نیازمندی های کنترل احراز هویت

۱	کنترل کنید که برای تمامی صفحات ومنابع احراز هویت انجام شود، به جز آن هایی که قصد داریم عمومی باشند.	
۲	کنترل کنید که هنگام ورود کلمه ی عبور توسط کاربر، فیلد کلمه ی عبور آن را نشان نمی دهد.	
۳	کنترل کنید که تمام کنترل های احراز هویت در سمت سرویس دهنده انجام می شود.	
۴	کنترل کنید که تمام کنترل های احراز هویت به صورت متمرکز پیاده سازی شده اند.	
۵	کنترل کنید که تمام کنترل های احراز هویت، در صورت بروز مشکل به صورت امن با شکست مواجه می شوند.	
۶	کنترل کنید که کلمات عبور انتخابی به اندازه کافی قوی باشند و از انتخاب کلمات عبور متعارف جلوگیری شود. همچنین فیلدهای کلمه عبور نباید مانع ورود کلمات پیچیده وطولانی شوند.	
۷	کنترل کنید که تمامی کارکردهای مربوط به احراز هویت (مانند ثبت نام،فراموشی کلمه ی عبور، وغیر فعال سازی حساب کاربری) حداقل به اندازه ی مکانیزم اولیه ی احراز هویت در برابر حملات مقاوم هستند.	
۱۰	کنترل کنید که کلمه های عبور به همراه یک عدد منحصر به فرد (مثلا" شناسه ی کاربری داخلی)ذخیره شوند و قبل از ذخیره سازی ، به کمک روش هایی مانند scrypt،bcrypt یا PBKDF2 در همسازی انجام شود. از طریق اقرارنامه بررسی گردد که الگوریتم استفاده شده غیرقابل بازگشت است.	
۱۱	کنترل کنید که تمام اعتبارنامه ها و اطلاعات شناسایی که برنامه با آن سر وکار دارد، از مسیرهای رمز نگاری نشده (یا رمز نگاری ضعیف)عبور نمی کنند.	
۱۲	کنترل کنید که مکانیزم های بازیابی کلمه عبور (در صورت فراموشی کاربر)کلمه ی عبور فعلی را نمایش نمی دهند وکلمه ی عبور جدید به صورت رمز نگاری شده برای کاربر ارسال شود.	
۱۳	کنترل کنید که تشخیص تعداد کاراکتر، نام های کاربری و کلمه عبور به کمک مکانیزم های ورود به سیستم و بازنشانی کلمه ی عبور امکان پذیر نباشد.	
۱۴	کنترل کنید که چارچوب ها و مولفه های جانبی مورد استفاده در برنامه، از کلمات عبور پیش فرض مانند (admin/password) استفاده نمی کنند.	
۱۵	کنترل کنید که فرایند ورود به سیستم در برابر حملات brut-force عمودی (یک حساب کاربری با تمام کلمه های عبور ممکن آزموده شوند) و یا افقی (تمام حساب های کاربری با یک کلمه ی عبور بخصوص آزمایش شوند) محافظت می کند. برای این منظور	

	در صورت سه بار ورود پسورد اشتباه، سیستم برای مدتی غیر فعال شود و یا اینکه از CAPTCHA برای جلوگیری از حملات ربات‌ها استفاده شود.	
۱۶	کنترل کنید که تمام اعتبارنامه های احراز هویت برای دسترسی به سرویس های خارجی برنامه رمزنگاری شده و در مکانی امن (خارج از کد) نگهداری می شوند .	
۱۷	کنترل کنید که مکانیزم های فراموشی کلمه ی عبور و بازیابی حساب کاربری، به جای ارسال خود کلمه ی عبور به کاربر، یک لینک حاوی نشانه با محدودیت زمانی به کاربر ارسال کنند تا از این طریق حساب خود را بازیابی کند. استفاده از مکانیزم های احراز هویت افزونه، مانند پیامک و برنامه های موبایل پیش از ارسال لینک به کاربر، نیز امکان پذیر است.	
۱۸	کنترل کنید که مکانیزم های فراموشی کلمه ی عبور، تا پس از اتمام موفقیت آمیز تغییر کلمه ی عبور، حساب کاربری را غیرفعال نمی کند. هدف این است که دسترسی کاربران معتبر به حسابشان با مانع مواجه نشود.	
۱۹	کنترل کنید که سؤالات انتخاب شده برای باز نشانی کلمه ی عبور با دانش عمومی قابل پاسخ نباشد.	
۲۰	کنترل کنید که سیستم قابلیت تنظیم برای منع استفاده از کلمه های عبور پیشین (به تعداد قابل تنظیم)را دارد.	
۲۱	کنترل کنید که پیش از صدور مجوز انجام عملیات حساس برنامه (با توجه به حساسیت برنامه) ، احراز هویت مجدد انجام شود. برای این کار می توان از مکانیزم های احراز هویت دو مرحله ای، مانند پیامک موبایل، نیز استفاده کرد.	
۲۲	کنترل کنید الگوریتم استفاده شده در CAPTCHA به اندازه‌ی کافی پیچیده باشد که به سادگی قابل دور زدن نباشد.	

نیازمندی های کنترل مدیریت نشست

۱	کنترل کنید برنامه برای کنترل مدیریت نشست ها از پیاده سازی پیش فرض چارچوب استفاده می کند	
۲	کنترل کنید که با خروج کاربر، تمام نشستهای او باطل می شود.	
۳	کنترل کنید که وقتی نشست برای مدتی مشخص غیر فعال باشد، نشست منقضی شوند.	
۵	کنترل کنید که تمام صفحاتی که برای دسترسی نیاز به احراز هویت دارند، لینک خروج داشته باشند.	
۶	کنترل کنید که شناسه های نشست تنها در کوکی ها آشکار شوند و هرگز در URL ها ، پیام های و گزارشات سیستمی آشکار نشوند.	
۷	کنترل کنید که شناسه های نشست هنگام ورود عوض شوند تا از تثبیت نشست جلوگیری شود.	

۸	کنترل کنید که شناسه ی نشست هنگام احراز هویت مجدد عوض شود	
۱۲	کنترل کنید که توکن های نشست احراز هویت شده، که از کوکی های ارسال شده توسط HTTP استفاده می کنند، با استفاده از HttpOnly حفاظت می شوند	
۱۴	کنترل کنید که برنامه ی کاربردی اجازه ی وجود دو نسخه ی همزمان از نشست کاربری را ، از سیستم های متفاوت، نمی دهد	

نیازمندی های کنترل دسترسی

۱	کنترل کنید که تنها کاربرانی که مجوز مخصوص دارند، می توانند به سرویس ها و قابلیتهای حفاظت شده دسترسی یابند. در واقع سطح دسترسی به قابلیت‌های سیستم بر اساس سیاست‌های سازمان و به درستی تنظیم شده باشد. در مواردی از این سند که نیاز به بررسی کنترل دسترسی دارد، ارزیاب بایستی به مستندات ارائه شده توسط کارشناس مربوطه مراجعه نماید.	
۲	کنترل کنید که تنها کاربرانی که مجوز مخصوص دارند، می توانند به URL های حفاظت شده دسترسی یابند.	
۳	کنترل کنید که تنها کاربرانی که مجوز مخصوص دارند، می توانند به پرونده ها و داده های حفاظت شده دسترسی یابند. برای مثال هر فرد بتواند تنها اطلاعات شخصی خود را مشاهده نماید یا هر مرکز تنها به اطلاعات مرکز خود دسترسی داشته باشد.	
۴	کنترل کنید که ارجاعات مستقیم به اشیا حفاظت شده اند، به گونه ای که کاربر تنها به اشیاء و داده های دارای مجوز دسترسی داشته باشد. برای مثال کدهایی که در آن‌ها به فایل‌ها، دیتابیس‌ها و دایرکتوری‌هایی ارجاع داده شده است به صورت حفاظت شده باشند یا دسترسی به آن‌ها کنترل شده باشد تا هکر نتواند آن‌ها را تغییر داده یا از آن‌ها استفاده کند و به داده‌های حیاتی دسترسی پیدا کند.	
۵	کنترل کنید که مرور دایرکتوری ممکن نباشد مگر آنکه تعمداً خواسته باشید. برای مثال در هنگام تنظیمات سرور Directory Browsing بسته شده باشد تا کاربر نتواند فولدرهای سایت را مشاهده نماید و به ساختار آن پی ببرد.	
۶	کنترل کنید که کنترل های دسترسی به صورت امن با شکست مواجه می شوند. در واقع هنگام بروز پیغام‌های سیستمی و پیام‌های دیتابیسی نمایش داده نشوند و تنها پیغام‌های مد نظر توسعه‌دهنده سیستم که حاوی هیچ اطلاعاتی از ساختار برنامه نیست نمایش داده شده و سیستم به یک حالت امن برود به گونه‌ای که کاربر به صفحات یا داده‌های غیرمجاز دسترسی پیدا نکند.	
۸	کنترل کنید که ویژگی های کاربری و داده ها، و مقررات کنترل دسترسی از طرف کاربران نهایی قابل دستکاری نباشد، مگر آنکه به طور خاص چنین مجوزی به آنها داده شود. به عنوان نمونه کاربران نتوانند سطح دسترسی، نام کاربری و اطلاعات فقط خواندنی خود و یا دیگران را تغییر داده و این قابلیت در انحصار مدیر سیستم باشد، مگر اینکه تعمداً بخواهد قسمتی از آن را به شخص دیگری واگذار کند.	
۹	کنترل کنید که تمام کنترل های دسترسی در سمت سرویس دهنده اعمال می شوند. (در صورت در دسترس بودن کد از طریق بررسی آن، در غیر این صورت گرفتن اقرارنامه)	

۱۱	کنترل کنید که تمام تصمیمات کنترل دسترسی در گزارش ها، ثبت می شوند. در واقع مشخص نمایید که دسترسی به هر قسمت سیستم توسط چه شخصی به کاربر اعطا شده است.	
۱۳	کنترل کنید که سیستم در برابر دسترسی های پی در پی و متمرکز به قابلیتها و منابع حفاظت شده مقاوم است. برای مثال تعداد اعمال تغییرات ممکن توسط کاربران به ازای هر ساعت محدود شود تا یک کاربر به تنهایی نتواند تمام پایگاه داده را دگرگون سازد. در موارد حساس مانند تلاش برای ورود ناموفق، بهتر است گزارشات ثبت شده و به مدیر سیستم هشدار داده شود.	
۱۴	کنترل کنید که تغییرات رخ داده بر روی داده‌های حیاتی به صورت کامل همراه با اطلاعات کاربری و IP شخص مسئول، به صورت مجزا از سیستم لاگ‌برداری ها ذخیره شود.	

نیازمندی های کنترل اعتبارسنجی ورودی مخرب

۱	کنترل کنید که محیط اجرای برنامه مستعد سرریز بافر نیست یا کنترل های امنیتی از این آسیب پذیری پیشگیری می کنند. در این مورد علاوه بر برر سی اعتبار سنجی‌ها از طریق رابط کاربری نیاز به برر سی کد و یا گرفتن اقرارنامه از تو سعه دهنده در برخی موارد مانند عملیات ریاضی و منطقی می‌باشد.	
۲	کنترل کنید که شکست اعتبارسنجی ورودی منجر به عدم پذیرش ورودی می شود.	
۳	کنترل کنید که مجموعه کاراکتری UTF-8 مانند برای تمام منابع ورودی مشخص شود	
۵	کنترل کنید که برنامه از یک کنترل اعتبارسنجی واحد برای تمام داده های پذیرفته شده استفاده می کند. به عنوان نمونه فرمت ایمیل در قسمت ثبتنام، ویرایش و سایر صفحاتی که نیاز به وارد کردن ایمیل است، یکی باشد.	
۹	کنترل کنید که محیط اجرای برنامه مستعد OS Command Injection نیست یا کنترل های امنیتی از این آسیب پذیری پیشگیری می کنند. بررسی کنید که کاربر قادر به سوءاستفاده از برنامه و ارسال داده‌های غیرقابل اعتماد از طریق فرم‌ها، کوکی‌ها، سرآیندهای Http و ... به ه سته سی ستم‌عامل نی ست. در این روش نفوذگر به دنبال اجرای د ستورات دلخواه بر روی سیستم عامل میزبان از طریق برنامه آسیب پذیر است. این حمله معمولا به دلیل اعتبارسنجی ورودی ناکافی رخ می‌دهد.	
۱۰	کنترل کنید که محیط اجرای برنامه مستعد حمله ی XML External Entity نیست یا کنترل های امنیتی از این حمله پیشگیری می کنند. این حمله به دلیل آسیب‌پذیری موجود در نرم‌افزارهایی که ورودی‌های XML را parse می‌کنند، به وجود می‌آید. و به دلیل وجود ارجاع به موجودیت خارجی مانند دایرکتوری‌ها بوجود می‌آید. ساده‌ترین راه برای حل این مشکل غیرفعال کردن کامل Document Type Definition (DTD) در XML می‌باشد. در صورتی که این امکان وجود ندارد entity و Doctypeهای خارجی را غیرفعال کنید. (اقرارنامه)	

۱۱	کنترل کنید که محیط اجرای برنامه مستعد XML Injection نیست یا کنترل های امنیتی از این آسیب پذیری پیشگیری می کنند. این حمله با دستکاری و تزریق تگ‌های XML مخرب و تغییر محتوای فایل‌ها مانند تغییر رمز عبور در یک سند XML رخ می‌دهد. معمولا این آسیب‌پذیری در وب سرویس‌هایی اتفاق می‌افتد که از DOM parser یا پارسرهای مبتنی بر جریان مانند SAX استفاده میکنند. همچنین برای جلوگیری از این حملات باید جزئیات دقیق المنت‌ها مانند نوع، حداقل و حداکثر سایز آن‌ها مشخص شود.	
۱۲	کنترل کنید که تمام داده های نامطمئن که در قالب خروجی HTML ظاهر می شوند (مانند مقادیر Javascript ، بلوک های CSS ، مشخصه های URI)، به قالب استاندارد تبدیل می شوند.	

نیازمندی های کنترل رمزنگاری

۱	اسامی پیوست و نام های تصادفی فایل ها بر اساس سیستم رمز نگاری باشد. بنابراین بایستی از روش‌هایی مثل GUID برای ذخیره فایل‌ها استفاده شود و از ذخیره فایل با نام واقعی آن‌ها خودداری گردد.	

نیازمندی های کنترل مدیریت و ثبت گزارش

۱	بررسی گردد برنامه اطلاعات حساس مانند: شناسه ی نشست و اطلاعات شخصی – اطلاعات بانک اطلاعاتی را در خروجی پیام نمایش ندهد. در واقع های مربوط به پایگاه داده و محیط توسعه غیرفعال شده و پیام‌های مد نظر توسعه‌دهنده سیستم که حاوی هیچ اطلاعاتی از ساختار برنامه نیست نمایش داده شود.	
۲	ثبت وقایع و رخدادها در سمت سرور انجام شود.	
۳	بایستی منطق مدیریت در کنترل دسترسی به طور پیش فرض از دسترسی جلوگیری کند . (اقرار نامه)	
۴	تاریخ ها و برچسب های زمانی از منبع مطمئن صادر شود .	
۵	در ثبت ها موارد مهم درج گردد (مانند IP - کاربر مرتبط – مربوطه –زمان .....)	
۶	در زمان نباید اطلاعات حساس ثبت گردد مانند اطلاعات نشست – اطلاعات شخصی و	

حفاظت داده

۱	بررسی شود تمام فرمهای که حاوی اطلاعات حساس هستند امکان ثبت در حافظه نهان سمت کاربر و همچنین تکمیل خودکار فرم را غیر فعال کرده اند.	

۲	بررسی کنید تمام داده های حساس درون بدنه ی پیام HTTP به سرویس دهنده ارسال می شود (برای مثال نباید این اطلاعات در پارامترهای URL ارسال گردند و بهتر است از طریق POST ارسال گردد.)	
۳	بررسی کنید که تمام نسخه های موقت و ذخیره شده در حافظه نهان سمت کاربر از دسترسی غیر مجاز حفاظت شده و پس از اتمام کار باطل یا پاک سازی میشوند	

نیازمندی های کنترل ارتباطات

۱	بررسی کنید که آیا می توان یک مسیر از هر CA (Certificate Authority) معتبر به گواهی نامه های لایه ی انتقال امن (TLS) سرور ایجاد کرد و گواهی نامه های هر سرور معتبر است. (عدم مصداق هم دارد)	
۲	بررسی شود که برای تمام ارتباطات احراز هویت شده یا دارای داده های حساس، از TLS استفاده می شود. (عدم مصداق هم دارد)	
۳	بررسی شود که تمام ارتباطات به سیستم های بیرونی که شامل اطلاعات یا توابع حساس هستند، احراز هویت شوند. (شامل وب سرویس ها و سایر ارتباطات سیستمی دیگر نیز می شود)	
۴	بررسی شود که تمام ارتباطات به سیستم های بیرونی که شامل اطلاعات یا توابع حساس هستند؛ از یک حساب کاربری با حداقل دسترسی لازم برای اجرای صحیح برنامه استفاده می کنند.	
۵	خروجی وب سرویس ها و یا سایر درگاه های ارتباطاتی که شامل داده ای حساس هستند، Encrype شده باشند.	

نیازمندی های کنترل امنیت HTTP

۱	بررسی شود که تمام آیتم های مربوط به کنترل سرآیند (در وب سرور و در کانفیگ برنامه) وجود داشته باشد.	

نیازمندیهای کنترل منطق کسب و کار

۱	آیا تایید می نمایید که برنامه اجازه نمی دهد که پارامترهای کسب و کار با ارزش مانند قیمت، موجودی حساب و شناسه دستکاری شود.؟	

۲	آیا تایید می نمایید که برنامه به کمک مکانیزمهایی مانند گزارش های حفاظت شده و قابل تصدیق از تراکنش ها، و گزارش های ثبت سیستمی، در برابر حملات انکاری محافظت می کند؟ برای مثال در صورت وارد کردن پسورد اشتباه در هنگام پرداخت وجه، IP، تاریخ و ... ثبت شوند.	
۳	آیا تایید می نمایید که برنامه دارای محدودیت های کسب و کار تعیین شده بوده که در مکانی امن (مانند یک سرویس دهنده حفاظت شده) نگهداری می شوند. این محدودیتها می‌توانند بر مبنای کاربر و مصرف روزانه، اعمال شوند. برای مثال کاربران جدید سیم کارت نباید روزانه بیش از ۱۰ دلار مصرف کنند، یا تعداد پرونده‌هایی که پزشکان می تواند به طور روزانه به آنها دسترسی داشته باشند نباید بیش از تعداد بیماران ممکنی باشد که یک پزشک می تواند در یک روز درمان کند؟ در واقع سیاستهای مورد نظر سازمان به طور کامل در برنامه اعمال شده باشد.	

نیازمندی های کنترل پرونده ها و منابع

۱	آیا تایید می نمایید که باز – ارسال ها و تغییر مسیرهای URL ها شامل داده های نامعتبر نباشند؟	
۲	آیا تایید می نمایید که نام پرونده ها و داده های مسیر که از منابع نامطمئن دریافت می شود، به قالب استاندارد و مناسب تبدیل شود تا از حملات پیمایش مسیر جلوگیری شود؟ برای مثال نام پرونده‌ها با کد ملی ذخیره نشود تا در صورت دانستن مسیر، نتوان به محتوای پرونده دسترسی داشت.	
۳	آیا تایید می نمایید که پرونده های دریافت شده از منابع نامطمئن توسط ابزارهای آنتی ویروس پویش شده تا از آپلود محتوای مخرب شناخته شده جلوگیری شود.؟	
۴	آیا تایید می نمایید که پارامترهای دریافت شده از منابع نامطمئن برای تغییرات نام فایلها، نام مسیرها، یا اشیاء سیستم بکار نمی روند مگر آنکه ابتدا به قالب استاندارد تبدیل شده و اعتبار سنجی ورودی شوند تا از حملات local file inclusionجلوگیری شود.؟ این آسیب پذیری به مهاجم این اجازه را می دهد که از طریق مرورگر، فایل های خود را در سرور قرار بدهد. این آسیب پذیری وقتی به وجود می آید که وب سایت ورودی ها را به درستی چک نمی کند و اجازه می دهد که مهاجم ورودی را دستکاری و **کاراکتر های پیمایش** مسیر را وارد کند و فایل هایی را در سرور قرار دهد. این حمله معمولا با غیر فعال کردن Directory Browsing قابل پیشگیری است.	
۵	آیا تایید می نمایید که پارامترهای دریافتی از منابع نامطمئن به قالب استاندارد تبدیل شده ، اعتبار سنجی ورودی شده و رمزگذاری خروجی شده تا از حملات remote file inclusionجلوگیری شود (به ویژه مواردی که ورودی قابل اجرا باشد، مانند سرآیندها)؟ این آسیب پذیری به مهاجم این اجازه را می دهد که از طریق دستکاری URL یا سایر پارامترهای ورودی، فایل‌های خود را که حاوی اسکریپتهای مخرب هستند و بر روی سرور دیگری قرار دارند را بر روی سرور یا کلاینت آپلود کنند. این کار به و سیله و سیله تزریق کد یا همان XSS انجام می گردد. بهترین راه برای جلوگیری از این حمله عدم امکان آپلود اتوماتیک فایل‌ها توسط ورودی کاربران می‌باشد، در غیر این صورت مشخص کردن لیست فایل‌های مجاز برای	

	آپلود در سامانه است. در PHP با قرار دادن allow_url_include در حالت Off از این حمله جلوگیری می‌شود ولی هنوز امکان حمله local file inclusion وجود دارد.	
۶	آیا تایید می نمایید که نرم افزار شما قابلیت اجرای کد های HTML در ادیتور های متنی را ندارد؟ بدین منظور کاربر نباید اجازه وارد کردن کدهای HTML در فیلدها را داشته باشد.	
۷	آیا تایید می نمایید که پرونده های دریافت شده از منابع نامطمئن خارج از webroot ذخیره می شوند؟	
۸	آیا تایید می نمایید که تنظیمات پیش فرض سرویس دهنده ی وب یا برنامه به گونه ای باشد که مانع دسترسی به منابع و سیستم های خارجی شوند؟ برای مثال یک سرور دسترسی به فایل‌های اشتراکی از سایر سرورها نداشته باشد تا نفوذ یا آلودگی یک سرور در سایر سرورها منتشر نشود.	
۹	آیا تایید می نمایید که برنامه داده های آپلود شده از منابع نامطمئن را اجرا نمی کند؟ بعنوان نمونه مجوز آپلود فایلهای اجرایی داده نشود یا قابلیت اجرای ماکروها یا اسکریپت‌ها در سرور بسته باشد.	
۱۰	آیا تایید می نمایید که فایل های Flash ، Silverlight در سامانه شما وجود ندارد؟ پسوندهای swf. و xap. در سامانه وجود نداشته باشد.	

نیازمندی های کنترل موبایل

۱	آیا تایید می نمایید که برنامه ی موبایل داده های حساس را در منابع اشتراکی موبایل (کارت حافظه، پوشه های اشتراکی) ذخیره نمی کند؟	
۲	آیا تایید می نمایید که داده های حساس بر روی پایگاه داده ی SQLlite در موبایل ذخیره نمی شود؟ برای مثال در سامانه‌های حساس، نام کاربری و کلمه عبور در دیتابیس موجود در موبایل ذخیره نشود و حتما نیاز به اتصال به سرور داشته باشد.	
۳	آیا تایید می نمایید که کلیدهای سری و کلمات عبور در کد برنامه ی اجرایی ذخیره نشده اند؟ (اقرارنامه)	
۴	آیا تایید می نمایید که داده های حساس برنامه به وسیله ی ویژگی auto-snapshotدر سیستم عامل iosافشا نمی شوند؟	
۵	آیا تایید می نمایید که منابع درخواست شده و مجوزهای دسترسی به آن با یکدیگر تطابق داشته باشند (در فایل‌های iOS Entitlements و AndroidManifest.xml این موضوع را بررسی نمایید.) ؟	
۶	آیا تایید می نمایید که گزارش های برنامه حاوی داده های حساس نباشند؟ برای مثال حاوی موجودی حساب‌ها و یا کلمه عبور نباشد.	
۷	آیا تایید می نمایید که کد برنامه مبهم سازی شده باشد تا عملکرد آن واضح نباشد؟ (اقرارنامه)	

۸	آیا تایید می نمایید که برنامه داده های حساس را در گزارشات سیستمی یا حافظه ذخیره ثبت نمی کند؟	
۹	آیا تایید می نمایید که برنامه قابلیت تکمیل خودکار را برای ورودی های حساس مانند کلمه عبور و اطلاعات بانکی غیرفعال کرده است؟	
۱۰	آیا تایید می نمایید که فایل تنظیمات نادرست نبوده (مجوزهای/خواندن نوشتن) و حالت پیش فرض تنظیمات حالت امنی است؟	
۱۱	آیا تایید می نمایید که برنامه فایل هایی با مجوز های MODE-WORLD-READABLE یا MODE-WORLD-WRITABLE را در سیستم عامل اندروید ایجاد نمی کند؟	
۱۲	آیا تایید می نمایید که اپلیکیشن شما از مکانیزم فعال سازی معتبر استفاده می نماید؟ بعنوان نمونه حتما برای فعال سازی به سرور متصل شده و اطلاعات مورد نیاز را به آن ارسال/دریافت کند و از فعال سازی دوعاملی برای نرم‌افزارهای حساس استفاده کند.	

نیازمندی‌های کنترل محیط توسعه

۱	بررسی کنید که کامپوننت‌های مورد استفاده در توسعه سیستم، از نظر نقص امنیتی مشکلی نداشته باشد. (اقرارنامه)	
۲	بررسی کنی که از آخرین ورژن تکنولوژی‌های موجود برای جلوگیری از سوءاستفاده از آسیب‌پذیری‌های موجود، استفاده شود. برای مثال آخرین ورژن SSL یا IIS که نقض امنیتی آن شناسایی نشده است. در بازه‌های زمانی مختلف از آپدیت بودن سرویس‌ها اطمینان حاصل نمایید.	