مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی و امداد)

دانشگاه صنعتی امیرکبیر

خدمات ارزیابی امنیتی نرم‌افزار و صدور گواهی امنیت

نسخه ۱,۰

فهرست مطالب

۱ مقدمه ۱
۱-۱ مراحل صدور گواهی امنیتی ۱
۱-۲ جزئیات تست‌های امنیتی نرم‌افزار ۱
۱-۲-۱ سطح یک ۱
۱-۲-۲ سطح دو ۲
۱-۲-۳ سطح سه ۲

۱ مقدمه

امروزه به علت اهمیت بالای امنیت اطلاعات، بسیاری از سازمان‌ها مایل‌اند تا نرم‌افزارهایی که مورد استفاده قرار می‌دهند، از نظر امنیتی مورد بررسی قرار گیرد تا نقاط ضعف امنیتی این نرم‌افزارها شناسایی شده و ریسک استفاده از آن‌ها برای سازمان تا حد امکان کاهش یابد.

جهت ارائه گواهی امنیتی، نرم‌افزار موردنظر از جنبه‌های مختلف امنیتی مورد بررسی قرار می‌گیرد. گزارش ارزیابی امنیتی در اختیار شرکت تولیدکننده نرم‌افزارنرم‌افزار قرار می‌گیرد و پس از اطمینان از رفع آسیب‌پذیری‌ها و مشکلات امنیتی، گواهی امنیتی صادر می‌شود.

گواهی امنیتی برای یک نسخه مشخص از نرم‌افزار با ماژول‌ها و امکانات معین صادر می‌شود و در صورت ارتقا و افزودن ماژول‌های جدید، بخش‌های جدید می‌بایست مجدداً از نظر امنیتی کنترل شوند.

۱–۱ مراحل صدور گواهی امنیتی

مرحله اول: تعیین وسعت / پیچیدگی نرم‌افزارنرم‌افزار و تخمین زمان تست

مرحله دوم: عقد قرارداد مالی، فنی و حقوقی

مرحله سوم: تست امنیتی نرم‌افزار و ارائه گزارش

مرحله چهارم: رفع آسیب‌پذیری‌ها و تست مجدد بخش‌های آسیب‌پذیر

مرحله پنجم: صدور گواهی

۱–۲ جزئیات تست‌های امنیتی نرم‌افزار

تست امنیتی نرم‌افزار بر اساس استاندارد OWAP ASVS نسخه ۳,۰ در سطوح امنیتی مختلف قابل انجام است.

۱–۲–۱ سطح یک

نرم‌افزار مورد نظر در صورت ایمن بودن در برابر آسیب‌پذیری‌های امنیتی نرم‌افزارها که به راحتی قابل کشف شدن هستند (شامل ۱۰ آسیب‌پذیری اول لیست OWASP و یا لیست‌های مشابه)، استاندارد ASVS سطح ۱ (مبتدی) را دریافت می‌کند.

سطح ۱ معمولاً برای نرم‌افزارهایی مناسب است که در آن‌ها اطمینان کمتری نسبت به نظارت‌های امنیتی صحیح مورد نیاز است و یا برای تأمین یک آنالیز سریع بر روی نرم‌افزارهای سازمانی و همچنین برای

کمک به ایجاد یک لیست اولویت‌بندی شده برای نیازمندی‌های امنیتی به عنوان بخشی از یک پروژه چند فازه استفاده می‌شود.

نظارت‌های سطح ۱ می‌تواند به صورت خودکار توسط ابزارها و یا به صورت دستی و بدون دسترسی به سورس‌کد انجام شود. ما سطح ۱ را به عنوان حداقل نیاز تمام نرم‌افزارها در نظر می‌گیریم.

اغلب تهدیدات نسبت به نرم‌افزارها از طرف مهاجمانی است که از تکنیک‌های ساده و آسان برای شناسایی آسیب‌پذیری‌هایی که راحت کشف و یا راحت بهره‌برداری می‌شوند، استفاده می‌کنند. این برخلاف روش یک مهاجم مصمم است که انرژی زیادی برای حمله به یک نرم‌افزار مشخص صرف می‌کند. بنابراین، اگر اطلاعات پردازش شده توسط نرم‌افزار شما دارای ارزش بالایی است، شما قطعاً نباید به استاندارد سطح ۱ اکتفا کنید.

۱-۲-۲ سطح دو

نرم‌افزار مورد نظر جهت ایمن بودن نسبت به بیشتر خطراتی که امروزه نرم‌افزارها با آن مواجه هستند، می‌بایست استاندارد ASVS سطح ۲ (استاندارد) را دریافت کنند. سطح ۲، اطمینان می‌دهد که مکانیزم‌های امنیتی درستی بکار گرفته شده، این مکانیزم‌ها مؤثر بوده و همچنین در داخل نرم‌افزار به درستی تعبیه شده‌اند. سطح ۲ معمولاً برای نرم‌افزارهایی مناسب است که معاملات B2B (Business2Business) را پردازش می‌کند. این نرم‌افزارها می‌توانند شامل این موارد باشند: نرم‌افزارهایی که اطلاعات مرتبط با بهداشت و درمان را ارزیابی می‌کنند، نرم‌افزار که مرتبط به کسب‌وکارهای حساس هستند، نرم‌افزارهایی که عملکرد آن‌ها از حساسیت بالایی برخوردار بوده و یا مربوط به پردازش اموال هستند.

تهدیدات نسبت به نرم‌افزارهای سطح ۲ معمولاً مربوط به مهاجمان باانگیزه و دارای مهارت بالاست که بر روی یک هدف خاص تمرکز کرده و از ابزارها و روش‌های مؤثر در کشف و بهره‌برداری از ضعف‌های نرم‌افزار، استفاده می‌کنند.

۱-۲-۳ سطح سه

سطح ۳، بالاترین سطح امنیتی در استاندارد ASVS است. این سطح معمولاً منحصر به نرم‌افزارهایی است که نیازمند سطوح قابل توجهی از تاییدات امنیتی هستند، مانند نرم‌افزارهایی که در زمینه نظامی، سلامت و امنیت، زیرساخت‌های حیاتی و غیره مورد استفاده قرار می‌گیرند. سازمان‌ها برای نرم‌افزارهایی که وظیفه اجرای امور حیاتی را دارند و ایجاد مشکل در آن‌ها می‌تواند تأثیر بسزایی در عملکرد و یا حتی بقای سازمان داشته باشد، نیازمند استاندارد سطح ۳ هستند.

یک نرم‌افزار اگر به‌طور مناسبی نسبت به آسیب‌پذیری‌های امنیتی پیشرفته ایمن باشد و همچنین از اصول طراحی امنیتی مناسبی برخوردار باشد، به استاندارد سطح ۳ (پیشرفته) دسترسی پیدا می‌کند. یک نرم‌افزار در سطح ۳ نیازمند آنالیز، معماری و همچنین برنامه‌نویسی دقیق‌تر نسبت به تمامی سطوح دیگر است. یک نرم‌افزار امن به‌گونه‌ای هدفمند (برای تسهیل کردن مقاوم‌بودن، مقیاس‌پذیری و مهم‌تر از همه لایه‌های امنیتی) ماژول بندی شده و هر ماژول از مسؤولیت‌های امنیتی مربوط به خود به صورت دقیق و کامل محافظت می‌کند. این مسؤولیت‌ها شامل نظارت به منظور حصول از محرمانگی (مثلاً با رمزنگاری)، جامعیت (برای مثال اعتبارسنجی ورودی)، دسترسی‌پذیری، احراز هویت (از جمله بین سیستم‌ها)، عدم انکار، مجوز دهی و بازرسی (loggong) است.