مستند امکانات امنیتی

سیستم‌ساز برسا

برسا نوین رای

تیر ۱۴۰۳

barsasoft.com

فهرست مطالب

۱ مقدمه

یکی از مهمترین جنبه‌های تولید نرم‌افزارهای سازمانی توجه به جنبه‌های مختلف امنیت نرم‌افزار و اطلاعات میباشد. حساسیت و اهمیت این موضوع به قدری است که لزوما باید از روش‌های آزموده شده و مطمئن استفاده نمود.

امروز نیاز به امنیت، تولید کنندگان محصولات نرم‌افزاری و سازمان‌هایی که از این محصولات استفاده میکنند را وارد میکند تا تدابیر لازم جهت مقابله با هرگونه سوء استفاده و خرابکاری و یا افشای اطلاعات حساس را در محصولات خود در نظر بگیرند.

امنیت یک مسیر است نه یک هدف چرا که هر روز ممکن است آسیب پذیریهای جدید کشف و مورد سوء استفاده کاربران بدخواه قرار گیرد. بنابراین لازم است در گام اول تولیدکنندگان محصولات نرم‌افزاری با کمک متخصصین امنیت نرم‌افزار و در نظر گرفتن موارد امنیتی بصورت کلان و در حوزه های طراحی، معماری و پیاده‌سازی نرم‌افزار و همچنین استفاده از سرویس‌ها و مکانیزمهای امنیتی مورد نیاز، خسارت ناشی از حمله کاربران بدخواه به سیستم را کاهش دهند.

سیستم‌ساز برسا از جنبه‌های گوناگون مقوله امنیت را مورد تحلیل و بررسی قرار داده و برای هر قسمت راهکار مناسب آن را ارائه نموده است. در ادامه برخی از این ویژگیها بصورت خلاصه مورد بررسی قرار میگیرد.

۱,۱ تولید تمامی بخش‌های سیستم‌ساز در درون شرکت برسا

از جمله موارد مهم که در امنیت کلی نرم‌افزارهای تولیدی مورد توجه میباشد این است که تمامی بخش‌های سیستم‌ساز بطور کامل در درون شرکت برسا نوین رای ساخته شده و کدهای منبع تمامی آنها وجود دارد. حتی کنترلهای واسط کاربری نیز تماما در درون شرکت تولید شده و کد منبع آنها وجود دارد.

این امر تضمین میکند که هیچگونه مشکل و یا شک و شبهه‌ای در استفاده از زیرساختهای سیستم‌ساز وجود نداشته و سازمان‌ها و شرکتها میتوانند با طیب خاطر از امکانات آن استفاده نمایند.

۲ جنبه های مختلف امنیت سیستم

امنیت یک هویت چندوجهی و دارای ابعاد گوناگون و مختلف می‌باشد که در یک برنامه جامع امنیت به تمامی این ابعاد توجه شده و همگی در بستر یکپارچه امنیت قرار گیرند.

برخی از جنبه های مهم امنیتی زیرساخت سیستم‌ساز به شرح ذیل می‌باشد.

۲,۱ تصدیق هویت و اعتبارسنجی (Authentication)

یکی از نمودهای اصلی امنیت در نرم‌افزار داشتن نام کاربری و رمز عبور برای هر کاربر میباشد. در زیرساخت سیستم‌ساز برسا هر کاربر برای ورود به سیستم بایستی دارای نام کاربری و رمزعبور مربوط به خود باشد. بنابراین هر شخص پس از ورود به سیستم شناخته شده و تمامی فعالیتهای وی قابل ردگیری خواهد بود.

برای ذخیره نمودن رمزهای عبور از یک روش غیرقابل بازگشت رمزنگاری استفاده شده است که بوسیله آن رمزعبور کاربران ذخیره شده و هیچ کس (حتی مدیر سیستم) قادر به شناسایی رمز نخواهد بود. از مزایای دیگر زیرساخت امنیت در سیستم‌ساز این است که کاربر با یکبار ورود میتواند از تمامی امکانات مجاز خود استفاده نماید و برای استفاده از امکانات زیرسیستم‌های مختلف نیازی به ورود مجدد در هر زیرسیستم را نخواهد داشت.

۲,۲ تصدیق حقوق دسترسی (Authorization)

یکی دیگر از جنبه‌های مهم امنیت در سیستم‌های نرم‌افزاری و خصوصا سازمانی تعیین میزان دسترسی هر کاربر به بخش‌های مختلف برنامه و اطلاعات است.

در هر سازمانی منابع اطلاعاتی و همچنین امکانات برنامه دارای ارزش خاص خود هستند که طبق سطوح تعریف شده سازمان، فقط عده خاصی حق اطلاع و یا تغییر آنها را خواهند داشت. بنابراین برای صحت عملکرد یک سامانه سازمانی این بحث از اهمیت خاصی برخوردار است که بتواند حدود مجاز هر کاربر از لحاظ دسترسی و یا تغییر اطلاعات را مشخص و کنترل نمود.

در سیستم‌ساز برسا یکی از منعطف‌ترین و کاربردی‌ترین روش‌های تعریف، نگهداری و کنترل دسترسیها استفاده شده است که قابلیتهای فراوانی را در اختیار تولید کنندگان قرار میدهد تا بسادگی و با کمترین هزینه بتوانند از زیرساخت کنترل دسترسیها استفاده نمایند. این زیرساخت در پروژه‌های مختلف مورد استفاده قرارگرفته و به بستری کامل و قابل اطمینان برای چک دسترسیها تبدیل گردیده است.

۲,۳ رمزنگاری اطلاعات (Data Encryption)

یکی از عناصر مهم در حفاظت اطلاعات سازمان رمزنگاری اطلاعات میباشد. این امر برای حفاظت از بخش‌های حیاتی اطلاعات و تضمین عدم دسترسی افراد غیرمجاز به اطلاعات از اهمیت خاصی برخوردار است.

رمزنگاری در زیرساخت سیستم‌ساز میتواند در بخش‌های مختلف مورد استفاده قرار گیرد که مهمترین آنها عبارتند از:

۱- **رمزنگاری اطلاعات اتصال به پایگاه داده:** با توجه به اینکه تمامی اطلاعات سازمان در پایگاه داده ذخیره میشود، زیرساخت سیستم‌ساز اطلاعات اتصال به پایگاه داده را رمز کرده تا هیچ کاربری نتواند از این اطلاعات به منظور اتصال به پایگاه داده استفاده نماید.

۲- **رمزنگاری برخی داده‌های مهم در برنامه:** در بخش‌هایی که اطلاعات بسیار مهم و محرمانه هستند میتوان مکانیزمهایی را برای رمزنمودن اطلاعات قبل از ذخیره در پایگاه داده مورد استفاده قرار داد. در صورت این نوع رمزنگاری حتی درصورتیکه کاربری اطلاعات اتصال به پایگاه داده را در اختیار داشته باشد نمیتواند از اطلاعات استفاده نماید.

۳- **رمزنگاری اطلاعات برای انتقال بر روی شبکه:** زیرساخت سیستم‌ساز این امکان را فراهم می‌آورد که سازمان بتواند برای ارتباط بین کلاینتها و سرور از یک بستر کاملا امن و تضمین شده استفاده نماید تا اگر احیانا شخصی از درون و یا بیرون سازمان اطلاعات بین کلاینت و سرور را پایش میکند، نتواند از آن استفاده نماید.

۲,٤ بررسی صحت ورودی و خروجی

در موضوع امنیت جامع توجه به صحت ورودی و خروجی اطلاعات بسیار حائز اهمیت می‌باشد. خصوصا این که مقادیر وارد شده توسط کاربر منجر به ایجاد اشکال در فراخوانیهای دیتابیس، اعتبارسنجیها و .. نگردد.

سیستم باید قوانین مشخص اعتبارسنجی برای فیلدهای اطلاعاتی را پوشش داده و علاوه بر آن در تمامی مراحل سیستم این قوانین به دقت در سطح واسط کاربری و در سطح منطقهای سمت سرور چک و کنترل شود.

۲,٥ رمزنگاری اطلاعات

در مقوله رمزنگاری استفاده از کلیدهای عمومی و اختصاصی، روش‌های رمزنگاری مصوب، نحوه ذخیره سازی اطلاعات و انتقال اطلاعات بر روی شبکه، امکان تنظیم رمز نگاری اطلاعات کاربران، نگهداری رمزهای عبور، نگهداری اطلاعات مهم در فضای وب و ... مورد بررسی قرار می‌گیرد که یکی از جنبه های مهم امنیت سیستم‌های اطلاعاتی را شامل میشود.

۲,٦ مدیریت خطاها و استثنائات

قطعا مدیریت خطاها بسیار در ردیابی مشکلات امنیتی و حل آنها تاثیر بسزایی دارد. برخی از انواع حمله های سایبری مبتنی بر ایجاد اخلال در اجرای کد برنامه می‌باشد که منجر به تولید خطا در عملکرد سیستم گشته و از طریق ثبت این موارد و ردیابی آنها می‌توان احتمال وقوع موارد امنیتی را مدیریت کرد.

۲,۷ امضا دیجیتال (PKI) و انکار ناپذیری

سیستم‌های اطلاعاتی پس از گسترده شدن جای خود را در روال‌های تعاملی سازمان‌ها بازکرده و منجر به استفاده وسیع در سطح سازمان‌ها خواهند گشت. نکته حائز اهمیت این است که در تعاملات سازمانی اتفاقات ثبت شده در سیستم قابل اطمینان و به دور از امکان انکار شدن باشند.

به نحوی که اگر یک کاربر در سیستم عملی را انجام داد به هیچ وجه نتواند اجرای آن مورد در سیستم را منکر شده و از پذیرفتن تبعات آن اجتناب نماید.

۲,۸ طراحی، معماری و کدنویسی امن

قطعا امنیت چیزی نیست که بتوان بصورت یک عامل بیرونی به یک برنامه سازمانی القا نمود. بلکه امنیت باید در تمامی مراحل طراحی و تولید سیستم مورد نظر بوده و عملا نرم‌افزار با یک نگاه امنیتی دقیق و صحیح طراحی و تولید گشته باشد.

از این رو توجه به معماری امن و نحوه کدنویسی مبتنی بر قواعد امنیتی از مسائل تاثیرگزار در امنیت جامع سیستم‌های اطلاعاتی است.

۲,۹ رویدادنگاری فعالیتهای کاربران و ردگیری (Log & Audit)

از عوامل مهم در جلوگیری و یا کشف دسترسیهای غیرمجاز و یا کنترل کاربران ثبت رویدادهای کاری کاربران(کارهای انجام شده توسط هر کابر از زمان ورود به نرم‌افزار) میباشد. سیستم‌ساز با ابزار لازم در زمینه رویدادنگاری این امکان را فراهم می‌آورد که کلیه فعالیتهای کاربران در سیستم ثبت شده و در آینده توسط مدیر سیستم قابل کنترل و بررسی باشد.

علاوه بر آن به دلیل آنکه ممکن است رویدادها حجم زیادی را اشغال نمایند تمهیدات لازم برای آرشیو آنها نیز لحاظ شده است.

۲,۱۰ امنیت دیتابیس

دیتابیس به عنوان ذخیره گاه کلیه اطلاعات سیستم مهمترین عنصر در موضوع امنیت محسوب میشود. چراکه اگر نرم‌افزار دارای مکانیزمهای امنیتی قوی باشد اما دسترسی به پایگاه داده بصورت مستقیم برای حمله کنندگان فراهم باشد عملا کلیه روش‌های امنیتی بی اثر بوده و مهاجمان می‌توانند مستقیما به اطلاعات دسترسی پیدا کنند.

بنابراین در نظر داشتن مکانیزم‌های امنیتی پایگاه داده از عوامل تاثیرگزار در جامعیت روش‌های امنیتی سیستم می‌باشد.

۲,۱۱ موارد نصب و بروزرسانی

داشتن روال‌های مدون نصب و راه‌اندازی و بهنگام سازی خودکار نیز در زمره رده بندیهای امنیتی سیستم قرار گرفته و وجود نقص در این روش‌ها می‌تواند منجر به بروز مشکلات امنیتی خاص در سیستم‌های اطلاعاتی گردد.

۳ نگهداشت داده

یکی از موضوعاتی که ممکن است در نگاه اول در قالب مساله امنیت اطلاعات لحاظ نشود، اما به شدت در حوزه حفاظت از اطلاعات و داده تاثیرگذار است، موضوع روش درست نگهداشت داده می‌باشد. خصوصا این امر زمانی که با داده‌های حجیم مواجه باشیم می‌تواند به یک مساله مهم تبدیل شود.

در این خصوص می‌توان به موارد ذیل اشاره کرد.

۳/۱ ایجاد راهکار هوشمند تهیه نسخه پشتیبان

طبیعتا تهیه نسخه پشتیبان با استفاده از امکانات و ابزارهای مدیریت پایگاه داده انجام می‌شود. اما گاها با افزایش حجم داده نیازمند راهکارهای هوشمندانه برای نگهداشت اطلاعات خواهیم بود.

یکی از این روش‌ها استفاده از مکانیزم‌های تفکیک دیتابیس برای نگهداری داده‌های سنگین و کمتر تغییریابنده هست تا دیتابیس‌های اصلی بتوانند به روش سریع‌تری ذخیره و بازیابی شوند.

۳/۲ تفکیک سرورهای عملیاتی بر روی شبکه داخلی و اینترنت

یکی دیگر از موضوعات بسیار مهم، وجود امکاناتی برای تفکیک سرورها می‌باشد. در این حالت با استفاده از ابزارهای سینک هوشمند اطلاعات، امکان جداسازی فیزیکی سرورها بین فضای عمومی مثل اینترنت و فضای محافظت شده مثل اینترانت برقرار میشود و اطلاعات از دسترس مهاجمین دور شده و امکان نگهداشت داده بسیار بالاتر خواهد بود.

۴ مقابله با حملات مرسوم

در موضوع مدیریت امنیت جامع آمادگی برای حملات متداول و مرسوم مهاجمین از درجه اهمیت بالایی برخوردار است و اگر یک زیرساخت نرم‌افزاری روش‌های مقابله با حملات مرسوم را تدارک ندیده باشد، با احتمال بالایی ممکن است دچار مشکلات امنیتی گردد.

در سیستم‌ساز برسا سعی شده روش‌های مقابله با انواع حملات مرسوم مد نظر قرار گیرد که در ادامه به چند مورد از آنها می‌پردازیم.

۴/۱ SQL Injection

۴/۱/۱ تعریف مساله

در این روش متداول حمله که محل اثر کرد آن پایگاه داده است مهاجم سعی میکند با قراردادن متنهای خاص SQL در عملکرد دیتابیس ایجاد اخلال کرده و بعضا حتی برخی داده‌ها را از بین ببرد.

مشکل اصلی برنامه ها در این نوع حمله این است که برای ساخت پرس و جوهای دیتابیسی از روش کنار هم گذاری متن (string concatenation) استفاده میکنند و مهاجم می‌تواند با وارد نمودن یک متن خاص در بخشی از پرس و جو منجر به اخلال در دیتابیس شود.

۴/۱/۲ روش مقابله

در زیرساخت سیستم ۲ روش اصلی برای مقابله اصولی با این تهدید فراهم دیده شده است.

۱- **استفاده از مدل command در ارتباط با پایگاه داده به جای ترکیب متن:** زمانی که سیستم‌ساز از مدل فراخوانی command در پایگاه داده استفاده میکند به هیچ وجه امکان وقوع چنین تهدیدی وجود نداشته و در این روش مکانیزمهای پایگاه داده برای مقابله با این حمله کفایت میکنند.

۲- **کنترل عبارات ورودی از طریق تعریف لیست سیاه:** مدیر سیستم می‌تواند برخی کلمات را که حاوی احتمال خطر در این نوع حمله هستند را برای سیستم تعریف نماید و برنامه قبل از ارسال اطلاعات به دیتابیس آنها را چک میکند.

۴/۲ Brute Force

۴/۲/۱ تعریف مساله

هر چند این نوع حمله روش‌های متنوعی دارد اما یکی از پرکاربردترین حالت آن استفاده از روش تخمین رمز عبور می‌باشد. به این شکل که مهاجم مثلا از طریق تخمین رمزهای قابل استفاده و یا یک لغت نامه (dictionary) اقدام به امتحان نمودن رمزهای عبور می‌نماید.

۴/۲/۲ روش مقابله

زیرساخت سیستم‌ساز چندین روش برای مقابله با این حمله در نظر گرفته است:

۱- **اعمال قوانین تعیین رمز عبور:** قوانین تعریف شده در سیستم‌ساز به گونه ای است که میزان سختی رمز عبور را چک کرده و کاربر را ملزم می‌نماید که از ترکیبهای مختلف کاراکتری برای رمز استفاده کرده و لزوما رمز عبور نباید در دامنه لغات مرسوم قرار گیرد و بسیار قواعد دیگر که احتمال حدس زدن رمز را به حداقل ممکن میرساند.

۲- **غیرفعال نمودن حساب کاربر در رمزهای عبور اشتباه متوالی:** سیستم بلافاصله پس از چندین تلاش ناموفق یک کاربر برای ورود به سیستم حساب را غیرفعال نموده و صرفا از طریق مدیر سیستم امکان فعال نمودن مجدد حساب کاربر امکان پذیر می‌باشد.

۳- **ثبت آی پی دستگاه مهاجم:** سیستم شناسه دستگاهی که حملات از طریق آن اتفاق افتاده است را ثبت میکند و این امکان پیگیری مهاجم را افزایش می‌دهد.

۴- **اطلاع‌رسانی به کاربر در ورود موفق بعدی:** در صورتیکه حساب کاربری یک شخص دچار حمله تست رمز شده باشد در ورود موفق بعدی کاربر به وی در این خصوص اطلاع‌رسانی میشود.

۴/۳ Buffer Overflow

۴/۳/۱ تعریف مساله

در این روش حمله سعی میشود با ورود اطلاعات نادرست ایجاد اخلال در مدیریت حافظه برنامه صورت گرفته و از طریق خطاهای سیستمی عملکرد برنامه متوقف و یا دچار اخلال شود.

۴/۳/۲ روش‌های مقابله

۱- **اعتبارسنجی ورودی کاربران:** ورودی کاربران به گونه ای اعتبارسنجی میشود که احتمال این حمله به شدت کاهش می یابد. مثلا طول رشته های متنی، فرمت ورود اطلاعات تاریخ و زمان، محدوده اعداد و ... قابلیت کنترل و اعتبارسنجی خودکار دارد.

۲- **مدیریت خطاها و رخدادها:** از آنجا که در سیستم‌ساز برسا تمامی خطاها و رخدادها با روش‌های اصولی مدیریت و ثبت میشود این موضوع بسیار قابل کنترل بوده و عملا بروز یک خطا در سایر بخش‌های سیستم ایجاد اخلال نمیکند.

۴/۴ XSS (Cross Site Scripting)

۴/۵ تعریف مساله

در این حالت سعی میشود که اسکریپتهای اجرایی برنامه وب توسط کدهای مخرب جایگزین شده و عملی غیر از آنچه در برنامه انتظار آن میرود انجام شود.

۴/۶ روش‌های مقابله

۱- **استفاده از روش‌های بهم ریختگی اسکریپتها:** در این روش اسکریپتهای منتقل شده به سمت کلاینت به گونه ای بهم ریخته میشوند که فهم آنها بشدت سخت بوده و مهاجم به راحتی نمی‌تواند اسکریپتهای معادل را جایگزین نماید.

۲- **اعتبارسنجی سمت سرور:** مساله بسیار مهم در برخورد با این حمله این است که تمامی قواعد کاری و اعتبارسنجیها سمت سرور مجدد انجام شده و به هیچ وجه به اعتبارسنجی سطح واسط کاربری بسنده نمیشود.

۵ لیست امکانات امنیتی سیستم‌ساز برسا

یکی از مسائل مهم در سطح امنیتی سیستم‌ساز برسا چک لیست های تایید شده در این زیرساخت می‌باشد که منجر به ایجاد سطح بالایی از امنیت اطلاعات در این بستر میگردد. این چک لیست دارای تنوعی از مسائل امنیتی مختلف بوده و همگی به دقت در ابزار سیستم‌ساز مورد بررسی و تایید قرار گرفته اند.

در ادامه به شرح ویژگیهای امنیتی سیستم‌ساز می‌پردازیم.

ردیف	ویژگی	شرح ویژگی	محل اجرا
	تشخیص و تصدیق هویت		
1	تصدیق هویت کاربران	برنامه کاربردی باید قبل از اعطای حق دسترسی به منابع و نقش‌ها باید هویت کاربران را تصدیق کند	برنامه
2	تصدیق هویت فرایندها	برنامه کاربردی باید هویت تمامی فرایندها،برنامه ها و دیگر موجودیت ها و اشیاء فعال را که از طرف کاربر عملی را انجام می‌دهند، بررسی و تصدیق کند.	برنامه
3	اخطار تصدیق هویت	قبل از اجازه دسترسی به منابع ، برنامه کاربردی باید پیام اخطاری را که شامل موارد زیر است به اطلاع کاربر برساند :۱-کاربر به سیستم ...سازمان...وارد شده است.۲-سیستم متعهد به رعایت حقوق شخصی کاربران است. ۳-طبقه بندی داده‌هایی که برنامه کاربردی به آن دسترسی دارد، براساس حساس ترین داده‌های مورد دستیابی.۴-اعلان ردگیری و بازبینی فعالیتهای کاربر.۵-مسؤلیت کاربر در قبال اطلاعات حساس مورد دستیابی	مستند - ابتدای برنامه
4	اعلان ورودی های قبلی	علاوه بر موارد مشخص شده در مورد "اخطار تصدیق هویت"اطلاعات مشخص شده در زیر نیز باید به اطلاع کاربر برسد.این اطلاعات برحسب هر شناسه کاربری مشخص میگردد: ۱- تاریخ، زمان، آدرس و نام دامنه چند ورود اخیر کاربر ۲-تعدات دفعات تلاش برای ورود ناموفق، قبل از آخرین ورود موفق	برنامه
5	استفاده از روش‌های تصدیق هویت خاص	فرایند تشخیص و تصدیق هویت کاربران علاوه بر استفاده از نام های کاربران و کلمات عبور باید از یکی از روش‌های زیر نیز استفاده کند : توکنهای سخت افزاری، روش‌های بیومتریک، PKI, Single Sign On	برنامه
6	زنجیره عاملهای تصدیق هویت شده	برای هر تراکنشی برنامه کاربردی باید مطمئن شود که زنجیره ای از عاملهای تصدیق هویت شده بین مرورگر>کارگزار وب>کارگزار برنامه کاربردی>سیستم‌های پشت صحنه مثل DBMS ایجاد شده باشد.	برنامه
7	مسیر تصدیق هویت امن شده	تمامی اطلاعات تصدیق هویت کاربران باید از طریق یک مسیر رمزنگاری و امن شده ارسال شود. این اطلاعات شامل نامهای کاربری و کلمات عبور، کوکی تصدیق هویت، گواهینامه های الکترونیکی و ... می‌باشد	مستندات راه‌اندازی SSL
8	ذخیره سازی اطلاعات هویتی کاربران بصورت امن شده	تمامی اطلاعات تصدیق هویت کاربران باید در رسانه های ذخیره سازی بصورت رمزنگاری شده ذخیره گردد.	برنامه

9	اعمال قاعده دفاع در عمق برای تصدیق هویت	تصدیق هویت برنامه کاربردی نباید به عنوان راهکار جایگزین تصدیق هویت سیستم‌های پشتیبان نظیر DBMSها در نظر گرفته شود	برنامه
10	تعداد دفعات تلاش برای اجرای ناموفق	برنامه کاربردی باید با ایجاد واسط های کاربری تعداد دفعات تلاش برای ورود ناموفق را، برای مدیران سیستم تنظیم پذیر کند.	برنامه
11	فعال کردن دوره ای شناسه های کاربران	برنامه کاربردی باید با ایجاد مکانیزم هائی، کاربرانی را که در یک مدت زمان مشخص تلاشهای ناموفق برای ورود به برنامه کاربردی داشته ان، در زمانی قابل تنظیم قفل کند.	برنامه
12	عدم وجود نقش‌هائی در سیستم بدون اطلاعات تصدیق هویتی	هیچ نقشی در سیستم نباید بدون اطلاعات تصدیق هویتی باشد	برنامه
13	تصدیق هویت در سطح نقش‌های موجود	برنامه کاربردی ابتدا باید هویت کاربر را بصورت جداگانه تصدیق کند و سپس صحت ادعای عضویت یک کاربر را برای عضویت او در یک گروه/نقش بررسی کند	برنامه
14	عدم استفاده از اطلاعات تشخیص هویتی در کد	برنامه کاربردی نباید از اطلاعات تصدیق هویتی نظیر کلمه عبور، کلیدهای رمزنگاری و ... در کد استفاده کند	
15	استفاده از کلمه های عبور قوی	برای جلوگیری از انجام حملات brute-force و Dictionary Attack باید کلمه های عبور براساس خط مشی انتخاب کلمه های عبور انجام شود و استفاده از کد امنیتی captcha	برنامه
16	خط مشی تغییر کلمه های عبور بوسیله کاربران	مدیریت کلمه های عبور در برنامه های کاربردی باید دارای خواص زیر باشد: ۱-مدیران سیستم قادر باشند به کاربران کلمه های عبور اختصاص دهند.۲-اجبار کاربران برای تغییر کلمه های عبوری که مدیر سیستم به آنها اختصاص داده است بعد از اولین ورود.۳-توانا کردن کاربران به قابلیت تغییر کلمه های عبور بصورت دوره ای برحسب خط مشی های سیستم و یا برحسب تقاضای کاربر ۴- اجبار کاربران به انتخاب کلمه های عبور جدید با حداقل ۴ کاراکتر جدید. ۵- قابل تنظیم بودن تعداد کلمات عبور قبلی که کاربر نمی‌تواند انتخاب نماید.	برنامه

17	انتخاب کلمه عبور جدید بعد از گذشتن تاریخ مصرف کلمه عبور قبلی	برنامه کاربردی باید تا زمانی که کاربر کلمه عبور تاریخ مصرف گذشته خودرا عوض نکند، اجازه ورود به سیستم ندهد.	برنامه
18	عدم اجازه انتخاب مجدد کلمه های عبور تاریخ گذشته	مدیریت کلمه های عبور در برنامه های کاربردی باید بگونه ای باشد تا تشخیص دهد آیا کاربر کلمه عبور تاریخ مصرف گذشته قبلی خود را انتخاب میکند؟ واز انجام این کار توسط کاربر جلوگیری کند. ملاحظه: کلمات عبوری که تاریخ مصرف آنها منقضی شده، در حالت محرمانه بعداز شش ماه و برای خیلی محرمانه بعداز دوازده ماه قابل استفاده خواهد بود.	برنامه
19	شناسه های کاربری یکتا	برنامه کاربردی نباید اجازه دهد یک شناسه کاربر با چند کلمه عبور انتخاب شده و یا با یک شناسه کاری یکسان امکان ورود چندین کاربر وجود داشته باشد.	
20	عدم ذخیره اطلاعات تصدیق هویت کاربر بطور نامناسب	برنامه کاربردی نباید اطلاعات تصدیق هویت کاربر را در کوکی ها، اسکریپت های سمت کارگزار ویا مشتری ویا دیگر فایل‌هائی که این اطلاعات بتواند ار آن بدست آید، ذخیره کند	
21	عدم وجود شناسه کاربری بدون هویت	برنامه کاربردی نباید شامل شناسه کاربری بدون هویت برای ورود باشد	
22	طبقه بندی نواحی برنامه کاربردی	نواحی عمومی برنامه کاربردی که برای دسترسی به آنها نیازی به راهکارهای تصدیق هویت نیست باید شناسائی شده و از نواحی خصوصی که برای دسترسی به آنها نیاز به تشخیص هویت است مجزا گردد	برنامه
23	قاعده کمترین حق دسترسی	برنامه کاربردی باید بطور پیشفرض کمترین حق دسترسی را برای شناسه کاربری در نظر بگیرد	برنامه
24	چگونگی ذخیره	رشته اتصال به پایگاه داده نباید در کد و یا فایل‌های پیکربندی بصورت شفاف ذخیره گردد	برنامه

25	عدم ارائه جزیات به کاربر در صورت ورود ناموفق	برنامه کاربردی نباید مشخص کند که علت شکست ورود، کلمه عبور نادرست بوده است	
26	ردگیری تلاشهای ورود ناموفق	برنامه کاربردی باید تلاشهای ناموفق برای ورود را برای ممیزی ردگیری کند	برنامه
27	عدم نمایش شناسه کاربری بعد از ورود ناموفق	برنامه کاربردی باید شناسه کاربری را بعداز ورود ناموق مجددا از کاربر بخواهد	برنامه
28	وجود خصیصه LockOut	اگر کاربر وارد سیستم گردید و سپس برای یک مدت زمان از سیستم استفاده ننمود، جهت استفاده مجدد باید احراز هویت شود	برنامه
29	احراز هویت مجدد برای صفحات حساس	جهت انجام هرگونه فعالیت حساس در سیستم احراز هویت مجدد از کاربر صورت گیرد	برنامه
تصدیق حقوق دسترسی			
30	ایجاد رابطهای کاربری برای مدیریت حقوق دسترسی	برنامه کاربردی باید رابطهای کاربری لازم را برای ایجاد و مدیریت لیست کنترل دسترسی ها و سایر اطلاعات حقوق دسترسی فراهم آورده باشد	برنامه
31	بررسی حقوق دسترسی بین فرآیندی	برنامه کاربردی باید کنترل حقوق دسترسی بین فرآیندهای سیستم را پیاده‌سازی کند	برنامه
32	قاعده کمترین حق دسترسی	حقوق دسترسی اعطا شده به برنامه کاربردی در هر زمان باید کمترین حق دسترسی مورد نیاز برای انجام فعالیت های لازم باشد	برنامه
33	استفاده از حقوق دسترسی نقش گرا	حقوق دسترسی در برنامه کاربردی باید بصورت نقش گرا پیاده‌سازی شود	برنامه

34	سازگار بودن نقش و حقوق دسترسی	نقشی که به یک فرآیند از یک برنامه کاربردی نگاشت میشود باید مطابق با وظیفه و عملکرد فرآیند مزبور باشد	برنامه
35	تفکیک وظایف نقش‌ها	کاربر انجام وظایف خودرا تنها با نگاشت یک نقش بتواند انجام دهد	برنامه
36	طبقه بندی داده‌ها برحسب حقوق	داده‌های کاربران باید براساس سطح دسترسی طبقه بندی شده و تنها نقش‌های مجاز بتواند تنها به داده‌های مورد نیاز خود دسترسی داشته باشد	برنامه
37	برچسب گذاری داده‌های طبقه بندی شده	برنامه کاربردی باید بتواند برچسبهای محرمانه و جامعیت مناسب را برروی داده‌هائی که ایجاد و یا تغییر می‌دهند اعمال کند. این برچسبها باید بتواند توسط راهکارهای کنترل دسترسی شناخته شده و استفاده گردند.	برنامه
38	برچسب گذاری داده‌های خروجی	داده‌های تولید شده توسط برنامه کاربردی که به سیستم دیگر انتقال میابند و یا توسط چاپگر چاپ میشوند باید برچسب طبقه بندی اطلاعات داشته باشند	برنامه
39	عدم پذیرش ورود مستقیم URL جهت دسترسی به منابع غیر مجاز	برنامه کاربردی نباید به کاربران اجازه دهد با تایپ مستقیم یک URL در خط آدرس مرورگر به صفحاتی که اجازه دسترسی ندارند، دسترسی پیدا کنند.	
40	استفاده از دیدهای(view) پایگاه داده	امکان استفاده از دیدهای پایگاه داده به عنوان راهکار مکانیزم منترل دسترسی نباید وجود داشته باشد	
41	تنظیم پذیر بودن راه کارهای کنترل دسترسی	برنامه کاربردی باید واسط های لازم برای مدیر سیستم جهت اعمال خط مشی های کنترل دسترسی به اشیاء برای کاربران، نقش‌ها و گروهها ایجاد کند.	برنامه
42	رعایت قاعده دفاع در عمق	برنامه کاربردی نباید به یک راهکار کنترل حقوق دسترسی اکتفا کند. راههای کنترل دسترسی باید در لایه‌های مختلف (مثل کارگزار وب، برنامه کاربردی، پایگاه داده) ایجاد شود	برنامه

43	استفاده از رویه های ذخیره شده (stord procedure) برای دسترسی به پایگاه داده	با استفاده از رویه های ذخیره شده در پایگاه داده و تعریف نقش‌های لازم برای کاربران برنامه کاربردی می‌توان کنترل حقوق دسترسی را برای هر رویه ذخیره شده اعمال کرد و بنابراین هر کاربر بتواند رویه های ذخیره شده خود را اجرا کند.	برنامه
مدیریت نشست			
44	حفاظت از نشستها هنگام انتقال برروی شبکه	نشستها هنگام انتقال روی شبکه باید بصورت رمز شده باشند	برنامه
45	انتخاب شناسه نشست	شناسه نشستها باید بگونه ای باشد که قابل حدس زدن نباشد	برنامه
46	تاریخ مصرف داشتن	در صورتیکه کاربر در یک زمان مشخص غیر فعال بود، نشست باید بطور خودکار منقضی شود. بعداز منقضی شدن نشست، کاربر مجدد باید تصدیق هویت شود	برنامه
47	تنظیم نشستهای همزمان	برنامه کاربردی باید راهکار تنظیم نشست های همزمان را برای هر کاربر، نقش یا گروه را از طریق واسطه هائی در اختیار مدیر سیستم قرار دهد ویا راهکارهای خودکار تنظیم تعداد نشستها را در خود داشته باشد	برنامه
48	تنظیم مکان ذخیره وضعیت نشستها	برنامه کاربردی باید راهکار تنظیم نشست را از طریق واسطه هائی در اختیار مدیر سیستم قرار دهد.	برنامه
49	عدم ذخیره اطلاعات حساس در کوکی های ماندگار	در سطوح طبقه بندی خیلی محرمانه نباید از کوکی های ماندگار استفاده شود	
50	زمان انقضای نشست	برنامه کاربردی باید راهکار تنظیم زمان غیر فعال بودن کاربر برای منقضی کردن نشست را از طریق واسط هائی در اختیار مدیر سیستم قرار دهد	برنامه
51	قابلیت Log Out	برنامه کاربردی باید بتواندفرمان پایان نشست را بطور صریح صادر کند	برنامه

52	رمزنگاری محتویات کوکی های تصدیق هویت	برنامه کاربردی باید محتویات کوکی های تصدیق هویت را رمزنگاری کنند	
53	عدم انتقال شناسه های نشست از طریق Query String	شناسه نشست نباید از طریق URL Query String انتقال یابد	
بررسی صحت ورودی و خروجی			
54	نقاط ورودی، خروجی و سطوح امنیتی	تمام ورودی ها، خروجی ها و ناحیه های امن برنامه کاربردی برای اعمال راه کارهای کنترلی باید مشخص شود	برنامه
55	تطبیق داده‌های ورودی	داده‌های ورودی باید براساس نوع، مقدار، شکل، اندازه و محدوده و نیز پاکسازی ورودی براساس لیست کاراکترها و الگوهای بدنیت بررسی و تطبیق داده شوند.	برنامه
56	کنترل متمرکز صحت داده‌های ورودی	برای کنترل متمرکز خط مشی های بررسی صحت ورودی، بررسی صحت ورودی در سطح برنامه کاربردی باید متمرکز و با استفاده از توابع و متدهای طراحی شده به این منظور انجام شود.	برنامه
57	واسط های کاربری مدیریتی	برنامه کاربردی باید واسط های کاربری لازم را برای تنظیم خط مشی های امنیتی برای مدیر سیستم فراهم کند	برنامه
58	عدم اعتماد به بررسی صحت ورودی در سمت کاربر	معماری برنامه کاربردی باید باید به گونه ای باشد که تنها به بررسی صحت ورودی در سمت کاربر اکتفا ننموده و صحت ورودی در سمت سرور نیز بررسی شود.	
59	رعایت قاعده دفاع در عمق برای بررسی صحت ورودی	بررسی صحت ورودی در تمامی لایه‌های مرورگر، برنامه کاربردی و پایگاه داده، باید انجام گیرد	

60	تطبیق داده‌های خروجی	داده‌های خروجی برنامه های کاربردی که از طرف کاربر فراهم آورده شده باشند باید براساس نوع, مقدار، شکل، اندازه و محدوده و نیز پاکسازی خروجی براساس لیست کاراکترها و الگوهای بدنیت بررسی و تطبیق داده شده تا امکان سوء استفاده نفوذگران از این ناحیه جلوگیری گردد.	برنامه
61	جلوگیری از آسیب پذیری XSS	برنامه کاربردی باید با استفاده از راه کارهای مناسب از قبیل کدگذاری، فیلترکردن برچسب های HTML و .... از بوجود آمدن آسیب پذیری XSS جلوگیری کند	برنامه
62	جلوگیری از آسیب پذیری SQL injection	برنامه کاربردی باید با استفاده از راه کارهای مناسب از قبیل فیلترکردن کاراکترهای خاص، استفاده از رویه های ذخیره شده پارامتری شده(stored procedure parameter) و .... از آسیب پذیری SQL Injection جلوگیری کند	برنامه
63	جلوگیری از آسیب پذیری Buffer Overflow	برنامه کاربردی باید با استفاده از راهکارهای مناسب نظیر کنترل حدود آرایه، محدود کردن اندازه داده ورودی، مدیریت صحیح اشاره گرها و ..... از آسیب پذیری Flow Buffer Over جلوگیری کند.	برنامه
64	بررسی صحت پارامترها	صحت پارامترها قبل از استفاده شدن براساس طول، نوع، مقدار و محدوده باید بررسی شود.	برنامه
65	رد ورودیهای نا معتبر (راه سختگیرانه)	برنامه کاربردی در صورت دریافت ورودی نامعتبر از کاربر، باید فرایند کاربر را خاتمه داده و یک پیام اخطار به او نمایش دهد در صورت تکرار این عمل شناسه کاربری وی غیرفعال گردد	برنامه
66	رد ورودیهای نا معتبر (راه ضعیف)	در صورتی که برنامه کاربردی ورودی های نامعتبر از کاربر دریافت کرد، از او درخواست کند مجددا ورودی را به صورت صحیح وارد نماید.در صورتی که برای باردوم کاربر ورودی نامعتبر فراهم آورد فرایند کاربر را خاتمه داده و یک پیام خطا مبنی بر خاتمه فرایند به علت ورودی های نامعتبر به او نمایش دهد	بند ۶۵ جایگزین
67	امضاء دیجیتالی کد	برنامه کاربردی نباید کدی را که دریافت کرده است اجرا کند تا زمانی که : ۱- بررسی کند که کد به صورت دیجیتالی امضاء شده است. ۲-صحت امضاء الکترونیکی کد را بررسی کند.	برنامه

68	مقداردهی اولیه متغییرها	برنامه کاربردی باید تمامی متغیرها را مقداردهی اولیه نماید.	برنامه
69	کنترل فیلدهای مخفی فرم های HTML	برنامه کاربردی باید صحت مبدا عامل تغییرات در فیلدهای مخفی فرم را بررسی کند	برنامه
70	نقاط ورودی، خروجی و سطوح امنیتی	تمام ورودی ها، خروجی ها و ناحیه های امن برنامه کاربردی برای اعمال راه کارهای کنترلی باید مشخص شود(پورتها و فراخوانی مستقیم و کاربران مهمان)	برنامه
محرمانگی			
71	رمزنگاری داده‌های حساس قبل از ارسال برروی شبکه	برنامه کاربردی باید داده‌های حساس را قبل از ارسال برروی شبکه رمزنگاری کند. داده‌ها در صورتی رمزنگاری میشوند که در یکی از طبقه های زیر قرارگیرند: ۱-سطح طبقه بندی داده‌ها بالاتر از طبقه بندی شبکه ای باشد که داده‌ها برروی آن ارسال میشوند. ۲-برخی از کاربران شبکه مجاز به دسترسی به داده‌های مربوطه نیستند. ۳-داده‌ها طبقه بندی شده باشند، ولی شبکه یک شبکه عمومی‌باشد.	مستند
72	رمزنگاری داده‌های حساسدر رسانه های ذخیره سازی	برنامه کاربردی باید داده‌های حساس را به صورت رمزنگاری شده در رسانه ها، ذخیره سازی کند.	برنامه - کلمه عبور
73	حفاظت از کلیدهای رمزنگاری	راهکارهای رمزنگاری باید به گونه ای باشد تا مانع از دسترسی غیر مجاز به کلیدهای رمزنگاری شود.	برنامه
74	پاک سازی محیط اجرا (Run time Environment)	برنامه کاربردی باید قبل از خاتمه، تمامی فایل‌های موقت، حافظه های نهان، داده‌ها و دیگر اشیائی را که ایجاد کرده است از محیط اجرا پاک کند	برنامه
75	استفاده از الگوریتم های رمزنگاری مصوب	برنامه کاربردی باید برای رمزنگاری داده‌ها از الگوریتم های رمزنگاری مصوب استفاده کند.	قابلیت الحاق الگوریتم را داشته باشد
76	ذخیره داده در اسکریپت	برنامه کاربردی نباید هیچگونه داده را در اسکریپتها ذخیره کند	

77	استفاده از متد HTTP POST	برای انتقال داده‌ها حتی اگر از پروتکل SSL هم استفاده شده باشد باید به جای متد GET از متد POST استفاده شود	
78	استفاده از قابلیتهای مرورگر	از plug-inها، کوکی ها و دیگر قابلیتهای مرورگر تنها در صورتی باید استفاده شود که راه کار جایگزین برای پیاده‌سازی عملکرد مورد نظر وجود نداشته باشد.	
79	انتقال داده‌های حساس توسط کوکی های رمزنگاری شده	برای انتقال داده‌های حساس از کوکی های ناپایدار که رمزنگاری شده اند باید استفاده کرد.	برنامه
80	استفاده از اطلاعات حساس در نوع های تغییر ناپذیر (Immutable Type)	برنامه کاربردی نباید داده‌های حساس نظیر کلمات عبور را در نوع های تغییر ناپذیر نظیر رشته های زبان java ویا نوع هائی که توسط سرویس‌های جمع آوری زباله (Garbage Collected Service) از حافظه پاک میشوند، قرار دهد	
81	ذخیره داده‌های حساس در سمت کاربر	هیچ داده حساسی نباید در سمت کاربر نگهداری شود.	
82	ذخیره داده‌های حساس در کد برنامه	داده‌های حساس نظیر کلمه های عبور و کلیدهای رمزنگاری نباید در کد ذخیره گردد.	برنامه
مدیریت خطاها و استثنائات			
83	صحت برنامه کاربردی برای دسترس پذیری داده‌ها	برنامه کاربردی نباید شامل خطاها، نقص ها و یا آسیب پذیری باشد که باعث شود فرایندی در برنامه کاربردی داده‌ها را سهوا پاک کرده یا برروی آن چیزی بنویسد ویا حقوق دسترسی آن را تغییر دهد که باعث شود داده‌های مزبور از دسترس خارج شوند.	برنامه
84	سرویس دهی دائمی کارکزار	برنامه کاربردی نباید شامل خطاها و آسیب پذیری هائی باشد که با سوء استفاده از آن برنامه کاربردی کارگزار از دسترس خارج شود.	برنامه

85	مدیریت آستانه بار	برنامه کاربردی باید از طریق واسط هائی راهبر سیستم را قادر سازد تا آستانه بار را مدیریت نماید.	برنامه
86	شکست برنامه کاربردی	در صورت بوجود آمدن خطا در برنامه کاربردی و با شکست مواجه شدن آن، خطا و یا نقص مربوطه نباید باعث شود برنامه کاربردی به یک وضعیت ناامن برود	برنامه
87	مدیریت خطاها و استثنائات	برنامه کاربردی باید خطاها و استثنائات را با ساختارهای تعریف شده در زبان برنامه سازی به شکل مناسبی مدیریت کند	برنامه
88	اخطار از سرویس خارج شدن برنامه کاربردی	ساختارهای مدیریت خطاها و استثنائات در برنامه کاربردی باید بتواند بعد از بوجود آمدن استثنائی که باعث از سرویس خارج شدن برنامه کاربردی شده است مدیر سیستم را از طریق ارسال پیام آگاه کند. (انتخاب روش اعلام پیام باید توسط سیستم قابل تنظیم باشد)	برنامه
89	شکست در سرویس‌های زیرساخت	در صورتیکه سرویس‌های زیرساخت به هر دلیلی با شکست مواجه شدند برنامه کاربردی باید به شکل امن خاتمه یابد.	برنامه
90	تنظیم پذیر بودن مدیریت خطاها و استثنائات	راهکارهای مدیریت خطا و استثنائات باید توسط واسط های کاربری، توانائی تعریف خطاهای جدید و روش‌های پاسخ به آن را در اختیار مدیر سیستم قرار دهد.	برنامه
91	استفاده از پیامهای خطای مناسب	برنامه کاربردی باید مراقب باشد تا خطاهای برگردانده شده به کاربر حاوی اطلاعات حساس نباشد	
92	رویدادنگاری از خطاها و استثنائات	ساختارهای مدیریت خطاها و استثنائات باید با سرویس رویدادنگاری مجتمع شده و تمامی خطاها و استثنائات بوجود آمده را ثبت کند	
93	مدیریت خطاها و استثنائات بصورت مرکزی	مدیریت خطاها و استثنائات در برنامه کاربردی باید توسط یک مولفه از پیش تعریف شده و به صورت مرکزی انجام شود.	
انکار ناپذیری			
94	امضاء دیجیتال	به منظور اثبات اصالت و هویت، برنامه کاربردی تولید کننده و یا فرستنده داده‌ها باید قادر باشد تا داده‌های مربوطه را به صورت دیجیتالی امضاءکنند.	برنامه

95	صحت امضاء دیجیتال	برنامه کاربردی باید بتواند از صحت امضاء های دیجیتال اطمینان حاصل نماید.	برنامه
96	محافظت از امضاء دیجیتال	برنامه کاربردی باید از کلیدها و گواهینامه هائی که برای امضاء دیجیتال استفاده میکند محافظت نماید.	برنامه
97	سازگاری امضاء دیجیتال	امضاهای دیجیتال استفاده شده در برنامه کاربردی باید با بسترهای امضای دیجیتال فراهم شده در نیروهای مسلح سازگار باشد.	برنامه
طراحی، معماری و کدنویسی			
98	سرویس‌های با مخاطرات امنیتی بالا	برنامه کاربردی نباید از سرویس‌ها و تکنولوژیهای با مخاطرات امنیتی بالا نظیر Mobile , Code, Telnet , ... استفاده کند.	مستند
99	توابع و متدهای اضافی	برنامه کاربردی نباید شامل توابع و یا متدهای استفاده نشده ای باشند که بطور صریح در برنامه کاربردی فراخوانی نشده باشند.	
100	مؤلفه های زمان اجرا	محیط زمان اجرای برنامه کاربردی نباید شامل توابع کتابخانه ای غیرضروری باشد.	
101	کمترین حق دسترسی	تمامی فرایندهای موجود در یک برنامه کاربردی برای انجام فراخوانی متدها و دسترسی لازم را داشته باشد.	
102	مؤلفه های ساده و کوچک	برنامه کاربردی باید شامل متدهای ساده که یک وظیفه مشخص را انجام می‌دهند باشد و نه یک مؤلفه که چندین کار پیچیده را انجام می‌دهد.	
103	مؤلفه های مستقل	برنامه کاربردی باید شامل مؤلفه های مستقلی باشد تا در صورت وجود آسیب پذیری در این مؤلفه ها، تغییر مؤلفه مزبور تاثیری در کارکرد سایر مؤلفه ها نداشته باشد.	
104	دور زدن واسط های کاربری	برنامه کاربردی باید بگونه ای طراحی شده باشد تا کاربران آن نتوانند واسطه های کاربری را دور زده و مستقیما به داده‌ها و فرایندهای موجود در برنامه کاربردی دسترسی پیدا کنند.	برنامه
105	گواهینامه های امنیتی مؤلفه ها و سرویس‌های جانبی (Third-party component)	در صورتیکه برنامه کاربردی از مؤلفه ها و سرویس‌های جانبی سایر برنامه ها ی کاربردی و یا متن باز استفاده میکند، باید تمامی آنها ارزیابی امنیتی شده و دارای گواهینامه امنیتی معتبر باشند.	امکان اضافه کردن

106	اطلاعات شخصی کاربران	برنامه کاربردی نباید توسط کوکی ها و یا سایر تکنولوژیهای تحت وب، اطلاعات شخصی کاربران نظیر لیست مرورشده، آدرس پست الکترونیکی و یا سایر اطلاعات شخصی آنها را جمع آوری کرده و یا پروفایل شخصی کاربران را ایجاد کند.	
107	پیشفرض های امنیتی	برنامه کاربردی نباید براساس هیچ پیش فرضی در مورد امنیت سایر اجزاء طراحی شده و حتما بصورت مستقل ملاحضات امنیتی را پیاده‌سازی نماید	
108	جریان اجرایی برنامه	برنامه کاربردی نباید از دستوراتی که جریان اجرائی برنامه را مبهم میکند، استفاده نماید.	
109	فراخوانهای سیستمی مطمئن	برنامه کاربردی نباید توابع سیستمی مظنون به آسیب پذیری را فراخوانی کند.	
110	نام گذاری سازگار	نام گذاری تمامی alias ها، اشاره گرها، متغیرها و دیگر اشیاء در برنامه کاربردی باید سازگار و روشمند باشد.	
111	شرایط رقابت (Race Condition)	برنامه کاربردی باید با استفاده از راهکارهایی از ایجاد شرایط رقابت پیشگیری و یا جلوگیری کند.	برنامه
رویدادنگاری و ردگیری			
112	رویدادنگاری وقایع امنیتی	برنامه کاربردی باید تمام رویدادهای امنیتی (که توسط مدیر سیستم تعریف میشود) را در محل امنی ذخیره کرده و یا به یک سیستم رویدادنگاری متمرکز برای بازبینی انتقال دهد، در یک رویکرد قوی این رکوردهای ذخیره شده به صورت برخط مورد بازبینی قرار می‌گیرد.	برنامه
113	تنظیم پذیر بودن پارامترهای رویدادنگاری	راهکارهای رویدادنگاری در برنامه کاربردی باید توسط رابط های کاربری، مدیر سیستم را قادر سازد تا بتواند رویدادهایی که باید ردگیری شوند را تعریف کند.	برنامه
114	رویدادنگاری براساس شناسه کاربر	راهکارهای رویدادنگاری در سطح برنامه کاربردی باید شناسه کاربری را که باعث بوجود آمدن رویدادی شده است را به رویداد مرتبط نماید.	برنامه

115	محتویات رکوردهای رویدادنگاری	رکوردهای رویدادنگاری شامل موارد زیر (باتوجه به رویدادهای خاص) است : ۱- شناسه کاربر و یا فرایند بوجود آورنده رویداد ۲-شکست یا موفقیت رویداد ۳- تاریخ و زمان رویداد ۴- نوع رویداد ۵- شدت تخطی ۶- شکست یا موفقیت ورود ۷- قفل شدن شناسه کاربر، ترمینال و یا درگاه دسترسی و علت آن ۸- فعالیتهایی با قصد دورزدن ویا از بین بردن راهکارهای محافظت امنیتی ۹- فعالیتهای که به سطح دسترسی خاص نیاز دارند ۱۰- زمان شروع و خاتمه استفاده از برنامه کاربردی ۱۱- فعالیتهایی که مربوط به تغییر دسترسی داده‌ها می‌باشد.	برنامه
116	رویدادنگاری در لایه‌های مختلف	رویدادنگاری باید در تمامی لایه‌های یک سیستم از جمله برنامه کاربردی، کارکزار وب و پایگاه داده انجام می‌گیرد.	برنامه
117	تحلیل رویدادها	برنامه کاربردی باید بتواند با برقراری ارتباط منطقی بین رویدادها یک نتیجه کلی (بدون ارائه جزئیات غیر ضروری) به مدیر سیستم ارائه دهد .	برنامه - سازگار با آنالیزورهای موجود
118	رمزنگاری فایل‌های رویدادنگاری	رکوردهای رویدادنگاری باید به صورت رمزنگاری شده ذخیره گردند.	برنامه
119	مدیریت رسانه ذخیره ساز	برنامه کاربردی باید راهکارهای مدیریت رسانه های ذخیره ساز رکوردهای رویدادنگاری را در اختیار مدیر سیستم قرار دهد.	برنامه
120	اخطار به مدیر سیستم به خاطر تخطی از مکانیزمهای امنیتی توسط کاربران	در صورت تخطی کاربران از خط مشی های امنیتی برنامه کاربردی، سیستم رویدادنگاری برنامه کاربردی باید یکی از ۲ رویکرد زیر را پیاده‌سازی کند : ۱-اخطاری را از طریق پست الکترونیکی، سرویس پیام کوتاه و ... (که روش اخطاردهی از طرف مدیر سیستم تنظیم پذیر باشد) را به مدیر سیستم ارسال کند ۲-مدیر سیستم را قادر سازد تا با تنظیم خودکار و با توجه بهشدت بالای تخطی، برنامه کاربردی را از دسترس خارج کند (shutdown)	برنامه
121	ابزار بازبینی و مرور رکوردهای رویدادنگاری	برنامه کاربردی باید واسط های لازم برای بازبینی فایل‌های رکوردهای رویدادها را در اختیار مدیر سیستم قراردهد.	سازگاری با ابزارهای موجود
موارد نصب			

122	مستندات نصب و راه‌اندازی امن و از رده خارج کردن سامانه	باید راهنمای کامل نصب و پیکربندی بویژه پیکربندی امنیتی و نیز پیکربندی امنیتی نرم‌افزارهای استفاده شده دیگر مانند سیستم عامل، پایگاه داده‌ها،سرویس دهنده وب و .... وجود داشته باشد.	مستند
123	برنامه نصب	تنظیمات و پیکربندی های امنیتی لازم توسط نرم‌افزاری که به منظور نصب تهیه شده است انجام گردد.	مستند
124	حسابها و گذرواژه های پیش فرض	حسابها و گذرواژه های پیش فرض برنامه کاربردی باید خذف و یا تغییر یابند.	مستند
125	اطلاعات اضافی پایگاه داده	تمام اطلاعات غیر ضروری در پایگاه داده هنگام نصب باید حذف شود.	مستند
126	تاثیر محیط برنامه ای کاربردی	شرایط امنیتی خاص برای شبکه (بسته بودن برخی پورتهای شبکه، قرار گرفتن کارگزار برنامه کاربردی یا کارگزار وب در DMZ، نیاز به دیوارآتش و ....)مستند شود.	مستند
امنیت پایگاه داده			
127	مستند طرح امنیتی پایگاه داده	برای اعمال این کنترل، میبایست روش اعمال یا علت عدم اعمال کنترلهای امنیتی که در این مستند از آنها نام برده شده است برای هر پایگاه داده به طور مجزا،در مستندی با عنوان طرح امنیتی پایگاه داده گردآوری شوند. این مستند میبایست مطالب زیر را پشتیبانی نماید : ۱-ارزیابی ریسک اطلاعات و تعیین طبقه بندی اطلاعاتیکه در پایگاه داده موجود می‌باشد. ۲-برنامه ها، روش‌های اجرایی و دلایل احتمالی عدم اعمال کنترل های امنیتی موجود در الگوی امنیتی پایگاه داده ۳- اسامی تمامی مسؤلان و کاربران مرتبط با پایگاه داده ۴-تعیین امتیازهای دسترسی هر یک از مسؤلان پایگاه داده و ثبت تغییرات احتمالی آن ها	
128	پشتیبانی از نسخه DBMS	برنامه به روزرسانی نسخه DBMS ، به نسخه های دارای اعتبار و قابل پشتیبانی از طرف فروشنده محصول	
129	برنامه بروزرسانی نسخه DBMS	طرح به روزرسانی نسخه های منقضی شده، پیشبینی هزینه برای هرگونه برنامه های تست و طرح های اضافی و زمان‌بندی انجام ارتقاء نسخه محصول باید در طرح لحاظ شود.	
130	وصله های امنیتی DBMS	به روز رسانی امنیتی نرم‌افزار پایگاه داده، بر مبنای دستورالعمل فروشنده محصول برای نصب وصله ها	

131	حساب های کاربری مالکیت اشیاء در برنامه های کاربردی	معمولا لیستی از کلیه اشیاء پایگاه داده به همراه مالکیت هرکدام در جدولی در پایگاه داده موجود است،حسابهای کاربری مربوط به مالک اشیاء باید یا در اختیار مدیر پایگاه داده باشد و یا این حسابهای کاربری پیش فرض در DBMS غیر فعال گردد.	
132	نقش حساب های کاربری مدیریت DBMS در سیستم عامل	امتیازهای دسترسی سیستم میزبان که برای حساب های کاربری مدیر پایگاه در نظر گرفته شده است و برای مدیریت DBMS نیاز نمی‌باشد باید حذف گردد.	مستند
133	پذیرش امنیت DBMS	تهیه مستندات مدیریتی و امنیتی فروشنده محصول DBMS و همچنین چک لیست های امنیتی برای محصولات DBMS و بررسی پایگاه داده برای چک کردن وجود توصیه های امنیتی عنوان شده.	مستند
134	مالکیت اشیاء برنامه کاربردی	حساب های کاربری مجاز برای مالکیت اشیاء باید در طرح امنیتی پایگاه داده ثبت شود.	مستند
135	مجوز کتابخانه های نرم‌افزار DBMS	دسترسی به کتابخانه نرم‌افزار DBMS باید فقط به معدود حسابهای کاربری که نیاز به این دسترسی دارند،داده شود.کنترل دسترسی مجاز باید مستند شده و کلیه دسترسی های که مشمول حسابهای کاربری مدیر پایگاه داده،پردازش DBMS و یا SA نمیشود، تایید شود.	مستند
136	پایش نرم‌افزار DBMS	مدیر پایگاه داده مسؤول تعیین روش‌های اجرایی برای پویش تغییرات برروی نرم‌افزار پایگاه داده است. کلیه فایل‌ها و دایرکتوری های پایگاه داده در سیستم میزبان باید مشخص گردد.روش‌های اجرایی مربوطه باید همراه با گزارش پویش های انجام گرفته مکتوب و مستند شود .(تیم ممیزی باید این مستندات را مورد ارزیابی قراردهد)	مستند
137	مدیریت پیکربندی DBMS	اعمال مدیریت پیکربندی کلیه گزینه‌ها و خصوصیات DBMS، مدیریت وصله ها و بروزرسانی و تعیین مسؤلیت آن.	مستند
138	محل ذخیره سازی نرم‌افزار DBMS	نصب برنامه های کاربردی برروی پارتیشن و دایرکتوری نصب DBMS انجام گیرد. برنامه های کاربردی که مشترکا از دارکتوری و پارتیشن DBMS استفاده میکنند از حالت نصب خارج و تغییر محل داده شوند.	مستند
139	روش اجرایی پشتیبان گیری از پایگاه داده	باید روش‌های اجرایی پشتیبان گیری از پایگاه داده و مستندات آن موجود باشد. (عملیات پشتیبان گیری باید با طرح پشتیبان گیری که در طرح امنیتی سیستمی در سازمان مربوطه مکتوب و عنوان شده، هماهنگ باشد)	مستند

140	پایگاه داده نمایشی	با مطالعه مستندات فروشنده محصول و بازبینی پایگاه داده، اشیاء و برنامه های کاربری نمونه و نمایشی که برروی پایگاه داده نصب شده است، باید از حالت نصب خارج گردد.	مستند
141	استفاده از زبان تعریف داده‌ها	استفاده از اشیاء استاتیک با داده‌های متغیر به جای استفاده از اشیاء متغیر.	مستند
142	اجزاء غیر ضروری DBMS	کلیه اجزاء و مشخصه های اختیاری موجود در محصول DBMS باید مورد بازبینی قرارگیرد. هر کدام از آنها که برای اجرای برنامه های کاربردی موردنیاز است و دسترسی به DBMS را موجب میشود باید در فهرست خصوصیات طراحی برنامه کاربردی و همچنین در طرح امنیتی سیستمی قید شود. در غیر این صورت باید از حالت نصب خارج گردیده و کلیه برنامه ها و اشیاء پایگاه داده که برای پشتیبانی از آن ایجاد شده است،خذف گردید	مستند
143	استفاده از DBMSهای پردازشی/تولیدی مشترک	کلیه پارامترهای پیکربندی و شناساننده های هویت اشیاء، پایگاه داده و برنامه های مورد استفاده در سیستم‌های کاربردی باید از سیستم‌های پردازشی کاملا متمایز باشند.	
144	مالکیت نرم‌افزار DBMS	مالکیت فایل‌ها و دایرکتوری های DBMS باید به حساب کاربری نصب و نگهداری نرم‌افزار اختصاص داده شود. نصب و نگهداری فایل‌های پیکربندی و کتابخانه نرم‌افزار اختصاص داده شود. نصب و نگهداری فایل‌های پیکربندی و کتابخانه نرم‌افزار DBMS باید با حساب کاربری مالک نرم‌افزار انجام گیرد.	مستند
145	تست بازیابی و پشتیبان گیری DBMS	روش‌های اجرایی تست و بررسی پشتیبان گیری و بازیابی پایگاه داده و کلیه فعالیت هایی که در این فرایند انجام می‌گیرد، باید در طرح امنیتی سیستمس طراحی و مستند شده باشد.	مستند
146	نحوه انجام پیکربندی DBMS	روش‌های اجرایی برای پیاده‌سازی و توسعه نرم‌افزار DBMS باید طراحی و برنامه ریزی شود. این برنامه های اجرایی باید کلیه فایل‌ها و دایرکتوری های نرم‌افزار DBMS را لحاظ کند و بعد از هرگونه فعالیت جدید نصب، بروزرسانی و نگهداری که شامل تغییراتی در طرح ریزی از قبل شده میشود	مستند
147	پذیرش رمزنگاری DBMS	پیکربندی و تنظیم توابع رمزنگاری باید بر مبنای استانداردهای معتبر انجام گیرد.	مستند
148	ممیزی پایگاه داده	ممیزی باید برروی پایگاه داده فعال گردد. در صورتیکه DBMS مورد استفاده به طور محلی و طبیعی دارای ابزار ممیزی نباشد. باید از یک ابزار ممیزی که حداقل شرایط ممیزی را تهیه میبینند، استفاده کرد.	مستند

149	طرح ممیزی پایگاه داده	روش اجرایی و سیاستی برای نگهداری و ظبط اطلاعات ممیزی باید تدوین و تعیین گردد. با توجه به قابلیت سخت افزار مورد استفاده در برنامه ممیزی، اطلاعات ممیزی باید در یک بازه زمانی به صورت آنلاین وجود داشته باشد.	مستند
150	بازبینی رویدادنگاری تبادلات	پیکربندی ممیزی پایگاه داده، باید هماهنگ با الزامات مورد نیاز برنامه های کاربردی انجام پذیرد.	مستند
151	دسترسی به رکوردهای ممیزی DBMS	مجوز دسترسی به فایل‌های ممیزی و اشیاء ممیزی پایگاه داده باید به مدیران پایگاه داده و ممیزکنندگان اختصاص یابد.	مستند

152	دسترسی به حساب دسترسی مالک نرم‌افزار DBMS	روش‌های اجرایی برای محدودیت از استفاده و دسترسی به حساب کاربری نصب نرم‌افزار DBMS، طراحی و اعمال گردد.	مستند
153	رویدادنگاری استفاده از حساب کاربری نصب DBMS	روش‌های اجرایی رویدادنگاری استفاده از حساب کاربری نصب نرم‌افزار DBMS باید طراحی و پیاده‌سازی شود، به نحوی که مسؤولیت انجام هر عملیات توسط این حساب کاربری را دقیقا مشخص نماید.	مستند
154	ستفاده از حساب کاربری نصب نرم‌افزار DBMS	ساستی در راستای آموزش کاربران مجاز برای محدودیت استفاده از ستفاده از حساب کاربری نصب نرم‌افزار DBMS صرفا برای عملیات های نصب،به روزرسانی و نگهداری باید اجرا شود.	مستند
155	پایش فایل پکربندی و نرم‌افزار DBMS	روش‌های اجرایی برای پایش تغییرات غیرمجاز برروی کتابخانه های نرم‌افزار DBMS، باید طراحی و اعمال شود	مستند
156	پایش صف وظایف برروی پایگاه داده	روش‌های اجرایی برای پایش صف وظایف پایگاه داده باید طراحی و اعمال شود	مستند
157	ممیزی دسترسی به نرم‌افزار DBMS	روش‌های اجرایی برای بازبینی رکوردهای ممیزی که نشان دهنده ارتباط برنامه های کاربردی با پایگاه داده می‌باشد، باید طراحی و اعمال گردد.	مستند
158	ارتباط ایستگاه کاری با DBMS	روش‌های اجرایی برای تعریف و تولید فایل‌های پیکربندی ارتباط مجاز کاربر دارای مجوز پایگاه داده، ایستگاه کاری، به پایگاه داده سایت ایجاد و هعمال شود.	مستند

159	حساب های کاربری مشترک در DBMS	برای هر یک از کاربران، برنامه های کاربردی و فرآیندهایی که نیاز به ارتباط با پایگاه داده دارند، باید یک حساب اختصاصی تولید شود. و عملیات رویدادنگاری فعالیتهای انجامی آنها صورت گیرد	مستند
160	مجوز ترمیم DBMS	نقشی برای ترمیم پایگاه داده باید تعیین گردد و عملیت ترمیم به این حساب کاربری مجوز دار اختصاص داده شود	مستند
161	محافظت از فایل‌های ترمیم و پشتیبان DBMS	روش‌های اجرایی برای ترمیم و پشتیبان گیری پایگاه داده طراحی و اعمال شود.	مستند
162	استفده از مکانیزم PKI در DBMS	تشخیص هویت PKI برای کلیه کاربران تعریف شده برروی پایگاه داده، اعمال شود.	مستند
163	رمز عبور	روش اجرایی برای اختصاص رمز عبور موقت به حسابهای کاربری، باید اعمال شود. تعیین رمز عبور در این روش اجرایی باید بر اساس سیاست ها و پیچیدگیهای تعیین شده در طرح امنیتی سیستمی‌باشد. برای ایجاد رمز عبور، کاربر باید بر اساس سیاست تدوین شده، محدودیت داشته باشد	مستند
164	رمز عبور DBMS در انباره های خارجی	لیستی از برنامه های کاربردی میزبان که به پایگاه داده دسترسی دارند، تهیه شود.در صورت استفاده از رمزهای عبور ذخیره شده،حفاظتهای امنیتی سیستم میزبان برای آنها ضروری باشد.	مستند
165	نمایش رمز عبور برنامه های کاربردی DBMS	پیکربندی برنامه های کاربردی که رمز عبور را به صورت واضح نمایش می‌دهند باید تغییر کند. و به کاربران آموزش داده شود که استفاده از این پارامتر ممنوع گردد.	مستند
166	داده‌های تولید شده در پایگاه داده	روش‌های اجرایی و محدودیت های اعمال شده برای خارج کردن اطلاعات از پایگاه داده، باید مستند شود. باید محدودیت های مربوطه به این عمل کاملا آگاه باشد.	مستند
167	تعیین سطح دسترسی حساب کاربری DBMS	روش اجرایی برای تعیین سطح دسترسی به پایگاه داده و سیستم میزان برای برای همه حساب های کاربری پایگاه داده باید وجود داشته باشد.	مستند
168	تغییر رمز عبور	تغییر پیکربندی و یا توسعه DBMS باید به نحوی باشد که در انتخاب رمز عبور جدید و همچنین محدودیت زمانی در تعیین رمز عبور در طی ۲۴ ساعت روبرو باشد.	مستند

169	قفل شدن حساب کاربری ناموفق	شمارش تعداد تلاش های ناموفق برای ورود به سیستم انجام گرفته و در نهایت آن حساب کاربری ناموفق باید قفل شود.	مستند
170	حسابهای کاربری غیر فعال DBMS	روش اجرایی برای پایش حساب های کاربری پایگاه داده به منظور شناسایی حساب های غیرفعال و منقضی شده، باید وجود داشته باشد	مستند
171	ارتباط بیرونی DBMS	کلیه ارتباطات بیرونی و یا از راه دوری که DBMS برای دسترسی به منابع بیرونی و یا بالعکس منابع بیرونی برای دسترسی به DBMS به کار میگیرند، باید مستند شود.این مستندات باید حسابهای کاربری ایمن و داده‌های حساس در مقابل تغییر را شامل شود.	مستند
172	بازبینی روش‌های اجرایی و سیساست های امنیتی پایگاه داده	میبایست روش‌های اجرایی برای بازبینی دوره ای و بررسی سیاست های جدید را تدوین و در سازمان جاری نمود.	مستند
173	تست پایگاه داده قبل از بروزرسانی	برای این کار لازم است که روش اجرایی تهیه شده و شواهد اجرای آن ها برای فرایند ممیزی، نگهداری شود	مستند
174	کنترل دسترسی پایگاه داده به اشیاء محلی خارج از پایگاه داده	میبایست دسترسی های پایگاه داده و برنامه های کاربردی را به اشیاء خارج از پایگاه داده مورد بررسی قرار داد و مستند نمود.	مستند
175	کنترل DBMS برای مجوز اجرای فرمان محلی خارجی	میبایست مجوز پایگاه داده و برنامه های کاربردی را برای اجرای اشیاء خارج از پایگاه داده مورد بررسی قرار داد و مستند نمود.همچنین مجوزهای غیر ضروری را محدود یا غیر فعال نمود.	مستند
176	تنظیم امتیازهای دسترسی حساب های کاربری Replication	برای کنترل این موضوع میبایست امتیاز دسترسی حساب های کاربری Replication را به کمترین امتیاز دسترسی ممکن محدود نمود و از استفاده حسابهای کاربری به شکل تکراری خودداری نمود.	مستند
177	تنظیم امتیازهای دسترسی فرایندهای DBMS	میبایست حساب های کاربری سیستم عامل که توسط برنامه های خارجی استفاده میشود را به گونه ای تنظیم نمود که کمترین امتیاز دسترسی لازم برای عمل کردن را نیاز داشته باشد.	مستند

178	جداسازی حسابهای کاربری سرویس‌های DBMS	سرویس‌های مختلف پایگاه داده میبایست تحت حسابهای کاری متفاوت و با حداقل امتیاز دسترسی اجرا شوند.یاداوری میشود که برای تنظیم حقوق دسترسی حساب کاربری سرویس مورد نظر، میبایست مستندات DBMS مطالعه شود	مستند
179	ایجاد محدودیت برای Listener های شبکه مرتبط با DBMS	ایجاد محدودیت میبایست به نحوی صورت پذیرد که تنها سیستم‌هایی با آدرس شبکه ip مجاز امکان دسترسی به DBMS را داشته باشد.همچنین لیست آدرسهای مجاز میبایست مستند شود	مستند
180	قابلیت شناسایی سرویس‌های پایگاه داده	نامهای پردازشها یا سرویس‌هایی که دارای تمایز آشکار و هدف های متمایز میباشند.برای تغییر نام پردازش یا سرویس‌هایی که مرتبط با DBMS میباشند، می‌توانید از مستندهای تولیدکنندگان DBMS استفده نمایید.	مستند
181	کنترل امتیاز دسترسی به نقش کاربر برنامه کاربردی DBMS	نقش‌های کاربران برنامه کاربردی میبایست مورد بررسی قرار گرفته و مجوزهای دسترسی آن ها با رعایت حداقل امتیاز دسترسی تنظیم و مستند شود.	مستند
182	رمزنگاری داده‌های پایگاه داده	برای اعمال رمزنگاری پایگاه داده میبایست ابتدا تحلیل حساسیت داده‌ها، حجم اطلاعات و روش‌های رمزنگاری مناسب مورد بررسی قرار گیرد سپس رمزنگاری مناسب اعمال شود	مستند
183	شناسایی داده‌های حساس پایگاه داده	میبایست تحلیل داده‌های پایگاه داده را با همکاری از مسؤلین ذیربط تعیین و مستند نمود و میزان دسترسی آن ها را نیز تعیین کرد	مستند
184	تعیین سیستم میزبانی اختصاصی برای پایگاه داده	هرگونه سرویس‌های اضافی یا برنامه های کاربردی که مرتبط با پایگاه داده نمی‌باشد. در مواردی که جداسازی ممکن نیست میبایست ملاحظات امنیتی آن سرویس رعایت شده و مستند گردد.	مستند
185	جداسازی سیستم میزبان پایگاه داده از سرویس‌های دایرکتوری	سرویس دارکتوری نمیبایست روی سیستم میزبان پایگاه قرار گرفته باشد.	مستند

186	جداسازی پارتیشن و دایرکتوری برنامه کاربردی و DBMS	پارتیشن و دایرکتوری نرم‌افزار پایگاه داده و دیگر داده‌های مرتبط با پایگاه داده را از برنامه های کاربردی دیگر، مجزا نموده و مجوزهای سیستم عامل را برای دسترسی به آن ها، تنظیم نماید.	مستند
187	جداسازی پارتیشن و داریکتوری فایل‌های پایگاه داده	پارتیشن و دایرکتوری فایل‌های اصلی پایگاه داده را اختصاصی نموده و مجوزهای سیستم عامل را برای دسترسی به آن ها، تنظیم نماید.	مستند
188	اختصاص پایگاه داده به یک برنامه کاربردی	با تولیدکنندگان پایگاه داده جلسه ای را ترتیب داده و این موضوع را بررسی نماید. در این مورد یک استثناء نیز وجود دارد و آن برنامه هایی هستند که هر یک جزئی از یک برنامه بزرگتر واحد میباشند.	مستند
189	محافظت در برابر خرابی سخت افزار برای پایگاه داده‌های بحرانی	برای فایل‌های مهم و حساس پایگاه داده از تجهیزات ذخیره سازی با قابلیت تحمل خطا استفاده نمایید .(استفاده از قابلیت RAID و خوشه بندی)	مستند
190	قابلیت اعتماد DBMS برای اجرای فایل‌ها در شروع سرویس	میبایست پیکربندی امنیتی DBMS را برای این مورد فعال نمود، در صورتی که DBMS دارای چنین مکانتیزمی نمی‌باشد میبایست به صورت دستی جامعیت فایل‌های مورد نظر را فراهم نمود.برای این کار می‌توان از نرم‌افزارهای از قبیل Tripwire یا قابلیتهای امضاء دیجیتالی ،سود جست.	مستند
191	تخصیص مجوزها با استفاده از قابلیت نقش	تخصیص نقش‌ها با امتیاز دسترسی بالا به کاربران پایگاه داده،میبایست تحت نظارت مستمر بوده و مستند شوند.	مستند
192	تعیین امتیاز دسترسی حساب کاربری مدیر اجرایی پایگاه داده	نقش‌هایی برای وظایف مدیریتی بسازید و امتیازهای ضروری را به آن نقش تخصیص دهید و سپس حسابهای کاربری که میبایست عضو این نقش شوند را مستند کنید.	مستند
193	بازبینی تغییرهای حساب کاربری مدیران اجرایی	با توجه به کنترل ۹۱، مستند حسابهای کاربری افرادی که به نقش مدیر اجرایی تخصیص داده شده است میبایست به صورت مستمر مورد بازبینی قرار گیرد و هرگونه عدم انطباق میبایست پیگیری شده و نتایج آن مستند شود.	مستند

194	دسترسی به داده‌های مدیر اجرایی پایگاه داده	معمولا در DBMSها اطلاعات پیکربندی در برخی جداول سیستمی نگهداری میشود.و از اعطای مجوز به کاربرانی کهمدیر اجرایی پایگاه داده خودداری نموده و در صورت الزام اعطای کنترل و مستند شود	مستند
195	استفاده از حسابهای کاربری مدیر اجرای پایگاه داده	میبایستی سیاستی برای کارکردهای مجاز و غیر مجاز از حساب کاربری مدیر اجرایی فراهم نمود ، در حقیقت تغییر در اشیاء و داده‌های پایگاه داده، و هر مؤلفه ای از پایگاه داده که به برنامه کاربردی مرتبط میشود.میبایست توسط مالک برنامه کاربردی انجام شود نه مدیر اجرایی، بنابراین مدیر اجرایی نمیبایست اقدام به فعالیت هایی که مربوط به داده‌ها و اشیاء پایگاه داده نماید.	مستند
196	تاریخ انقضای رمز عبور حسابهای کاربری پایگاه داده	رمزهای عبور را در زمانی حداقل ۶۰ روزه تغییر دهید. برخی از DBMSها امکان تنظیم برای تعیین دوره زمانی انقضاء رمز عبور را دارا میباشند، در صورت وجود این پیکربندی را اعمال نمایید.	مستند
197	عدم استفاده مجدد از رمز حسابهای کاربری DBMS	میبایست مراقب بود که حسابهای کاربری DBMS مورد استفاده مجدد تا ۱۰تغییر یا در یک سال قرار نگیرد. معمولا در صورتی که DBMS قابلیت تنظیم را داشته باشد	مستند
198	پیچیدگی رمز عبور حسابهای کاربری DBMS	رمزهای عبوری که استفاده میشوند میبایست حداقل دارای ۸ کاراکتر با ترکیبی از حروف و اعداد و کاراکترهای خاص باشند	مستند
199	رمزهای عبور پیشفرض DBMS	رمزهای عبور پیش فرض پایگاه داده را به مقداری غیر پیش فرض تغییر دهد.	مستند
200	انتقال رمز عبور حساب کاربری DBMS به صورت رمز شده	را برای رمز نمودن اطلاعات رمز عبور حساب های کاربری ورود به DBMS، پیکربندی نمایند.در صورتی که DBMS قابلیت پیکربندی رمزنگاری را دارا نیست، این قابلیت را در سطح سیستم عامل یا شبکه فراهم نمایید.	مستند
201	رمز عبور پایگاه داده در برنامه های کاربردی و فایل‌های اجرایی	میبایست رمزهای عبور موجود در برنامه های کاربردی و فایل‌های اجرایی مبتنی بر سیاست رمزنگاری سازمان به صورت رمز شده نگهداری نمود.	

202	تغییر نام های پیشفرض حسابهای کاربری	میبایست نام حسابهای کاربری پیشفرض تغییر داده شوند (در صورتی که امکان تغییر توسط DBMS فراهم شده باشد)	
203	تنظیم DBMS برای قفل کردن حسابهای کاربری	میبایست در صورتی که DBMS قابلیت قفل نمودن حساب کاربری را دارا است، پیکربندیهای لازم را انجام داد.(در صورت تشخیص اقدام به تلاش های سعی و خطا برای کشف رمز عبور حساب کاربری)	
204	محدود نمودن اتصالهای موازی به DBMS	برخی از DBMSها قابلیت کنترل جریان اتصال به پایگاه داده را دارند، لذا در صورت وجود چنین مکانیزمی در DBMS، میبایست تنظیمات مورد نیاز اعمال و مستند شوند.	

از ایده تا تحقق
فاصله کوتاهی است.

برسانوین رای
راهکارهای نوین نرم افزاری

تهران، میدان ونک، ابتدای گاندی جنوبی، نبش بیستم، پلاک ۱۴۲، واحد ۳۴
www.barsasoft.com
شماره های تماس: ۸۸۲۰۱۵۸۵ - ۰۲۱ ۸۸۸۸۱۱۸۰