سند هدف امنیتی

اتوماسیون طراحان مقدم نسخه وب

تاریخ تهیه	شماره ویرایش	تهیه کننده	موضوع
1400/01/25	**1.4**	**واحد فنی شرکت طراحان بهینه**	**سند هدف امنیتی برنامه های کاربردی تحت شبکه**

فهرست مطالب

1- معرفی

1-1- مشخصات سند و محصول

عنوان سند هدف امنیتی	سند هدف امنیتی
نسخه	1.4
تاریخ	1400/01/25
نویسندگان	واحد فنی شرکت صنایع فن آوری طراحان بهینه

نام شرکت	صنایع فن آوری طراحان بهینه
نام محصول	اتوماسیون طراحان مقدم تحت وب
نوع محصول	محصولات کاربردی سازمانی
نسخه‌ی محصول	96.0.6

حداقل نیازمندی نرم‌افزاری /سخت‌افزاری /میان‌افزاری محصول

سخت‌افزار /نرم‌افزار /میان‌افزار	**حداقل الزامات**
پیش نیاز نرم افزارهای خاص (مورد نیاز سامانه و نصب توسط پیمانکار)	sql server 2019Management Studio 17 , Management Studio 18
نوع OS (Linux-windows)	windows
فضای ذخیره سازی موردنیاز شامل نوع و حجم Data (برآورد رشد دیتا و ...)	C : 100 GB OS D : 200+ GB MDF LDF F : 200+ GB Backup
میزان Ram مورد نیاز	32-64 GB
تعداد CPU Core مورد نیاز	16-32

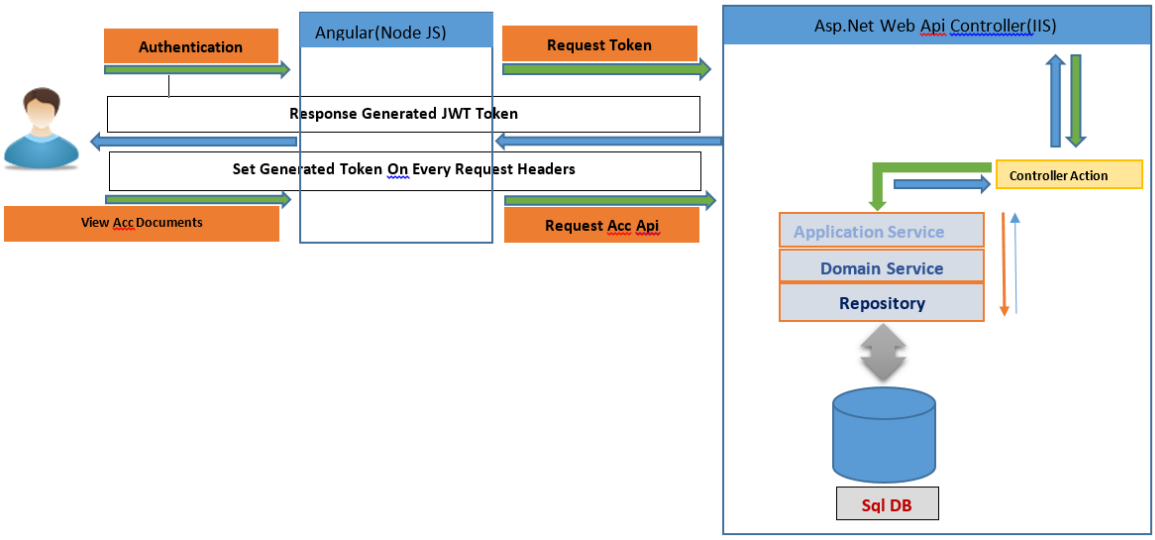
2- ادعای انطباق

2-1- انطباق با استاندارد ارزیابی امنیتی معیار مشترک

انطباق با استاندارد ارزیابی امنیتی معیار مشترک	ISO 15408 V3.1 R4
نام پروفایل حفاظتی	پروفایل حفاظتی برنامه های کاربردی تحت شبکه
سطح تضمین امنیتی	EAL1

2-2- شرح محصول

2-2-1- حوزه فیزیکی



شکل 1: حوزه فیزیکی محصول با تفکیک حوزه محصول و محیط عملیاتی آن

2-2-2- حوزه منطقی

کارکردها	توصیف
احراز هویت	ارتباط نرم افزار با سرور Directory Active و شناسایی هویت فرد ، احراز هویت با استفاده از ارسال پیامک
رویداد نگاری	تمامی فعالیت های انجام شده توسط کاربران ثبت شده و قابل مشاهده می باشد
کنترل دسترسی ها	هدف از این ارزیابی کنترل سطوح دسترسی هم درسطح عملیات و هم در سطح دیتا می باشد. بطوریکه تنها موجودیت های مجاز خاص دارای دسترسی به داده و کارکردها هستند. برای کاربران مجاز کنترل سطوح دسترسی معمولا با استفاده از داده احراز هویت انجام می گیرد.

3- مسائل امنیتی

3-1- تهدیدات

تهدیدات	توضیحات
دسترسی غیرمجاز	مهاجم میتواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا نماید. این دسترسی میتواند با استفاده از هویت سرقتی، آدرس IP جعلی و غیره صورت گیرد. مهاجم میتواند با سود بردن از نقضهای امنیتی همچون تغییر ندادن کلمه عبور و نام کاربری، استفاده از کلمه عبور ساده، غیرفعال نکردن حساب کاربری تست بر روی سیستم واقعی به محصول دسترسی پیدا نماید. همچنین مهاجم میتواند از داده باقیمانده کاربر قبلی/کاربر فعال یا داده باقیمانده که در طول ارتباطات و عملیات داخلی یا خارجی ایجاد شده سود ببرد. این داده ها میتوانند داده های حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم میتواند با دسترسی به داده ها و خود محصول سبب آسیب شود.

تهدیدات	توضیحات
تغییر غیرمجاز	رکوردهای، مستندات و داده های حفاظت شده توسط محصول میتواند بدون مجوز تغییر یابند. مهاجم میتواند با گمراه نمودن مدیر سیستم، وارد کننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. مهاجم می تواند از طرق غیر قانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده های حفاظت شده توسط محصول را تغییر دهد. این تهدید زمانی رخ میدهد که صحت رکوردها و مستندات تضمین شده نمیباشد. مهاجم ممکن است در صدد تغییر داده ممیزی یا کد منبع برآید. و بدین ترتیب با سود بردن از این تهدید دسترسی غیرمجازی به محصول پیدا نماید.
انکار	یک اقدام یا یک تراکنش صورت گرفته بر روی محصول میتواند رد گردد. این حمله غالباً آخرین اقدام مهاجم بر روی محصول میباشد تا نسبت به آگاه نشدن مدیر سیستم از حمله اطمینان یابند. همچنین مهاجم میتواند از رکوردهای ممیزی جلوگیری کند (به عنوان مثال با ایجاد سرریز در دنباله ممیزی) یا مهاجم میتواند با اضافه نمودن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه نماید.
افشای اطلاعات	داده های محرمانه که توسط محصول محافظت میشوند میتواند بدون مجوز افشاء گردد. برای مثال، کاربر عادی میتواند به یک رکورد، سند یا داده دسترسی غیرمجازی یابد. پارامترهای کنترلی ناکافی میتواند منجر به این حمله گردد. یک کاربر عادی یا اپراتور وارد کننده داده میتواند عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.

تهدیدات	توضیحات
انکار سرویس	مهاجم میتواند سبب گردد محصول در یک بازه زمانی غیر قابل دسترسی یا بلا استفاده گردد. این امر معمولاً با ارسال درخواستهای بسیار در یک بازه زمانی کوتاه صورت میگیرد طوریکه محصول قادر به پاسخ نخواهد بود. نوع ساده ای از حمله شامل ارسال درخواستهای بسیار از یک رنج IP مشخص میباشد که به نام حمله DoS شناخته میشود. نوع دیگر پیشرفته تر حمله DDoS میباشد که از BOTNET استفاده مینماید و محدودیتی بر روی آدرس IP ورودی ندارد.
داده های ورودی مخرب	مهاجم میتواند یک رکورد، سند یا داده مضر را در داخل محصول وارد نماید. با استفاده از این تهدید، مهاجم میتواند به داده کاربر خاص دسترسی پیدا نماید، حساب کاربری یک کاربر را به دست گیرد یا به بخشی از کارکردها یا تمام کارکردهای محصول دسترسی یابد.
سطح دسترسی بالاتر	مهاجم میتواند با سود بردن از دسترسی غیرمجاز، ورود داده های مخرب و تغییر داده ها، دسترسی محدودی به محصول یابد و سپس سعی در به دست آوردن سطح مجوز بالاتر نماید.
شنود شبکه	در حمله شنود شبکه، مهاجم در مکانی در شبکه مستقر میشود تا انتقال دادههای حساس بین محصول و مقصد موردنظر را مورد نظارت قرار دهد. این حمله شامل نظارت بر دادههای ردوبدل شده بین محصول و یک یا چند کاربر از راه دور و یا محلی است. به عنوان مثال میتوان به موردی اشاره کرد که در آن یک کاربر تلاش میکند تا جهت احراز هویت و ورود به برنامه، اطلاعات محرمانه خود را وارد میکند.

3-2- خط‌مشی امنیتی

خط مشی ها	توضیحات
ممیزی کامل	تمام رخدادها بر روی محیط کاری محصول باید ثبت گردد، رکوردها محافظت شده هستند و معمولاً به منظور تشخیص و جلوگیری از نقض امنیتی مورد بررسی قرار میگیرند.

خط مشی ها	توضیحات
ارتباطات امن مبتنی بر TLS	تمام کانالهای ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطیTLS استفاده نمایند.
پیکربندی مناسب	پیکربندی پیشفرض محصول و مولفه های تعاملی تحت کنترل محصول باید تغییر یابند. طوریکه مهاجم نتواند اطلاعاتی در رابطه با محصول و محیط عملیاتی آن به دست آورد. سرویسهایی که مورد استفاده نیستند، باید غیرفعال گردند. پارامترهای پیکربندی همچون دایرکتوری root پیشفرض، خطاهای پیشفرض و صفحات 404 ، مقادیر احراز هویت پیشفرض، نام کاربری پیشفرض، پورتهای پیشفرض، صفحات پیشفرض که اطلاعات داخلی همچون شماره نسخه را آشکار مینمایند. این خط مشی سازمانی بسیار مهم است به خصوص زمانیکه محصول یا هر مولفه تعاملی به طور گسترده مورد استفاده قرار میگیرد. بنابراین با تضمین نمودن منحصر به فرد بودن پارامترهای پیکربندی میتوان از حملهی مهاجم با اطلاعاتی که از محصول مشابه به دست آورده جلوگیری نمود.
امضای دیجیتال	امضای دیجیتال مورد استفاده باید مطابق با استانداردهای مورد تائید موجود باشد.

3-3- فرضیات

فرضیات	توضیحات
کاربران آموزش دیده	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده اند و قوانین را دنبال مینمایند.
توسعه دهندگان آموزش دیده	فرض شده است که افراد مسئول توسعه محصول (همانند برنامه نویس، طراح، غیره) افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال مینمایند.
توسعه دهندگان مجرب	فرض شده است تمام کارمندان توسعه دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب پذیری های شناخته شده را اتخاذ مینمایند.

فرضیات	توضیحات
محیط امن	فرض شده است که تمام پیش بینی های محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته شده است. فرض شده است که دسترسی به محیط کاری محصول به طور مناسب محدود شده و رکوردهای دسترسی برای یک بازه زمانی منطقی حفظ شده است. فرض شده است که سازوکاری وجود دارد تا رکوردها و مستندات که غیر قانونی از محصول به دست آمده را تشخیص دهد. همچنین فرض شده است که در قبال حملات DoS اقدامات مناسبی صورت میگیرد.
پشتیبان گیری مناسب	فرض شده است که هرگونه داده ایجاد شده یا وارد شده توسط محصول، واحد ذخیره سازی و دیگر مولفه های سخت افزاری دارای پشتیبان مناسبی هستند، و بنابر وجود نسخه پشتیبان هیچ داده ای از دست نمیرود همچنین به علت شکست در سیستم، قطع سرویسی رخ نمیدهد
ارتباطات	فرض شده است که تمام ارتباطات و کانالهای ارتباطی مورد استفاده توابع امنیتی محصول جهت ارتباط با نهادهای خارجی که تحت حفاظت توابع محصول نیستند؛ به طور مناسبی در قبال حملاتی چون DoS و شنود شبکه و غیره حفاظت میشوند.
تحویل امن	فرض شده است که تمام اقدامات امنیتی لازم در طول تحویل محصول اتخاذ شده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت میگیرد.
انکار سرویس توزیع شده	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ میشود.

4- اهداف امنیتی

4-1- اهداف امنیتی برای محصول

هدف امنیتی	توضیحات
ممیزی	محصول باید هر رخدادی که در زمینه امنیتی دارای ارزش است را در حوزه مالکیتش رکورد نماید. محصول باید از این رکوردها در قبال تغییرات و حذف محافظت نماید. محصول باید به

هدف امنیتی	توضیحات
	کاربران مجاز امکان بررسی آسان و سریع رکوردها را بدهد و مدیر سیستم را به موقع از رخداد امنیتی بحرانی آگاه نماید.
احراز هویت	محصول باید هر کاربری را تعریف نموده و آنها را به طور امن احراز هویت نماید و مطابق با نقش و مجوزهایشان مجاز نماید. محصول باید برای احراز هویت کاربر، قوانینی تعریف نماید طوریکه کاربران را ملزم به استفاده از کلمه های عبور قدرتمند نماید. محصول باید اجازه طبقه بندی رکوردها و مستندات را دهد و با توجه به طبقه بندی آنها قوانینی را تعریف نماید. همچنین برای مستندات و رکوردهای شخصی امکان تعریف مجوز دسترسی را فراهم مینماید. محصول باید برای کاربران به صورت انفرادی یا گروهی از کاربران سازوکار کنترل دسترسی به مستندات و رکوردها فراهم نماید. مهاجم در تلاش است تا از تهدیدی چون رسیدن به سطح دسترسی بالاتر نهایت سود را ببرد. برای جلوگیری از این تهدید، محصول باید با استفاده از سازوکارهای قویتری مدیر سیستم را احرازهویت نماید. از جمله سازوکارها میتوان به محدود نمودن رنج IP ، محدود نمودن بازه زمانی، احرازهویت براساس توکن، احرازهویت چند فاکتوری و ترکیبی از این روشها اشاره نمود.
کنترل جریان داده	محصول باید گردش داده های غیرمجاز را کنترل و مدیریت نماید. داده های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواستها از یک رنج IP تعریف شده میتواند بیانگر حمله DoS باشد. محصول باید برای مدیر سیستم واسطی را فراهم نماید که به وی اجازه حفظ ترافیک شبکه تحت نظارتش را دهد همچنین در صورت لزوم بتواند از سازوکارهای فیلترینگ استفاده نماید.
صحت داده	محصول باید نسبت به صحت داده ممیزی و داده ی رکورد با تشخیص هرگونه تغییر بر روی این داده ها اطمینان حاصل نماید و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد
مدیریت	محصول باید برای مدیر سیستم تمام کارکردها را جهت مدیریت امن و کارامد سیستم فراهم نماید. محصول باید سازوکارهای کنترل دسترسی مناسبی جهت حفاظت از واسطهای مدیریتی در نظر گیرد. محصول باید برای مدیر سیستم امکان تغییر مجوزها و نقشهای کاربران را فراهم آورد و مدیر بتواند برای یک کاربر خاص و/یا گروهی از کاربران نقشها و مجوزهایی تنظیم نماید.

هدف امنیتی	توضیحات
مدیریت خطا	محصول باید صورت امن و کارآمد سازوکار مدیریت خطا فراهم نماید. خطاهای رخ داده در طول عملیات محصول باید به کاربر به صورت امن و معنادار نشان داده شود. برای مثال، محصول باید اطلاعات کلی مربوط به احراز هویت ناموفق را برگرداند، همچنین برای کاربر عادی نباید اطلاعات جزئی چون شماره خط خطا برگردانده شود. از سوی دیگر مدیر سیستم باید سریعاً از شکست بحرانی که رخ داده مطلع گردد. جزئیات خطای برگشتی باید منجر به اقدام مناسب مدیر گردد. محصول در صور رخ دادن خطا باید وضعیت امنی را حفظ نماید.
مدیریت داده های باقیمانده	محصول باید اطمینان دهد که هر داده ی باقیمانده از محصول زمانیکه دیگر به آن نیاز نیست از محصول برداشته شده یا برای کاربران غیرقابل دسترس میگردد.
ارتباطات امن مبتنی بر TLS	تمام کانالهای ارتباطی تحت کنترل توابع امنیتی محصول باید از پروتکل ارتباطی TLS استفاده نمایند.

2-4- اهداف امنیتی برای محیط عملیاتی

هدف امنیتی	توضیحات
محیط امن	محیط عملیاتی محصول باید نسبت به امنیت محیطی و فیزیکی محصول اطمینان دهد. دسترسی غیرمجاز باید محدود گردیده و تمام مولفه ها در محیط عملیاتی باید امن گردد و تنها افراد مجاز باید اجازه دسترسی به مولفه های حساس را داشته باشند. محیط عملیاتی محصول باید اطمینان دهد محصول به طور مناسب در قبال هر حمله DoS یا DDoS محافظت شده است. از جمله سازوکارهای حفاظتی میتوان به غیرفعال نمودن سرویسها، پورتها و دیگر موارد استفاده شده اشاره نمود.
ارتباطات	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه های ارتباطی امن فراهم گردد.
کاربران آموزش دیده	محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده مینمایند.
توسعه دهندگان آموزش دیده	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده مینمایند.

هدف امنیتی	توضیحات
توسعه دهندگان مجرب	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه دهندهی محصول در زمینه امنیت تجربه داشته و آنها اقدامات مقابلهای لازم برای تمام آسیبپذیریهای امنیتی شناخته شده را در نظر میگیرد.
ممیزی کامل	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مولفه های غیر از محصول نیز مورد ممیزی قرار میگیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط عملیاتی محصول میباشد. رکوردهای ممیزی محصول در صورت ترکیب با باقی رکوردهای ممیزی بسیار معنادار خواهند بود
تحویل امن	تحویل و نصب محصول باید بدون به خطر افتادن هرگونه محدودیت امنیتی انجام شود. علاوه بر این، کارکردها و/یا پارامترهای استفاده شده به منظور تست باید پاک یا غیر قابل دسترس گردند.
پشتیبان-گیری مناسب	نسخه پشتیبان باید ایجاد گردیده و برای یک بازه زمانی منطقی تمام داده های باقیمانده در محیط عملیاتی محصول را حفظ نماید. برای این منظور ممکن است از روالهای از پیش تعریف شده استفاده گردد. همچنین باید از واحدهای ذخیره سازی و دیگر مولفه های سختافزاری نیز نسخه پشتیبان تهیه گردد.

5- الزامات امنیتی

الزامات امنیتی این سند بر اساس نسخه 1.1 پروفایل حفاظتی «برنامه‌های کاربردی تحت شبکه» تهیه شده است. ساختار این سند بدین صورت است که برای هر کلاس در پروفایل حفاظتی مربوطه، یک دسته الزام بیان شده است.

5-1- ممیزی امنیت (لاگ)

در این کلاس توانایی‌های محصول از نظر امکان تولید داده ممیزی (لاگ) مناسب برای فعالیت‌های مختلفی که در محصول صورت می‌گیرد، در شرایط مختلف سنجیده می‌شود.

شماره الزام	کلاس ممیزی (لاگ)				توضیحات
1	**محصول باید برای موارد مشخص شده که در ذیل آمده است، رکورد ممیزی تولید کند (لاگ ثبت نماید).**			☑	
	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.	شروع و اتمام توابع	☑		
		تلاشهای ناموفق برای خواندن اطلاعات از رکوردهای لاگ	☑		
		خواندن اطلاعات از رکوردهای لاگ	☑		
		تمامی تغییرات در پیکربندی لاگ	☑		
		عملیات انجام شده به دلیل سرریز حافظه لاگ از حد آستانه	☑		
		عملیات انجام شده به دلیل شکست در ذخیره‌سازی لاگها	☑		
		تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.	☑		
		تمام کاربردهای سازوکار احراز هویت	☑		
		نتایج نهایی عملیات احراز هویت	☑		
		تلاش موفق و ناموفق هر کلمه عبور تست شده توسط محصول	☑		
		شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند شکت و موفقیت ایجاد موجودیت فعال)	☑		
		تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی	☑		
		تمامی درخواستهای (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول	☑		
		تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه مشخصه‌های امنیتی)	☑		
		همه تلاش‌ها برای خارج کردن اطلاعات از محصول	☑		
		تمامی تغییرات در رفتارهای توابع کارکردی محصول	☑		
		استفاده از کارکردهای مدیریتی	☑		
		تغییرات در گروه کاربران	☑		

		☑	شکست در کارکردهای امنیتی محصول		
		☑	تمامی قابلیت‌هایی از محصول که به دلیل شکست، نمی‌توانند عملیات موردنظر را انجام دهند.		
		☑	تلاش موفق یا ناموفق برای برقراری نشست.		
		☑	عدم ایجاد نشست به دلیل محدودیت نشست‌های هم‌زمان (حداقل)		
		☑	خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست		
		☑	خاتمه به نشست غیرفعال توسط مدیر سیستم		
		☐	سایر موارد		
2	**محصول باید برای هر رکورد ممیزی تولید شده، مشخصاتی که درذیل آمده است را ثبت نماید.**			☑	
	مشخصاتی که در رکوردهای ممیزی وجود دارد مشخص شود.	☑	تاریخ و زمان رویداد		
		☑	نوع رویداد		
		☑	هویت ایجادکننده رویداد		
		☑	نتیجه رویداد		
		☑	آدرس IP ایجادکننده رویداد		
		☐	سایر موارد		
3	**محصول باید رکوردهای ممیزی را در برابر دسترسی غیرمجاز محافظت نماید.**			☑	
4	**رکوردهای ممیزی که محصول تولید می‌نماید باید برای کاربر ساده و قابل فهم باشند.**			☑	
	مواردی که در رکوردهای ممیزی وجود دارند، مشخص شوند.	☑	عدم وجود داده نامفهوم در رکوردها		
		☑	عدم وجود فیلدهای نامرتبط		
		☑	وجود داده معتبر و مناسب در هر فیلد		
5	**محصول باید امکان انتخاب و مرتب‌سازی برای رکوردهای ممیزی تولید شده را بر اساس فیلدها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید.**			☑	

	موارد‌ی که بر اســـاس آنها مرتـب‌ســـازی وجود دارد، مشخص شود.	هویت موجودیت فعال	☑		
		نوع حساب کاربری	☑		
		تاریخ/زمان	☑		
		روش اتصال کاربر	☐		
		نوع رخداد	☑		
		مکان رویداد	☑		
		سایر موارد	☑		
6	**محصول باید هرگونه حذف و تغییر غیرمجاز در رکوردهای ممیزی راتشخیص دهد و در صورت امکان جلوگیری نماید.**			☑	
	روش‌هـای تشـــخـیـص مشخص شود. (وجـود یـک مورد لازم و کـافی است)	استفاده از هش برای تشخیص تغییرات	☑		
		پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)	☐		
		فقط خواندنی کردن ممیزی‌ها در محصول	☐		
		سایر موارد	☑		
7	**محصول باید وقتی که حجم داده‌های ممیزی، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.**			☑	
	روش‌های اطلاع رسانی مشخص شود (وجود یـک مـورد لازم و کافی است)	استفاده از یک کانال ارتباطی	☐		
		ارسال پیام	☑		
		از طریق واسط کاربر مجاز	☐		
		سایر موارد	☐		
8	**محصول باید توانایی ممیزی (ثبت لاگ) هنگام از کار افتادن محصول و/یا پر شدن حافظه ممیزی را داشته باشد و برای این کار از رویکردهای بیان شده استفاده نماید.**			☑	
	رویکردهای مـــورد استفاده در محصـول مشـخص گردد (وجود یـــــک مورد لازم و کافی است)	نادیده گرفتن رویدادهای ممیزی	☐		
		ذخیره‌هســـازی محدود رویدادهای ممیزی، (آنهایی که توســـط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند)	☑		
		بازنویسی روی قدیمی‌ترین رکوردهای ممیزی ذخیره شده	☑		
		سایر موارد	☐		

5-2- رمزنگاری

در این کلاس، توانایی محصول در پیاده‌سازی یا به‌کارگیری ماژولهای رمزنگاری، بررسی می‌گردد. برای حفظ محرمانگی داده از رمزنگاری استفاده می‌گردد و این رمزنگاری‌ها می‌تواند به صورت متقارن و نامتقارن صورت گیرد. در رمزنگاری متقارن از یک کلید مشترک برای رمزگذاری و رمزگشایی، استفاده می‌شود ولی در رمزنگاری نامتقارن این کار با استفاده از یک زوج کلید (کلید عمومی و کلید خصوصی) صورت می‌گیرد. الگوریتمها میتوانند با طول کلیدهای مختلف و به روشهای مختلفی (مد عملیاتی) به رمزگذاری و رمزگشایی داده بپردازند که در این کلاس، توانایی محصول از این حیث مورد بررسی قرار گرفته است. در کلاس رمزنگاری همچنین از الگوریتمهای درهم‌سازی (هش) برای برقراری جامعیت داده استفاده می‌گردد.

شماره الزام	کلاس رمزنگاری				توضیحات
1	**محصول باید قابلیت رمزنگاری یا ماژول رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف‌شده ISO 18033-3) با توجه به موارد زیر انجام دهد.**			☑	
	مد عملیاتی که الگوریتم از آن استفاده می‌کند را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)	مد عملیاتی CBC و طول کلید 128 یا 192 یا 256 بیتی (تعریف‌شده در NIST SP 800-38A)	☑		
		مد عملیاتی GCM و طول کلید 128 یا 192 یا 256 بیتی (تعریف‌شده در NIST SP 800-38D)	☑		
		مد عملیاتی CTR و طول کلید 128 یا 192 یا 256 بیتی (تعریف‌شده در ISO10116)	☐		
2	**محصول باید بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب می‌نماید، توانایی تولید داده درهم‌سازی شده (هش) را داشته باشد؛ بنابراین باید برای تولید درهم‌سازی از موارد زیر بر اساس ISO/IEC 10118-3:2004 استفاده نماید.**			☑	
	الگوریتم و اندازه خلاصه پیام مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)	الگوریتم SHA-1 با اندازه خلاصه پیام 160 یا 256 یا 384 یا 512	☐		
		الگوریتم SHA-256 با اندازه خلاصه پیام 160 یا 256 یا 384 یا 512	☑		

	مورد لازم و کافی است.)	الگوریتم SHA-384 با اندازه خلاصه پیام 160 یا 256 یا 384 یا 512	☑		
		الگوریتم SHA-512 با اندازه خلاصه پیام 160 یا 256 یا 384 یا 512	☐		
3	**در صورتی که تولید کلید رمزنگاری در محصول وجود دارد، نیازاست که تخریب کلید رمزنگاری نیز بر اساس موارد زیر صورت پذیرد. (اختیاری)**			☑	
	روش نابودی کلید مشخص گردد. (وجود یک مورد لازم و کافی است)	نابودی با استفاده از بازنویسی ساده (بازنویسی با صفرها، یکها، مقدار تصادفی، مقدار جدیدی از کلید)	☐		
		نابودی با استفاده از یک واسط مشخص	☐		
		از طریق توابع امنیتی محصول	☑		
		سایر موارد	☐		
4	**در صورتی که امضاء دیجیتال در محصول پشتیبانی می‌شود، نیاز است که سرویس‌های امضاء رمزنگاری (تولید و تائید) بر اساس الگوریتم‌های رمزنگاری زیر انجام گیرد. (اختیاری)**			☑	
	الگوریتم و اندازه کلیدهای مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است)	الگوریتم‌های امضاء دیجیتال RSA با کلیدهای رمزنگاری 2048 بیت و بزرگتر (بر اساس FIPS PUB 186-4، استاندارد امضاء دیجیتال (DSS) بخش 5.5، الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSA-PKCS1v_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال 2 و یا الگوی امضای دیجیتال 3)	☑		
		الگوریتم‌های امضاء دیجیتال ECDSA با کلیدهای رمزنگاری 256 بیت یا بزرگتر (بر اساس ISO/IEC 14888-3 بخش 6.4، استاندارد امضای دیجیتال (DSS) بخش 6 و پیوست D، با استفاده از منحنی P-256 یا P-384 یا P-521)	☐		

3-5- شناسایی و احراز هویت

در این کلاس توانایی‌های محصول از نظر امکان شناسایی و احراز هویت کاربر در حالت‌های مختلف و اقدامات متقابل در راستای عدم برقراری آنها، بررسی می‌گردد.

شماره الزام	کلاس شناسایی و احراز هویت				توضیحات
1	**محصول باید بتواند تعداد تلاش‌های ناموفقی را که برای احراز هویت شدن صورت گرفته است (در هر بخش یا قسمتی که نیاز به احراز هویت وجود دارد)، بر اساس موارد زیر مشخص نماید.**			☑	
	مقدار یا یازه‌ی مورد استفاده در هریک باید مشخص گردد. (وجود یک مورد لازم و کافی است)	یک عدد مثبت ثابت	☐		
		یک عدد مثبت قابل تنظیم توسط مدیر	☑		
		یک بازه‌ی قابل قبولی از مقادیر	☐		
2	**محصول باید زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین شده رسید، برای پیچیده‌تر کردن احراز هویت از موارد زیر استفاده نماید.**			☑	
	روش استفاده شده برای پیچیده‌تر کردن احراز هویت را انتخاب نمایید. (وجود یک مورد لازم و کافی است.) لازم به ذکر است روش‌های فوق با توجه	غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)	☑		
		غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)	☑		

	به نوع کاربرد می‌تواند از حالت انتخابی به حالت الزامی تغییر یابد. برای مثال غیرفعال کردن حساب کاربری در تمامی کاربردها مفید نیست.	استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود)	☐		
		سایر موارد	☐		
3	**محصول باید برای هر کاربر، مشخصه‌های امنیتی که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت باشند را نگهداری نماید.**		☑	☑	
	مشخصه‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند.	شناسه کاربر	☑		
		روش احراز هویت مورد استفاده	☐		
		داده احراز هویت	☑		
		وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)	☑		
		نقش کاربر	☑		
		سایر موارد	☐		
4	**محصول باید قابلیت مدیریت کلمه عبور را فراهم آورد.**		☑	☑	
	موارد نیاز که باید در تعریف کلمه‌عبور استفاده شوند.	استفاده از حروف کوچک	☑		
		استفاده از حروف بزرگ	☑		
		استفاده از اعداد	☑		
		استفاده از کاراکترهای خاص ("@"، "#"، "$"، "٪"، "^"، "!" "&"، "*"، "(" , ")" و ...)	☑		
		حداقل طول 8 یا بیشتر (قابل تنظیم)	☑		
		سایر موارد	☐		
5	**محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجاماقدامات محدودی را فراهم نماید.**		☑	☑	

	اقدامات عمومی که کاربر می‌تواند قبل از احراز هویت انجام دهد، انتخاب شود.	مشاهده راهنمای نحوه ورود به سیستم	☐		
		بازیابی کلمه‌عبور	☑		
		هیچ اقدامی	☐		
		سایر موارد	☐		
6	**محصول باید از سازوکار احراز هویت پشتیبانی نماید (برای احراز هویت کاربران راه‌دور، باید بیش از یک سازوکار احراز هویت در محصول به کار رفته باشد).**			☑	
	سازوکارهای احراز هویت موجود در محصول مشخص شوند.	نام کاربری و کلمه عبور	☑		
		امضاء دیجیتال	☐		
		Active Directory	☐		
		OTP یا توکن	☑		
		احراز هویت دو فاکتوری	☐		
		سایر موارد	☐		
7	**محصول باید برای هر کاربر فعال، مشخصه‌های امنیتی نگهداری نماید.**			☑	
	مشخصه‌هایی امنیتی که محصول برای هر کاربر نگهداری می‌کند، مشخص گردد (در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین در «سایر موارد» بیان می‌شوند).	شناسه کاربر	☑		
		نقشها و یا مجموعه دسترسی‌های کاربر به قسمتهای مختلف برنامه	☑		
		جزئیات واسط کلاینت	☐		
		پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)	☑		
		سایر موارد	☐		
8	**محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.**			☑	

	در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین در «سایر موارد» بیان می‌شوند).	از بین رفتن اعتبار نشستهای قبلی هنگام برقراری یک نشست جدید (به جزء مواردی که فعال بودن همزمان چندین نشست موردنیاز کارکردی برنامه باشد. در این موارد، هنگام فعال شدن نشست‌های جدید، باید به صفحه کاربر اصلی (نشست اول) اطلاع داده شود.)	☑		
		به‌روزرسانی اطلاعات پیشینه احراز هویت	☑		
		سایر موارد	☐		
9	**محصول باید بر روی تغییرات مشخصه‌های امنیتی کاربر فعال قوانینی را اعمال نماید.**			☑	
	قوانینی که در صورت تغییر مشخصه‌های امنیتی کاربر فعال، اعمال می‌شود، مشخص گردد.	غیرمجاز بودن هرگونه تغییر در طول نشست فعال	☑		
		سایر موارد	☐		

5-4- حفاظت از داده‌ی کاربری

داده کاربری در واقع هر نوع داده‌ای است که کاربر تولید می‌کند یا مالک آن است. توضیح کامل داده کاربری در سند «راهنمای سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه» در قسمت اصطلاحات بیان گردیده است. در این کلاس، توانایی محصول در حفاظت از این داده‌ها مورد بررسی قرار می‌گیرد.

شماره الزام	کلاس حفاظت از داده‌ی کاربری				توضیحات
1	**محصول باید برای موجودیتها و عملیات، خط‌مشی‌های کنترل دسترسی اعمال نماید.**			☑	
	موجودیت‌های فعالی که خط‌مشی‌های کنترل دسترسی در مورد آنها اعمال می‌شوند، مشخص گردد.	مدیر سیستم	☑		
		کاربر عادی	☑		
		سایر موارد	☐		
	موجودیت‌های غیرفعالی که خط‌مشی‌های کنترل دسترسی در مورد آنها اعمال می‌شوند، مشخص گردد.	رکوردها، مستندات و فراداده[1]	☑		
		داده متعلق به کاربران	☑		
		داده احراز هویت	☑		
		سایر موارد	☐		
	عملیاتی که خط‌مشی‌های کنترل	ایجاد موجودیت غیرفعال جدید	☑		
		حذف موجودیت غیرفعال	☑		

[1] Metadata

	دسترسی در رابطه با آنها اعمال می‌شوند، مشخص گردد.	تغییر دسترسیها به موجودیت غیرفعال	☑		
		عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال	☑		
		سایر موارد	☐		
2	**محصول باید بر اساس مشخصه‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.**			☑	
	مشخصه‌هایی که بر اساس آن خط‌مشی‌ها تعریف می‌شوند، انتخاب گردد.	نقش‌ها و مجوزهای کاربر مجاز	☑		
		اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند.	☑		
		سایر موارد	☐		
3	**محصول باید بر اساس قاعده‌های عملیات بین موجودیت فعال تحت‌کنترل و موجودیت غیرفعال کنترل‌شده را مجاز نماید (این قاعده می‌تواند بدین شکل باشد که در لیست کنترل دسترسی، رکوردی وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف شده حق دسترسی به موجودیت غیرفعال را بدهد).**				☑	
4	**محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.**			☑	
	قوانین ممانعت از دسترسی مشخص شوند (در صورت اعمال قوانین بیشتر توسط محصول، در «سایر موارد» بیان شود).	تجاوز چندین نشست آغاز شده با نام کاربری مشابه ازمقدار آستانه[۲] از پیش تعریف شده	☑		
		سایر موارد	☐		
5	**محصول باید تضمین نماید تمام اطلاعات قبلی منابع یا در هنگام تخصیص و یا در هنگام آزادسازی آنها، غیرقابل دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد.**			☑	

[۲] Threshold

6	**محصول باید هنگام دریافت داده کاربری خط‌مشی کنترل دسترسی را اعمال نماید و برای این کار از مشخصه‌های امنیتی مرتبط با داده کاربری استفاده کند.**			☑	
	مشخصه‌های امنیتی مرتبط با داده کاربری که در هنگام ورود آن به محصول استفاده می‌شوند، مشخص شود (در صورتی که کنترل دسترسی برای موارد دیگری نیز صورت می‌گیرد، در قسمت «سایر موارد» بیان گردد).	نوع داده	☑		
		حجم و اندازه	☑		
		فرمت	☑		
		تعداد دفعات Import	☐		
		سایر موارد	☐		
7	**محصول باید از یک پروتکل امن برای انتقال داده استفاده نماید.** **این پروتکل ارتباط و همبستگی شفافی را بین داده کاربری دریافت شده و مشخصه‌های امنیتی آن فراهم می‌کند و همچنین از شنود و گمشدن داده حین انتقال جلوگیری می‌کند.**			☑	
8	**محصول باید هنگام انتقال داده به بیرون از محصول، خط‌مشی کنترل دسترسی اعمال نماید و برای این کار از مشخصه‌های امنیتی مرتبط با داده کاربری استفاده کند.**			☑	
	مشخصه‌های امنیتی مرتبط با داده کاربری که در هنگام خروج آن از محصول استفاده می‌شوند، مشخص شوند	نوع داده	☐		
		حجم و اندازه	☐		
		فرمت	☑		
		سایر موارد	☑		
9	**محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.**			☑	

	قوانینی که در هنگام خروج داده از محصول اعمال می‌شوند، مشخص شوند	مدیر سیستم باید خروج رکوردها را محدود نماید، به طوریکه کاربران محصول، قادر به خروج بدون هدف داده به خارج از محصول نباشند.	☑		
		سایر موارد	☐		
10	**محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره شدهدر محصول تشخیص دهد.**		☑		
	چگونگی تشخیص تغییر در داده‌های کاربری حساس، مشخص شود.	درهم شده[۳] داده‌های کاربری ذخیره شده، نگهداری می‌شود	☑		
		سایر موارد	☐		
11	**محصول باید در صورت تشخیص خطای صحت در داده‌ها، اقدامات مقابله‌ای زیر را انجام دهد.**		☑		
	اقدام مقابله‌ای در صورت تشخیص خطا، مشخص شود (وجود یک مورد لازم و کافی است)	ایجاد هشدار/اخطار برای نقش‌های مجاز	☐		
		تصحیح داده بر اساس مقادیر قبل	☐		
		سایر موارد	☑		

[۳] Hash

5-5- مدیریت امنیت

در این کلاس توانایی‌های محصول در مدیریت (حذف، تغییر، فعال کردن و ...) کارکردهای امنیتی (جمع‌آوری داده‌های سیستم، پیکربندی‌ها و ...) مورد بررسی قرار می‌گیرد. همچنین توانایی محصول در مدیریت نقش‌ها و دسترسی آنها برای اعمال مدیریت بر روی کارکردهای امنیتی سنجیده می‌شود.

شماره الزام	کلاس مدیریت امنیت				توضیحات
1	**محصول باید برای مدیر سیستم و هر کاربری که مجوز لازم را دارد،امکان فعالیتهای مدیریتی زیر را بر روی توابع و تمام کارکردهای مربوط به مدیریت محصول فراهم آورد.**			☑	
	فعالیت‌های مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند.	تعیین و تغییر رفتار	☑		
		غیرفعال نمودن	☑		
		فعال نمودن	☑		
		سایر موارد	☐		
2	**محصول باید با اعمال خط‌مشی کنترل دسترسی؛ امکان تغییر پیش‌فرض و سایر عملیات زیر را بر روی مشخصه‌های امنیتی الزام 7 از کلاس شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.**			☑	
	عملیات بر روی مشخصه‌های امنیتی که در محصول پشتیبانی می‌شوند، مشخص گردد.	پرس‌وجو	☑		
		تغییر	☑		
		حذف	☑		
		تغییر پیش‌فرض	☑		
		سایر موارد	☐		
3	**محصول باید برای داده‌های محصول، امکان کارکردهای زیر را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.**			☑	
	عملیات بر روی داده‌های محصول که	تغییر پیش‌فرض	☑		
		حذف نمودن	☑		

	در محصول پشتیبانی می‌شوند، مشخص شود.	پرس‌وجو	☑		
		مقداردهی	☑		
		ایجاد	☑		
		مشاهده	☑		
		سایر موارد	☐		
4	**محصول باید توانایی انجام کارکردهای زیر را داشته باشد.**			☑	
	در صورتی که هرکدام از موارد مطرح شده، توسط محصول قابل اجرا نیست، در قسمت توضیحات باید دلایل مطرح گردد.	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی	☑		
		پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی	☑		
		پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی	☑		
		مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول	☑		
		انتخاب زمان اجرای حفاظت از اطلاعات باقیمانده که می‌تولند در محصول قابل پیکربندی باشد. (برای مثال، زمان تخصیص و یا زمان آزادسازی منابع)	☐		
		ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول	☐		
		در نظر گرفتن یک عملیات از پیش تعیین شده پس از تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی نیز باشد.	☑		
		1. مدیریت حد آستانه برای تلاشهای ناموفق 2. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد.	☑		
		مدیریت معیارها برای تنظیم کلمات عبور	☑		
		1. مدیریت دادههای احراز هویت توسط مدیریا کاربر مربوطه 2. مدیریت یکسری عملیاتی که قبل از احراز شدن هویت کاربر انجام میشوند.	☑		
		1. مدیریت سازوکارهای احراز هویت	☑		

		2. مدیریت قوانین مرتبط با احراز هویت			
		مدیریت تغییرات و فرایندهایی مانند (اختصاص آدرسIP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می‌تواند قبل از شناسایی کاربر انجام دهد.	☑		
		مدیر مجاز می‌تولند مشخصه‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد.	☑		
		مدیریت مقادیر پیشفرض برای کنترل دسترسی محصول	☑		
		مدیریت نقشها در محصول	☑		
		مدیریت حداکثر تعداد مجاز نشستهای همزمانکاربران توسط مدیر	☑		
		مدیریت شرایط آغاز نشست توسط مدیر مجاز	☑		
		1. تعیین زمان غیرفعال بودن برای یک کاربرمشخص که پس از آن، نشست آن کاربر خاتمه یابد. 2. تعیین زمان پیشفرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد.	☑		
5	**محصول باید توانایی تعریف نقشهای مختلف را داشته باشد.**			☑	
	نقش‌هایی که در محصول پشتیبانی می‌شوند، مشخص گردد.	مدیر سیستم	☑		
		کاربر پیشرفته	☑		
		کاربر عادی	☑		
		سایر موارد	☐		
6	**محصول باید قادر باشد کاربران را به نقش‌های تعریف شده یا قابل تعریف مرتبط نماید، همچنین لازم است هر حساب کاربری تنها به یک نقش مرتبط شده باشد، اما ممکن است نقش‌ها تنها به یک کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند.**			☑	

5-6- حفاظت از توابع امنیتی محصول

در این کلاس، توانایی محصول در حفظ وضعیت امن در زمان رخ دادن شکست و همچنین حفاظت از داده‌ها هنگام تبادل بین اجزای محصول یا تبادل با موجودیت‌های دیگر، مورد بررسی قرار گرفته است.

شماره الزام	کلاس حفاظت از توابع امنیتی محصول				توضیحات
1	**محصول باید هنگام رخ دادن هرگونه شکست مانند از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول، در وضعیت امنی قرار گرفته و صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ نماید.**			☑	
	هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول حفظ می‌شود، مشخص گردد.	شکست‌های نرم‌افزاری	☑		
		شکست‌های سخت‌افزاری	☑		
2	**محصول باید از طریق فراهم نمودن بستر و زیرساخت امن، توانایی محافظت از افشاء یا تغییر داده، هنگام انتقال بین بخش‌های مجزای خود را داشته باشد.**			☑	
3	**در صورتی که محصول از محصولات امن IT استفاده می‌کند، بایدتفسیر سازگار و یکسانی را از داده امنیتی در زمان اشتراک گذاری آن بین خود و دیگر محصولات امن IT، فراهم آورد.**			☑	
	داده امنیتی قابل اشتراک گذاری که در محصول پشتیبانی می‌شوند، مشخص گردد.	داده‌های احراز هویت	☐		
		کلید	☐		
		امضای دیجیتال	☐		
		داده‌های ممیزی	☐		

		☑	سایر موارد	☐	
4	**محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین بایدمهره‌های زمانی معتبر، تولید یا استفاده نماید.**			☑	
	روش‌های ایجاد مهرهای زمانی معتبر انتخاب شود. (دیگر روشهای موجود در محصول، در قسمت «سایر موارد» بیان شود).	☐	گرفتن مهرهای زمانی از سرور NTP		
		☐	تنظیم مهرهای زمانی از طریق اینترنت		
		☑	تنظیم مهرهای زمانی به صورت پیشفرض (معتبر و عدم امکان دستکاری غیرمجاز)		
		☐	سایر موارد		
5	**محصول باید امکان به‌روزرسانی نرم افزار و میان افزار محصول رابرای مدیر سیستم فراهم نماید.**			☑	
	روش به‌روزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).	☑	به‌روز رسانی دستی		
		☐	جستجوی خودکار به روزرسانی ها		
		☐	به روزرسانی‌های خودکار		
		☐	به‌روزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل به‌روزرسانی		
6	**در صورت استفاده از به‌روزرسانی به روش خودکار، محصول بایدپیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، امکان احراز اصالت میان‌افزار یا نرم‌افزار را فراهم نماید.**			☐	
	سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی) به‌روزرسانی‌ها انتخاب گردد.	☐	امضاء دیجیتال		
		☐	درهم‌ساز منتشرشده		

5-7- تخصیص منابع

در این کلاس، به بررسی وضعیت عملکردهای محصول و منابع مورد استفاده توسط آن در زمانهای مختلف از جمله زمان شکست پرداخته می‌شود.

شماره الزام	کلاس تخصیص منابع		توضیحات
1	**محصول باید در زمان رخداد هرگونه شکست نرم‌افزاری؛ از عملکردکارکردهای اصلی محصول اطمینان حاصل نماید.**	☑	

5-8- دسترسی به محصول

در این کلاس توانایی محصول در مدیریت نشست‌های صورت گرفته شده توسط کاربر، ارزیابی می‌شود.

شماره الزام	کلاس دسترسی به محصول			توضیحات
1	**محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.**		☑	
2	**محصول باید کلیه نشست‌های تعاملی راه‌دور[۴] را پس از مدت زمانی که غیرفعال هستند (و می‌بایست توسط مدیر قابل تنظیم باشد)، خاتمه دهد.**		☑	
3	**محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.**		☑	
4	**در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس موارد زیر باشد.**		☑	
	انتخاب یک مورد لازم و کافی است.	روز	☑	
		زمان	☑	
		سایر موارد	☐	
5	**در صورت برقراری نشست به طور موفقیت آمیز، محصول باید قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست بر اساس موارد زیر و تعداد تلاش‌های ناموفق تا آخرین ایجاد نشست موفقیت‌آمیز باشد.**		☑	
	انتخاب یک مورد لازم و کافی است.	روز	☑	
		زمان	☑	
		سایر موارد	☐	
6	**محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.**		☑	

[۴] Remote

7	**محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.**			☑	
	پارامترهای موجود برای جلوگیری از نشست، مشخص شوند (وجود یک مورد لازم و کافی است).	مکان	☑		
		شماره پورت	☐		
		روز	☐		
		زمان	☑		
		سایر موارد	☐		

5-9- کانال‌ها/مسیرهای مورد اعتماد

در این کلاس به بررسی پروتکل‌های امنی که برای برقراری کانال/مسیر مورد اعتماد، بین محصول و موجودیت‌های IT خارجی، یا بین اجزای محصول، استفاده می‌شوند، پرداخته می‌شود.

<table>
<tr><th>شماره الزام</th><th colspan="4">کلاس کانال‌ها/مسیرهای مورد اعتماد</th><th>توضیحات</th></tr>
<tr><td rowspan="3">1</td><td colspan="3">محصول باید قادر باشد مسیر ارتباطی امنی بین خود، کاربران و دیگر محصولات IT فراهم نماید که به طور منطقی از دیگر کانال‌ها متمایز باشد. سپس از طریق این کانال احراز هویت را انجام داده و از تغییر و افشاء داده تبادلی حفاظت نموده و تغییرات را تشخیص دهد. در صورت انتخاب مورد HTTPS، رعایت الزام 1-6- و در صورت انتخاب TLS، رعایت الزامات 2-6- تا 4-6- که در بخش 6- بیان گردیده است، الزامی است.</td><td>☑</td><td rowspan="3"></td></tr>
<tr><td rowspan="2">پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد.</td><td>HTTPS</td><td>☑</td></tr>
<tr><td>TLS</td><td>☐</td></tr>
<tr><td>2</td><td colspan="3">محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.</td><td>☑</td><td></td></tr>
<tr><td>3</td><td colspan="3">محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.</td><td>☑</td><td></td></tr>
</table>

6- الزامات امنیتی مبتنی بر انتخاب

این بخش به بیان الزاماتی می‌پردازد که رعایت آنها وابسته به برخی از الزاماتی است که در بخش‌های پیشین بیان شده است. برای مثال اگر در الزامات مربوط به کلاس کانال امن، پروتکل HTTPS انتخاب شود، آنگاه رعایت الزامات HTTPS که در این بخش بیان شده است، اجباری می‌گردد.

6-1- پروتکل HTTPS

شماره الزام	کلاس کانال‌ها/مسیرهای مورد اعتماد				توضیحات
1	**محصول باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کند.**			☑	
2	**محصول باید پروتکل HTTPS را با استفاده از TLS اجرا کند.**			☑	
3	**در صورتی که گواهی‌نامه ارائه شده از سمت دیگر محصولات IT (درهنگام برقراری ارتباط) نامعتبر باشد، محصول باید بر اساس موارد زیر عمل نماید.** **اعتبارسنجی گواهی‌نامه بر اساس الزامات بخش 5-6- انجام می‌شود که در این صورت الزامات بخش 5-6- الزامی است.**			☑	
		محصول تنها از موارد بیان شده می‌تواند استفاده نماید.	اتصال را برقرار نکند.	☑	
			برای برقراری اتصال درخواست مجوز کند.	☐	

6-2- پروتکل TLS Client

شماره الزام	پروتکل TLS Client					توضیحات
1	**محصول باید TLS 1.2 (RFC 5246) و/یا TLS 1.1 (RFC 4346) را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه رمزهای زیر پیاده‌سازی نماید.**				☑	
		مجموعه رمز مورد استفاده و پیاده‌سازی شده	TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	☐		
			TLS_RSA_WITH_AES_192_CBC_SHA	☐		

	محصول، انتخاب گردد.	مطابق با RFC 3268			
		TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	☐		
		TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	☐		
		TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268	☐		
		TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	☐		
		TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	☐		
		TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492	☐		
		TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	☐		
		TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	☐		
		TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492	☐		
		TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	☐		
		TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246	☐		
		TLS_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246	☐		
		TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246	☐		
		TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246	☐		
		TLS_DHE_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246	☐		
		TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246	☐		

		☐	TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288		
		☐	TLS_RSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5288		
		☐	TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288		
		☐	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA384 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289		
		☑	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289		
		☑	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289		
		☐	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289		
	☑	**محصول باید مطابقت شناسه ارائه شده با شناسه مرجع را با توجه به بخش 6 از RFC 6125، تأیید نماید.**			2

3	**محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد؛ بنابراین اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید بر اساس موارد زیر رفتار نماید.**			☑	
	در صورت پشتیبانی ازاقدامات دیگر، در «سایر موارد» بیان گردد.	ارتباط را برقرار نکند	☑		
		برای برقراری ارتباط درخواست مجوز کند	☐		
		سایر موارد	☐		
4	**محصول باید در پیام ClientHello برای استفاده از منحنی‌ها، بر اساس موارد زیر عمل نماید.**			☑	
	در صورت که محصول از منحنی استفاده می‌نماید، طول کلید باید مشخص گردد.	Supported Elliptic Curves Extension را ارائه نکند	☐		
		Supported Elliptic Curves Extension را به همراه NISTهای Curve secp256r1 یا secp384r1 یا secp521r1 ارائه نماید	☑		
		هیچ منحنی دیگری	☐		

3-6- پروتکل TLS Server

شماره الزام	پروتکل TLS Server				توضیحات
5	**محصول باید TLS 1.2 (RFC 5246) را پیاده‌سازی کند. همچنین محصول باید TLS رابا پشتیبانی از مجموعه رمزهای زیر پیاده‌سازی نماید.**			☑	
	مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.	TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	☐		
		TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	☐		
		TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	☐		

		☐	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492		
		☐	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492		
			TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492		
		☐	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492		
		☐	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492		
		☐	TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246		
		☐	TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246		
		☐	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246		
		☐	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246		
		☐	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289		
		☑	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289		
		☑	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289		
	☑	**محصول باید اتصالهای کاربرانی که درخواست TLS1.0، SSL3.0، SSL2.0 و SSL1.0 TLS1.1 دارند را رد نماید.**		6	

7	**محصول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید.**			☑	
	در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.	استفاده از RSA با اندازه کلید 2048 یا 3072 یا 4096 بیت	☐		
		پازامترهای ECDH با استفاده از NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگری	☑		
		پارامترهای دیفی- هلمن با اندازه کلید 2048 یا 3072 بیت	☐		

4-6- پروتکل TLS مشترک کلاینت و سرور

لازم به ذکر است که الزاماتی که با عنوان پروتکل‌های TLS Server و TLS Client مطرح شده است، برای مباحث مرتبط به احراز هویت TLS Server و TLS Client نیز مطرح می‌گردد. در این بخش چند الزام که برای احراز هویت این پروتکل‌ها مطرح می‌گردد و برای هر دوی کلاینت و سرور نیز یکسان است و باید برای هر کدام مورد بررسی قرار گیرد، آورده شده است.

شماره الزام	پروتکل TLS مشترک کلاینت و سرور		توضیحات
1	**محصول باید احراز هویت دوطرفه کلاینت‌ها/سرورهای TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید.**	☐	
2	**محصول در صورت مطابقت نداشتن نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه از شناساننده[5] کلاینت مورد انتظار بوده است، نباید کانال امن را برقرار سازد.**	☐	

[5] Identifier

5-6- اعتبارسنجی گواهی‌نامه

شماره الزام	شناسایی و احراز هویت				توضیحات
1	**محصول باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند.**			☑	
		تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.	☑		
		مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.	☑		
		محصول باید برای تأیید مسیر یک گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم شده است.	☑		
	روش‌های تأیید وضعیت فسخ گواهی‌نامه	پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص شده در RFC 696	☐		
		لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش 6.3	☐		
		لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش 5	☐		
		هیچ روش فسخ دیگری	☐		
	قوانین تأیید فیلد extendedKeyUsage	گواهی‌نامه‌های مورد استفاده برای تأیید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی باید هدف «Code Signing» (id-kp3 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.	☐		
		گواهی‌نامه‌های سرور ارائه شده برای TLS باید هدف «Server Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.	☑		
		گواهی‌نامه‌های کلاینت ارائه شده برای TLS باید هدف «Client Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.2)	☐		

			را در فیلد extendedKeyUsage خود داشته باشند.		
		☐	گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ OCSP باید «OCSP Signing» (id-pk9 با OID 1.3.6.1.5.5.7.3.9) را در فیلد extendedKeyUsage خود داشته باشند.		
2	**محصول باید تنها در صورتی که افزونه مربوط به basicConstraints از پیش تنظیم شده باشد و همچنین، پرچم CA به حالت «TRUE» تنظیم شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA بپذیرد.**			☑	
3	**محصول باید جهت پشتیبانی احراز هویت برای موارد زیر از گواهی‌نامه‌های X509v3 تعریف شده در RFC 5280 استفاده کند.**			☑	
	در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.	☑	HTTPS		
		☐	TLS		
		☐	امضای کد برای به‌روزرسانی‌های نرم‌افزار سیستم		
		☐	امضای کد برای تأیید یکپارچگی		
		☐	سایر موارد		