بسمه تعالی

سوالات مربوط به ارائه درس امنیت

کتاب نرم افزار امن – بخش سوم – فصول ۱۰-۱۱-۱۲-۱۳

بهنام مشرف – ۹۵۱۶۳۸۴

زیر نظر جناب آقای دکتر علی فانیان

۱. آقای McGraw در کتاب و مقاله خود یک دسته بندی مترقی برای اشکالات کدنویسی مطرح کرده اند. ۷+۱ قلمرو آن دسته بندی را نام برده و هر کدام را مختصرا توضیح دهید.

الف. ارزیابی ورودی و نمایش آنها: اکثر خطاها به دلیل بررسی نکردن ورودی برنامه‌هاست. برنامه‌ها میبایست تنها ورودی های مجاز را قبول کنند و از ورود ورودیهای غیر مجاز ممانعت ورزند.

ب. سو استفاده از api ها: انواع اختلالاتی که بین درخواست کننده API و پذیرنده اتفاق میافتد. از مثالهای این قلمرو استفاده از API های غیر امن است که باعث سواستفاده میشود.

پ. ویژگی های امنیتی: اگر نرم افزار مزبور یک نرم افزار امنیتی است روالهای امنیتی آن باید به خوبی کار کنند.

ت. زمان و حالت: در پردازش‌های موازی و گسترده چون سنکرون بودن نقش مهمی دارد لذا زمان عنصر کلیدی در اینگونه برنامه هاست. برنامه‌هایی از این دست یا انواع دیگر نباید با دستکاری زمان، توقف یا تندتر اجرا شدن و ... از کار بیفتند.

ث. اداره کردن خطاها: برنامه ها در حالاتی که به استثنا برمیخورند باید به خوبی آن را کنترل کنند و با exception از حالت اجرا خارج نشوند.

ج. کیفیت کد: کیفیت برنامه نویسی از موارد بسیار مهم است. به طور مثال عدم استفاده از اشارگرهای تهی یا عدم آزاد کردن دوباره حافظه گرفته شده و یا مشکل نشت حافظه از موارد این قلمرو هستند

چ. کپسوله سازی: مرزبندی و ایجاد مو انع بین قسمتها و اشیا در برنامه به طوری که به طور مستقیم به یکدیگر دسترسی نداشته باشند.

ح. محیط: هر چیزی که بیرون از کد برنامه است اما مربوط به امنیت برنامه میشود

۲. بخش کلی دانش تشخیص (diagnostic knowledge) **شامل سه دسته جزیی الگوی حملات، اکسپلویت ها و آسیب پذیری ها میشود. این سه مورد را به طور کامل توضیح دهید و روابط آنها با هم را مشخص نمایید.**

آسیب پذیری ها: این دانش شامل گزارش ها و توضیحاتی در مورد ضعف های تجربه شده در نرم افزارهای مختلف است.

اکسپلویت ها: توضیحاتی در مورد اینکه چگونه میتوان از آسیب پذیری ها استفاده نمود و برنامه های خاصی را از کار انداخت یا تصاحب کرد.

الگوی حملات: مجموعه‌ای منظم از اکسپلویتها که برای نیل به هدفی امنیتی استفاده میشوند.

۳. یک جدول در پایگاه داده برای کاربران را در نظر بگیرید. این جدول شامل (uid, name, password, level) است که uid کلید اصلی جدول خواهد بود. کاربر پس از احراز اصالت برای دسترسی به یک منبع باید تایید شود. برای کنترل دسترسی از API مربوط به دسترسی ها به نام checkAccessList که در ۲ حالت گرفتن نام یا شناسه کار میکند، استفاده میشود. کدام یک از دو کد زیر امن تر است؟ چرا؟ این اشکال مربوط به کدام دسته از قلمروهای سوال قبل میباشد؟

کد ۱	کد ۲

field = user.id;
If (checkAccessList(field, resource)){
Allow();
Else
Deny();
	field = user.name;
	If (checkAccessList(field, resource)){
	Allow();
	Else
	Deny();

کد ۱ امن تر میباشد چرا که ممکن است دوکاربر با نام یکسان باشند ولی دو کاربر با یک شناسه یکسان امکان وجود در پایگاه داده را ندارد. پس حمله گر میتواند با تغییر یا گذاشتن نامی خاص که با کاربر دیگر یکسان باشد به منبع دسترسی پیدا کند. این اشکال به دلیل عدم استفاده صحیح از API به وجود آمده است و مربوط به قلمرو سواستفاده از API هاست.

٤. دانش امنیت توسط آقای McGraw به سه بخش کلی تقسیم شده است. آنها را نام برده و دو تا از آنها را به اختیار توضیح دهید.

دانش چشم انداز(prespective knowledge)، دانش تشخیص(diagnostic knowledge)، دانش تاریخی(historiclal knowledge)

دانش چشم انداز: این دانش سه دسته جزئی از دانش های امنیتی را در خود جا میدهد. اصول، راهنماها و قوانین این سه دسته هستند. این بخش زنجیره‌ای از اصول سطح بالا که فلسفی میشود(مثلا اصول حداقل دسترسی) تا قوانین بسیار خاص و تکنیکی (مثل عدم استفاده از gets() در C به دلیل عدم اعمال محدودیت در اندازه ورودی) را شامل میشود.

دانش تشخیص: شامل سه دسته دانش جزئی الگو حملات، اکسپلویت ها و آسیب پذیری ها میشود. این دانش به تمام متخصیصین کمک میکند تا بتوانند اکثر مشکلات و مسائلی را که باعث ضعف امنیتی میشوند را شناخته و راه مقابله با آنها را یادبگیرند.

٥. هر یک از موارد زیر مربوط به کدام دسته بندی های سوال قبل میشوند؟

الف. Sql injection ارزیابی ورودیها

ب. مولد شبه تصادفی نتواند عددی واقعا تصادفی برای رمزنگاری تولید کند ویژگی‌های امنیتی

ج. استفاده از متغییری بدون مقدار دهی اولیه کیفیت کد

د. خطای سرریز بافر ارزیابی ورودیها

ه. race condition زمان و حالت

و. استفاده اشتباه از SSL ویژگی‌های امنیتی

٦. سه گام ساخت نرم افزارهای برزگ در شرکتهای بزرگ را نام برده و دو مورد را به دلخواه توضیح دهید.

برنامه ریزی و ارزیابی، ساختن و آزمون، توزیع و بهبود

برنامه ریزی و ارزیابی: این گام شامل مطلع شدن از اهداف برنامه بزرگ، جمع آوری اطلاعات برای ارزیابی حالت کنونی و مقایسه با حالت هدف است. اگر بازبینی کد در یک مرحله توسط توسعه دهندگانی انجام شود که از ابزارهای static analysis (آنالیز استاتیک) استفاده نمیکنند قطعا به وضوح در برنامه های بزرگ بین هدف مورد انتظار و واقعیت فاصله زیادی خواهد بود.

ساختن و آزمون: این مرحله بهتر است با شناخت بسیار خوبی از پروژه شروع شود تا برای آزمون امکانات کافی در اختیار باشد

٧. مدیریت بدون اندازه گیری و آموزش بدون ارزیابی را در شرکتها برزگ نرم افزاری توضیح دهید.

یک نظریه پایه مدیریت میگوید: شما نمیتوانید چیزی را که سنجه نکردید مدیریت کنید. بسیاری از شرکت های بزرگ نرم افزاری که ادعای ساخت نرم افزارهای امن را دارند وقتی از انها میپرسی کارایی نرم افزار خود را چگونه سنجیدید چیزی برای گفتن ندارند. مدیریت بدون اندازه گیری و سنجیدن امور غیر ممکن است. فلذا برای امن سازی نرم افزارها نیازمند معیارهایی برای سنجیدن میزان امنیت هستیم

آموزش تنها برای توسعه دهندگان نرم افزارهای امنیتی نیست بلکه هر کس در ساختن اینگونه نرم افزارها نقش دارد باید آموزش ببیند. این آموزشها بدون آزمون و بررسی در حوزه امنیت نرم افزاری بدون فایده است.

٨. ٦ فازی که Cigital برای تغییر نرم افزارها دنبال میکند را نام برده و یکی را به دلخواه توضیح دهید.

الف. توقف خونریزی(stop the bleeding) ب. برداشت میوهای آویزان دم دستی(hravast the low-hanging fruit) ج.ساختن شالوده(establish foundation) د. شایستگی هسته مهارت ها (craft core competencies) ه. توسعه دادن تفاوتها(develop diffrentiators) و. ساختن آنچه نیاز است(build out nice-to-haves)

الف. هدف این فاز یافتن جایی از برنامه است که احتمال مشکل از آنجا داده میشود. به طور مثال برای مشکل سرریز بافر استفاده از یک نرم افزار اسکن کد برنامه برای مشخص شدن محل‌های محتمل برای بروز خطا میتواند انجام ایده آل این فاز برای مشکل سرریز بافر باشد.

۹. در طبقه بندی علوم امنیتی اصول، راهنماها و قوانین را شرح دهید.

اصول مجموعه از گزارهاست که در مورد دانش عمومی امنیت ناظر به تجربه صحبت میکند

راهنماها مجموعه از توصیه ها هستند که در مورد انجام یا عدم انجام امری در توسعه نرم افزار نظر میدهند. این نظرات معمولا مفهوما موضوع را منتقل میکنند

قوانین نیز مانند راهنماها مجموعه از توصیه ها هستند که انجام یا عدم انجام امری در توسعه نرم افزار نظر را توضیح میدهند با این تفاوت که این توصیه ها در لایه نگارش برنامه(syntax) وارد می‌شوند.

۱۰. یک حمله TOCTOU(time of check, time of use) مربوط فایل ها را مثال بزنید.

تابع open مربوط به POSIX یک API لینوکسی برای باز کردن فایل و یا ساختن فایل است. فرض کنید برنامه ای برای استفاده از فایلی با نام خاص ابتدا بررسی میکند فایل وجود دارد یا نه و اگر وجود نداشت آن را میسازد و درصورت وجود آن را پاک کرده و از نو میسازد. حال فرض کنید برنامه ابتدا اقدام به بررسی وجود فایل کند سپس براساس وجود یا عدم وجود اقدام به ساختن یا پاک کردن و ساختن کند. در این صورت اگر حمله گر پس از فرآیند چک کردن فایل را از طریقی دیگر ایجاد کند یا از بین ببرد برنامه در هنگام اجرا عمل متناظر چک کردن خودش به مشکل برخورده و از حالت اجرا خارج میشود. متاسفانه تابع open مربوط به POSIX در نسخه های قدیمی به این حمله آسیب پذیر بوده است.