**جدول1: تشخیص و تصدیق هویت**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ردیف | ویژگی | شرح ویژگی | محرمانه | خیلی محرمانه | تحت وب | غیر وب | توضیح |
| 1 | تصديق هويت كاربران | برنامه‌ي كاربردي بايد قبل از اعطاي حق دسترسي به منابع[[1]](#footnote-2) و نقش‌ها[[2]](#footnote-3)، هويت كاربران را تصديق كند | \* | \* | \* | \* |  |
| 2 | تصديق هويت ساير برنامه ها | برنامه‌ي كاربردي بايد هويت تمامي برنامه‌ها و موجوديت‌هاي[[3]](#footnote-4) بيروني را كه از طرف كاربر عملي را انجام مي‌دهند، بررسي و با حداقل حقوق دسترسي تصديق كند. | - | \* | \* | \* | با Scope |
| 3 | اخطار تصديق هويت | بعد از احرازهویت کاربر و قبل از اجازه‌ي دسترسي به منابع، برنامه‌ي كاربردي بايد پيام اخطاري را که شامل موارد زير است به اطلاع كاربر برساند: (1) كاربر به سيستم ... سازمان ... وارد شده است. (2) اعلان ردگيري و بازبيني فعاليت‌هاي كاربر (3) مسئوليت كاربر در قبال اطلاعات حساس مورد دستيابي. | \* | \* | \* | \* | در حال حاضر این قابلیت در سامانه ایجاد نشده است. |
| 4 | اعلان ورودهاي قبلي | اطلاعات مشخص شده برحسب شناسه‌ي كاربري شامل تاريخ، زمان، آدرس ‌IP و آخرین ورود موفق اخير كاربر |  | \* | \* | \* | در حال حاضر این قابلیت در سامانه ایجاد نشده است. |
| 5 | استفاده از روش‌هاي تصديق هويت چندعاملی | فرايند تشخيص و تصديق هويت كاربران علاوه‌ بر نام‌ كاربری و كلمه عبور بايد از عامل دوم (نوع عامل دوم به عهده توسعه دهنده سامانه است)نیز استفاده نماید. |  | \* | \* | \* | در حال حاضر این قابلیت در سامانه ایجاد نشده است. |
| برای برنامه‌های سری باید یکی از روش‌ها بیومتریک یا زیرساخت کلید عمومی(به صورت دو طرفه) استفاده شود. |  |  | \* | \* | توکن گذاشتیم توی کوکی |
| 6 | زنجيره‌ي عامل‌هاي تصديق هويت شده | برنامه‌ی کاربردی باید مطمئن شود که زنجیره‌ای از عامل‌های تصدیق هویت شده بین کارگزار برنامه‌ی کاربردی وبین کاربر و برنامه و همچنین بین برنامه و زنجیره تصدیق هویت وجود دارد.در زنجیره عامل های تصدیق هویت بین کارگذار برنامه­ی کاربردی و سیستم های پشت صحنه نظیر سیستم مدیریت پایگاه داده موارد زیر رعایت شود:  1- از کلمه عبور پیش فرض استفاده نشود  2- از کلمه عبور خالی استفاده نشود  3- کلمه عبور دارای پیچیدگی باشد  4- جهت اتصال قانون حداقل سطح دسترسی رعایت شود. | \* | \* | \* | \* | وجود دارد |
| 7 | مسیر امن[[4]](#footnote-5) تصدیق هویت | تمامی اطلاعات تصدیق هویت کاربران باید از طریق یک مسیر امن ارسال شود. | \* | \* | \* | \* | اگر منظور راه اندازی SSL باشد که این مسئله می بایست در بستر استفاده فعال گرددو ربطی به سورس برنامه ندارد |
| 8 | ذخيره‌سازي اطلاعات هويتي كاربران بصورت امن شده | تمامي اطلاعات تصديق هويت كاربران بايد در رسانه‌هاي ذخيره‌سازي به صورت رمزنگاري شده ذخيره گردد. | \* | \* | \* | \* | در این برنامه خروجی اطلاعات کاربران در رسانه های ذخیره ساز ذخیره نمی شود |
| 9 | اعمال قاعده‌ي دفاع در عمق براي تصديق هويت | تصديق هويت برنامه‌ي كاربردي نبايد به عنوان راهكار جايگزين تصديق هويت سيستم‌هاي پشتيبان نظير سیستم‌های مدیریت پایگاه داده‌ها در نظر گرفته شود. | \* | \* | \* | \* | وجود دارد |
| 10 | تعداد دفعات تلاش براي ورود ناموفق | برنامه‌ي كاربردي بايد با ايجاد واسط‌هاي كاربري تعداد دفعات تلاش براي ورود ناموفق را، توسط مديران سيستم تنظيم‌پذير كند.در تنظیمات حد آستانه باید مقدار حد آستانه در یک بازه مشخص تغییر کند به عنوان مثال بین 1 تا 6. این مقدار علاوه بر برنامه باید در سطح بانک نیز اعتبارسنجی شود. (اگر اعتبارسنجی فقط در سطح برنامه باشد از طریق ورود مستقیم مقدار در بانک این مکانیزم دچار مشکل خواهد شد. به عنوان مثال دامنه تغیرات 1 الی 6 در نظر گرفته شده ولی مقدار 100 بطور مستقیم در بانک ثبت شده است.) | \* | \* | \* | \* | در حال حاضر این قابلیت در سامانه ایجاد نشده است. |
| 11 | جلوگیری از تلاش ناموفق جهت ورود | برنامه‌ي كاربردي بايد با ايجاد سازوکارهايي، كاربراني را كه در يك مدت زمان مشخصي تلاش‌هاي ناموفقي براي ورود به برنامه‌ي كاربردي داشته‌اند،  به منظور مقابله با حملات brute force و dictionary attack راهکارهای زیررا مورد استفاده قرار دهد:   * قفل کردن موقت * Slowdown * Captcha | \* | \* | \* | \* | در حال حاضر این قابلیت در سامانه ایجاد نشده است. |
| 12 | تصديق هويت مرتبط با نقش‌ | برنامه‌ي كاربردي ابتدا بايد هويت كاربر را بصورت جداگانه تصديق كند و سپس صحت عضويت يك كاربر را در يك گروه/نقش خاص بررسی کند. | \* | \* | \* | \* | باید بررسی شود |
| 13 | اطلاعات تشخيص هويتي در كد برنامه | اطلاعات تصدیق هویتی نباید در کد برنامه ذخیره شود | \* | \* | \* | \* | وجود ندارد |
| 14 | استفاده از كلمه‌هاي عبور قوي | براي جلوگيري از انجام حملات جستجوی حالات ممکن[[5]](#footnote-6) و حمله لغت نامه اي[[6]](#footnote-7) بايد كلمه‌هاي عبور براساس خط مشي انتخاب كلمه‌هاي عبور انجام شود. تعداد کلمات عبور حداقل 8 کاراکتر باشد و از کاراکترهای خاص، حروف بزرگ و کوچک و اعداد تشکیل شده باشد. همچنین دارای توالی نباشد. | \* | \* | \* | \* |  |
| 15 | خط‌مشي تغيير كلمه‌هاي عبور بوسيله‌ي كاربران | مديريت كلمه‌هاي عبور در برنامه‌هاي كاربردي بايد داراي خواص زير باشد: (1) مديران سيستم بايد قادر باشند به كاربران كلمه‌هاي عبور اختصاص دهند. (2) اجبار كاربران براي تغيير كلمه‌هاي عبوري كه مدير سيستم به آنها اختصاص داده است بعد از اولين ورود. (3) توانا كردن كاربران به قابليت تغيير كلمه‌هاي عبور بصورت بازه زمانی قابل تنظیم برحسب خط‌مشي‌هاي سيستم و يا برحسب تقاضاي كاربر (4) اجبار كاربران به انتخاب كلمه‌هاي عبور جديد با حداقل 4 كاراكتر جديد. (5) قابل تنظيم بودن تعداد كلمات عبور قبلي كه كاربر نمي تواند انتخاب نمايد. (در سطح سری حداکثر 5، سطح خیلی محرمانه حداکثر 3، سطح محرمانه حداکثر 2 و سطح فاقد طبقه بندی حداکثر 1 کلمه عبور قبلی) (6)نمايش گرافيکي قوت و ضعف کلمه عبور | \* | \* | \* | \* | کلمه عبور کاربر هش میشه. از کجا بفهمیم با کلمه عبور قبلی چند کاراکتر مشترک داره؟! |
| 16 | انتخاب كلمه‌ي عبور جديد بعد از گذشتن تاريخ مصرف كلمه‌ي عبور قبلي | برنامه‌ي كاربردي بايد تا زماني كه كاربر كلمه‌ي عبور تاريخ مصرف گذشته‌ي خود را عوض نكند، اجازه‌ي ورود به سيستم ندهد. | \* | \* | \* | \* |  |
| 17 | شناسه‌هاي كاربري يكتا | برنامه‌ي كاربردي نبايد اجازه دهد يك شناسه‌ي كاربر با چند كلمه‌ي عبور انتخاب شده يا با يك شناسه كاري يكسان امكان ورود چندين كاربر وجود داشته باشد. | \* | \* | \* | \* |  |
| 18 | عدم ذخيره‌ي اطلاعات تصديق هويت كاربر بطور نامناسب | برنامه‌ي كاربردي نبايد اطلاعات تصديق هويت كاربر را در کوکی ها، اسکريپت های[[7]](#footnote-8) سمت كارگزار و يا مشتري ويا ديگر فايل‌هائي كه اين اطلاعات بتواند از آن بدست آيد، ذخيره كند. | \* | \* | \* | \* |  |
| 19 | شناسه‌ي كاربري بدون هويت | برنامه‌ي كاربردي نبايد شامل شناسه‌ي كاربري بدون هويت (بدون انتصاب به شخص) براي ورود باشد. | \* | \* | \* | \* |  |
| 20 | تفکیک اطلاعات برنامه کاربردی | اطلاعات برنامه‌ي كاربردي كه براي دسترسي به آنها نيازي به راهكارهاي تصديق هويت نيست بايد شناسائي شده و از اطلاعات خصوصي كه براي دسترسي به آنها نياز به تشخيص و تصديق هويت است تفكيك گردد. | \* | \* | \* | \* |  |
| 21 | چگونگي ذخيره‌ي رشته‌ي اتصال به پايگاه داده | رشته‌ي اتصال به پايگاه داده نبايد در كد و يا فايل‌هاي پيكربندي بصورت شفاف ذخيره گردد. | \* | \* | \* | \* |  |
| 22 | ارائهندادن جزئيات به كاربر در صورت ورود ناموفق[[8]](#footnote-9) | برنامه‌ي كاربردي نبايد مشخص كند كه علت شكست ورود كلمه‌ي عبور نادرست بوده است. | \* | \* | \* | \* |  |
| 23 | ردگيري تلاش‌هاي ورود ناموفق[[9]](#footnote-10) | برنامه‌ي كاربردي بايد تلاش‌هاي ناموفق براي ورود را براي مميزي، ردگيري كند. | \* | \* | \* | \* |  |
| 24 | وجود خصيصه LockOut | اگر کاربر وارد سيستم گرديد و سپس برای يک مدت زمان از سيستم استفاده ننمود، جهت استفاده مجدد بايد احراز هويت شود. | \* | \* | \* | \* |  |
| 25 | احراز هويت مجدد برای صفحات حساس | جهت انجام هرگونه فعاليت حساس در سيستم، احراز هويت مجدد از کاربر صورت گيرد. صفحات حساس قابل تنظيم براي مدير باشد.  براي تمامی سامانه ها، پس از احراز هویت مجدد، شناسه نشست باید تغيير کند. | - | \* | \* | \* |  |

**جدول2: تصدیق حقوق دسترسی**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ردیف | ویژگی | شرح ویژگی | محرمانه | خیلی محرمانه | تحت وب | غیر وب |
| 1 | تصديق حقوق دسترسي كاربران | برنامه‌ي كاربردي بايد قبل از فراخواني فرايندها توسط كاربران و يا دسترسي به منابع سيستم حقوق دسترسي آنها را بررسي كند و مشخص كند آيا اجازه‌ي فراخواني توابع و يا دسترسي به منبع مربوطه توسط كاربر اعمال شده است يا خير؟ | \* | \* | \* | \* |
| 2 | ايجاد رابط‌هاي كاربري براي مديريت حقوق دسترسي | برنامه‌ي كاربردي بايد رابط‌هاي كاربري لازم را براي ايجاد و مديريت ليست کنترل دسترسی ها و ساير اطلاعات حقوق دسترسي فراهم آورده باشد. | \* | \* | \* | \* |
| 3 | قاعده‌ كمترين حق دسترسي | حقوق دسترسي اعطا شده به برنامه‌ي كاربردي در هر زمان بايد كمترين حق ‌دسترسي مورد نياز براي انجام فعاليت‌هاي لازم باشد. | \* | \* | \* | \* |
| 4 | استفاده از حقوق دسترسي نقش‌گرا | حقوق دسترسي در برنامه‌ي كاربردي بايد به‌صورت نقش‌گرا پياده‌سازي شود. | \* | \* | \* | \* |
| 5 | تفكيك وظايف نقش‌ها | كاربر انجام وظايف خود را با نگاشت حداقل يك نقش بتواند انجام دهد. | \* | \* | \* | \* |
| 6 | برچسب گذاري داده‌هاي طبقه بندي شده | برنامه‌ي كاربردي بايد بتواند برچسب‌هاي محرمانگي و جامعيت مناسب را برروي داده اعمال كند و يا كاربران را قادر سازد تا اين برچسب‌ها را برروي داده‌ها و فراداده‌هایی كه ايجاد و يا تغيير مي‌دهند اعمال ‌كنند. اين برچسب‌ها بايد بتوانند توسط راهكار‌هاي كنترل دسترسي شناخته شده و استفاده گردند.  ملاحظه: برچسب گذاري داده ها براساس نياز براي فيلد و رکورد امکان پذير باشد. | \* | \* | \* | \* |
| 7 | برچسب گذاري داده‌هاي خروجي | داده‌هاي توليد شده توسط برنامه‌‌ي كاربردي كه به سيستم‌هاي ديگر انتقال مي‌يابند و يا توسط چاپگر چاپ مي‌شوند و تمامی گزارش­های سامانه، بايد برچسبی حاوی اطلاعات طبقه‌بندي سند، شناسه کاربر، IP سیسم، زمان درخواست را داشته باشد. | \* | \* | \* | \* |
| 8 | ارجاع ندادن به مسير نامعتبر | اگر كاربري يك آدرس URL نامعتبر را درخواست نمايد، برنامه‌ي كاربردي نبايد فهرست دايركتوري را به كاربر نشان دهد | \* | \* | \* |  |
| 9 | عدم پذيرش ورود مستقيم URL جهت دسترسي به منابع غير مجاز | برنامه‌ي كاربردي نبايد به كاربران اجازه دهد با تايپ مستقيم يك URL در خط آدرس مرورگر به صفحاتي كه اجازه‌ي دسترسي ندارند، دسترسي پيدا كنند | \* | \* | \* |  |

**جدول3: مدیریت نشست**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ردیف | ویژگی | شرح ویژگی | محرمانه | خیلی محرمانه | تحت وب | غیر وب |
| 1 | حفاظت از نشست‌ها | در صورتی که نیاز به انتقال اطلاعات نشست روی شبکه باشد لازم است رمزنگاری اطلاعات حساس نشست انجام شود. از مصادیق انتقال نشست عبارت اند از:  کلاستر کردن اطلاعات  جداسازی اطلاعات سرور و پایگاه داده و ایجاد نشست روی پایگاه داده | \* | \* | \* | - |
| 2 | انتخاب شناسه‌ي نشست | شناسه‌ي نشست‌ها بايد بگونه اي باشد كه قابل حدس زدن نباشد . | \* | \* | \* | - |
| 3 | زمان انقضای نشست | برنامه‌ی کاربردی باید راهکار تنظیم زمان غیرفعال بودن کاربر برای منقضی کردن نشست را با حداقل مقدار 15 دقیقه و حداکثر مقدار 30 دقیقه از طریق واسط‌هایی در اختیار مدیر سیستم قرار دهد تنظیم شود.  بعداز منقضي شدن نشست، کاربر مجدد بايد تصديق هويت شود. | \* | \* | \* | - |
| 4 | نشست‌های همزمان | امکان نگاشت شناسه ی نشست یا IP و Agent مربوطه برای جلوگیری از نشست های همزمان در نظر گرفته شود. | \* | \* | \* | - |
| 5 | ذخيره‌ نشدن اطلاعات حساس در کوکی های ماندگار | اطلاعات حساس نظیر کلمه عبور، آدرس URL نباید در کوکی‌های ماندگار ذخیره شود. | \* | \* | \* | - |
| 6 | قابليت Log Out | در صورتی که برنامه کاربردی بنا به دلایل زیر بسته شد نسبت به بسته شدن نشست اقدامات مطرح شده انجام گیرند:  در صورتی که کاربر به صورت صریح از سیستم خارج شود نشست به اتمام برسد.  در صورتی که بنا به عوامل ناخواسته مثل قطع ناگهانی برق سیستم کلاینت دسترسی کاربر از بین برود کاربر بتواند با مکانیزمی امن Login کند. | - | - | \* | - |
| 7 | رمزنگاري محتويات کوکی هاي تصديق هويت | برنامه‌ي كاربردي بايد محتويات کوکی های تصديق هويت را رمز كند | \* | \* | \* | - |
| 8 | انتقال ندادن شناسه‌هاي نشست از طريق Query Stringها | شناسه‌هاي نشست نبايد از طريق Query Stringهاي URL انتقال يابد | \* | \* | \* | - |

**جدول4: بررسی صحت ورودی و خروجی**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ردیف | ویژگی | شرح ویژگی | محرمانه | خیلی محرمانه | تحت وب | غیر وب |
| 1 | نقاط ورودي، خروجي و سطوح امنيتي | تمام ورودي‌ها، خروجي‌ها و ناحيه‌هاي امن برنامه‌ي كاربردي منطبق بر مدل سازی تهدیدات مشخص و اسناد مدلسازی تهدید انجام شده توسط توسعه دهنده براي اعمال راه‌كارهاي كنترلي مشخص بايد ارائه شود. | \* | \* | \* | \* |
| 2 | اعتبار سنجي داده هاو پارامترهاي ورودي | داده‌هاي ورودي بايد براساس نوع، مقدار، شكل، اندازه و محدوده و نيز پاكسازي ورودي براساس ليست كاركترها و الگوهاي بد نيتبررسي و تطبيق داده شوند.  بررسي صحت داده هاي ورودي در سطح برنامه کاربردي بايد به صورت متمرکز و با استفاده از توابع و متدهاي طراحي شده در اين راستا انجام شود. | \* | \* | \* | \* |
| 3 | عدم اعتماد به بررسي صحت ورودي در سمت كاربر | معماري برنامه‌ي كاربردي بايد به گونه‌اي باشد كه تنها به بررسي صحت ورودي در سمت كاربر اكتفا ننموده و صحت ورودي در سمت سرويس دهنده نيز بررسي شود. | \* | \* | \* | \* |
| 4 | کد گذاري و تطبيق داده هاي خروجي | داده هاي خروجي برنامه‌هاي كاربردي كه از طرف كاربر فراهم آورده شده باشند بايد پاكسازي شده و خروجي براساس ليست كاركترها و الگوهاي بد نيت[[10]](#footnote-11)بررسي و تطبيق داده شده تا امكان سوء استفاده نفوذگران از اين ناحيه جلوگيري گردد. | \* | \* | \* | \* |

**جدول5: محرمانگی**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ردیف | ویژگی | شرح ویژگی | محرمانه | خیلی محرمانه | تحت وب | غیر وب |
| 1 | رمزنگاري داده‌هاي داراي طبقه بندي | برنامه‌ي كاربردي بايد داده‌هاي دارای طبقه بندي را هنگام Import/Export به صورت رمزنگاري شده در رسانه‌، ذخيره‌سازي كند. | \* | \* | \* | \* |
| 2 | حفاظت از كليدهاي رمزنگاري( استفاده صحيح از ماژول رمزنگاري) | راه‌كارهاي رمزنگاري بايد به گونه‌اي باشد تا مانع از دسترسي غير مجاز به كليد‌هاي رمزنگاري شود. | \* | \* | \* | \* |
| 3 | [[11]](#footnote-12)پاك‌سازي محيط اجرا[[12]](#footnote-13) | برنامه‌ی کاربردی باید قبل از خاتمه، تمامی فایل‌های موقت،حافظه‌هاي نهان، داده‌ها و ديگر اشيائي را كه ايجاد كرده است از محيط اجرا پاك كند. | \* | \* | \* | \* |
| 4 | استفاده از الگوريتم‌هاي رمزنگاري مورد تاييد س.ک.ن.م | برنامه‌ي كاربردي بايد براي رمزنگاري داده‌ها از الگوريتم‌هاي رمز‌نگاري مصوب استفاده كند. | \* | \* | \* | \* |
| 5 | استفاده از قابليت‌هاي مرورگر | از Plug-inها،‌ كوكي ها و ديگر قابليتهای مرورگر تنها در صورتي بايد استفاده شود كه راه‌كار جايگزيني براي پياده‌سازي عملکرد مورد نظر وجود نداشته باشد. | \* | \* | \* |  |
| 6 | انتقال داده‌هاي حساس توسط کوکی هاي رمزنگاري شده | براي انتقال داده‌هاي حساس(نظير نام کاربري و کلمه عبور) از کوکی های ناپايدار كه رمزنگاري شده‌اند بايد استفاده كرد. | \* | \* | \* |  |
| 7 | ذخيره‌نشدن داده‌هاي داراي طبقه بندي و حساس در سمت كاربر | هيچ داده‌ي داراي طبقه بندي و حساسي نبايد در سمت واسط‌هاي سمت كاربر نگهداري شود. | \* | \* | \* |  |

**جدول6: دسترس­پذیری**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ردیف | ویژگی | شرح ویژگی | محرمانه | خیلی محرمانه | تحت وب | غیر وب |
| 1 | صحت برنامه‌ی کاربردی برای دسترس‌پذیری داده‌ها | برنامه‌ی کاربردی با فراهم آوردن امکانات پشتیبان‏گیری بایستی از دسترس خارج شدن داده‎‏ها جلوگیری به عمل آورند. | \* | \* | \* | \* |
| 2 | سرویس‌دهی دایمی برنامه کاربردی | برنامه‌ی کاربردی نباید شامل خطاها و آسیب‌پذیری‌هایی باشد که با سوء استفاده از آن برنامه‌ی کاربردی از دسترس خارج شود. | \* | \* | \* | \* |
| 3 | مدیریت آستانه‌ی بار[[13]](#footnote-14) | برنامه‌ی کاربردی با مدیریت آستانه‌ی بار باید ویژگی در دسترس‌پذیری را فراهم نماید. | \* | \* | \* | \* |

**جدول7: مدیرت خطاء و استثنائات**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ردیف | ویژگی | شرح ویژگی | محرمانه | خیلی محرمانه | تحت وب | غیر وب |
| 1 | شكست برنامه كاربردي | در صورت بوجود آمدن خطا در برنامه‌ي كاربردي و با شكست مواجه شدن آن، خطا و يا نقص مربوطه نبايد باعث شود برنامه‌ي كاربردي به يك وضعيت ناامن برود. | \* | \* | \* | \* |
| 2 | ساختار مديريت خطاها واستثنائات | برنامه‌ي كاربردي بايد خطاها و استثنائات را با ساختار‌هاي تعريف شده در زبان برنامه‌سازي به شكل مناسب و متمرکز مديريت كند. | \* | \* | \* | \* |
| 3 | محتوای پیام هاي خطا | برنامه‌ کاربردی باید به گونه‌ای باشد که محتوای خطاهای برگردانده شده به کاربر حاوی اطلاعات حساس نباشد. | \* | \* | \* | \* |
| 4 | رويداد نگاري از خطاها و استثنائات | ساختارهاي مديريت خطاها و استثنائات بايد تمامي خطاها واستثنائات بوجود آمده را ثبت كند. | \* | \* | \* | \* |
| 5 | سطوح خطاها واستثنائات | متناسب با سطح طبقه بندي، برنامه کاربردي بايد هر شش سطح خطا و استثنائات را ثبت نمايد.   1. info 2. warn 3. error 4. fatal 5. debug 6. trace   در سطح سری هر شش مورد، در سطح خیلی محرمانه موارد 1و2و3و در سطح محرمانه موارد 1و2 الزامی است. | \* | \* | \* | \* |

**جدول8: انکارناپذیری**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ردیف | ویژگی | شرح ویژگی | محرمانه | خیلی محرمانه | تحت وب | غیر وب |
| 1 | استفاده از امضاء ديجيتال | به منظور اثبات اصالت و هويت، برنامه‌ي كاربردي بايد قادر باشد تا داده‌هاي مربوطه را به ‌صورت ديجيتالي امضاء كنند. | \_ | \* | \* | \* |
| 2 | سازگاري امضاء ديجيتال | سامانه بایستیPKEnable باشد، به طوری که امضاء دیجیتال استفاده شده در برنامه كاربردي بايد با ساختار CA نیروهای مسلح سازگار باشد.[[14]](#footnote-15) | \_ | \* | \* | \* |
| 3 | برچسب گذاري داده هاي خروجي | به ردیف 7 بخش تصدیق حقوق دسترسی مراجعه شود. | \* | \* | \* | \* |

**جدول9:طراحی، معماری و کدنویسی امن**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ردیف | ویژگی | شرح ویژگی | محرمانه | خیلی محرمانه | تحت وب | غیر وب |
| 1 | مدل‌سازی تهدیدات | برای استخراج تهدیدات متصور هر برنامه کاربردی ابتدا باید تهدیدات مدل سازی شده و سپس ماتریس تهدیدات ارائه گردد تا بتوان نیازمندی‌های امنیتی آن برنامه کاربردی را متناسب با تهدیدات و سطح طبقه بندی احصاء نمود. | \* | \* | \* | \* |
| 2 | طراحی و معماری امن | با توجه به تهدیدات استخراج شده در بند 1 ساز و کارهای امنیتی متناسب باید طراحی و معماری شود. | \* | \* | \* | \* |
| 3 | کد نویسی امن[[15]](#footnote-16) | متناسب با زبان برنامه‌سازی قواعد[[16]](#footnote-17) کدنویسی امن باید رعایت گردد. | \* | \* | \* | \* |
| برنامه کاربردي بايد با استفاده از راه کارهاي مناسب از آسيب پذيري هاي رايج نظير XSS، CSRF، Injection ، Overflow و ...[[17]](#footnote-18) جلوگيري کند. |
| برای انتقال داده‌ها حتی اگر از پروتکل SSl هم استفاده شده باشد باید به جای متد GET از متد POST استفاده شود.  برنامه‌ی کاربردی نباید هیچ گونه داده حساس را در اسکریپت‌ها ذخیره کند. |
| داده هاي داراي طبقه بندي و حساس نظير کلمات عبور و کليدهاي رمزنگاري نبايد در کد برنامه ذخيره گردد. |
| کد اجرايي برنامه کاربردي از فايل هايي که ايجاد و استفاده مي کند بايد مجزا باشد. |
| برنامه‌ي كاربردي نبايد داده هاي حساس نظير کلمات عبور را در نوع هاي تغيير ناپذير نظير ثابت هاي زبان جاوا و يا نوع هائي که توسط سرويس هاي جمع آوري زباله[[18]](#footnote-19) از حافظه پاک مي شوند، قرار دهد. |
|  | مقدار دهي اوليه‌ي متغيرها | برنامه‌كاربردي بايد تمامي متغيرها را مقداردهي اوليه نمايد | \* | \* | \* | \* |
| 4 | استفاده نکردن از سرويس هايي با مخاطرات امنيتي بالا | برنامه‌ي كاربردي نبايد از سرويس‌ها و تكنولوژي‌هایي با مخاطرات امنيتي بالا نظير Telnet استفاده كند. | \* | \* | \* | \* |
| 5 | حذف توابع ومتدهاي اضافي | حذف توابع ويا متدهاي استفاده نشده برنامه کاربردي که به طور صريح فراخواني نشده باشند. | \* | \* | \* | \* |
| 6 | [[19]](#footnote-20)گواهينامه‌‌ي امنيتي مولفه‌ها و سرويسهاي جانبي[[20]](#footnote-21) | در صورتي كه برنامه‌ي كاربردي از مولفه‌ها و سرويسهاي جانبي ساير برنامه‌هاي كاربردي و يا متن‌باز استفاده مي‌كند، بايد تمامي آنها ارزيابي امنيتي شده باشند. | \* | \* | \* | \* |
| 7 | پيش فرضهاي امنيتي | برنامه‌ي كاربردي نبايد بر اساس هيچ پيش فرضي در مورد امنيت ساير اجزاء، طراحي شده و حتما بصورت مستقل ملاحظات امنيتي را پياده سازي کند. | \* | \* | \* | \* |
| 8 | مبهم سازی کد | برای محافظت از کد برنامه در مقابله با مهندسی معکوس، مبهم سازی کد انجام شود.  برای سامانه‌های سری رمزنگاری انجام شود. | \* | \* |  | \* |

**جدول 10 - رویدادنگاری و ممیزی**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ردیف | ویژگی | شرح ویژگی | محرمانه | خیلی محرمانه | تحت وب | غیر وب |
| 1 | رويدادنگاري وقايع امنيتي | برنامه‌ي كاربردي بايد تمام رويدادهاي امنيتي تعریف شده را به صورت امن و به صورت فقط خواندنی (دور از دسترس کاربران به جز مدیر بانک اطلاعاتي) ذخيره نماید و یا به یک سیستم رویدادنگاری متمرکز برای بازبینی انتقال دهد. مناسبتر است قابلیت مشاهد برخط این رکوردهای ذخیره شده وجودا داشته باشد. | \* | \* | \* | \* |
| 2 | محتويات ركوردهاي رويدادنگاري | ركوردهاي رويدادنگاري باید شامل موارد زير باشد:  شناسه‌ي كاربر و يا فرآيند بوجود آورنده رويداد  شكست يا موفقيت رويداد  تاريخ و زمان رويداد  انواع رویدادها نظیر:  شکست و یا موفقیت ورود  قفل شدن شناسه‌ي كاربر، ترمينال و يا درگاه دسترسي و علت آن  فعاليت‌هائي با قصد دورزدن ويا از بين بردن راهكارهاي محافظتامنيتي  فعالیت‌هایی که به سطح دسترسی خاص نیاز دارند  زمان شروع و خاتمه‌ی استفاده از برنامه کاربردی  فعالیت‌هایی که مربوط به تغییر کنترل دسترسی داده‌ها می‌باشد | \* | \* | \* | \* |
| 3 | گزارش گيري پويااز رويدادها | برنامه کاربردي بايد بتواند گزارش‌هاي موردنياز را به مدير سامانه ارائه دهد | - | \* | \* | \* |

**جدول11: موارد نصب**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ردیف | ویژگی | شرح ویژگی | محرمانه | خیلی محرمانه | تحت وب | غیر وب |
| 1 | مستندات نصب و راه اندازی امن | راهنماي کامل نصب و پيکربندي بويژه پيكربندي امنيتي و نيز پيكربندي امنيتي نرم افزارهای استفاده شده ديگر مانند سيستم عامل، پايگاه داده‌ها، سرويس دهنده وب وجود داشته باشد. | \* | \* | \* | \* |
| 2 | استقرار سامانه با رعايت قاعده‌ي دفاع در عمق | دراستقرارسامانه بايد تمام موارد بند1 رعايت گردد. | \* | \* | \* | \* |
| 3 | برنامه نصب | تنظيمات و پيکربندي­های امنيتی لازم توسط نرم افزاری که به منظور نصب تهيه شده است انجام گردد. | \* | \* | - | \* |
| 4 | حسابها و گذر واژه های پيش فرض | حساب‌ها و گذرواژه‌هاي پيش‌فرض برنامه کاربردی بايد حذف و يا تغيير يابند. | \* | \* | \* | \* |
| 5 | اطلاعات اضافي پايگاه داده | تمام اطلاعات غير ضروری در پايگاه داده هنگام نصب بايد حذف شود. | \* | \* | \* | \* |
| 6 | شرایط محیط استقرار | پیکربندی امنیتی شبکه باید متناسب با سطح طبقه‌بندی برنامه کاربردی باشد. | \* | \* | \* | \* |
| 7 | صحت سنجي سامانه هنگام نصب (يکپارچگي[[21]](#footnote-22)) | قبل از نصب سامانه صحت برنامه کاربردي تاييد شده اعتبارسنجي شود. | \* | \* | \* | \* |
| 8 | رويداد نگاري درلايه هاي مختلف | رويدادنگاري علاوه بربرنامه کاربردي بايد درساير لايه‌ها نظير کارگزار وب و پايگاه داده انجام گيرد. | \* | \* | \* | \* |
| 9 | معماري بانک اطلاعاتي | معماري هاي بانک اطلاعاتي بايد به صورت چند لايه (حداقل سه لایه) توليد گردند به نحوي که نرم افزار بانک اطلاعاتي و نرم افزار کاربردي روي سرورهاي جداگانه اي در نظر گرفته شود. | \* | \* | \* | \* |

1. Resource [↑](#footnote-ref-2)
2. Role [↑](#footnote-ref-3)
3. Entity [↑](#footnote-ref-4)
4. منظور مسیر بین برنامه کاربردی و پایگاه داده است. [↑](#footnote-ref-5)
5. brute-force [↑](#footnote-ref-6)
6. Dictionary Attack [↑](#footnote-ref-7)
7. Script [↑](#footnote-ref-8)
8. در بند مدیریت خطا و استثنائات پیاده‌سازی شود. [↑](#footnote-ref-9)
9. در بند ممیزی و رویدادنگاری پیاده‌سازی شود. [↑](#footnote-ref-10)
10. Malicious pattern [↑](#footnote-ref-11)
11. [↑](#footnote-ref-12)
12. Run-time Enviroment [↑](#footnote-ref-13)
13. load balancing [↑](#footnote-ref-14)
14. پس از پیاده‌سازیCAدر سازمان‌های نیروهای مسلح [↑](#footnote-ref-15)
15. برای کدنویسی امن از آخرین استانداردهای موجود در هر زبان برنامه‌نویسی باید استفاده نمود. [↑](#footnote-ref-16)
16. rule [↑](#footnote-ref-17)
17. آسیب‌پذیری‌های رایج مطابق استانداردهای owasp – Top 10 و 25 CWE-Mitre [↑](#footnote-ref-18)
18. Garbage Collected Service [↑](#footnote-ref-19)
19. [↑](#footnote-ref-20)
20. Third-party component [↑](#footnote-ref-21)
21. [↑](#footnote-ref-22)