به نام خدا

**سند توصیف مشخصات کارکردها**

شهرسازی وب نسخه 1402.03.10.01

تحلیلگران آمارد

خردادماه 1402

نسخه 1.7

**فهرست**

[1 مقدمه..... 3](#_Toc137541014)

[2 شرح کارکردهای امنیتی محصول 3](#_Toc137541015)

[3 نگاشت بین واسطهای کاربری کارکردهای امنیتی محصول و الزامات کارکرد امنیتی 21](#_Toc137541016)

# مقدمه

این سند مشخصات کارکردهای محصول را توضیح می­دهد که شامل اطلاعات ضروری برای پاسخ­گویی به نیازمندی­های مولفه­ ADV\_FSP در استاندارد ارزیابی امنیتی معیار مشترک برای سطح EAL1 بکار می­رود.

این سند، توصیف سطح بالایی از واسط­های کاربری محصول ارائه می­دهد، محدوده این سند تنها به واسط­های «کارکردهای امنیتی هدف ارزیابی» با موجودیت­های خارجی می­باشد، همانند واسط بین هدف ارزیابی و پایگاه داده.

# شرح کارکردهای امنیتی محصول

در هر جدول قسمتی به اسم " نتایج و پیام‌های خطا" وجود دارد که خروجی هر واسط را تشریح می‌کند. معنای چند عبارت که در این بخش استفاده شده است، به‌صورت زیر است:

* پیام خطا: زمانی استفاده شده است که خروجی سامانه با خطایی همراه بوده باشد.
* نتیجه ناموفق: زمانی استفاده شده است که خروجی واسط با خطا مواجه نشده است و بااینحال نتیجه‌ی موفقی نیز بهمراه نداشته است.
* نتیجه موفق: زمانی استفاده شده است که سامانه با موفقیت به نتیجه رسیده‌است.
* نتیجه: زمانی استفاده شده است که فارغ از موفق یا ناموفق بودن نتیجه ویا هنگام بروز خطا، اجرا می‌شود.

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **1** | **تولید داده ممیزی** |
| **توصیف واسط** | هدف(ها) | 1. ثبت رویدادهای ممیزی 2. ثبت اطلاعات امنیتی کافی برای هر رکورد رویداد ممیزی | |
| متد(ها) | 1. ثبت کنش‌های هر کاربر قبل و/یا هنگام و/یا بعد از هر عمل در سامانه | |
| فعالیت(ها) | 1. تمامی داده‌های موردنیاز هویتی و آماری و امنیتی برای ثبت یک رویداد ممیزی جمع‌آوری شده و در پایگاه داده ذخیره می‌گردند. | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: شناسه‌ی یکتایی که هر کاربر داراست. 2. نام واقعی کاربر: نام و شهرت کاربر که در سامانه ثبت است. 3. نام کاربری: یک عبارت حاوی نویسه و ارقام که فرد با آن وارد سامانه می‌شود. 4. نوع عمل: نوع کلی عمل مانند مشاهده، ویرایش، ایجاد، بارگیری و ... 5. نام بخش: بخشی از سامانه که کاربر عمل خود را صورت‌داده مانند بخش مدیریت کاربران. 6. شرح عملیات: شرح دقیق عملی که رخ‌داده با جزئی‌ترین اطلاعات. 7. تاریخ و ساعت: تاریخ و زمان عملی که کاربر انجام‌داده‌است. 8. نشانی IP: شناسه‌ی IP دستگاه کاربر که درون شبکه‌ قراردارد. | |
| نتایج و پیام‌های خطا | 1. نتیجه ناموفق: عدم‌توانایی ثبت رویداد بدلیل خالی‌نبودن فضای ذخیره‌سازی اطلاعات ممیزی در پایگاه داده 2. نتیجه موفق: ثبت موفق رویداد | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **2** | **بازبینی داده‌های ممیزی** |
| **توصیف واسط** | هدف(ها) | 1. امکان خواندن اطلاعاتِ ممیزی ِقابلِ تفسیر تحت شرایط خاص و مهارشده | |
| متد(ها) | 1. فراهم‌کردن امکان خواندن اطلاعات ممیزی برای کاربران مجاز 2. جلوگیری از دسترسی کاربران غیرمجاز به اطلاعات ممیزی 3. فراهم‌آوری امکان مرتب‌سازی و پالایش (انتخاب یا filter) اطلاعات ممیزی | |
| فعالیت(ها) | 1. تنها کاربران دارای دسترسی‌های زیر قادر به مشاهده (خواندن) همه‌ی انواع اطلاعات ممیزی هستند:    * دسترسی "رویدادهای ممیزی > لاگین‌های کاربران"    * دسترسی "امکانات > گزارش کابران سیستم"    * دسترسی "امکانات > گزارش خطاهای سیستم"    * دسترسی "امکانات > گزارش پیام‌های IIS" 2. هر کاربری که دسترسی‌های بالا را نداشته باشد، امکان خواندن، مرتب‌سازی و پالایش داده‌ها را ندارد. 3. اطلاعات ممیزی براساس موارد زیر قابل مرتب‌سازی و پالایش هستند:    * نام کاربری    * تاریخ    * IP    * شرح عملیات | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: برای تشخیص اینکه آیا این کاربر اجازه دسترسی به بخش مشاهده اطلاعات ممیزی دارد یا خیر. | |
| نتایج و پیام‌های خطا | 1. پیام خطا: عدم امکان خواندن اطلاعات ممیزی برای کاربران غیرمجاز | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **3** | **انتخاب داده‌های ممیزی** |
| **توصیف واسط** | هدف(ها) | 1. امکان انتخاب اینکه کدام رویداد ممیزی ذخیره‌شود. | |
| متد(ها) | 1. امکان انتخاب اینکه کدام رویداد ممیزی ذخیره‌شود. | |
| فعالیت(ها) | 1. کاربر مجاز (دارای دسترسی "تعاریف > فیلتر رویدادهای ممیزی" می‌تواند بین مواردی که در مسیر "تعاریف > فیلتر رویدادهای ممیزی" وجود دارد، انتخاب نماید که کدام رویداد ممیزی ثبت شود. | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: برای بررسی دسترسی‌های کاربر 2. الزام ثبت رویدادهای فعالیت کاربران: درصورت انتخاب شدن رویدادهای فعالیت کاربران ثبت می‌شوند. 3. الزام ثبت رویدادهای ورود/خروج کاربران: درصورت انتخاب شدن رویدادهای ورود/خروج کاربران ثبت می‌شوند. 4. الزام ثبت رویدادهای پیام‌های سیستم: درصورت انتخاب شدن رویدادهای پیام‌های سیستم ثبت می‌شوند. | |
| نتایج و پیام‌های خطا | 1. پیام خطا: نمایش خطا درصورت عدم دسترسی کاربر به بخش مذکور 2. نتیجه موفق: ویرایش سیاست‌های فیلتر رویدادهای ممیزی | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **4** | **ذخیره رویدادهای ممیزی** |
| **توصیف واسط** | هدف(ها) | 1. حفاظت از اطلاعات ممیزی موجود درون پایگاه داده | |
| متد(ها) | 1. جلوگیری از حذف غیرمجاز اطلاعات ممیزی 2. تشخیص و جلوگیری از ویرایش غیرمجاز اطلاعات ممیزی | |
| فعالیت(ها) | 1. کاربران غیرمجاز قادر به حذف غیرمجاز اطلاعات نیستند. 2. هر رکورد ممیزی دارای یک فیلد درهم‌شده (Hash) است. هر تغییری در رکورد که ازطریق سامانه صورت نگیرد، باعث عدم تطابق مقدار درهم‌شده می‌شود. نتیجه اعتبارسنجی براساس Hash به کاربر درقالب نمایش واژه‌ی "معتبر" و "نامعتبر" صورت می‌گیرد. | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: برای تشخیص اینکه آیا این کاربر اجازه دسترسی به بخش مشاهده اطلاعات ممیزی دارد یا خیر. 2. رکورد ممیزی: بمنظور بازدرهم‌سازی رکورد که درنهایت این مقدار درهم جدید با مقدار درهم موجود در پایگاه‌داده سنجیده‌شده و نتیجه این سنجش به کاربر نمایش‌داده‌می‌شود. | |
| نتایج و پیام‌های خطا | 1. نتیجه موفق: سنجش اعتبارسنجی به کاربر نمایش‌داده می‌شود. 2. نتیجه ناموفق: عدم‌توانایی ثبت رویداد بدلیل خالی‌نبودن فضای ذخیره‌سازی اطلاعات ممیزی در پایگاه داده 3. پیام خطا: درصورت عدم دسترسی کاربر به بخش مذکور | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **5** | **ازبین‌رفتن داده‌های ممیزی** |
| **توصیف واسط** | هدف(ها) | 1. جلوگیری از حالتی که سامانه دیگر نتواند داده‌ی ممیزی ذخیره‌سازد. | |
| متد(ها) | 1. سامانه درصورت تجاوز دنباله‌ی ممیزی، کاربران مربوطه را مطلع سازد. 2. سامانه درصورت پرشدن دنباله ممیزی، باید اقدامی انجام دهد تا فضای خالی برای داده‌های ممیزی جدید فراهم شود. | |
| فعالیت(ها) | 1. ازطریق پیامک به کاربر(ان) مربوطه اطلاع‌رسانی می‌شود. 2. درصورت پرشدن یکی از جداول مربوط به داده‌های ممیزی، پس از اطلاع‌دادن ازطریق پیامک، ده درصد قدیمی‌ترین داده‌ها حذف می‌شود. | |
| نام و تشریح پارامتر(ها) | 1. شماره تماس کاربر: شماره تماسی که برای فرستادن پیامک اطلاع‌رسانی استفاده می‌شود. 2. نام جدول ممیزی پُرشده: جدول ممیزی پرشده که قصد خالی‌سازی فضای آنرا داریم. | |
| نتایج و پیام‌های خطا | 1. نتیجه ناموفق: درصورت ثبت‌نبودن شماره تماس کاربر مربوطه، یک رکورد ممیزی با همین مضمون ثبت می‌گردد. 2. نتیجه ناموفق: درصورت عدم توانایی فرستادن اعلان پیامکی، یک رکورد ممیزی با همین مضمون ثبت می‌گردد. 3. نتیجه موفق: درصورت موفق‌آمیز بودن، فضای خالی برای ثبت رکوردهای ممیزی جدید فراهم می‌گردد. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **6** | **عملیات رمزنگاری** |
| **توصیف واسط** | هدف(ها) | 1. استفاده از الگوریتم‌های مشخص و استاندارد بمنظور رمزنگاری | |
| متد(ها) | 1. استفاده از الگوریتم رمزنگاری برای صحت‌سنجی داده‌های احراز هویت، داده‌های ممیزی و داده‌های رکورد 2. استفاده از الگوریتم رمزنگاری برای تولید داده‌های درهم‌شده (Hash) | |
| فعالیت(ها) | 1. از الگوریتم SHA256 برای درهم‌سازی فیلد رمزعبور کاربر و همچنین برای درهم‌سازی فیلد Hash موجود در هر رکورد ممیزی استفاده می‌شود. برای امنیت‌افزایی اقدام به استفاده از اصطلاحا افزودن نمک و فلفل (Salting & Peppering) درون الگوریتم رمزنگاری می‌شود.    * نمک: به یک رشته‌ی تصادفی گفته می‌شود که به ازای هر رکورد ممیزی، یکتا است. و هیچ دو داده‌ی ممیزی را نمی‌توان یافت که نمک یکسانی داشته‌باشند. این مقدار به انتهای متن ساده (Plain) افزوده می‌شود. این مقدار در کنار مقدار درهم‌سازی‌شده درون پایگاه داده ذخیره می‌شود.    * فلفل: به یک رشته تصادفی گفته می‌شود که درون کد برنامه جایگذاری شده و همواره یک مقدار ثابت است. درنتیجه اگر فرد غیرمجاز مستقیما به اطلاعات پایگاه داده دسترسی یافت، باز هم نمی‌تواند الگوریتم درهم‌سازی را جعل‌کند. زیرا به مقدار فلفل دسترسی ندارد. این مقدار به ابتدای متن ساده (Plain) افزوده می‌شود.    * متن ساده: به داده‌های موجود در هر رکورد ممیزی یا رمزعبور کاربر گفته می‌شود که قرار است براساس آن مقدار درهم‌شده تولیدگردد.   درنهایت ساختار داده‌ قبل‌از درهم‌شدن به شکل زیر خواهد بود:   |  |  |  | | --- | --- | --- | | نمک | متن ساده | فلفل |   در بالا گفته‌شد که مقدار نمک در کنار مقدار درهم‌شده درون پایگاه داده قرار می‌گیرد. پس از ساخت رشته درهم‌سازی‌شده، مقدار درهم‌شده (H) را به 4 بخش تقسیم می‌کنیم. همین کار را برای مقدار نمکِ استفاده‌شده (S) انجام می‌دهیم. به‌صورت زیر با هم ترکیب کرده و درون فیلد Hash مربوط‌به هر رکورد ممیزی قرار می‌دهیم:   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | H2 | H1 | S2 | S0 | H3 | S1 | H0 | S3 |   فرد غیرمجاز درصورت ندانستن اینکه مقدار نمک با مقدار درهم‌شده به این شکل با هم ترکیب شده‌اند، قادر به رمزگشایی نخواهد بود. | |
| نام و تشریح پارامتر(ها) | 1. نوع الگوریتم: نوع الگوریتم درهم‌ساز را مشخص می‌کند. 2. متن ساده: حاوی یک رکورد ممیزی ویا یک رمز عبور کاربر است که قرار است روی آن درهم‌سازی صورت گیرد. | |
| نتایج و پیام‌های خطا | 1. نتیجه موفق: یک مقدار درهم‌شده خواهد بود. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **7** | **خط‌مشی و عملیات مهار دسترسی** |
| **توصیف واسط** | هدف(ها) | 1. تعیین و مهار دسترسی‌های مجاز و غیرمجاز موجودیت‌های فعال به موجودیت‌های فعال دیگر (دسترسی مجازی) ویا موجودیت‌های غیرفعال | |
| متد(ها) | 1. اختصاص خط‌مشی‌های مهار دسترسی برروی موجودیت‌های فعال و غیرفعال 2. وجود دسترسی کاربران غیرمجاز (عادی) به تمامی بخش‌های عمومی سامانه 3. وجود دسترسی کاربران مجاز سطح مدیر به بخش‌های مدیریتی سامانه 4. قطع‌دسترسی کاربر درصورت تجاوز تعداد نشست‌های فعال او از حد آستانه | |
| فعالیت(ها) | 1. کاربر سطح مدیر می‌تواند به کاربران دیگر اجازه دسترسی به بخش‌های مختلف سامانه و همچنین اجازه اعمال کنش‌هایی مانند ایجاد، ویرایش، حدف، بارگیری، بارگذاری، مشاهده و ... دهد ویا سلب‌کند. 2. کاربران سطح پایین (یا سطح عادی) قادر به دسترسی به تمام بخش‌های عمومی سامانه هستند. همینطور از دسترسی این افراد به بخش‌های دارای جواز لازم، درصورت نداشتن دسترسی ممانعت به عمل می‌آید. 3. کاربران سطح بالا می‌تواند تمامی تنظیمات مدیریتی سامانه را مدیریت کنند. 4. درصورت وجود محدودیت برای تعداد نشست‌های هم‌زمان یک کاربر، اگر کاربری از حد آستانه‌ی مذکور تجاوز کرده و با تعداد غیرمجازی دستگاه به حساب کاربری خود وارد شود، از ورود جدید جلوگیری می‌کند. همچنین به اولین فردی که وارد این حساب شده‌باشد، ازطریق پیامک اطلاع‌رسانی می‌شود که فردی با شرایط مذکور بهمراه زمان و شناسه‌ی IP تلاش برای ورود به حساب داشته‌است. | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: برای شناسایی اینکه آیا کاربر به بخش درخواستی خود دسترسی دارد یا خیر استفاده می‌شود. 2. شماره تماس کاربر: درصورتی رخداد مورد (د) در بخش متد‌ها، از شماره تماس کاربر برای فرستادن اعلان پیامکی استفاده‌ می‌شود. | |
| نتایج و پیام‌های خطا | 1. پیام خطا: درصورتی که کاربر به بخش درخواستی خود دسترسی نداشته باشد. 2. نتیجه موفق: درصورتی که کاربر بخش مذکور دسترسی داشته باشد، عملیات صورت می‌گیرد. 3. نتیجه: در هر دو حالت قبل یک رویداد ممیزی مرتبط ثبت می‌شود. 4. نتیجه: درصورتی تجاوز از حد آستانه تعداد نشست‌های هم‌زمان، پیامکی ارسال می‌شود. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **8** | **حفاظت کامل از اطلاعات باقیمانده در منابع** |
| **توصیف واسط** | هدف(ها) | 1. حدف تمامی اطلاعات باقیمانده حاصل‌از دسترسی به موجودیت غیرفعال ویا نگهداری ارتباط امن با آن موجودیت | |
| متد(ها) | 1. حدف تمامی اطلاعات باقیمانده حاصل‌از دسترسی به موجودیت غیرفعال ویا نگهداری ارتباط امن با آن موجودیت | |
| فعالیت(ها) | 1. سامانه بعد از اتمام ارتباط خود با هر موجودیت غیرفعالی، هرگونه اطلاعات باقیمانده را معدوم می‌نماید. | |
| نام و تشریح پارامتر(ها) | 1. موجودیت غیرفعال | |
| نتایج و پیام‌های خطا | 1. نتیجه: حذف اطلاعات باقیمانده | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **9** | **ورود داده کاربری به محصول با مشخصه امنیتی** |
| **توصیف واسط** | هدف(ها) | 1. مهار دسترسی کاربر بابت بارگذاری داده | |
| متد(ها) | 1. مهار دسترسی کاربر بابت بارگذاری داده | |
| فعالیت(ها) | 1. کاربر می‌تواند به مسیر زیر رفته و پس‌از انتخاب شماره پرونده اقدام به بارگذاری داده کند: منو > آرشیو > آرشیو الکترونیک > آپلود درنهایت رویکرد ممیزی شامل شناسه و نام کاربر و دیگر مشخصه‌های امنیتی و حائز اهمیت ثبت می‌گردد. بایست خاطرنشان کرد که سامانه فعلی از سازوکار امضای دیجیتال پشتیبانی نمی‌کند. | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: بابت شناسایی او و اینکه چه دسترسی‌هایی دارد. 2. داده بارگذاری‌شده: هر آنچه که کاربر قصد بارگذاری آن را دارد. | |
| نتایج و پیام‌های خطا | 1. نتیجه موفق: درصورت موفقت‌آمیز بودن، داده کاربر در سرور ذخیره می‌شود. 2. پیام خطا: درصورت بروز مشکل اعم‌از عدم دسترسی ویا موارد دیگر. 3. نتیجه: در هر دو حالت قبل رویداد ممیزی ثبت می‌گردد. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **10** | **خروج داده کاربری به محصول با مشخصه امنیتی** |
| **توصیف واسط** | هدف(ها) | 1. مهار دسترسی کاربر بابت بارگیری داده | |
| متد(ها) | 1. مهار دسترسی کاربر بابت بارگیری داده | |
| فعالیت(ها) | 1. کاربر می‌تواند درصورت داشتن دسترسی بارگیری در بخش‌های دارای این دسترسی (مثلا دکمه‌هایی با متن "خروجی اکسل")، اقدام به بارگیری (download) کند. درنهایت رویکرد ممیزی شامل شناسه و نام کاربر و دیگر مشخصه‌های امنیتی و حائز اهمیت ثبت می‌گردد. | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: بابت شناسایی او و اینکه چه دسترسی‌هایی دارد. 2. داده قابل‌بارگیری: هر آنچه که کاربر قصد بارگیری آن را دارد. | |
| نتایج و پیام‌های خطا | 1. پیام خطا: درصورت بروز مشکل اعم‌از عدم دسترسی ویا موارد دیگر. 2. نتیجه: رویداد ممیزی مرتبط شامل اطلاعات حائز امنیت ثبت می‌گردد. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **11** | **صحت داده کاربری ذخیره‌شده** |
| **توصیف واسط** | هدف(ها) | 1. پایش و اعتبارسنجی داده‌های ذخیره‌شده در پایگاه داده | |
| متد(ها) | 1. پایش و اعتبارسنجی داده‌های ذخیره‌شده در پایگاه داده | |
| فعالیت(ها) | 1. باتوجه به توضیحات ارائه شده در *بند (أ) بخش فعالیت‌های واسط کاربری 6 با نام "عملیات رمزنگاری"*، این امکان وجود دارد که هرگونه تغییر غیرمجاز در داده‌های حساس تشخیص داده شده و نتیجه سنجش را درقالب اعلان به کاربر نشان‌دهد. | |
| نام و تشریح پارامتر(ها) | 1. نوع الگوریتم: نوع الگوریتم درهم‌ساز را مشخص می‌کند. 2. متن ساده: حاوی یک رکورد ممیزی ویا یک رمز عبور کاربر است که قرار است روی آن درهم‌سازی صورت گیرد. | |
| نتایج و پیام‌های خطا | 1. نتیجه: نتیجه یکی از دو حالت "معتبر" یا "نامعتبر" است که به کاربر نمایش‌داده‌می‌شود. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **12** | **مدیریت احراز هویت ناموفق** |
| **توصیف واسط** | هدف(ها) | 1. توانایی محصول در تشخیص تعداد تلاش‌های ورود ناموفق کاربران 2. پیچیده‌سازی فرآیند ورود کاربران پس‌از تعداد مشخصی تلاش ورود ناموفق | |
| متد(ها) | 1. توانایی محصول در تشخیص تعداد تلاش‌های ورود ناموفق کاربران 2. پیچیده‌سازی فرآیند ورود کاربران پس‌از تعداد مشخصی تلاش ورود ناموفق | |
| فعالیت(ها) | 1. کاربر سطح مدیر می‌تواند عددی مثبت را به‌منزله‌ی حد آستانه تلاش ناموفق ورود کاربران تعیین کند. این حد موقع احراز هویت کاربر بصورت ورود بررسی شده و اگر از این حد گذشته باشد و کاربر ورود ناموفقی داشته باشد، اقدامات بعدی صورت می‌گیرد.   همچنین سامانه‌ی فعلی از سازوکار ارتباط از راه‌دور ازطریق SSH پشتیبانی نمی‌کند.   1. درصورت تعدد ورود ناموفق، واردکردن کد کپچا ضروری می‌گردد. همچنین کاربر مدیر سیستم می‌تواند با تعیین مدت جریمه زمانی، کاربری که تلاش ناموفق فراوان داشته است را تا مدت زمان مشخصی مسدود نماید. کاربر در این مدت زمان حتی با واردکردن اطلاعات هویتی صحیح نیز قادر به ورود به سامانه نخواهد بود. پس از این مدت زمان همه چیز به روال عادی خود برمی‌گردد و کاربر درصورت واردکردن اطلاعات هویتی صحیح می‌تواند وارد سامانه گردد. | |
| نام و تشریح پارامتر(ها) | 1. حد آستانه تلاش ناموفق ورود: عددی مثبت که کاربر سطح مدیر وارد سامانه می‌کند. 2. کد کپچا: یک عبارت تصادفی که برای پیچیده‌سازی فرآیند ورود بکار می‌رود. 3. جریمه زمانی: مدت زمانی که در آن کاربری که تلاش ناموفق فراوان داشته، نمی‌تواند به سامانه وارد شود. این مقدار توسط کاربر مدیر سیستم (سطح بالا) قابل تنظیم است. 4. داده‌های احراز هویت کاربر: نام کاربری و رمزعبوری که کاربر برای ورود استفاده می‌کند. | |
| نتایج و پیام‌های خطا | 1. پیام خطا: درصورت تجاوز از حد آستانه، پیام مرتبط به کاربر نمایش‌داده‌می‌شود. 2. نتیجه ناموفق: درصورت تجاوز از حد آستانه، کد کپچا فعال می‌شود. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **13** | **تعریف مشخصات کاربر** |
| **توصیف واسط** | هدف(ها) | 1. نگهداری مشخصه‌های امنیتی مهم کاربر | |
| متد(ها) | 1. نگهداری مشخصه‌های امنیتی مهم کاربر | |
| فعالیت(ها) | 1. مشخصه‌های زیر از کاربر ثبت و ذخیره می‌گردد:    * شناسه کاربر    * متد احراز هویت مورد استفاده    * داده احراز هویت    * وضعیت حساب کاربری   کاربر با مراجعه به منوی بالا سمت چپ سامانه و با فشردن دکمه "تغییر رمز عبور" می‌تواند اقدام به تغییر رمز عبور خود کند. | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: نام کاربری که در سامانه تعریف‌شده‌باشد. 2. متد احراز هویت: روش ورود کاربر به سامانه. مانند ورود با رمزعبور، ورود با کد یکبارمصرف و ... 3. داده احراز هویت: شامل نام کاربری و رمزعبور کاربر. | |
| نتایج و پیام‌های خطا | 1. نتیجه موفق: داده‌ها و مشخصه‌های امنیتی کاربر ذخیره می‌شوند. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **14** | **مدیریت کلمه عبور** |
| **توصیف واسط** | هدف(ها) | 1. تعریف و اعمال سیاست‌های پذیرش رمزعبور | |
| متد(ها) | 1. کلمه عبور باید تواند هر ترکیبی از ارقام، حروف کوچک و بزرگ و نویسه‌های خاص باشد. 2. کلمه عبور باید دارای یک حداقل طول تعیین‌شده توسط کاربر سطح مدیر باشد. | |
| فعالیت(ها) | 1. کاربر سطح مدیر می‌تواند تمامی این سیاست‌ها را در مسیر "تعاریف > پنل کاربری > تنظیمات پسورد" تعیین کند. | |
| نام و تشریح پارامتر(ها) | 1. شامل عدد بودن: الزامی بودن وجود ارقام در کلمه عبور را مشخص می‌کند. 2. شامل حروف بودن: الزامی بودن وجود حروف در کلمه عبور را مشخص می‌کند. 3. شامل علائم بودن: الزامی بودن وجود نویسه‌های خاص در کلمه عبور را مشخص می‌کند. مانند: ~×!@#$%^&\*() 4. طول پسورد: حداقل طول کلمه عبور را مشخص می‌کند. | |
| نتایج و پیام‌های خطا | 1. نتیجه موفق: درصورت موفقیت‌آمیز بودن، تنظیمات جدید ثبت می‌شوند. 2. نتیجه: رویداد ممیزی ثبت می‌شود. 3. پیام خطا: بدلیل عدم دسترسی کاربر به بخش موردنظر. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **15** | **احراز هویت کاربر** |
| **توصیف واسط** | هدف(ها) | 1. فراهم‌بودن اقداماتی نظیر بازیابی رمزعبور قبل از احراز هویت کاربر 2. الزام احراز هویت کاربر قبل از ورود به سامانه | |
| متد(ها) | 1. فراهم‌بودن اقداماتی نظیر بازیابی رمزعبور قبل از احراز هویت کاربر 2. الزام احراز هویت کاربر قبل از ورود به سامانه | |
| فعالیت(ها) | 1. در صفحه ورود کاربران (LOGIN) کاربر می‌تواند اقدامات میانی زیر را بدون نیاز به احراز هویت انجام دهد:    * بازیابی رمزعبور    * شناسایی کاربر 2. باقی موارد و امکانات سامانه نیازمند به احراز هویت موفق کاربر هستند. کاربری می‌تواند احراز هویت کند که از قبل هیچ نشست فعالی نداشته‌باشد. در شرایطی که احراز هویت دو مرحله ای فعال باشد، کاربر باید اقدام به دریافت رمز یکبار مصرف از طریق پیامک و واردکردن آن در فیلد مربوطه نماید. | |
| نام و تشریح پارامتر(ها) | 1. داده احراز هویت: نام کاربری و رمزعبور کاربر بمنظور ورود موفق به سامانه 2. شماره تماس کاربر: بمنظور بازیابی رمزعبور 3. کد تایید دومرحله‌ای: درصورتی که این تنظیمات فعال باشد، کاربر بایست کد تاییدی که دریافت کرده است را وارد سامانه نماید. | |
| نتایج و پیام‌های خطا | 1. پیام خطا: درصورت عدم انطباق شماره تماس کاربر با اطلاعات ذخیره‌شده در سامانه 2. پیام خطا: درصورت ورود ناموفق کاربر 3. نتیجه موفق: ورود موفق درصورت تصدیق داده‌های هویتی کاربر | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **16** | **سازوکار احراز هویت چندگانه** |
| **توصیف واسط** | هدف(ها) | 1. محصول باید بتواند از طرق مختلف احراز هویت صورت‌دهد. | |
| متد(ها) | 1. محصول باید بتواند از طرق مختلف احراز هویت صورت‌دهد. مانند:    * نام کاربری و رمزعبور    * امضای دیجیتال    * تایید دومرحله‌ای    * استفاده از رمز یکبارمصرف | |
| فعالیت(ها) | 1. سامانه فعلی سازوکارهای زیر را برای احراز هویت اتخاذ می‌کند:    * نام کاربری و رمزعبور    * تایید دومرحله‌ای    * ارسال رمز یکبارمصرف به شماره تماس کاربر برای احراز هویت او | |
| نام و تشریح پارامتر(ها) | 1. نام کاربری و رمزعبور: اطلاعاتی که کاربر برای ورود نیاز دارد. 2. شماره تماس: بمنظور ارسال کد تایید در سازوکار ورود با شماره تماس 3. کد تایید دومرحله‌ای: یک دنباله تصادفی برای تایید گام دوم ورود کاربر | |
| نتایج و پیام‌های خطا | 1. پیام خطا: درصورت اشتباه‌بودن کد تایید، نام کاربری و رمزعبور. 2. نتیجه موفق: کاربر باموفقیت وارد سامانه می‌شود. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **17** | **انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر** |
| **توصیف واسط** | هدف(ها) | 1. تطابق و انقیاد تام مشخصه‌های امنیتی کاربر با موجودیت فعال فعلی | |
| متد(ها) | 1. نگهداری مشخصه‌های امنیتی مشخص برای کاربر فعال 2. محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه‌های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت می‌کند، اعمال کند. 3. محصول باید قوانینی را که حاکم بر تغییرات است به مشخصه‌های امنیتی کاربر فعال اعمال کند. | |
| فعالیت(ها) | 1. برای هر کاربری که ورود می‌کند، مشخصه‌های امنیتی زیر ذخیره می‌گردد:    * شناسه کاربر    * نشانی IP    * جزئیات واسط کلاینت    * متد احراز هویت 2. زمانی‌که نشست جدید ایجاد می‌شود، درصورت فعال بودن نشست‌های هم‌زمان و با درنظرگرفتن عدم‌تجاوز از حد آستانه تعداد نشست‌های هم‌زمان، کاربر وارد می‌شود. به کاربرهایی که قبلا به این حساب وارد‌شده‌باشند، اعلان پیامکی جهت اطلاع‌رسانی فرستاده‌می‌شود. پیشینه احراز هویت کاربر نیز بروز می‌شود. 3. سامانه این موضوع را که در طول نشست فعال کاربر تغییری در مشخصه‌های امنیتی او رخ‌دهد، می‌پاید. درصورت رخداد تغییر، کاربر بطور خودکار از حساب خود خارج می‌شود و نشست او خاتمه‌می‌یابد. | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: شناسه‌ی یکتایی که هر کاربر داراست. 2. نشانی IP: شناسه‌ی IP دستگاه کاربر که درون شبکه‌ قراردارد. 3. جزئیات واسط کلاینت: اطلاعاتی ازقبیل نام مرورگر، نسخه‌ی آن و ... 4. متد احراز هویت: روش ورود کاربر به سامانه. مانند ورود با رمزعبور، ورود با کد یکبارمصرف و ... | |
| نتایج و پیام‌های خطا | 1. نتیجه: درصورت تغییر مرورگر یا دستگاه کاربر فعال، او از حساب خود خارج می‌گردد. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **18** | **مدیریت کارکرد در محصول** |
| **توصیف واسط** | هدف(ها) | 1. محدودسازی امکان تغییر رفتار سامانه تنها به کاربر سطح مدیر | |
| متد(ها) | 1. محدودسازی امکان تغییر رفتار سامانه تنها به کاربر سطح مدیر | |
| فعالیت(ها) | 1. تنها کاربر سطح بالا یا کاربر مجاز یا کاربر سطح مدیر می‌تواند تنظیمات مدیریتی و بنیادین سامانه را ویرایش کند. از دسترسی‌های غیرمجاز جلوگیری می‌شود. برای تمامی سناریوها رویدادهای ممیزی ثبت می‌شود. | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: برای شناسایی کاربر و تعیین سطوح دسترسی او | |
| نتایج و پیام‌های خطا | 1. پیام خطا: درصورت دسترسی غیرمجاز خطایی مرتبط دریافت می‌کند. 2. نتیجه موفق: درصورت موفقیت‌آمیز بودن تنظیمات ویرایش شده و بروز می‌شوند. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **19** | **مدیریت مشخصه‌های امنیتی** |
| **توصیف واسط** | هدف(ها) | 1. فراهم‌آوری امکان مشاهده، حذف، ویرایش و ... مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر، تنها برای کاربران مجاز (سطح مدیر) | |
| متد(ها) | 1. فراهم‌آوری امکان مشاهده، حذف، ویرایش و ... مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر، تنها برای کاربران مجاز (سطح مدیر) | |
| فعالیت(ها) | 1. کاربر سطح مدیر می‌تواند مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر را ویرایش، حذف یا مشاهده کند. این امکان برای دیگر کاربران فراهم نیست و جلوی آن گرفته می‌شود.   برای مثال می‌تواند به رجوع به بخش "منو > مدیریت کاربران > تعریف کاربران" داده‌های احراز هویت کاربر هدف را ویراسته و ذخیره نماید. درصورت وجود نشست فعال برای کاربر هدف، این نشست خاتمه‌یافته و کاربر مذکور نیازمند ورود مجدد خواهد بود. | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: برای تشخیص اینکه آیا این کاربر دسترسی سطح مدیر دارد یا خیر. 2. مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر: داده‌هایی که مدیر می‌تواند آنرا دستخوش تغییر کند. | |
| نتایج و پیام‌های خطا | 1. پیام خطا: درصورت دسترسی غیرمجاز، کاربر خطای مرتبط دریافت می‌کند. 2. نتیجه موفق: درصورت موفقیت‌آمیز بودن، نشست کاربری که مشخصه‌های امنیتی او تغییر کرده است، منقضی شده و لازم است تا دوباره به سامانه وارد شود. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **20** | **مدیریت داده‌ی محصول** |
| **توصیف واسط** | هدف(ها) | 1. محدودسازی دسترسی افزودن، ویرایش، حذف و ... داده‌های محصول تنها به کاربران مجاز | |
| متد(ها) | 1. محدودسازی دسترسی افزودن، ویرایش، حذف و ... داده‌های محصول تنها به کاربران مجاز | |
| فعالیت(ها) | 1. باتوجه به دسترسی‌هایی که برای کاربر ورودکرده در پایگاه داده موجود است، اینکه می‌تواند به داده‌ای دسترسی داشته باشد یا خیر، مشخص می‌شود. چه دسترسی مجاز باشد چه نباشد، رویداد ممیزی مرتبط با این رخداد ثبت می‌گردد. | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: برای تشخیص اینکه آیا این کاربر دسترسی سطح مدیر دارد یا خیر. | |
| نتایج و پیام‌های خطا | 1. درصورت دسترسی غیرمجاز، کاربر خطای مرتبط دریافت می‌کند. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **21** | **کارکردهای مدیریتی محصول** |
| **توصیف واسط** | هدف(ها) | 1. محصول باید قادر به انجام کارکردهای مدیریتی باشد. | |
| متد(ها) | 1. محصول باید قادر به انجام کارکردهای مدیریتی موجود در پروفایل حفاظتی برنامه‌های کاربردی تحت شبکه باشد. | |
| فعالیت(ها) | 1. تمامی موارد کارکردهای مدیریتی موجود در پروفایل حفاظتی برنامه‌های کاربردی تحت شبکه توسط سامانه فعلی انجام می‌پذیرد. | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: برای شناسایی او و تعیین و تشخیص دسترسی‌های او | |
| نتایج و پیام‌های خطا | 1. پیام خطا: درصورت عدم دسترسی به بخش موردنظر | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **22** | **نقش‌های امنیتی محصول** |
| **توصیف واسط** | هدف(ها) | 1. وجود و معرفی نقش‌های پیشفرض در سامانه و ارتباط‌گیری با آن‌ها | |
| متد(ها) | 1. وجود و معرفی نقش‌های پیشفرض در سامانه 2. محصول، باید قادر به مرتبط نمودن کاربران با نقش‌ها و دسترسی‌های مجاز تعریف شده باشند. | |
| فعالیت(ها) | 1. سامانه فعلی از سازوکار نقش پشتیبانی نمی‌کند. درعوض دسترسی‌ها به حساب کاربری اختصاص می‌یابند. با این توصیف، دو حساب کاربری پیشفرض وجود دارد:    * حساب مدیر سیستم (admin)    * حساب توسعه‌گر (developer)   هر دوی این حساب‌ها دارای دسترسی کامل بوده و درنتیجه قادر به دسترسی دادن یا سلب‌کردن دسترسی کاربران دیگر هستند.   1. محصول می‌تواند با کمک شناسه‌ی کاربر دسترسی‌های او را تشخیص دهد. | |
| نام و تشریح پارامتر(ها) |  | |
| نتایج و پیام‌های خطا |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **23** | **حفظ وضعیت امن در زمان شکست** |
| **توصیف واسط** | هدف(ها) | 1. محصول باید در زمان رخداد انواع شکست‌های نرم‌افزاری و سخت‌افزاری، وضعیت امن را حفظ نمایند. | |
| متد(ها) | 1. محصول باید در زمان رخداد انواع شکست‌های نرم‌افزاری و سخت‌افزاری، وضعیت امن را حفظ نمایند. | |
| فعالیت(ها) | 1. درصورت بروز هرگونه شکست نرم‌افزاری، وضعیت امن سامانه حفظ شده و اطلاعاتی که برای رفع مشکل لازم است، در قسمت پیام‌های سیستم ذخیره می‌گردد. | |
| نام و تشریح پارامتر(ها) | 1. رخداد شکست: هرگونه رخدادی که باعث اختلال در عملکرد سامانه گردد. | |
| نتایج و پیام‌های خطا | 1. نتیجه: وضعیت امن حفظ شده و یک رویداد ممیزی مرتبط با آن که شامل اطلاعات خطای پیش‌آمده است، ثبت می‌گردد. درنهایت شماره‌ی خطای پیش‌آمده به کاربر نمایش‌داده می‌شود تا بعدا قابل ردگیری کاربر باشد. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **24** | **انتقال داده‌ی امنیت در داخل محصول** |
| **توصیف واسط** | هدف(ها) | 1. محصول باید توانایی داشته‌باشد که درصورت فراهم‌نمودن بستر و زیرساخت امن، از افشا یا تغییر داده در هنگام انتقال بین بخش‌های مجزای خود که با هم ارتباط دارند، محافظت نمایند. | |
| متد(ها) | 1. محصول باید توانایی داشته‌باشد که درصورت فراهم‌نمودن بستر و زیرساخت امن، از افشا یا تغییر داده در هنگام انتقال بین بخش‌های مجزای خود که با هم ارتباط دارند، محافظت نمایند. | |
| فعالیت(ها) | 1. در سامانه فعلی تمامی اجزای اجرایی و پایگاه داده درون یک دستگاه کامپیوتر نصب و راه‌اندازی می‌شود. یعنی سامانه یک هسته دارد و monolothic است. درنتیجه داده‌های امنیتی محفوظ می‌مانند. | |
| نام و تشریح پارامتر(ها) | 1. داده‌های امنیتی: شامل تمامی داده‌های حساس و حائز اهمیت است. | |
| نتایج و پیام‌های خطا |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **25** | **سازگاری داده‌ی امنیتی بین محصول و موجودیت امن** |
| **توصیف واسط** | هدف(ها) | 1. محصول درصورت استفاده از محصولات امن IT، باید تفسیر سازگار را در زمان اشتراک‌گذاری داده امنیتی بین خود و دیگر محصولات IT فراهم‌آورد. | |
| متد(ها) | 1. محصول درصورت استفاده از محصولات امن IT، باید تفسیر سازگار را در زمان اشتراک‌گذاری داده امنیتی بین خود و دیگر محصولات IT فراهم‌آورد. | |
| فعالیت(ها) | 1. برای مثال هنگام ارتباط‌گیری با سرور پنل پیامکی از کانال امن HTTPS استفاده‌می‌شود. | |
| نام و تشریح پارامتر(ها) |  | |
| نتایج و پیام‌های خطا | 1. ارتباط امن با دیگر محصولات IT | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **26** | **مهرهای زمانی** |
| **توصیف واسط** | هدف(ها) | 1. توانایی محصول در ایجاد مهرهای زمانی قابل‌اطمینان | |
| متد(ها) | 1. توانایی محصول در ایجاد مهرهای زمانی قابل‌اطمینان | |
| فعالیت(ها) | 1. محصول فعلی از سرور NTP به نشانی <http://time.day.ir> بهره می‌برد. | |
| نام و تشریح پارامتر(ها) | 1. نشانی سرور NTP: سروری که زمان و تاریخ فعلی معتبر از آن واکشی می‌شود. | |
| نتایج و پیام‌های خطا | 1. نتیجه موفق: واکشی زمان و تاریخ معتبر | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **27** | **بروزرسانی امن** |
| **توصیف واسط** | هدف(ها) | 1. فراهم‌کردن امکان بروزرسانی سامانه 2. احراز هویت میان‌افزار بروزرسانی قبل‌از اجرای بروزرسانی خودکار | |
| متد(ها) | 1. فراهم‌کردن امکان بروزرسانی سامانه 2. احراز هویت میان‌افزار بروزرسانی قبل‌از اجرای بروزرسانی خودکار | |
| فعالیت(ها) | 1. سامانه فعلی از هیچ‌گونه سازوکار بروزرسانی پشتیبانی نمی‌کند. | |
| نام و تشریح پارامتر(ها) |  | |
| نتایج و پیام‌های خطا |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **28** | **تحمل خطا** |
| **توصیف واسط** | هدف(ها) | 1. محصول باید از عملکرد تمام کارکردهای اصلی هنگام رویداد شکست‌های نرم‌افزاری و سخت‌افزاری اطمینان حاصل کند. | |
| متد(ها) | 1. محصول باید از عملکرد تمام کارکردهای اصلی هنگام رویداد شکست‌های نرم‌افزاری و سخت‌افزاری اطمینان حاصل کند. | |
| فعالیت(ها) | 1. درصورت بروز هرگونه شکست نرم‌افزاری، وضعیت امن سامانه حفظ شده و اطلاعاتی که برای رفع مشکل لازم است، در قسمت پیام‌های سیستم ذخیره می‌گردد. | |
| نام و تشریح پارامتر(ها) | 1. رخداد شکست: هرگونه رخدادی که باعث اختلال در عملکرد سامانه گردد. | |
| نتایج و پیام‌های خطا | 1. وضعیت امن حفظ شده و یک رویداد ممیزی مرتبط با آن که شامل اطلاعات خطای پیش‌آمده است، ثبت می‌گردد. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **29** | **محدودیت برروی چندین نشست هم‌زمان** |
| **توصیف واسط** | هدف(ها) | 1. محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود کند. | |
| متد(ها) | 1. محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود کند. | |
| فعالیت(ها) | 1. کاربر سطح مدیر می‌تواند حد آستانه تعداد نشست‌های همزمان را تعیین‌کند. | |
| نام و تشریح پارامتر(ها) | 1. حد آستانه تعداد نشست‌های همزمان 2. شناسه کاربر: برای شناسایی او و دسترسی‌هایش | |
| نتایج و پیام‌های خطا | 1. پیام خطا: درصورت دسترسی غیرمجاز به حد آستانه تعداد نشست‌های همزمان، خطایی مرتبط نمایش داده می‌شود و رویداد ممیزی مرتبط ثبت می‌گردد. 2. نتیجه موفق: درصورت موفقیت‌آمیز بودن رویه، حد آستانه جدید ذخیره می‌گردد. 3. نتیجه: ثبت رویداد ممیزی مرتبط | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **30** | **خاتمه دادن به نشست‌ها** |
| **توصیف واسط** | هدف(ها) | 1. محصول باید پس‌از مدت زمان خاصی از غیرفعال‌ماندن سامانه، به نشست جاری خاتمه دهد. 2. محصول باید به کاربری که خود آغازگر نشست بوده است، امکان و اجازه خاتمه نشست را بدهد. | |
| متد(ها) | 1. محصول باید پس‌از مدت زمان خاصی از غیرفعال‌ماندن سامانه، به نشست جاری خاتمه دهد. 2. محصول باید به کاربری که خود آغازگر نشست بوده است، امکان و اجازه خاتمه نشست را بدهد. | |
| فعالیت(ها) | 1. کاربر مجاز می‌تواند مقدار این تنظیمات را مشخص‌کند. سامانه پس از گذشت مدت زمان مشخص‌شده توسط کاربر مجاز از آخرین درخواست HTTP کاربر، نشست او را خاتمه می‌دهد. 2. هر زمان که کاربر مایل باشد می‌تواند با فشردن گزینه خروج از حساب، به نشست خود خاتمه دهد. | |
| نام و تشریح پارامتر(ها) | 1. بازه‌ زمانی مرتبط با خاتمه نشست غیرفعال: عددی که براساس آن سامانه حدود زمانی مجاز برای ماندن درحالت بی‌کار (IDLE) را برای کاربر جایز می‌داند. | |
| نتایج و پیام‌های خطا | 1. نتیجه: درصورت تجاوز از بازه زمانی مذکور، کاربر پیام با مضمون مرتبط دریافت‌کرده و نیازمند ورود مجدد به سامانه است. 2. نتیجه: درصورت فشردن دکمه خروج از حساب، کاربر داوطلبانه به نشست خود خاتمه می‌دهد. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **31** | **سوابق دسترسی به محصول** |
| **توصیف واسط** | هدف(ها) | 1. دسترسی و مدیریت سوابق ورودهای موفق و ناموفق کاربر توسط خود او | |
| متد(ها) | 1. درصورت برقراری موفقیت‌آمیز نشست، محصول باید آخرین تلاش‌های موفق و ناموفق کاربر با به اون نمایش دهد. 2. محصول نباید اطلاعات سوابق دسترسی کاربر را بدون بازدید او حذف نماید. | |
| فعالیت(ها) | 1. کاربر پس از ورود خود، می‌تواند به بخش تاریخچه فعالیت خود رفته و از سوایق ورودهای موفق و ناموفق خود بازدید نماید. 2. کاربر می‌تواند درصورت تمایل سوابق دسترسی خود را در همان بخش مذکور حذف کند. | |
| نام و تشریح پارامتر(ها) | 1. شناسه کاربر: برای شناسایی او و واکشی سوابق ورود او از پایگاه داده | |
| نتایج و پیام‌های خطا | 1. نتیجه: نمایش سوابق ورود موفق و ناموفق | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **32** | **برقراری نشست** |
| **توصیف واسط** | هدف(ها) | 1. محصول باید قادر به ممانعت از ایجاد نشست بر اساس مکان، شماره پورت، روز، زمان باشد. | |
| متد(ها) | 1. محصول باید قادر به ممانعت از ایجاد نشست بر اساس مکان، شماره پورت، روز، زمان باشد. | |
| فعالیت(ها) | 1. کاربر مجاز می‌تواند با مراجعه به مسیر "منو > تعاریف > پنل کاربری > محدودسازی لاگین" تنظیمات مرتبط با محدودسازی ورود را ویرایش‌کند. | |
| نام و تشریح پارامتر(ها) | 1. از تاریخ – تا تاریخ: بازه زمانی مجاز برای ورود کاربران را نگه‌می‌دارد. 2. از آی‌پی – تا آی‌پی: بازه نشانی IP مجاز برای ورود کاربران را نگه‌می‌دارد. 3. از پورت – تا پورت: بازه مقادیر پورت مجاز برای ورود کاربران را نگه‌می‌دارد. | |
| نتایج و پیام‌های خطا | 1. پیام خطا: درصورت دسترسی نداشتن به بخش تنظیمات، خطای مرتبط به کاربر نشان‌داده‌می‌شود. 2. نتیجه موفق: درصورت موفقیت‌آمیز بودن، تنظیمات جدید ثبت می‌گردد. نتیجه‌ی این تنظیمات به محدودشدن شرایط ورود کاربر منجر می‌شود. 3. نتیجه: رویداد ممیزی مرتبط ثبت می‌شود. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ردیف و نام واسط کاربری** | | **33** | **مسیر امن** |
| **توصیف واسط** | هدف(ها) | 1. ایجاد کانال امن برای برقراری ارتباط راه‌دور | |
| متد(ها) | 1. توانایی محصول در ایجاد ارتباط امن بین خود و کاربران راه‌دور 2. محصول به مدیر اجازه دهد تا ارتباط راه‌دور را ازطریق کانال امن برقرار کند. 3. محصول باید از کانال امن برای احراز هویت و سایر فعالیت مدیر صورت‌دهد. | |
| فعالیت(ها) | 1. سامانه فعلی از سازوکار ارتباط راه‌دور کاربران پشتیبانی نمی‌کند. | |
| نام و تشریح پارامتر(ها) |  | |
| نتایج و پیام‌های خطا |  | |

# نگاشت بین واسط­های کاربری کارکردهای امنیتی محصول و الزامات کارکرد امنیتی

|  |  |  |
| --- | --- | --- |
| **واسط‌های کاربری کارکرد امنیتی محصول** | **الزام کارکرد امنیتی** | **ویژگی‌های امنیتی در حوزه منطقی** |
| تولید داده ممیزی | FAU\_GEN.1.1 FAU\_GEN.1.2 FAU\_GEN.2.1 |  |
| بازبینی داده‌های ممیزی | FAU\_SAR.1.1 FAU\_SAR.1.2 FAU\_SAR.2.1 FAU\_SAR.3.1 |  |
| انتخاب داده‌های ممیزی | FAU\_SEL.1.1 |  |
| ذخیره رویدادهای ممیزی | FAU\_STG.1.1 FAU\_STG.1.2 |  |
| ازبین‌زفتن داده‌های ممیزی | FAU\_STG.3.1 FAU\_STG.4.1 |  |
| عملیات رمزنگاری | FCS\_COP.1.1(1) FCS\_COP.1.1(2) |  |
| خط‌مشی و عملیات مهار دسترسی | FDP\_ACC.1.1 FDP\_ACF.1.1 FDP\_ACF.1.2 FDP\_ACF.1.3 FDP\_ACF.1.4 |  |
| حفاظت کامل از اطلاعات باقیمانده در منابع | FDP\_RIP.2.1 |  |
| ورود داده کاربری به محصول با مشخصه امنیتی | FDP\_ITC.2.1 FDP\_ITC.2.2 FDP\_ITC.2.3 |  |
| خروج داده کاربری به محصول با مشخصه امنیتی | FDP\_ETC.2.1 FDP\_ETC.2.2 FDP\_ETC.2.4 |  |
| صحت داده کاربری ذخیره‌شده | FDP\_SDI.2.1 FDP\_SDI.2.2 |  |
| مدیریت احراز هویت ناموفق | FIA\_AFL.1.1 FIA\_AFL.1.2 |  |
| تعریف مشخصات کاربر | FIA\_ATD.1.1 |  |
| مدیریت کلمه عبور | FIA\_PMG\_EXT.1.1 |  |
| احراز هویت کاربر | FIA\_UAU.1.1 FIA\_UAU.1.2 |  |
| سازوکار احراز هویت چندگانه | FAU\_UAU.5.1 FAU\_UAU.5.2 |  |
| انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر | FIA\_USB.1.1 FIA\_USB.1.2 FIA\_USB.1.3 |  |
| مدیریت کارکرد در محصول | FMT\_MOF.1.1 |  |
| مدیریت مشخصه‌های امنیتی | FMT\_MSA.1.1 |  |
| مدیریت داده‌ی محصول | FMT\_MTD.1.1 |  |
| کارکردهای مدیریتی محصول | FMT\_SMF.1.1 |  |
| نقش‌های امنیتی محصول | FMT\_SMR1.1 FMT\_SMR.1.2 |  |
| حفظ وضعیت امن در زمان شکست | FPT\_FLS.1.1 |  |
| انتقال داده‌ی امنیت در داخل محصول | FPT\_ITT.1.1 |  |
| سازگاری داده‌ی امنیتی بین محصول و موجودیت امن | FPT\_TDC.1.1 |  |
| مهرهای زمانی | FPT\_STM.1.1 |  |
| بروزرسانی امن | FPT\_TUD\_EXT.1.2 FPT\_TUD\_EXT.1.3 |  |
| تحمل خطا | FRU\_FLT.1.1 |  |
| محدودیت برروی چندین نشست هم‌زمان | FTA\_MCS.1.1 |  |
| خاتمه دادن به نشست‌ها | FTA\_SSL3.1 FTA\_SSL.4.1 |  |
| سوابق دسترسی به محصول | FTA\_TAH.1.1 FTA\_TAH.1.2 FTA\_TAH.1.3 |  |
| برقراری نشست | FTA\_TSE.1.1 |  |
| مسیر امن | FTP\_TRP.1.1 FTP\_TRP.1.2 FTP\_TRP.1.3 |  |