تست نرم افزار

ارزیابی امنیت محصولات نرم افزاری

آسیب پذیری چیست؟

- آسیب پذیری یک نقص یا حفره امنیتی در سیستم‌های اطلاعاتی می‌باشد. به طوریکه یک مهاجم می‌تواند با استفاده از این حفره‌ها، به بخشی یا تمام سیستم اطلاعاتی دسترسی، خسارت، دستکاری یا اختلال وارد نماید. تمرکز تست امنیت بر روی شناسایی همه آسیب پذیری‌ها و متصلات آن‌ها می‌باشد. پنجره آسیب پذیری از زمانی که آسیب پذیری تولید می‌شود تا زمانی که حفره امنیتی متصل و تهدید امنیتی خنثی شود، وجود دارد.

امنیت نرم افزار

- امنیت نرم افزار بر تشخیص خطرات بالقوه‌ای تاکید دارد که ممکن است بر نرم افزار تاثیر منفی داشته و همچنین باعث خرابی کل سیستم شوند. اگر خطرات در فرآیند مهندسی نرم افزار زود تشخیص داده شوند، اشکالات طراحی نرم افزار قابل تشخیص هستند و باعث حذف یا کنترل خطرات بالقوه می‌شوند.

فناوری اطلاعات و امنیت

- نیازمندی‌های امنیت در فناوری اطلاعات می‌تواند به طور گسترده و در قالب‌های امنیت نرم افزار، امنیت داده‌ها، امنیت اطلاعات و امنیت شبکه طبقه بندی شود.
- امنیت نرم افزار یا برنامه کاربردی: امنیت برنامه کاربردی بر روی مراحل مختلف چرخه حیات توسعه نرم افزار، فرآیند، ابزارها و تحویل‌ها تمرکز دارد بطوریکه می‌تواند به سمت آسیب پذیری یا نقص نرم افزاری هدایت کند.
- امنیت داده‌ها: امنیت داده‌ها روی سیاست‌ها و روش‌هایی تمرکز دارد که به جلوگیری از خرابی، دسترسی یا سواستفاده تصادفی و عمدی داده‌ها با مجوز دادن یا ندادن به کاربران و برنامه ها می‌پردازد. امنیت داده‌ها در درجه اول روی پشتیبان گیری، رمز نگاری، یا پنهان کردن داده‌ها تمرکز دارد. داده‌ها ممکن است به شکل قابل خواندن و فهمیدن برای انسان باشند یا نباشند.

فناوری اطلاعات و امنیت

- امنیت اطلاعات: به حفاظت اطلاعات از دسترسی غیر مجاز، سواستفاده، دستکاری یا خرابی می‌پردازد. امنیت اطلاعات معمولا به صورت یک نام متناوب از امنیت فناوری اطلاعات استدلال می‌شود. به هر حال امنیت اطلاعات برای فناوری اطلاعات و غیر فناوری اطلاعات کاربردی است. شما ممکن است مستندات با برچسب‌های خیلی مخفی، مخفی یا محرمانه دیده باشید. سه اصل امنیت اطلاعات، محرمانگی، دسترس پذیری و یکپارچگی می‌باشد.
- محرمانگی به سطح دسترسی مربوط می‌شود، تقش‌های دسترسی تعریف می‌شوند و محدودیت‌های دسترسی اعمال می‌شوند.
- دسترس پذیری یعنی اطلاعات زمانی که نیاز است برای کاربران مجاز و قانونی در دسترس باشند.
- یکپارچگی یعنی اطلاعات ارایه شده صحیح و با بیرون سازگار باشد.

فناوری اطلاعات و امنیت

- امنیت شبکه: اکثر سیستم‌های اطلاعاتی برروی شبکه مورد دسترسی قرار می‌گیرند. امنیت شبکه به نظارت و ممانعت از ورود کاربران غیر مجاز یا سو استفاده کنندگان، تهدیدات خنثی کننده روی شبکه مربوط می‌شود.

چه کسی مسئول امنیت اطلاعات است؟

- هر نگهدارنده بانک اطلاعات که با هر یک از فازهای چرخه حیات توسعه نرم افزار درگیر است تا زمان انهدام سیستم اطلاعات مسئول است.

تعریف تست امنیت

- طراحی و تست سیستم‌های نرم افزاری برای اطمینان از ایمن بودن سیستم، مسئله‌ای اساسی است که توسعه دهندگان نرم افزار و متخصصان تست با آن مواجه هستند. اخیرا مسئله‌ی ایمنی و مطمئن بودن به خاطر ازدیاد برنامه‌های کاربردی تجاری برای استفاده روی اینترنت اهمیت مازادی یافته است.
- تست امنیت نرم افزارها، فرآیندی است که توسط یک تیم واجد شرایط ارزیابی، نرم افزار یا برنامه‌های کاربردی را به منظور شناسایی فرصت‌ها جهت بهبود در کنترل امنیت و اعتبارسنجی داده‌ها ارزیابی می‌کند.

دلایل تست امنیت

- امنیت اطلاعات و دسترسی: تست امنیت به یافتن نقاط ضعفی کمک می‌کند که باعث از دست دادن اطلاعات مهم یا اجازه نفوذ به سیستم‌ها می‌شود.
- ثبات سیستم: تست امنیت به بهبود سیستم کمک می‌کند و در نهایت باعث می‌شود تا آن سیستم مدت زمان طولانی‌تری کار کند.
- یکپارچگی سیستم: اگر در مراحل اولیه چرخه حیات توسعه باشیم، تست امنیت این امکان را می‌دهد تا معایب احتمالی در طراحی و پیاده‌سازی سیستم را از بین ببریم.
- بازده اقتصادی: جلوگیری از مشکلات احتمالی نسبت به تلاش برای حل و فصل و عواقب آن بسیار ارزان‌تر است.

ضرورت تست امنیت

- مدت از کار افتادگی: اکثر کاستی‌های امنیتی منجر به از کار افتادن سرویس و از دست دادن درآمد می‌شوند. تصور کنید یک وب سایت مخابراتی مشهور به مدت یک روز پایین بیاید، این امر می‌تواند منجر به از دست دادن درآمد، مشتریان و اعتبار و غیره شود.
- مسائل حقوقی: مسائل امنیتی می‌تواند منجر به مسائل حقوقی و پیچیدگی‌ها شوند. برخی حادثه‌ها می‌توانند منجر به مسائل حقوقی و جرایم شوند.
- آسیب‌های نام تجاری: با از کار افتادن‌های مکرر یا کمبود اعتبار محرمانگی اطلاعات شرکت می‌تواند به شدت آسیب دیده شود و می‌تواند منجر به از دست دادن یا خاموشی کسب و کار شود.
- هزینه: هزینه هر مسئله امنیتی استخراج شده چندین برابر بیشتر از هزینه شناسایی و تعمیر آن‌ها در طول فازهای توسعه و تست نرم افزار می‌باشد.

چه زمانی از تست امنیت استفاده می‌شود؟

- تست امنیت زمانی انجام می‌شود که برخی اطلاعات و دارایی‌های مهم که اهمیت قابل توجهی برای سازمان دارند توسط نرم افزار کاربردی مدیریت می‌شوند.
- فعالیت‌های دقیق تست امنیت انجام می‌شوند تا نشان دهند که سیستم پاسخ‌گوی نیازهای مشخص شده امنیتی می‌باشد و آسیب پذیری‌های امنیتی را شناسایی می‌کند. وسعت تست تا حد زیادی به خطرات امنیتی بستگی دارد و مهندسین تست برای انجام تست امنیت با توجه به مهارت‌هایشان انتخاب می‌شوند.

چه کسی باید تست امنیت را انجام دهد؟

- اکثر تکنیک‌های تست امنیت راهنما هستند و نیاز به یک فرد برای آغاز و انجام تست دارند. ابزارهای خودکار می‌توانند در اجرای کارهای ساده مفید باشند در حالی که کارهای پیچیده همچنان تا حد زیادی به افراد باهوشی از مهندسین تست نیاز دارند.
- صرف نظر از نوع تست، مهندسین تست که امنیت را بررسی کرده و انجام می‌دهند باید دانش کافی مرتبط با شبکه و امنیت را داشته باشند، که از جمله آن‌ها تخصص و مهارت در زمینه‌های زیر:
- امنیت شبکه
- دیواره های آتش
- سیستم تشخیص نفوذ
- سیستم عامل‌ها
- پروتکل‌های برنامه نویسی و شبکه

اهداف تست امنیت

- نقص‌های امنیتی به راحتی انواع دیگر نقص‌ها ظاهر نمی‌شوند. بنابراین تست امنیت برای شناسایی نقص‌هایی که شناسایی آن‌ها واقعا مشکل است انجام می‌شود. اهداف تست امنیت می‌تواند موارد زیر باشد:
- حصول اطمینان از اینکه دقت کافی جهت شناسایی ریسک‌های امنیتی اعمال می‌شود.
- حصول اطمینان از این که یک مکانیسم واقعی برای تعریف دسترسی به سیستم وجود دارد.
- حصول اطمینان از اینکه تخصص کافی برای تست امنیت وجود داشته باشد.
- برای انجام تست‌های معقول جهت تایید عملکرد مناسب اقدامات امنیتی، پیاده سازی شده، می‌باشد.

شاخص‌ها یا خصوصیات تست امنیت نرم افزارها

- یک هدف امنیت، سطحی از امنیت اطلاعات می‌باشد که یک سیستم یا محصول باید آن را در نظر بگیرد. اهداف امنیتی معمولا توسط ارزیابی تهدیدات احتمالی امنیت اطلاعات و اقدامات متقابل آن‌ها تعیین می‌شوند. به طور کلی، اهداف امنیتی باید تعریف شوند تا در اولویت بندی نیازمندی‌های امنیتی سیستم کمک کنند. این اهداف امنیتی بیان کننده یک سری شاخص‌ها می‌باشند که در زیر به چند نمونه از شاخص‌هایی که از فرآیندهای مختلف تست امنیت نرم‌افزارها استخراج گردیده است اشاره می‌کنیم.
- احراز هویت: شناسایی یک شخص یا یک برنامه قبل از دسترسی به سیستم اطلاعات است. احراز هویت می‌تواند به شکل‌های مختلف پیاده‌سازی شود مانند نام کاربری و رمز عبور، سوال و جواب‌های محرمانه، احراز هویت یا توکن و یا حتی رمز عبور یکبار موقتی ارسال شده با اس ام اس. برخی از برنامه‌های کاربردی ممکن است از یک روش یا ترکیبی از چند روش برای احراز هویت استفاده نمایند.

شاخص‌ها یا خصوصیات تست امنیت نرم افزارها

- مجوز دسترسی: کاربر یا برنامه یکبار احراز هویت می‌شود، سیستم اطلاعات باید دسترسی به هر مجوز یا مجموعه مجوزها را برای کاربر یا برنامه محدود نماید. مجوز دسترسی معمولا با یک لیست کنترل دسترسی یا با گروه‌بندی کاربران و تعریف امتیازات و محدودیت‌ها برای هر یک از گروه‌ها یا اعطا نمودن و یا لغو دسترسی‌ها برای کاربران پیاده‌سازی می‌شود.
- محرمانگی: به قابلیت حفاظت اطلاعات یا داده‌های سیستم‌های اطلاعاتی از دسترسی کاربران غیر مجاز مربوط می‌شود. سیستم اطلاعاتی باید محرمانگی اطلاعات را در همه مراحل پردازش، ذخیره سازی و نمایش اطلاعات حفظ نماید.
- دسترسی پذیری: دسترس پذیری سیستم اطلاعاتی ممکن است مرتبط با تست امنیت به نظر نرسد، با این حال سیستم‌های کاربردی می‌توانند با مدت از کار افتادن طولانی مواجه باشند و همچنین بروزرسانی بسته امنیتی باید به حداقل زمان از کار افتادن محدود شوند. دسترس پذیری منجر به دستیابی پذیری سیستم اطلاعات و سرویس‌های آن زمانی که لازم است توسط کاربران مجاز استفاده گردد می‌شود.

شاخص‌ها یا خصوصیات تست امنیت نرم افزارها

- یکپارچگی: به قابلیت اطمینان، ثبات و صحت اطلاعات ارایه شده توسط سیستم اطلاعات به کاربران مربوط می‌شود. اطلاعات ارایه شده به کاربران باید به ازای گروه‌های کاربری، امتیازات و محدودیت‌ها باشد.
- انکار ناپذیری: زمانی که یک دریافت کننده سرویس‌های درخواست شده را از فرستنده دریافت می‌کند به فرستنده یک پیام تایید به صورت دیجیتالی ارسال می‌کند که اطلاعات با موفقیت دریافت شدند به عنوان مثال گواهی‌های دیجیتال. این نه فقط به عنوان تصدیق به کار برده می‌شود بلکه به اعتبارسنجی فرستنده و گیرنده که واقعی هستند کمک می‌کند.

شاخص‌ها یا خصوصیات تست امنیت نرم افزارها

- حفاظت از منابع: طرح حفاظت از منابع تضمین می‌کند که تنها کاربران مجاز می‌توانند به اجزای سیستم دسترسی داشته باشند.
- فعالیت‌های ممیزی امنیت: نظارت بر رویدادهای امنیتی جهت ارایه یک گزارش از دسترسی و عدم دسترسی را انجام می‌دهد. سوابق دسترسی موفق به شما می‌گوید که چه کسی چه کاری را روی سیستم شما انجام می‌دهد. سوابق دسترسی ناموفق به شما می‌گوید که چه کسی در تلاش است امنیت شما را از بین ببرد و یا شخصی در دسترسی به سیستم شما دچار مشکل شده است.
- قابلیت همکاری: در سیستم‌های ارتباطی متقابل، این قابلیت وجود دارد که دو یا چند سیستم یا مولفه جهت تبادل داده‌ها و اطلاعات، ذاتا مبتنی بر نرم افزار باشند. قابلیت همکاری حاکی از وجود سیستم‌های متنوعی است که باید داده‌ها و سرویس‌هایی را مبادله کنند.

شاخص‌ها یا خصوصیات تست امنیت نرم افزارها

- سازگاری: قابلیت اجرا شدن بدون تغییر نرم افزار بر روی کامپیوتری دیگر را سازگاری می‌نامند.
- استحکام: درجه‌ای که یک سیستم همچنان به عملکرد خود در مقابل ورودی های نامعتبر و یا شرایط محیطی استرس زا ادامه می‌دهد یا به عبارتی به توانایی سیستم‌های نرم افزاری برای نشان دادن واکنش مناسب به شرایط غیر طبیعی گفته می‌شود.
- قابلیت استفاده: درجه‌ای که یک محصول می‌تواند توسط کاربران خاصی برای رسیدن به هدفی معین، مورد استفاده قرار گرفته و در حین استفاده، ضمن داشتن اثر بخشی و کارایی، رضایت کاربر را در زمینه‌ی مورد استفاده تامین کند.

شاخص‌ها یا خصوصیات تست امنیت نرم افزارها

- مصونیت: نیازمندی مصونیت یک نیازمندی امنیتی می‌باشد که مشخص می‌کند تا چه حدی یک برنامه یا کامپوننت باید خودش را از نفوذ برنامه‌های غیر مجاز نامطلوب محافظت کند.
- بقا و ماندگاری: تست امنیت به بهبود سیستم کمک می‌کند و در نهایت باعث می‌شود تا آن سیستم به مدت زمان طولانی‌تر کار کند.

چه برنامه‌هایی به تست امنیت نیاز دارند؟

- برنامه‌های کاربردی تحت وب
- برنامه‌هایی با اطلاعات شخصی یا تجاری حساس
- سیستم‌های پرداخت و گزارش‌های آماری
- برنامه‌های کاربردی حساس به اعوجاج داده‌ها
- برنامه‌های کاربردی اجتماعی

مدیریت ریسک و تست‌های امنیت

- پزشکان امنیت نرم افزار کارهای متفاوتی برای مدیریت ریسک‌های امنیتی نرم افزار انجام می‌دهند از جمله:
- ایجاد موردهای سو استفاده امنیتی
- لیست کردن نیازهای اصلی امنیتی
- انجام تحلیل معماری ریسک
- ساخت برنامه‌های تست امنیت مبتنی بر ریسک
- خوب به کار بردن ابزارهای تحلیل استاتیک
- انجام تست‌های امنیت
- انجام تست نفوذ در محیط نهایی

تست امنیت در مقابل تست متعارف نرم افزار

- تست امنیت به جای تایید کردن آنچه که برنامه باید انجام دهد، آنچه که برنامه نباید انجام دهد را تست می‌کند. تست امنیت الزامات منفی را که هرگز نباید رخ دهند تست می‌کند. به عنوان مثال یک کاربر خارجی نباید قادر به تغییر محتویات وب باشد. تست متعارف یک نیازمندی قطعی را برای ایجاد شرایطی که این نیازمندی تایید شود تست می‌کند.

روش‌های اصلی تست امنیت

- تست امنیت رسمی: ایده اصلی روش رسمی آن است که یک مدل ریاضی از نرم افزار بسازد و مشخصات نرم افزار را با حمایت برخی از خصوصیات زبان رسمی فراهم کند. ایده اصلی آن است که مدل رسمی نیازمندی‌های امنیتی را مانند مدل ماشین حالت دایر کند. تست امنیت با جستجوی فضای حالت برای حالت خاص در نقض محدودیت‌های امنیتی که آن همچنین یک حالت ناامن است انجام می‌شود.
- مشکل این روش این است که به کارمندان با سطح کیفیت بالا جهت تجزیه و تحلیل نیاز دارد که بسیار وقت گیر است.

روش‌های اصلی تست امنیت

- تست امنیت مبتنی بر مدل: تست مبتنی بر مدل، مدلی را بر اساس رفتار و ساختار نرم افزار می‌سازد و سپس موارد تست را از مدل تست استنتاج می‌کند. در نهایت نرم افزار برای اجرای موارد آزمون برده می‌شود. رفتار سیستم نرم افزار می‌تواند به وسیله دنباله ورودی و خروجی، نمودار فعالیت، نمودار دنباله، نمودار همکاری، شرایط و یا جریان داده‌ها شرح داده شود. مدل رفتار نرم افزار و مدل ساختار، توصیف دقیقی از نرم افزار تست شده می‌باشد که می‌تواند برای تولید موارد آزمون مورد استفاده قرار گیرد.

روش‌های اصلی تست امنیت

- تست امنیت مبتنی بر تزریق خطا: تزریق خطا بر روی تعامل بین نرم افزار و محیط، شامل ورودی کاربر، فایل سیستم، واسط شبکه و متغیر محیط تمرکز دارد. ایده اصلی تست این مورد است که آیا نرم افزار می تواند با استفاده از انواع مختلف بسته‌های پروتکل به درستی پاسخگو باشد. به منظور کشف آسیب پذیری‌های نرم افزار برخی داده‌های ناقص باید به داخل بسته‌های مختلف پروتکل تزریق شود.

روش‌های اصلی تست امنیت

- تست فازی: برای کشف آسیب پذیری‌های امنیتی که بیشتر مورد توجه هستند، موثر است. تست فازی داده‌های تصادفی را به برنامه تزریق می‌کند. این روش برای تست اینکه آیا آن برنامه می‌تواند به طور نرمال با ورودی درهم و برهم اجرا شود یا خیر، می‌باشد. تست فازی غیر منطقی است، فقط داده‌های درهم ایجاد می‌کند. تست فازی نقص‌های نرم افزار تست شده را پیدا می‌کند به طوریکه برای روش‌های دیگر تست منطقی مشکل است.

روش‌های اصلی تست امنیت

- تست بررسی آسیب پذیری: به عنوان یک روش مهم برای یافتن خطرات امنیتی نرم افزار شامل بررسی فضای تست و بررسی نقص‌های شناخته شده می‌باشد. بررسی فضای تست با پورت شبکه، رشته، داده‌های شبکه و بررسی عناصر دیگر سروکار دارد. مانند از طریق بررسی پورت شبکه می‌تواند پی ببردکه آیا پورت نرم افزار باز شده است یا خیر که نباید باز باشد.

روش‌های اصلی تست امنیت

- تست مبتنی بر صفت خاص: این روش کد مربوط به صفت خاص را توسط تکنولوژی برنامه برش استخراج می‌کند و خطای کد را در برابر ویژگی صفت امنیتی کشف می‌کند. تست مبتنی بر صفت بر روی برخی از ویژگی‌های امنیتی خاص تمرکز دارد که می‌توانند نیازمندی‌های طبقه بندی و اولویت بندی را ملاقات کنند.

روش‌های اصلی تست امنیت

- تست امنیت مبتنی بر جعبه سفید: تحلیل استاتیک به عنوان یکی از روش های معمول مبتنی بر جعبه سفید، در پیدا کردن باگ های امنیتی مانند سرریز شدن بافر خوب است. تکنولوژی‌های اصلی تحلیل استاتیک، استنتاج، تجزیه و تحلیل جریان داده‌ها و تجزیه و تحلیل محدودیت هستند.

روش‌های اصلی تست امنیت

- تست امنیت مبتنی بر ریسک: اولین گام در تست مبتنی بر ریسک، شناسایی خطرات امنیتی و پتانسیل از دست رفته احتمالی مرتبط با آن خطرات می‌باشد. این روش برای تایید ایمنی در برابر خطرات خاصی که از طریق تلاش‌های تجزیه و تحلیل خطر شناسایی شده‌اند تلاش می‌کند. تست مبتنی بر ریسک به نیازمندی‌های منفی اشاره می کند، آنچه که یک سیستم نرم افزاری نباید انجام دهد. تست برای نیازهای منفی از تجزیه و تحلیل خطر مشتق شده است و به طور کلی نه تنها خطرات سطح بالای شناسایی شده در طول فرآیند طراحی را پوشش می‌دهد بلکه همچنین به خطرات سطح پایین حاصل از خود نرم افزار نیز می‌پردازد.

مراحل تست امنیت

تست امنیت در چرخه حیات امنیت در چهار مرحله است. همه آن مراحل در فرآیند تست امنیت به یک اندازه حائز اهمیت می‌باشند.

- جمع‌آوری نیازهای تست امنیت
- تحلیل و طراحی تست
- پیاده‌سازی بستر تست
- تهیه گزارش از تست

مراحل تست امنیت

- جمع‌آوری نیازهای تست امنیت: این مرحله محدوده تست امنیت را تعریف می‌کند، این کار به شناسایی همه عناصر از دست رفته یا رخنه‌های موجود در تسخیر نیازهای امنیتی کمک خواهد کرد. مرحله بعدی اختصاص وزن‌های مناسب به زیر پارامترهای مختلف امنیتی، خواهد بود. این وزن‌ها به طور معمول توسط طبیعت حوزه کسب و کار که نرم افزار برآورده می‌سازد و داده‌های اکتشافی موجود توسط کارشناسان تست امنیت تعیین خواهند شد.

مراحل تست امنیت

- تحلیل و طراحی تست امنیت: ابتدا وزن‌ها برای هر یک از پارامترهای امنیتی نهایی می‌شوند، کار بعدی ایجاد سناریوی تست برای تست نیازمندی‌های امنیتی می‌باشد. وزن‌های اختصاص یافته به هر یک از زیر پارامترها، تعدادی از سناریوهایی را پیشنهاد می‌کنند که جهت تست یک نیازمندی خاص و پیچیده درگیر هستند.
همچنین رویکرد پارامتریک در شناسایی میزان داده‌هایی که برای اجرای تست مورد نیاز خواهند بود و همچنین توزیع داده‌ها بر اساس سناریوهای مختلف کمک می‌کند. همچنین این رویکرد به شناسایی انواع ابزارهایی که مورد نیاز خواهند بود، کمک می‌کند و تعیین کننده مناسب بودن یک ابزار برای انواع تست می‌باشد.

مراحل تست امنیت

- پیاده سازی بستر تست امنیت: در مورد تست در سطح برنامه کاربردی، رویکرد تست آسیب پذیری‌های امنیتی باید بسیار منطقی باشد. در اینجا امنیت منطقی با کاربرد پردازش‌های کامپیوتری و یا قابلیت‌های ارتباطی جهت دسترسی نادرست به اطلاعات سرو کار دارد. دوم این که کنترل دسترسی می‌تواند بر اساس نوع مجرم و همانند گروه‌بندی کارکنان، تقسیم شود مانند کارمند، مشاور، پرسنل خدمات. نوع تست برای انجام شدن بستگی به شرایط مختلف در حال تست دارد و می‌تواند شامل:
تعیین این که منابع حفاظت شده شناسایی می‌شوند، و دسترسی برای هر یک از منابع تعریف می‌شود، باشد.
دسترسی می‌تواند برای یک برنامه یا شخص تعریف شود، ارزیابی اینکه آیا رویه‌های امنیتی طراحی شده به درستی پیاده سازی شده‌اند و عملکرد آنها مطابق با مشخصات می‌باشد. دسترسی‌های غیر مجاز می‌توانند در سیستم‌های آنلاین برای حصول اطمینان از اینکه سیستم قادر به شناسایی و جلوگیری از دسترسی منابع غیر مجاز می‌باشد، جستجو شوند.

مراحل تست امنیت

- بسیاری از سناریوهای تست امنیت به سمت تست سیستم در شرایط غیر عادی در حال حرکت هستند. این از چالش برای شبیه سازی شرایط واقعی زندگی که سناریوهای تست نیاز دارند کناره‌گیری می‌کنند. ابزارهای مختلفی وجود دارند که می‌توانند برای تست آسیب پذیری‌های مختلف که سیستم ممکن است داشته باشد مورد استفاده قرار می‌گیرند. انتخاب چنین ابزاری بوسیله میزان آسیب پذیری تعیین می‌شود، این ابزار قادر به تست می‌باشد و سفارشی کردن ابزار و تست سیستم با استفاده از هر دو دیدگاه داخلی و خارجی باید امکان پذیر باشد. کاربران محلی دید داخلی هستند و کاربران خارجی دید خارجی را تشکیل می‌دهند. ابزارهای مختلفی وجود دارند که می‌توانند برای شبیه سازی رخنه‌های مختلف کنترل دسترسی برنامه ریزی شوند.

مراحل تست امنیت

- تفسیر کردن گزارشات تست امنیت: تست‌ها یکبار اجرا شده‌اند و شکاف‌های امنیتی شناسایی شده‌اند، شکاف‌ها به منظور پیشنهاد بهبودها نیاز به تجزیه و تحلیل دارند. گزارش‌ها در صورت امکان بیش از یکبار نیاز به ارزیابی دارند. این گزارشات ممکن است گمراه کننده باشند و نقاط ضعف واقعی ممکن است در جاهای دیگر وجود داشته باشند یا ممکن است اصلا وجود نداشته باشند.
در گزارشات تست امنیت وجود یک کارشناس امنیتی برای کشف آسیب پذیری‌های گزارش شده و استخراج گزارش مشکل واقعی ضروری است. ابزارهای مختلفی برای تهیه گزارش امنیتی وجود دارد. در هنگام انتخاب یک ابزار گزارش‌گیری امنیتی، باید پارامترهای زیر در نظر گرفته شوند:
- با وسعت آسیب پذیری، ابزار قادر به تهیه گزارش باشند.
- باید سفارشی کردن ابزار امکان پذیر باشد.
- تست سیستم با استفاده از دیدهای داخلی و خارجی.

مراحل تست امنیت

- تجزیه و تحلیل، گزارش فهرستی از آسیب پذیری‌ها و مجموعه‌ای از ویژگی‌های امنیتی که در حین کار تولید می‌شوند را به اتمام می‌رساند. فهرست آسیب پذیری‌ها طبقه بندی می‌شوند. سطح طبقه بندی آسیب پذیری توسط میزان خطر موجود در رخنه امنیتی و هزینه رفع نقص تعیین می‌شود. طبقه بندی انجام می‌شود آسیب پذیری برطرف شده و مجددا تست می‌شود.

رویکرد تست امنیت

- **برنامه ریزی:** قوانین شناسایی می‌شوند، تصویب مدیریت نهایی میشود و اهداف تست مقرر می‌شوند. مرحله برنامه ریزی زمینه را برای یک تست نفوذ موفقیت آمیز فراهم می‌کند. هیچ تست واقعی در مرحله برنامه ریزی رخ نمی‌دهد.
- **کشف:** تست واقعی را شروع می‌کند. قسمت دوم مرحله کشف تحلیل آسیب پذیری است. در طی این مرحله، خدمات، برنامه‌ها و سیستم عامل‌های میزبانان بررسی شده در برابر آسیب پذیری پایگاه داده‌ها مقایسه شوند(برای اسکنرها آسیت پذیری این روند به طور اتوماتیک انجام می‌شود). به طور کلی تسترها برای شناسایی آسیب پذیری‌ها، از پایگاه داده خود یا پایگاه داده‌های عمومی بطور دستی استفاده می‌کنند. این فرآیند دستی، برای شناسایی آسیب پذیری‌های جدید یا مبهم بهتر است اما بسیار کندتر از یک اسکنر خودکار می‌باشد.
- حمله: در قلب هر تست نفوذ می‌باشد. این جایی است که آسیب پذیری‌های بالقوه از قبل شناسایی شده با تلاش برای استخراج آنها بازبینی می‌شوند. اگر یک حمله موفقیت آمیز باشد، آسیب پذیری تایید شده و حفاظ‌های امنیتی شناسایی می‌شوند. اغلب سواستفاده‌هایی که در حین اجرای حمله اعمال می شود حداکثر سطح دسترسی را که می‌تواند توسط یک حمله‌گر به دست آورده شود بیان نمی‌کنند.

رویکرد تست امنیت

- **گزارش گیری:** در پایان تست یک گزارش کلی تست برای توصیف آسیب پذیری‌های شناسایی شده توسعه داده می‌شود، یک رتبه بندی ریسک ارائه می‌شود و راهنمایی برای کاهش نقاط ضعف کشف شده ارایه می‌شود. همیشه چهار نکته زیر را قبل از تست امنیت نرم افزار یادآوری می‌کنیم:
- درک عمیق آنچه شما تست می‌کنید.
- فکر از روی بدخواهی در مورد هدف.
- حمله به هدف با استفاده از ایده‌های مخرب
- مطلع شدن از حملات جدیدی که ممکن است روی هدفی که شما تست می‌کنید تاثیر بگذارد.

استراتژی تست امنیت

۱. مدل‌سازی تهدید برای تست امنیت:

- مدل‌سازی تهدید بخش مهمی از تست امنیت می‌باشد. در فرآیند ایجاد مدل تهدید باید نمایندگانی از تیم طراحی، تیم برنامه‌نویسی و تیم تست، حضور داشته باشند. هر عضو دید و دانش متفاوتی را در مورد محصول به ارمغان می‌آورد. مدل تهدید به طور معمول از پنج بخش اصلی تشکیل شده است:
- شناسایی اهداف امنیت
- نمای کلی برنامه
- تجزیه برنامه
- شناسایی تهدیدها
- شناسایی آسیب پذیری‌ها

استراتژی تست امنیت

۲. **یافتن نقاط ورود:** یک نقطه ورود مکان ورود برنامه می‌باشد. برای یک مهاجم یا حمله‌گر، نقطه ورودی، محل مطلوبی برای یافتن تلاش در شکست برنامه می‌باشد. در تست امنیت، مهم است نقطه ورودی که در معرض خطر هستند را شناسایی و بررسی کنید.

استراتژی تست امنیت

- در زیر فهرست بعضی از شایع‌ترین نقاط ورودی که مهاجمان برای آسیب پذیری های امنیتی در برنامه‌های کاربردی جستجو می‌کنند، بیان شده است اما این لیست به هیچ وجه همه موارد را شامل نمی‌شود:
  فایل‌ها، سوکت‌ها، درخواست‌های پروتکل انتقال ابر متن، پاسخ‌های مخرب سرور، زبان پرس‌وجوی ساختار یافته، رجیستری، ایمیل، آرگومان‌های خط فرمان
- در تست امنیت مهم است که نقاط ورودی بسیاری را تا آنجایی که می توانید شناسایی کنید. در ادامه شما نقاط ورودی برنامه‌های خود را می‌دانید، بهتر است قادر به اولویت بندی و هدفمند سازی تلاش‌های تست امنیت خود باشید. در غیر این صورت ممکن است آسیب پذیری‌های متعددی را از دست بدهید.

استراتژی تست امنیت

۳. حملات امنیتی مختلف

۳.۱مدیریت session: به منظور حفظ هویت کاربر در طول درخواست‌های متعدد لازم است. کوکی‌ها اطلاعاتی هستند که توسط سرور بر روی دستگاه کلاینت ذخیره می‌شوند. آنها اساسا جفت اطلاعات نام-مقدار می‌باشند که وب سایت برای بازیابی داده‌ها هنگامی که کاربر دوباره از سایت بازدید می‌کند یا در طول درخواست‌ها استفاده می‌کند. مهاجمان می‌توانند در این داده‌ها برای به دست آوردن اطلاعات فضولی کنند. حملات مختلفی که می‌توانند اتفاق بیفتد عبارتند از:

- انقضای session ناکافی: در این نوع حمله نرم افزار به مهاجم اجازه می‌دهد که از شناسه‌های session قدیمی استفاده مجدد کند. مهاجم نیاز دارد که شناسه session قدیمی را بداند و می‌تواند از آن مجددا استفاده کند.

سناریو: همه صفحات برنامه

تست: آزمون باید انجام شود تا مطمئن شویم که استفاده از برنامه خاتمه یافت یا session پس از مدتی منقضی شده است.

استراتژی تست امنیت

- ربودن session: اگر شناسه‌های session قابل پیش‌بینی باشند، این احتمال وجود دارد که مهاجم بتواند شناسه session را حدس زده و از آن استفاده کند.
- سناریو: هر صفحه پس از ورود به سایت
- تست: تست باید برای بررسی اینکه آیا شناسه‌های session قابل پیش بینی هستند یا خیر، انجام شود. تست برای بررسی چندین session از همان کاربر مجاز نمی‌باشد. تست بررسی می‌کند که اطلاعات مهم با استفاده از پروتکل HTTPS منتقل می‌شوند.

استراتژی تست امنیت

- ۳.۲رفع خطا: این اشتباه رایج توسعه دهنده است که خطاها را بدرستی رفع نمی‌کند و بسیاری از اطلاعات افشا می‌شوند که منجر به آشکار شدن اطلاعات برای حمله می‌گردد. حملات مختلفی که می‌توانند اتفاق بیفتد عبارتند از:
- موارد عمومی امنیت: برای کاربرد نافذ، باید برخی از موارد تست طراحی شوند که حاوی موارد زیر که شامل تعداد زیادی از موارد تست هستند می‌باشند:
- تست سرریز شدن بافر
- تست تزریق sQl
- تست فرمت رشته
- تست داده‌های تصادفی
- جهش اتفاقی داده‌های معتبر تست