بسمه تعالی

سوالات امنیت شبکه

جواد مظاهری 9516494

1-ابزارهای vulnerability scanning به چه شکل عمل می‌کنند؟

کاوش اپلیکیشن ها و استفاده از پایگاه داده‌های امضاها برای مبادرت به شناسایی نقاط آسیب‌پذیری

2-علت استفاده از ابزار های اتوماتیک برای vulnerability scanning علی رغم اینکه هیچ جایگزینی برای مرور واقعی Source code توسط خود انسان نمی‌باشد، چیست؟

علاوه بر صرفه‌جویی در زمان و منابع ، اجرای تست بازگشتی(regression testing) به عنوان یک بررسی دوباره به این منظور که آسیب-پذیری‌های احتمالی سهوا یکبار دیگر به کد برنامه معرفی نشده باشند و همچنین آسیب‌پذیری‌هایی که قبلا شناسایی شده‌اند ، در طول پروسه بهبود یابند.همچنین توانایی انجام آنالیزهای dataflow و روش بسیار سریع برای کشف آسیب‌پذیری‌های به اصلاح root-cause level در مقایسه با انسان.

3-Exceptionو Riskها در vulnerability scan چه موقع به وجود می‌آیند؟

Exceptionزمانی که رفع آسیب‌پذیری موجب جلوگیری از اجرای بهینه‌ی نرم‌افزار یا محدود ساختن یک وظیفه‌ی حیاتی و یا حتی نیازمند به طراحی دوباره‌ی کل معماری نرم‌افزار بشود.

Riskها آسیب‌پذیری‌های قابل قبولی هستند که با وجود کنترل‌های جبرانی در محل مناسب یا با کمترین تلاش برای ایجاد این کنترلها ، بهبود می‌یابند.

4-در انجام vulnerability scan برای web applicationها چه آسیب‌پذیری‌هایی باید مورد بررسی قرار بگیرند؟

نباید تنها آسیب‌پذیری‌های "OWASP "TOP 10 مورد بررسی قرار بگیرند، بلکه تمام آسیب‌پذیری‌های نرم افزاری باید چک شود.

5- OWASP top 10چیست و دو نمونه از ابزارهای بررسی آسیب پذیری در حوزه‌ی وب اپلیکیشن را نام ببرید.

لیستی که 10 تا از بحرانی‌ترین خطرات امنیتی در حوزه‌ی web application را در خود جای داده است.

علاوه بر این خطرات ، نمونه‌هایی از آسیب‌پذیری‌ها ، حملات و راه‌های دوری از آن‌ها ارائه شده است.

Nessu توسط شرکت Tenable و AppScan توسط شرکت IBM

6-چرا در حوزه‌ی web application تنها نباید به آسیب‌پذیری‌های خود application پرداخت؟

به این دلیل که Software stack ، شامل سیستم عامل، وب سرورها و همچنین اپلیکیشن سرورها هم می‌توانند دارای آسیب‌پذیری باشند و ما را تهدید کنند.

7-در استفاده‌ی از نرم‌افزارهای open-source در محصول چه چیزهایی باید مراعات شود؟چرا؟

تحقق license و امنیت برای دوری از دعاوی قضایی پرهزینه و زمان‌گیر ؛ بدین معنا که به عنوان یک دارایی مدیریت بشود و در حوزه امنیت باید به همان‌اندازه استانداردها و نیازمندی‌های نرم‌افزار توسعه یافته داخلی امن باشد.

8-در Final Security Review چه مواردی مورد بررسی قرار میگیردند؟

تمام فعالیت‌های امنیتی شامل مدل‌سازی تهدیدات ، خروجی ابزارها و اجرای نیازمندی‌های مطرح شده در ابتدای فرآیند.

9-در فاز 5ام SDL چه متریک‌هایی باید جمع‌آوری شوند؟

درصد تحقق سیاست‌های کمپانی

تعداد ، نوع و شدت مشکلات امنیتی کشف شده در طول تست‌های آسیب پذیری و نفوذ

تعداد مشکلات امنیتی که حل شده‌اند

درصد تحقق نیازمندهای امنیتی و حفظ حریم خصوصی

10-استانداردهای ISO 29147 و ISO 30111 در فاز بعد از نشر محصول چه استفاده‌ای دارند؟

استاندارد ISO 29147 ، راهنمایی‌های برای چگونگی برخورد فروشندگان با گزارشات آسیب‌پذیری دریافتی که بوسیله خریداران و یا کاشفین مطرح شده و نحوه‌ی ارتباط با این کاشفین حال چه خیرخواه و چه ذاتا دشمن باشند را بیان می‌کند.

استاندارد ISO 30111 به بررسی چگونگی حل آسیب پذیری‌ها کشف‌شده که بوسیله یابندگان خارجی یا تست‌های داخلی فراهم شده، می-پردازد.