به نام خدا

سوالات فصل‌های ۵ و ٦ کتاب Core Software Security

شبنم میرشاهزاده

۹۵۱۷٤۳٤

۱- تکنیک های تست امنیت نرم افزار را با چه عناوینی طبقه‌بندی می‌کنند ؟

با عناوین :

- جعبه سفید : تست از نگاه داخلی با داشتن اطلاعات کامل از داخل نرم افزار ؛ به عنوان مثال، سورس کد ، مستندات معماری و طراحی و فایل های پیکربندی باید برای تجزیه و تحلیل ، در دسترس باشند.
- جعبه خاکستری : تجزیه و تحلیل سورس کد با هدف طراحی موردهای تست اما با استفاده از تکنیک های تست جعبه سیاه. هم سورس کد و هم کد باینری اجرایی (binary executable)باید برای تجزیه و تحلیل در دسترس باشند.
- جعبه سیاه : تست نرم افزار از نگاه خارجی با داشتن هیچ دانش قبلی از آن. تنها کد اجرایی باینری یا کد میانی بایتی (intermediate byte code) برای تجزیه و تحلیل در دسترس هستند.

۲- در مورد تحلیل کد باینری به عنوان یکی از تکنیک‌های تست امنیت توضیح دهید و بگویید در چه طبقه‌ای قرار دارد ؟

اسکنرهای کد باینری، کد ماشین را تحلیل می‌کنند تا با استفاده از رفتارهای برنامه، جریان‌های داده، درختان فرخوانی (call trees) و فراخوانی‌های توابع خارجی، یک مدل با زبان بی‌طرف ارایه شود. پس از آن ممکن است چنین مدلی توسط یک اسکنر اتوماتیک آسیب پذیری ، نادیده گرفته شود و آسیب پذیری-هایی استقرار یابند که ناشی از خطاهای رایج کدنویسی و backdoor های ساده ،هستند. منتشر کننده‌ی سورس کد، می تواند از این مدل برای تولید یک سورس کد خوانا برای انسان، استفاده کند؛ همچنین گزارشی دقیق از نقطه ضعف‌های امنیتی سطح طراحی و backdoor های که توسط اسکنرهای اتوماتیک یافته نمی شوند ، تهیه کند.

این تکنیک در طبقه‌ی جعبه‌ی سیاه است.

۳- امتیاز حداقل، به عنوان یکی از دستورالعمل های طراحی امنیت که توسط سالتر و شرودر معرفی شد، چیست؟

اصل حداقل امتیاز بیان می‌کند که به یک فرد، فرآیند، یا هر نوع موجودیت دیگر باید حداقل امتیازات, منابع و حداقل زمان مورد نیاز برای تکمیل یک کار ، داده شود. این رویکرد فرصت دسترسی غیر مجاز به اطلاعات حساس را از بین می برد.

٤- میانجیگری کامل (Complete mediation)، به عنوان یکی از دستورالعمل های طراحی امنیت که توسط سالتر و شرودر معرفی شد، چیست؟

در یک سیستم کامپیوتری، زمانی که درخواستی از یک نهاد ، جهت دسترسی به سرویسی صادر می-شود، باید توسط authority چک شود و روندی مجاز، معتبر و موثر را طی کند. این اصل، هنگامی که به طور سیستماتیک اعمال می شود، زیربنای اصلی سیستم حفاظت است . حتی در زمان مقداردهی اولیه, در حالت restart , shutdown و یا در حالت تعمیر و نگهداری ،نباید بتوان این اصل را به تعلیق درآورد یا دور زد . میانجیگری کامل مستلزم: (الف) شناسایی از نهادی که درخواست دسترسی کرده است؛ (ب) تایید شود که درخواست از زمان ایجادش تغییری نکرده است. (ج) استفاده از روش های مجاز مناسب؛ و (د) بازنگری در درخواست‌های قبلی همان نهاد که مجوز دریافت کرده‌اند.

٥- انواع تست‌هایی که بر روی یک محصول نرم‌افزاری و سیستم‌های وابسته به آن اعمال می‌شود چگونه دسته‌بندی می‌شوند ؟

- محک‌ها (Benchmark) : این نوع تست نتایج واقعی را با نتایج تخمین مقایسه می‌کند.
- تست های زمانبندی شده : این تست ها شامل نیازمندی‌های اجباری برای تایید امنیت نرم افزار و سیستم های مرتبط با آنهاست که باید بدون توجه به اینکه مشکلات یا آسیب پذیری‌های امنیتی تشخیص داده شده اند یا نه، تنظیم مورد نیاز است یا نه؛ انجام گیرند.
- تست های اکتشافی: بر روی آزادی عمل و مسئولیت پذیری شخص آزمایشگر تاکید دارد تا آزمایشگر بتواند به طور پیوسته کیفیت کار خود را از طریق یادگیری های مرتبط ، طراحی, اجرا، و تفسیر نتایج تست،بهینه کند.

٦- در فرآیند مرور و بررسی کد چهار تکنیک اساسی چیست و مراحل چهارگانه‌ی آن کدامند؟

اسکن اتوماتیک ، تست نفوذ دستی ، آنالیز استاتیک , مرور دستی کد، چهار تکنیک اساسی بررسی کد یک اپلیکیشن هستند که سریع‌ترین و دقیق‌ترین راه برای یافتن و حل بسیاری از مشکلات امنیتی می-باشند در حالی که هم کم هزینه‌اند و هم زمان کمتری را نیز نسبت به چیزی که انتظار می رود مصرف می کنند. ، به خصوص اگر آنها داخل SDLC به عنوان بخشی از پروسه قرار گیرند، از پروسه‌های گران قیمت رسیدگی، مکان یابی، و حل آسیب پذیری امنیتی در طول مراحل بعدی توسعه یا بعد از ارائه محصول، جلوگیری می‌شود. و شامل چهار مرحله‌ی زیر هستند :

١. بررسی موردی امنیت کد
٢. اسکن مقدماتی
٣. بازبینی مشکلات امنیتی کد
٤. بازبینی مشکلات امنیتی مختص معماری

٧- روند ایده‌آلی که برای موفقیت در بررسی کد معرفی شد شامل چه فعالیت‌هایی است ؟

(a) مدل کردن تهدید: به کد و جریان داده توجه کنید، مناطق با ریسک بالا و نقاط ورودی را مشخص کنید.
(b) مرور کد: تمام یافته‌ها و همچنین خود پروسه را با روشی مناسب پرونده کنید.

(c) حل مسائل: با مالکین کد برای اعمال تعمیر و تلاش های بیشتر، همکاری کنید.
(d) فراگیری: ابزارها را بروزرسانی کنید، تیم‌های توسعه را آموزش دهید، پروسه را بهبود بخشید، و برای تکرارهای آینده را برنامه ریزی کنید.

۸- چند مورد از مزایا و محدودیت‌های تست‌های استاتیک را توضیح دهید ؟

مزایای آنالیز استاتیک کد

- ✓ دسترسی به دستور واقعی که نرم افزار اجرا می کند(هیچ نیازی به حدس زدن یا تفسیر رفتار نمی‌باشد، دسترسی کامل به تمام رفتارهای ممکن نرم افزار وجود دارد)
- ✓ توانایی یافتن مکان دقیق ضعف در کد
- ✓ در صورت استفاده از ابزار اتوماتیک نسبتا سریع می باشند.
- ✓ عیوب در چرخه‌ی توسعه اولیه یافت شوند، که هزینه تعمیر را کاهش میدهد.

محدودیت‌های آنالیز استاتیک کد

- ❖ نیازمند دسترسی به کد منبع یا حداقل کد باینری است.
- ❖ مشکلات مربوط به محیط سیستم عامل مورد استفاده را ، پیدا نخواهد کرد.
- ❖ در صورت اجرای دستی، زمانبر می باشد.
- ❖ ابزارهای اتوماتیک false positive و false negative تولید می کنند.
- ❖ آسیب پذیری‌های موجود در محیط اجرای معرفی شده را پیدا نمی کند.

۹- چند مورد از مزایای تست‌های دینامیک را توضیح دهید و اگر فقط بتوان یکی از تست‌های دینامیک و استاتیک را انجام داد کدام را انتخاب می‌کنید ؟

- ✓ برای انجام تست فقط نیاز به یک سیستم در حال اجرا دارد.
- ✓ هیچ نیازی به دسترسی به کد های منبع یا کد های باینری ندارد.
- ✓ آسیب پذیری ها را در محیط اجرا مشخص می کند.
- ✓ اجازه آنالیز نرم افزار بدون دسترسی به کد واقعی را می دهد.

اگر هیچ دسترسی به منابع یا کدهای باینری نداشته باشیم ، توسعه‌دهنده‌ی نرم افزار نباشیم، ساختمان نرم افزار را متوجه نشویم، یا در حال اجرای pen test (تست نفوذ) یا سایر تست ها بر روی محیط سیستم عامل باشیم، ابزار دینامیک ، در غیر این صورت، از ابزار آنالیز استاتیک استفاده خواهیم کرد. به طور ایده آل، از هر دو استفاده می‌شود.

۱۰- تست فاز هوشمند و گنگ چیست؟

تست فاز هوشمند: فرد داده‌ها را با روشی منطقی به برنامه اعمال می‌کند و معمولا برای پاسخ منتظر می‌ماند و پشته را تغییر می‌دهد. این روش نیازمند دانشی عمیق از هدف و ابزارهای خاص است، اما آنالیز خرابی کمتری مورد نیاز می‌باشد و همچنین نسبت به تست فاز گنگ به تکثیر کمتری از یافته‌ها نیاز دارد.

تست فاز گنگ: فرد به طور سیستماتیک داده ها را به برنامه بدون انتظار برای واکنش مناسب اعمال می‌کند. این روش بسیار نزدیک به حمله‌های DOS می باشد و نیازمند هیچ دانشی در رابطه با هدف و ابزارهای موجود نمی باشد. ولی در هر صورت، آنالیزهای شکست بیشتر ، و تکثیر های بیشتری از یافته-ها نسبت به فازینگ "هوشمند" نیاز دارد.