحلیل نرم افزاری است که بدون اجرای برنامه ها برای بررسی یک نسخه از کد نویسی انجام میشود. این تحلیل به عنوان آزمایش امنیتی استاتیک نرم افزار شناخته می شود که آسیب پذیری نرم افزار را در مرحله ی توسعه یا کنترل کیفیت انجام می دهد و چون خطوط کد را تشخیص می دهد امکان رفع سریع آسیب پذیری را فراهم می کند.

۴- منظور از تحلیل دینامیکی نرم افزار چیست؟

تحلیل نرم افزاری است که با اجرای برنامه ها روی پردازنده ی واقعی یا مجازی انجام میشود و هدف یافتن خطاهای امنیتی در حین اجرای برنامه است نه بررسی مکرر کدهای برنامه.و از مزایای آن عدم نیاز به ایجاد خطاهای مصنوعی است.

۵- یکی از عناصر حیاتی در تولید نرم افزار را نام برده و اهمیت آن را مختصرا شرح دهید.

حداقل مجوز دسترسی- افزایش سطح دسترسی باعث می شود مهاجم مانند کاربر عادی به اطلاعات سیستم دسنرسی پیدا کند.پس باید با حداقل کردن سطح دسترسی از فاش شدن داده های حساس جلوگیری کرده و مانع از دسترسی کاربران غیرمجاز به حافظه، cpu ،شبکه و برنامه ها و حوزه هایی که نباید به آن ها دست یابند، شد.

۶- یک روش برای حداقل کردن سطح دسترسی معرفی کنید؟

تقسیم نرم افزار به بخش های مجزا به طوری که برای کنترل دسترسی نیازمند بررسی های چندگانه باشد، یکی از روش هاست و از دسترسی مهاجم به کل سیستم جلوگیری می کند.در این حالت اگر مهاجم به یک مجوز دست یافت ولی نتواند به دومی دست یابد حمله منتفی می شود.

۷- یکی از اهداف SDL پیاده کردن ایرادات در تمامی فرآیند به صورت فیلتر کردن چند مرحله ای است. منظور از فیلتر کردن را توضیح دهید؟

رفع هر نقص می تواند به عنوان یک فیلتر محسوب شود که درصدی از نواقصی که می تواند منجر به آسیب پذیری سیستم شود را حذف می کند. یافتن نواقص به تیم کمک می کند تا تصمیم بگیرند مرحله ی بعدی را شروع کنند یا اقدامات بهبود دهنده را متوقف کنند و به آن ها می گوید نسبت به هدف خود در کجا قرار دارند و کجای فرآیند را باید تصحیح کنند.

۸- هر نمونه از SDL برای عملکرد موثر باید به SDLC جاری نگاشت شود.مزیت این کار در زمینه ی امنیت را شرح دهید؟

با این کار امنیت در هر فاز SDLC برقرار می شود.در این صورت نرم افزار به طور پیش فرض امنیت بالاتری دارد و تغییرات نرم افزاری که بعدا روی آن انجام می شود، امنیت کلی نرم افزار را کمتر تحت تاثیر قرار می دهد.

۹- ویژگی های توسعه ی آبشاری(یکی از روش های توسعه ی نرم افزار ) را بیان کنید؟

این روش توسعه دارای ریسک بالا و هزینه ی بیشتر نسبت به مدل agile است.در مواردی که همه ی الزامات قابل فهم و غیر پیچیده باشند ممکن است مورد استفاده قرار گیرد.این روش از ۵مرحله ی اصلی شامل: plan- build- test- review- deploy تشکیل شده و در صورتی که هر مرحله به درستی انجام شود، به مرحله ی بعد میرود.(مشابه خط مونتاژ).

۱۰- ویژگی های توسعه ی agile (یکی از روش های توسعه ی نرم افزار ) را بیان کنید؟

براساس روش های افزایشی و تکراری می باشد.مقررات و روش ها از طریق همکاری بین تیم های خودسازمان یافته و متقابل استنتاج می شود و راه حلی که از طریق هریک از تکرار ها نتیجه می شود در کل فرآیند مورد

بررسی و پالایش منظم قرار می گیرد. در این روش وظایف به بخش های کوچکتری تقسیم شده که نیازمند برنامه ریزی حداقلی می باشد و زمان کمتری نیاز دارد.دو نمونه از این روش ها Lean Development و Scrum را میتوان نام برد.