الزامات فنی-امنیتی-شرکت کنندگان

"۱۴۰۲۱۲"

نسخه	تاریخ	شرح
۱	۱۴۰۲/۱۲/۱۶	شرح درخواست

نام پروژه:	**الزامات فنی-امنیتی-شرکت کنندگان**
تعداد صفحات	۱۱ صفحه
تاریخ آخرین تغییرات:	۱۴۰۲/۱۲/۱۶
چکیده:	این سند حاوی الزامات فنی-امنیتی-شرکت کنندگان مستند RFP مورد نظر می باشد

فهرست مطالب

۱. مساله ۴

۱-۱. الزامات فنی ۴

۱-۲. الزامات امنیتی ۵

چک لیست امنیتی سیستمهای نرمافزاری تحت وب ۸

ASSEMBLY-LEVEL CHECKS ۹

۱-۳. الزام شرکت های شرکت کننده ۱۰

۱. مساله

بانک توسعه تعاون"امور فناوری اطلاعات و ارتباطات" در این سند الزامات فنی و امنیتی و شرکت کنندگان پروژه تامین سامانه صندوق امانات و دستگاه های کنترل تردد مرتبط را مطرح می کند. رعایت کلیه بندهای اعلامی از سوی شرکت پیمانکار الزامیست و مسولیت خوداظهاری آن برعهده شرکت می باشد.

۱-۱. الزامات فنی

عناوین الزامات
بکارگیری سیستم عامل(Centos Linux نسخه ۸ به بالا یا Oracle Linux نسخه ۸ به بالا جهت سرورهای پایگاه داده Oracle و سرورهای خدمات دهنده Web Logic) یا (Windows Advance Server 2019 X64 جهت پایگاه داده های SQL Server و سرورهای خدمات دهنده IIS) یا (سیستم عامل Debian نسخه ۱۱ و به بالا برای پایگاه داده MariaDB و سرور خدمات دهنده Apache 2.4 و به بالا)
بکارگیری VM (Linux ESX 6.7) در زیرساخت مجازی سازی
استفاده از معماری Web Application
ارایهWeb Service و یا برون سپاری آن با استانداردهای Soap API یا Rest API
بکارگیری پایگاه دادهOracle Database نسخه 19 یا SQL Server نسخه 2019 جهت سامانه‌هایی که پایگاه داده رابطه‌ای (Relational) در آنها کاربرد دارد.
پشتیبانی از مدیریت خطا در تبادل داده‌های مبتنی بر Web Service
مدیریت خطا، مدیریت بارگزاری موفق و امکان عقب گرد (Rollback)
گزارش‌گیری کامل از تمام تراکنش‌ها با log کامل از فعالیت کاربران و امکان ارسال Log File ها و Log های تولیدی به سامانه Syslog موجود در بانک
پشتیبانی سامانه از امکان Clustering و Load Balance (درصورت نیاز بکارگیری آن، در لایه‌های مختلف سامانه)
ذخیره سازی برخی از اطلاعات محرمانه به شکل رمز گذاری شده (Encrypted)

انتقال اقلام اطلاعاتی (Export) در گزارشات سامانه به شکل یکی از استانداردهای رایج و درخواستی بانک مانند xls. ، pdf. ، doc. ، txt. یا سایر پسوندهای استاندارد موجود
فایل‌های به گونه‌ای تولید شوند که نرم افزارهای امنیتی و آنتی ویروس استاندارد نصب شده در بانک، فایل‌های مذکور را به‌عنوان بد افزار شناسایی نکند.
تضمین توسعه پذیری، مقیاس پذیری، انعطاف پذیری فریم سخت افزار
توسعه سامانه و رابط های (Interface) آن با استفاده از توابع کتابخانه‌ای و SDK های لازم، جهت ارایه سرویس‌های آتی

۲-۱. الزامات امنیتی

کنترل (کنترل های فرعی)-توضیحات	کنترل اصلی
مشخص بودن لیست کامل مجوزهای اعطا شده به همراه ثبت رخداد	اختصاص مجوز ها به کاربران
عدم قبول گذرواژه خالی	
پشتیبانی از احراز هویت چند عاملی (بسته به نیاز پروژه)	
اعتبار سنجی در تمام نشست ها	
قابلیت تنظیم Session Timeout برای مدیر سیستم	
احراز هویت مجدد برای تنظیمات حساس	
قابلیت تنظیم حداکثر تلاش ناموفق	
ثبت وقایع با جزئیات برای تلاش های ناموفق	
گرفتن مجدد گذرواژه برای عملیات حساس (بسته به پروژه)	
بررسی گذرواژه و عدم پذیرش گذرواژه ساده	
مدت زمان اجباری تعویض گذرواژه	
اجبار در تغییر گذرواژه در زمان اولین ورود کاربر	
عدم قبول دو کاربر با شناسه یکسان	
تغییر یا حذف حساب های پیش فرض سیستم	
عدم نمایش گذرواژه هنگام ورود	

عدم ذخیره گذرواژه در حافظه موقتی (Cache)	
نگهداری گذرواژه بصورت درهم (Hash)	
رمزنگاری قوی گذرواژه حین انتقال در شبکه HTTPS	
کنترل دسترسی جهت دسترسی به اطلاعات احراز هویت	
رمزنگاری اطلاعات حساس هنگام ذخیره سازی	حفاظت از اطلاعات حساس
استفاده از http post بجای http get در صورتی که برنامه مبتنی بر web می باشد	
وجود امکان امضاء دیجیتالی	
مستند بودن تمام واسط های دسترسی به برنامه	
امکان فیلترینگ IP و MAC جهت دسترسی مدیر سیستم	
امکان جلوگیری از Upload فایل بر روی سیستم	
عدم ایجاد شناسه ها بصورت ترتیبی	مدیریت نشست
عدم تولید شناسه ضعیف و قابل حدس	
عدم استفاده از داده های محرمانه مانند اسم رمز در تولید شناسه	
رمزنگاری اطلاعات نشست هنگام ارسال	
هشدار به کاربر قبل از ذخیره کوکی در مرورگر	
عدم ذخیره اطلاعات حساس در کوکی یا مکانیزمهای مشابه دیگر بدون رمزنگاری	
احراز هویت جهت هر نشست جدید	
رعایت حداکثر نشست برای هر کاربر	
امکان تعریف انقضای نشست پس از عدم فعالیت به مدت قابل تنظیم معتبر	
امکان قطع و یا به تعلیق درآوردن یک نشست توسط مدیر سیستم	
باز پس گیری تمام اطلاعات نشست پس از خاتمه نشست ها	
امکان هماهنگی با NTP و ثبت وقایع	رویداد نگاری و ممیزی
وجود مکانیزمی برای هشدار به مدیر هنگام پر شدن فایل ممیزی (فایل لاگ)	

اطمینان از ثبت کلیه ی رویدادهای مستند شده ی ثبت شدنی بسته به حساسیت و نوع برنامه های کاربردی به همراه جزئیات مورد نیاز	واکنش در برابر خطا و استثنا
امکان تعریف روال جهت بایگانی فایل های وقایع	
وجود مجوز صحیح و کنترل دسترسی مناسب برای فایل های رویدادنگاری	
عدم فعالیت برنامه ی کاربردی بعد از توقف مکانیزم رویدادنگاری	
وجود ویژگی های واکنش به خطا /استثنا در رویدادنگاری	
رویدادنگاری صحیح و کامل هر خطا	
عدم اجازه ی دسترسی های غیر معمول در شرایط پس از خطا در سیستم	
وجود روال های پیش بینی شده پس از شکست یا خطا در هر بخش از سیستم	
انجام اعتبارسنجی ورودی ها بطور کامل	مقاوم بودن در مقابل حملات
عدم وجود آسیب‌پذیری سرریز بافر	
عدم وجود آسیب‌پذیریXSS	
عدم آسیب‌پذیری در برابر تزریق کد	
پاک کردن object ها از حافظه موقت	
عدم وجود کدهای حساس در برنامه : در فرانت	
قابلیت پشتیبان گیری و بازیابی	مقاومت در برابر خرابی
وجود مکانیزم های امنیتی در پشتیبان گیری	
وجود طرح ترمیم خرابی ناشی از حوادث	
وجود راهنمای کامل نصب و پیکربندی امنیتی شامل هر گونه پیکربندی امنیتی لازم برای سیستمها	امکان نصب نرم افزار بصورت امن
حذف یا تغییر حساب و یا گذرواژه های پیش فرض	
غیرفعال بودن توابع خطائی	
مستند سازی پیکربندی و تنظیمات مربوط با گواهی نامه ها و رمزنگاری	مستندسازی (بسته به نیاز پروژه)

مستند شرائط امنیتی خاص برای شبکه (بسته بودن پورت ها ، نیاز به دیواره آتش و ...)	
مستند سازی کنترل های لازم مورد نیاز برنامه در ارتباط با سیستم عامل	
مستند شدن پیکربندی مورد نیاز برنامه کاربردی برای حفاظت و ارتباط با پایگاه داده	

چک لیست امنیتی سیستم‌های نرم‌افزاری تحت وب

بررسی آسیب‌پذیری Cross site Scripting
بررسی آسیب‌پذیری SQL Injection
بررسی آسیب‌پذیری LDAP Injection
بررسی آسیب‌پذیری ORM Injection
بررسی آسیب‌پذیری XML Injection
بررسی آسیب‌پذیری XXE Injection
بررسی آسیب‌پذیری SSI Injection
بررسی آسیب‌پذیری XQuery Injection
بررسی آسیب‌پذیری IMAP/SMTP Injection
بررسی آسیب‌پذیری Command Injection
بررسی آسیب‌پذیری HTTP Splitting
بررسی آسیب‌پذیری HTTP Verb Tampering
بررسی آسیب‌پذیری Local File Inclusion
بررسی آسیب‌پذیری Remote File Inclusion
بررسی آسیب‌پذیری CSRF(Cross Site Request Forgery)
بررسی آسیب‌پذیری SSRF(Server Sider Request Forgery)
بررسی آسیب‌پذیری Click jacking
بررسی نشت کاربر در تمامی صفحه‌ها: برای این منظور می‌بایست از Session ID های پیچیده استفاده شود و در تمام صفحات نشست کار بررسی شود.
استفاده از CAPTCHA در صفحه‌های ورود اطلاعات: تا نفوذگران نتوانند درخواست‌های بی شماری تولید کنند و پایگاه داده را پر کنند.

بررسی فایل‌های آپلود شده از سمت کاربر از نظر نوع و حجم فایل: تا امکان آپلود فایل‌های وب شل پیشگیری شود. نفوذگران می‌توانند با آپلود این فایل‌ها، دسترسی کامل سرور را به دست بگیرند.
مدیریت Exception های تولید شده: تا از نمایش پیغام‌های خطایی که حاوی اطلاعات هستند به کاربر جلوگیری شود.
امکان استفاده از قوانین اجبار کارکنان به استفاده از کلمات عبور پیچیده: برای این منظور کاربران می‌بایست کلمات عبور خود را با ترکیب حروف بزرگ، کوچک، علائم و اعداد می‌سازند و از شکستن پسورد با تکنیک dictionary و brute force پیشگیری شود.
استفاده از هدرهای ○ X-Frame-options ○ X-XSS-Protection ○ X-Content-Type-options ○ Http Only (این تنظیمات معمولاً در فایل web.config انجام می‌گیرد.)
استفاده از الگوریتم‌های رمزنگاری قوی برای ذخیره کلمات عبور: تا با به خطر افتادن پایگاه داده، کلمات عبور کاربران به خطر نیفتد.
استفاده از Salt برای ذخیره کلمات عبور: برای این منظور عباراتی به انتهای کلمه عبور استفاده می‌شود و hash نهای، تلفیقی از hash پسورد اصلی و hash عبارت salt خواهد بود. با این کار از شکستن پسورد با استفاده از تکنیک Rainbow table پیشگیری می‌شود.

چک لیست امنیتی سیستم‌های نرم‌افزاری Client/Server (مربوط به Desktop Applications)

Assembly-level checks

محافظ‌های فعال روی نرم‌افزار • محافظ DEP (Data Execution Prevention): یک قابلیت امنیتی است که در سیستم عامل‌های پیشرفته وجود دارد. در این ویژگی، نواحی مختلف حافظه به عنوان« اجرایی» یا «غیراجرایی» نشانه گذاری می‌شود و تنها به داده‌هایی که در ناحیه اجرایی قرار دارند اجازه می‌دهد که توسط برنامه‌ها، سرویس‌ها، درایورهای دستگاه‌ها و ... اجرا شوند. • محافظ ASLR (Address space layout randomization): یک تکنیک امنیت کامپیوتری است که در برابر حملات سرریزی بافر محافظت به عمل میآورد. برای جلوگیری از اینکه نفوذگر بتواند به تابع قابل اکسپلویت در حافظه پرش کند استفاده می‌شود. به عبارتی دیگر با استفاده از این تکنیک، نفوذگر نمی‌تواند از شل کد استفاده کند. • محافظ GS: این تابع از حملات سرریزی بافر محافظت می‌کند و مواردی مانند تابع آسیب پذیر را پوشش می‌دهد.

محافظ‌های فعال ضد Debugging بر روی نرم افزار • محافظ تشخیص Debugger: با استفاده از یک یا چند تکنیک در اجرای کد که مانع عمل مهندسی معکوس می‌شود. • محافظ تشخیص Emulator: از قسمت‌های محافظت شده کد حفاظت می‌کند (تبدیل کد محافظت شده به p-code) • محافظ تشخیص API-Tracer: روشی برای جلوگیری از دسترسی به فایل اجرایی محافظت شده • محافظ تشخیص Decompiling: روشی برای ممانعت از تجزیه کد اجریی می‌باشد.

Secrets

○ ذخیره نکردن کلمات عبور به صورت Clear-text در فایل‌های پیکربندی نرم‌افزار: برای اینکه با به دست آوردن این فایل، کلمات عبور آشکار نشود.
○ ذخیره نکردن کلمات عبور به صورت Clear-text در RAM برای مدت زمان طولانی
○ ذخیره کلمات عبور به صورت رمز شده: با به خطر افتادن پایگاه داده، کلمات عبور بصورت رمز شده خواهد بود و امکان دسترسی را برای نفوذگر بسیار دشوارتر می‌کند.

Exception management

مدیریت تمام Exception ها: تا پیغام‌های خطایی که حاوی اطلاعات هستند به کاربر نشان داده نشود.
ثبت تمام Exception های تولید شده
عدم نمایش اطلاعات حساس در اطلاعات بازگشتی به سمت کاربر در صورت بروز Exception

Unmanaged code access

بررسی داده‌های ورودی و خروجی از نظر طول و نوع داده: با بررسی ورودی‌ها از نظر تعداد و نوع و همچنین فیلتر کردن کاراکترهای مخرب، احتمال بروز بسیاری از آسیب‌پذیری‌ها کاهش می‌یابد.
استفاده نکردن از APIهایی که مدیریت حافظه روی آنها انجام نمی‌شود.
تعریف اشاره‌گرها در برنامه به صورت Private (در برنامه‌های تولید شده با C/C++)

۳-۱. الزام شرکت های شرکت کننده

- شرکت تولید کننده سامانه ودستگاه های کنترل تردد باشند.
- شرکت دانش بنیان باشد.
- شرکت دارای گواهی افتا و یا در حال باشد.
- حداقل در یک بانک تجربه اجرای موفق پروژه سامانه صندوق امانات و دستگاه کنترل تردد مرتبط را داشته باشد.

- در استانها دارای نمایندگی باشد.
- پشتیبانی از سامانه ودستگاه های فروخته شده به مدت ۱۰ سال

پایان