به نام خدا

پروفایل حفاظتی
سامانه مدیریت محتوی/پرتال

مهر ۹۵

نسخه ۱,۰

فهرست

۱ مقدمه

در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه‌دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی که در این سند برای برآورده نمودن الزامات ارائه‌شده‌اند را در محصول خود فراهم نمایند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد نمود. مرکز افتا با مشارکت سازمان فناوری اطلاعات این سند را بر اساس سند نظام ارزیابی امنیتی و مطابق با استاندارد IRISI/ISO 15408 V3.1R4 در راستای این هدف تهیه نموده است. این پروفایل حفاظتی، به بیان الزامات سامانه‌های مدیریت محتوی/پرتال می‌پردازد.

۲ اصطلاحات

مستند: به هر سند حاوی اطلاعات که برای اجرا و پشتیبانی عملیات و فعالیت‌های سازمانی استفاده می‌شوند، مستند گفته می‌شود.

رکورد: مستندی که اطلاعات فعالیت‌ها، رویدادها و نتایج حاصله را نگهداری می‌کند؛ به عبارت دیگر یک رکورد، مستندی است که مدرک انجام یک فعالیت مشخص است. یک رکورد می‌تواند شامل دو یا چند مستند باشد.

رکورد ممیزی: رکوردی که حاوی اطلاعات رویدادهایی است که برای ممیزی سامانه‌های مدیریت محتوی/پرتال‌ها نیاز است و در محل ذخیره‌سازی ممیزی، ذخیره می‌شود.

داده‌های کاربری ذخیره‌شده: فایل‌های داده و اطلاعاتی هستند که توسط کاربر ایجاد و ذخیره می‌شوند. این داده‌ها می‌تواند شامل خبر، آلبوم تصاویر، رکوردهای فرم‌های فرم ساز باشد.

موجودیت فعال: موجودیتی در محصول که عملیاتی را بر روی موجودیت‌های غیرفعال انجام می‌دهد. همانند نقش‌هایی همچون مدیر، کاربر نهایی و غیره.

موجودیت غیرفعال: موجودیتی در محصول، که حاوی اطلاعات است و یا اطلاعات را دریافت می‌نماید و توسط موجودیت‌های فعال، عملیاتی بر روی آن انجام می‌گیرد. همانند فهرست کردن رکوردها توسط مدیر سیستم، حذف فایل‌ها توسط مهاجم. (رکوردها و فایل‌ها موجودیت‌های غیرفعال هستند.)

مشخصه‌های موجودیت فعال: مشخصه‌های هر موجودیت فعال از قبیل نام کاربری، کلمه عبور، آدرس IP کاربر می‌تواند باشد.

مشخصه‌های موجودیت غیرفعال: مشخصه‌های هر موجودیت غیرفعال از قبیل نوع، نام و اندازه مستند می‌تواند باشد.

مشخصه‌های امنیتی: می‌تواند شامل مشخصه‌های امنیتی موجودیت فعال (از قبیل شناسه کاربر، کلمه عبور، نقش‌های کاربر، جزئیات واسط کاربر، پیشینه احراز هویت) و یا مشخصه‌های امنیتی غیرفعال (از قبیل نوع، نام و اندازه مستند) باشد.

داده‌های محصول: می‌تواند شامل داده‌های ممیزی، کلیدها، مقادیر تنظیمات محصول و داده‌های احراز هویت و از این نوع داده‌ها باشد.

انتخاب: «انتخاب» یکی از عملیاتی است که در الزامات پروفایل جهت منعطف شدن پروفایل به منظور تدوین سند هدف امنیتی توسط تولیدکننده آمده است. در الزاماتی با این عملیات نویسنده با توجه به کارکرد امنیتی محصول یک یا چند مورد از موارد ذکرشده در الزام را انتخاب می‌نماید و به عنوان ادعا در بخش الزامات کارکردی سند هدف امنیتی ذکر می‌نماید.

اختصاص: «اختصاص» یکی از عملیاتی است که در الزامات پروفایل جهت منعطف شدن پروفایل به منظور تدوین سند هدف امنیتی توسط تولیدکننده آمده است. در الزاماتی با این عملیات نویسنده با توجه به کارکرد امنیتی محصول، مقدار یا پارامتر مشخصی را اختصاص می‌دهد.

۳ شرح محصول

محصول مورد ارزیابی، سامانه‌های مبتنی بر شبکه است که برای مدیریت رکوردها و مستندات استفاده می‌شود. از جمله وظایف سامانه‌ها می‌توان به جمع‌آوری، ذخیره و توزیع مستندات، پیام‌ها و فرم‌های ارتباطات اداری بین افراد اشاره نمود.

به‌طور کلی سامانه مدیریت محتوی/پرتال‌ها برای رکوردها و مستندات الکترونیکی از فعالیت‌های زیر استفاده می‌کند:

- ثبت رکوردهای الکترونیکی
- مدیریت گردش کار رکوردهای الکترونیکی
- ایجاد و مدیریت فرآیندهای آرشیو
- انجام امور جستجو و گزارش دهی
- قابلیت مدیریت کاربران
- پشتیبانی از سازوکارهای امن‌سازی ارتباطات
- سازوکارهای احراز هویت و کنترل دسترسی

محصول اعمال فوق را با کمک مؤلفه‌های نشان داده‌شده در شکل ۱ انجام می‌دهد.

شکل ۱: مؤلفه‌های سامانه‌های مدیریت محتوی/ پرتال

۳,۱ مؤلفه‌های محیط عملیاتی

یک سامانه، برنامه اجرایی بر روی بستر شبکه است و با مؤلفه‌های شبکه در تعامل است که بر روی سیستم‌عامل اجرایی در محیط شبکه اجرا می‌گردد. محصول با واحد/واحدهای ذخیره‌سازی به منظور نگهداری رکوردها و با مؤلفه‌های ممیزی به منظور نگهداری رکوردهای ممیزی در تعامل است؛ در ادامه، این مؤلفه‌ها با جزئیات شرح داده می‌شوند.

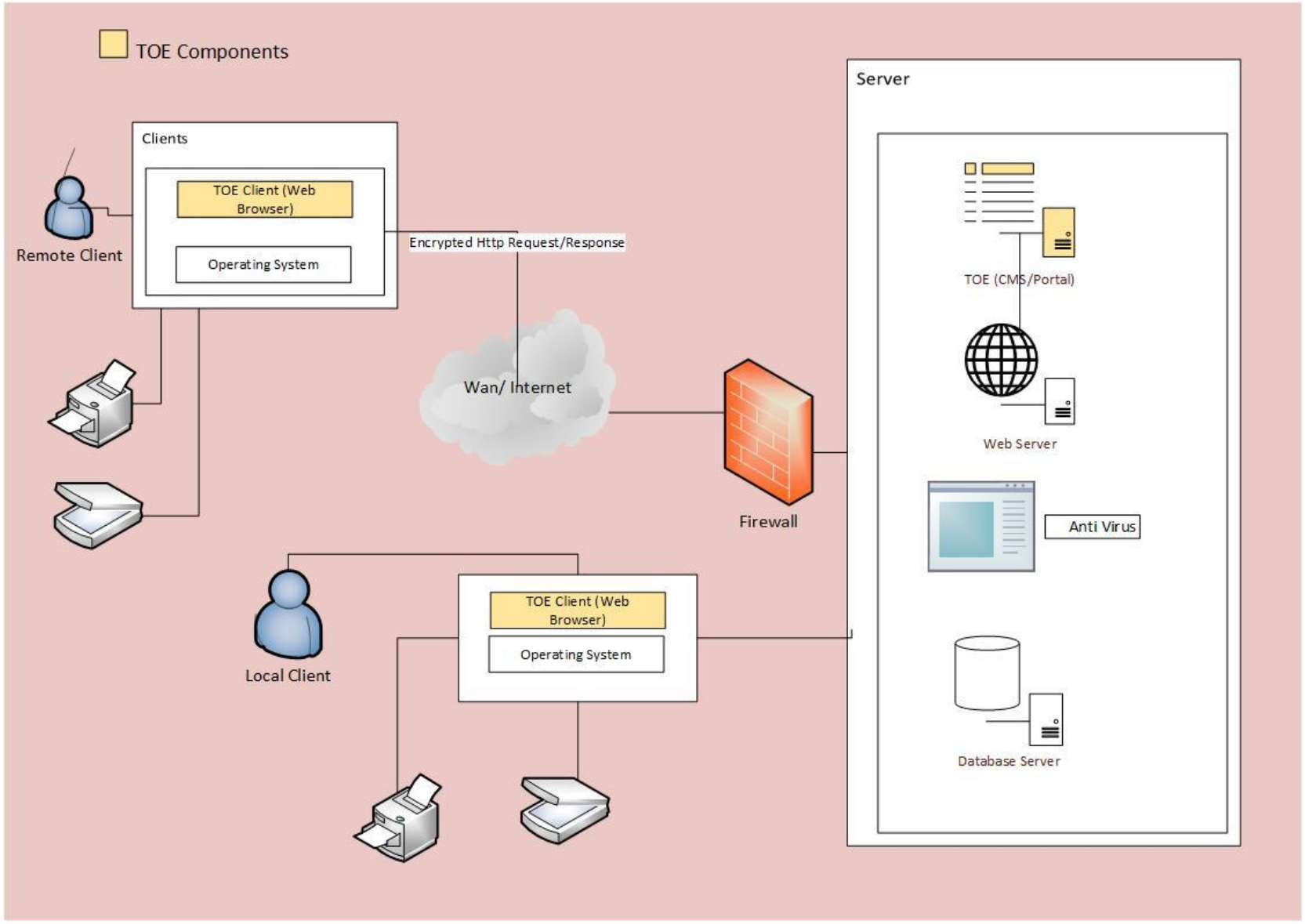
محیط عملیاتی محصول شامل مؤلفه‌های نرم‌افزاری و سخت‌افزاری و همچنین ویژگی‌های کارکردی و امنیتی اصلی است که در این سند پوشش داده‌شده‌اند. شکل ۲ بیانگر سخت‌افزار و نرم‌افزارهایی است که محصول با آن‌ها در تعامل است، این شکل چگونگی تعاملات محصول با محیط عملیاتی را نمایش می‌دهد:

سرور: سرور مؤلفه سخت‌افزاری است که مؤلفه سروری محصول بر روی آن اجرا می‌گردد. سرور می‌تواند به صورت فیزیکی یا مجازی باشد، در هر دو حالت امنیت سرور به امنیت محصول بستگی دارد. پیکربندی و قابلیت‌های سرور می‌تواند با توجه به تعداد کاربران، تعداد اتصالات و غیره متفاوت باشد.

سیستم کاربر: سخت‌افزار و سیستم‌عاملی است که به کاربران اجازه دسترسی به محصول را می‌دهد. این مؤلفه معمولاً یک کامپیوتر بوده ولی می‌تواند یک تبلت یا گوشی هوشمند نیز باشد، در این پروفایل حفاظتی فرض شده که کلاینت یک کامپیوتر است. دو نوع کلاینت وجود دارد. یکی برای کاربر پایانی و نوع دیگر برای کاربرانی که رکوردها و مستندات را به داخل محصول وارد می‌نمایند. اتصالات بین کلاینت‌ها و مؤلفه‌های مرکزی محصول می‌تواند به صورت اینترنت، اینترانت یا VPN باشد.

سیستم‌عامل: محصول بر روی یک سیستم‌عامل اجرا می‌شود و ارتباطات بین محصول و واحد ذخیره‌سازی، واحد رکوردهای ممیزی، مؤلفه‌های شبکه و سرور توسط سیستم‌عامل ارائه می‌شود.

مؤلفه‌های شبکه: محصول به واسطه سیستم‌عامل و سرور با مؤلفه‌های شبکه در تعامل است. لازم است اتصالات شبکه بین کلاینت‌ها و سرور محصول به صورت امن باشد. کلاینت محصول قادر به انجام اقداماتی همانند چاپ، اسکن و غیره است. اتصالات بین این مؤلفه‌ها و سرور معمولاً به صورت یک شبکه محلی است.



شکل ۲: محیط عملیاتی محصول

پایگاه داده: محصول با یک پایگاه داده برای حفظ و نگهداری داده‌های خود در تعامل نزدیک است. رکوردها و مستندات می‌توانند در پایگاه داده یا به صورت مجزا حفظ و نگهداری شوند. در زمان نیاز به یک مجموعه داده خاص، یک درخواست به پایگاه داده ارسال و نتایج آن گرفته می‌شود.

واحد ذخیره‌سازی مستندات و رکوردها: رکوردها و مستندات می‌توانند به صورت مجزا در سمت سروری که محصول بر روی آن اجرا می‌گردد باقی مانده تا محصول به آسانی تحت تأثیر آسیب‌پذیری امنیتی بالقوه در واحد ذخیره‌سازی قرار نگیرد.

واحد ذخیره رکوردهای ممیزی: همانند واحدهای ذخیره‌سازی، واحد رکوردهای ممیزی در سمت سروری قرار می‌گیرد که محصول بر روی آن اجرا می‌گردد. این واحد می‌تواند به صورت مؤلفه مجزا و یا بخشی از واحد ذخیره‌سازی باشد.

اسکنر و درایور آن: کاربران مجاز برای اسکن نمودن، رکوردها و مستنداتی که به شکل کاغذی دریافت می‌کنند را اسکن می‌نماید.

پرینتر: مؤلفه‌ای است که به کاربران محصول مطابق با مجوز کاربر، اجازه چاپ هر رکورد یا مستندی را می‌دهند.

۳,۲ انواع کاربران

حداقل سه دسته کاربر برای محصول وجود دارد:

- کاربر عمومی
- کاربر عادی
- مدیر سیستم

علاوه بر نقش‌های فهرست شده در بالا، محصول ممکن است دارای نقش‌های دیگری نیز باشد. در صورت وجود نقش‌های دیگر لازم است در سند هدف امنیتی ذکر گردد.

کاربر عمومی: افراد بازدیدکننده از صفحات وب و پرتال‌ها که مجوزی برای درج و یا ویرایش داده‌ها ندارند.

کاربر عادی: کاربر عادی از محصول به صورت یک جعبه سیاه استفاده می‌نماید و قادر به مدیریت داده‌های تحت مالکیتش است. کاربر عادی در صورت داشتن مجوز می‌تواند رکوردها و مستندات را جستجو، فهرست و مشاهده نماید. علاوه بر آن کاربر عادی می‌تواند سند یا رکورد جدیدی ایجاد نماید یا سند و رکوردی که مالک آن است را حذف نماید. این نوع کاربر می‌تواند مستندات را بایگانی نماید و باید قادر به دسترسی اسناد بایگانی‌شده خود باشد.

مدیر سیستم: مدیر، دارای مجوز خاص برای مدیریت محصول است. مدیر سیستم می‌تواند یک نفر باشد یا برای بخش‌های مختلف محصول مدیران مختلفی وجود داشته باشد، همانند مدیر پایگاه داده، مدیر شبکه، مدیر برنامه کاربردی و غیره. همچنین مدیر دارای سطح دسترسی کامل برای دسترسی به برنامه کاربردی، پایگاه داده، فایل سیستم و دیگر موجودیت‌ها است.

۳,۳ ویژگی‌های امنیتی محصول

احراز هویت و مجوزدهی: عملیات احراز هویت و مجوزدهی باید به صورت اثرگذاری انجام شود. احراز هویت به طور کلی با بررسی و تائید نام کاربری و کلمه عبور صورت می‌گیرد. لازم به ذکر است برای مدیریت کلمه عبورهای مورد استفاده باید روال‌های امن وجود داشته باشد. در صورتی که محصول به سطح بالایی از امنیت نیاز داشته باشد، از یک سازوکار احراز هویت دیگر یا ترکیبی از دو یا بیشتر از دو سازوکار استفاده می‌شود. از جمله سازوکارهای احراز هویت می‌توان به وارسی نام کاربری و کلمه عبور، وارسی SMS، احراز هویت از طریق یک برنامه موبایل، گواهی دیجیتال، وارسی بیومتریک و توکن سخت‌افزاری اشاره نمود.

کنترل دسترسی: محصول قابلیت محدود کردن دسترسی را دارد؛ بطوریکه تنها موجودیت‌های مجاز، امکان دسترسی به داده و کارکردهای محصول را دارا هستند. برای کاربران مجاز، کنترل دسترسی معمولاً با استفاده از داده احراز هویت انجام می‌گیرد. همچنین محصول ممکن است آدرس‌های IP اتصالات فعال را کنترل نماید و تنها به آدرس‌های IP از پیش تعریف‌شده در یک بازه زمانی خاص برای عملیات حساس اجازه اتصال دهد.

ممیزی: محصول به صورت خودکار، رکوردهای ممیزی را به منظور ردیابی و کنترل فعالیت‌های کاربر بر روی دارایی‌ها، تغییرات کنترل دسترسی و پیکربندی جمع‌آوری می‌نماید. محتوای رکوردهای ممیزی، روش‌های حفظ رکورد و فواصل نگهداری را می‌توان توسط رابط گرافیکی محصول پیکربندی نمود. هیچ فردی جز افرادی که محصول، مجاز نموده همچون مدیر، امکان تغییر یا حذف محتویات رکوردهای ممیزی را ندارند.

مدیریت: محصول، برای مدیریت کاربران و دسترسی‌ها واسط‌های مدیریتی لازم را فراهم می‌نماید. سرعت و دقت این واسط‌ها در تصمیم‌گیری در طول یک رخداد امنیتی بسیار مهم است.

صحت رکوردها و بررسی منابع: حذف یا تغییر هر رکورد توسط محصول مجاز نمی‌باشد؛ بنابراین، دسترسی و تغییر سند و/یا فراداده[۱] آن باید محدود گردد. صحت رکوردهای ذخیره‌شده، توسط روشی مانند امضای دیجیتال فراهم می‌گردد.

پشتیبان‌گیری: عملیات پشتیبان‌گیری بر روی داده، مستندات و رکوردهای ممیزی که محصول از آن‌ها محافظت می‌نماید، می‌تواند توسط خود محصول و یا یک ابزار خارجی که بدین منظور استفاده می‌گردد، صورت گیرد. عملیات پشتیبان نسبت به عدم از دست رفتن داده اطمینان می‌دهد.

کنترل گردش مستندات و اطلاعات: حداکثر اندازه فایل می‌تواند به صورت پویا برای هر نوع سند تعریف شود. محصول، فضای خالی ذخیره‌سازی را در نظر گرفته و در برابر سرریز ذخیره‌سازی اقدامات احتیاطی لازم را اتخاذ می‌نماید. همچنین تنها کاربران مجاز، مجوز صدور و ارسال هر رکورد یا سندی را دارند.

درهم‌سازی/رمز نمودن داده‌ی حساس: مثالی از داده‌ی حساس کلمه‌های عبور یا رکوردهای محرمانه است. داده‌ی حساس بر روی محصول به صورت واضح ذخیره نمی‌شوند و با سازوکاری از آن‌ها حفاظت می‌شود. همچنین باید رکوردهای محرمانه به صورت رمز شده نگهداری شود. ارتباط بین کاربر و سرور باید با استفاده از رمزنگاری امن شود تا از افشای محتوی رکوردها جلوگیری گردد. روش درهم‌سازی و رمزنگاری انتخاب‌شده باید به اندازه کافی قوی باشد طوری که توسط فناوری‌های امروزی در یک بازه‌ی منطقی قابل شکسته شدن نباشد.

[۱] MetaData

۴ مسائل امنیتی

۴,۱ تهدیدات

تهدیدات	توضیحات
دسترسی غیرمجاز	مهاجم می‌تواند با استفاده از هویت جعلی/سرقتی به محصول دسترسی پیدا نماید. این دسترسی می‌تواند با استفاده 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 آزمون» بر روی سیستم واقعی به محصول دسترسی پیدا نماید. همچنین مهاجم می‌تواند از داده‌ی باقیمانده کاربر قبلی/کاربر فعال یا داده باقیمانده که در طول ارتباطات و عملیات داخلی یا خارجی ایجاد شده سود ببرد. این داده‌های می‌توانند داده‌های حساس مرتبط با کاربران محصول یا خود محصول باشند. مهاجم می‌تواند با دسترسی به داده‌ها و خود محصول سبب آسیب شود.
تغییر غیرمجاز	رکوردهای مستندات و داده‌های حفاظت‌شده توسط محصول، می‌تواند بدون مجوز تغییر یابند. مهاجم می‌تواند با گمراه نمودن مدیر سیستم، واردکننده داده یا کاربر عادی، داده کاربر یا داده محصول را به دست آورد. همچنین می‌تواند از طرق غیرقانونی خود را مجاز نشان داده و مستندات و رکوردها یا دیگر داده‌های حفاظت‌شده توسط محصول را تغییر دهد. این تهدید زمانی رخ می‌دهد که صحت رکوردها و مستندات تضمین‌شده نمی‌باشد. مهاجم ممکن است درصدد 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 است 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) همچنین می‌تواند با اضافه نمودن تعداد رکوردهای بالا یا رکوردهای غلط به دنباله ممیزی، مدیر سیستم را گمراه نماید.

تهدیدات	توضیحات
افشای اطلاعات	داده‌های 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 واردکننده داده می‌تواند عمداً یا غیر عمد موجب افشاء اطلاعات محرمانه گردد.
انکار سرویس	مهاجم می‌تواند سبب گردد محصول در یک بازه‌ی زمانی، غیرقابل‌دسترسی یا بدون استفاده گردد. این امر معمولاً با ارسال درخواست-های بسیار در یک بازه زمانی کوتاه صورت می‌گیرد طوری که محصول قادر به پاسخ نخواهد بود. نوع ساده‌ای از حمله شامل ارسال درخواست‌های بسیار از یک رنج IP مشخص است که به نام حمله DoS شناخته می‌شود. نوع دیگر پیشرفته‌تر حمله DDoS است که از BOTNET استفاده می‌نماید و محدودیتی بر روی آدرس IP ورودی ندارد.
داده‌های 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 داده‌های مخرب و تغییر داده‌ها، 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 تبادل 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 نماید.

۴,۲ خط‌مشی امنیتی

خط‌مشی‌ها	توضیحات
ممیزی کامل	تمام رخدادها بر روی محیط کاری محصول باید ثبت گردد، رکوردها محافظت‌شده هستند و معمولاً به منظور تشخیص و جلوگیری از نقض امنیتی بررسی می‌شوند.
پیکربندی مناسب	پیکربندی پیش‌فرض محصول و مؤلفه‌های تعاملی تحت کنترل محصول باید تغییر یابند. طوری که 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 خط‌مشی سازمانی بسیار مهم است به خصوص زمانی که محصول یا هر مؤلفه 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.

۴,۳ فرضیات

فرضیات	توضیحات
کاربران آموزش‌دیده	فرض شده است که تمام کاربران مسئول نصب، پیکربندی و مدیریت محصول آموزش کافی دیده‌اند و قوانین را دنبال می‌نمایند.
توسعه‌دهندگان آموزش‌دیده	فرض شده است که افراد مسئول توسعه محصول (همانند برنامه‌نویس، طراح، غیره) افراد مورد اعتمادی بوده و بدون هیچ نیت مخربی قوانین را دنبال می‌نمایند.
توسعه‌دهندگان مجرب	فرض شده است تمام کارمندان توسعه‌دهنده محصول در زمینه امنیت تجربه کافی داشته و تمام راهکارهای لازم برای مقابله با تمام آسیب‌پذیری‌های شناخته‌شده را اتخاذ می‌نمایند.

فرضیات	توضیحات
محیط امن	فرض شده است که تمام پیش‌بینی‌های محیطی و فیزیکی لازم برای محیط کاری محصول در نظر گرفته‌شده است. فرض شده است که دسترسی به محیط کاری محصول به طور مناسب محدودشده و رکوردهای دسترسی برای یک بازه زمانی منطقی حفظ‌شده است. فرض شده است که سازوکاری وجود دارد تا رکوردها و مستندات که غیرقانونی 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 واردشده توسط محصول، واحد ذخیره‌سازی و دیگر مؤلفه‌های سخت‌افزاری دارای پشتیبان مناسبی هستند و بنا بر وجود نسخه پشتیبان هیچ داده‌ای 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 اتخاذشده است. فرآیند تحویل توسط نهادهای مطمئن و واجد شرایط صورت می‌گیرد.
انکار سرویس توزیع‌شده	فرض شده است که اقدامات امنیتی لازم در قبال حملات DDoS اتخاذ می‌شود.

۵ اهداف امنیتی

۵,۱ 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 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 طوری که کاربران را ملزم به استفاده از کلمه‌های عبور قدرتمند نماید. محصول باید اجازه طبقه‌بندی رکوردها و مستندات را دهد و با توجه به طبقه‌بندی 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 مدیر سیستم را با استفاده از سازوکارهای قوی‌تری احراز هویت نماید. از جمله سازوکارها می‌توان به محدود نمودن رنج IP، محدود نمودن بازه زمانی، احراز هویت بر اساس توکن، احراز هویت چند فاکتوری و ترکیبی از این روش‌ها اشاره نمود.
کنترل جریان داده	محصول باید گردش داده‌های غیرمجاز را کنترل و مدیریت نماید. داده‌های ورودی باید تحت فیلتر محتوایی قرار گیرند. تعداد بالایی از درخواست‌ها از یک رنج IP تعریف‌شده 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.

هدف امنیتی	توضیحات
صحت داده	محصول باید نسبت به صحت داده ممیزی و داده‌ی رکورد با تشخیص هرگونه تغییر بر روی این داده‌ها اطمینان حاصل نماید و در صورت رخ دادن هرگونه تغییر اقدامات لازم را انجام دهد.
مدیریت	محصول باید تمام کارکردها را برای مدیر سیستم به منظور مدیریت امن و کارآمد 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.
مدیریت خطا	محصول باید صورت امن و کارآمد سازوکار مدیریت خطا را فراهم نماید. خطاهای رخ‌داده 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 رخ‌داده مطلع گردد. جزئیات خطای برگشتی باید منجر به اقدام مناسب مدیر گردد. محصول در صورت رخ دادن خطا باید وضعیت امنی را حفظ نماید.
مدیریت داده‌های باقیمانده	محصول باید اطمینان دهد که هر داده‌ی باقیمانده از محصول زمانی که دیگر به آن نیاز نیست از محصول برداشته‌شده 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.

۵,۲ اهداف امنیتی برای محیط عملیاتی

اهداف امنیتی محیطی	توضیحات
محیط امن	محیط عملیاتی محصول باید نسبت به امنیت محیطی و فیزیکی محصول اطمینان دهد. دسترسی غیرمجاز باید محدود گردیده و تمام مؤلفه‌ها در محیط عملیاتی باید امن گردد و تنها افراد مجاز باید اجازه دسترسی به مؤلفه‌های حساس را داشته باشند. محیط عملیاتی محصول باید اطمینان دهد محصول به طور مناسب در قبال هر حمله DoS یا DDoS محافظت‌شده است. از جمله سازوکارهای حفاظتی می‌توان به غیرفعال نمودن سرویس‌ها، پورت‌ها و دیگر موارد استفاده‌شده اشاره نمود.
ارتباطات	محیط عملیاتی باید برای ارتباط محصول با ابزارها و/یا رسانه‌های ارتباطی امن فراهم گردد.
کاربران آموزش‌دیده	محیط عملیاتی باید اطمینان دهد تمام کاربران استفاده‌کننده از کارکردهای محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه‌دهندگان آموزش‌دیده	محیط عملیاتی محصول باید اطمینان دهد تمام کاربران توسعه‌دهنده محصول آموزش کافی دیده و الزامات امنیتی را برآورده می‌نمایند.
توسعه‌دهندگان مجرب	محیط عملیاتی محصول باید اطمینان دهد تمام کارمندان توسعه‌دهنده‌ی محصول در زمینه امنیت تجربه داشته و آن‌ها اقدامات مقابله‌ای لازم برای تمام آسیب‌پذیری‌های امنیتی شناخته‌شده را در نظر می‌گیرد.
ممیزی کامل	محیط عملیاتی محصول باید اطمینان دهد که هر رخداد مرتبط امنیتی برای مؤلفه‌های غیر از محصول نیز مورد ممیزی قرار می‌گیرند. این هدف امنیتی مکمل هدف ممیزی برای محیط عملیاتی محصول است. 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 استفاده‌شده به منظور آزمون باید پاک یا غیرقابل دسترس گردند.

اهداف امنیتی محیطی	توضیحات
پشتیبان‌گیری مناسب	نسخه پشتیبان باید ایجاد گردیده و برای یک بازه زمانی منطقی تمام داده‌های باقیمانده در محیط عملیاتی محصول را حفظ نماید. برای این منظور ممکن است از روال‌های از پیش تعریف‌شده استفاده گردد. همچنین باید از واحدهای ذخیره‌سازی و دیگر مؤلفه‌های سخت‌افزاری نیز نسخه پشتیبان تهیه گردد.

۶ الزامات کارکرد امنیتی

الزامات کارکرد امنیتی محصول مطابق با جدول زیر هستند. در ادامه هر یک از الزامات شرح و بسط داده‌شده‌اند.

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**تولید داده ممیزی ۱**	FAU_GEN.1.1
۲	**تولید داده ممیزی ۲**	FAU_GEN.1.2
۳	**تولید داده ممیزی ۳**	FAU_GEN.2.1
۴	**بازبینی داده ممیزی ۱**	FAU_SAR.1.1
۵	**بازبینی داده ممیزی ۲**	FAU_SAR.1.2
۶	**بازبینی داده ممیزی ۳**	FAU_SAR.2.1
۷	**بازبینی داده ممیزی ۴**	FAU_SAR.3.1
۸	**ذخیره‌سازی رویدادهای ممیزی ۱**	FAU_STG.1.1
۹	**ذخیره‌سازی رویدادهای ممیزی ۲**	FAU_STG.1.2
۱۰	**ذخیره‌سازی رویدادهای ممیزی ۶**	FAU_STG.3.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۱	**ذخیره‌سازی رویدادهای ممیزی ۷**	FAU_STG.4.1
۱۲	**انتخاب داده ممیزی ۱**	FAU_SEL.1.1
۱۳	**عملیات رمزنگاری ۱(۱)**	FCS_COP.1.1(1)
۱۴	**عملیات رمزنگاری ۱ (۲)**	FCS_COP.1.1(2)
۱۵	**ذخیره‌سازی اسرار ۱**	FCS_STO_EXT.1.1
۱۶	**مدیریت کلمه عبور ۱**	FIA_PMG_EXT.1.1
۱۷	**مدیریت کلمه عبور ۲**	FIA_PMG_EXT.2.1
۱۸	**مدیریت کلمه عبور ۳**	FIA_PMG_EXT.3.1
۱۹	**مدیریت کلمه عبور ۴**	FIA_PMG_EXT.4.1
۲۰	**مدیریت کلمه عبور ۵**	FIA_PMG_EXT.5.1
۲۱	**مدیریت احراز هویت ناموفق ۱**	FIA_AFL.1.1
۲۲	**مدیریت احراز هویت ناموفق ۲**	FIA_AFL.1.2
۲۳	**تعریف مشخصات کاربر ۱**	FIA_ATD.1.1
۲۴	**احراز هویت کاربر ۷**	FIA_UAU.5.1
۲۵	**احراز هویت کاربر ۸**	FIA_UAU.5.۲
۲۶	**احراز هویت کاربر ۱۰**	FIA_UAU.7.1
۲۷	**سازوکار احراز هویت بر اساس رمز عبور ۳**	FIA.UAU.EXT.۳,۱
۲۸	**سازوکار احراز هویت بر اساس رمز عبور ۴**	FIA.UAU.EXT.۴,۱

شماره الزام	نام الزام	تطابق الزام با استاندارد
۲۹	انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱	FIA_USB.1.1
۳۰	انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲	FIA_USB.1.2
۳۱	انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳	FIA_USB.1.3
۳۲	حفاظت از اطلاعات باقیمانده در منابع ۲	FDP_RIP.2.1
۳۳	ورود داده‌های کاربری به محصول ۴	FDP_ITC.2.1
۳۴	ورود داده‌های کاربری به محصول ۵	FDP_ITC.2.2
۳۵	ورود داده‌های کاربری به محصول ۶	FDP_ITC.2.3
۳۶	ورود داده‌های کاربری به محصول ۷	FDP_ITC.2.4
۳۷	ورود داده‌های کاربری به محصول ۸	FDP_ITC.2.5
۳۸	صحت داده‌های کاربری ذخیره‌شده ۲	FDP_SDI.2.1
۳۹	صحت داده‌های کاربری ذخیره‌شده ۳	FDP_SDI.2.2
۴۰	خط‌مشی کنترل دسترسی ۱	FDP_ACC.1.1
۴۱	عملیات کنترل دسترسی ۱	FDP_ACF.1.1
۴۲	عملیات کنترل دسترسی ۲	FDP_ACF.1.2
۴۳	عملیات کنترل دسترسی ۳	FDP_ACF.1.3
۴۴	عملیات کنترل دسترسی ۴	FDP_ACF.1.4
۴۵	حفاظت از منابع و داده‌ها ۱	FDP_DEC_EXT.1.6
۴۶	انتقال امن کوکی‌ها ۱	FDP_STR_EXT.1.1
۴۷	رمزگذاری داده‌های حساس برنامه کاربردی ۱	FDP_DAR_EXT.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۴۸	مدیریت کارکرد در محصول ۱	FMT_MOF.1.1
۴۹	مدیریت مشخصه‌های امنیتی ۱	FMT_MSA.1.1
۵۰	مدیریت مشخصه‌های امنیتی ۳	FMT_MSA.3.1
۵۱	مدیریت مشخصه‌های امنیتی ۴	FMT_MSA.3.2
۵۲	مدیریت داده‌های محصول ۱-مدیر سیستم	FMT_MTD.1.1(1)
۵۳	مدیریت داده‌های محصول ۱-کاربر عادی، واردکننده داده	FMT_MTD.1.1(2)
۵۴	کارکردهای مدیریتی محصول ۱	FMT_SMF.1.1
۵۵	نقش‌های امنیتی ۱	FMT_SMR.1.1
۵۶	نقش‌های امنیتی ۲	FMT_SMR.1.2
۵۷	حفظ وضعیت امن در زمان شکست ۱	FPT_FLS.1.1
۵۸	سازگاری داده‌های امنیتی بین محصول و موجودیت امن ۱	FPT_TDC.1.1
۵۹	سازگاری داده‌های امنیتی بین محصول و موجودیت امن۲	FPT_TDC.1.2
۶۰	انتقال داده امنیتی در داخل محصول ۱	FPT_ITT.1.1
۶۱	مهرهای زمانی ۱	FPT_STM.1.1
۶۲	قابلیت‌های ضد اکسپلویت ۴	FPT_AEX_EXT.1.4
۶۳	مدیریت داده‌های محصول ۱	FPT_EXP_EXT.1.1
۶۴	مدیریت کلیدهای موجود در محصول ۱	FPT_KST_EXT.1.1
۶۵	محدودیت بر روی چندین نشست هم‌زمان ۱	FTA_MCS.1.1
۶۶	محدودیت بر روی چندین نشست هم‌زمان ۲	FTA_MCS.1.2

شماره الزام	نام الزام	تطابق الزام با استاندارد
۶۷	**قفل‌کردن و خاتمه دادن به نشست‌ها ۵**	FTA_SSL.3.1
۶۸	**قفل‌کردن و خاتمه دادن به نشست‌ها ۶**	FTA_SSL.4.1
۶۹	**سوابق دسترسی به محصول ۱**	FTA_TAH.1.1
۷۰	**سوابق دسترسی به محصول ۲**	FTA_TAH.1.2
۷۱	**سوابق دسترسی به محصول ۳**	FTA_TAH.1.3
۷۲	**برقراری نشست ۱**	FTA_TSE.1.1
۷۳	**کانال امن ۱**	FTP_ITC.1.1
۷۴	**کانال امن ۲**	FTP_ITC.1.2
۷۵	**کانال امن ۳**	FTP_ITC.1.3
۷۶	**مسیر امن ۱**	FTP_TRP.1.1
۷۷	**مسیر امن ۲**	FTP_TRP.1.2
۷۸	**مسیر امن ۳**	FTP_TRP.1.3
۷۹	**استفاده کاربر از یک سرویس بدون افشاء هویت ۴**	FPR_ANO_EXT.1.1
	الزامات پیوست یک	
۸۰	**عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی ۱(۲)**	FCS_COP.1.1(3)
۸۱	**عملیات رمزنگاری ۱ (۴)**	FCS_COP.1.1(4)
۸۲	**تولید کلید رمزنگاری ۱**	FCS_CKM.1.1
۸۳	**مدیریت کلید رمزنگاری ۱**	FCS_CKM_EXT.4.1
۸۴	**الزامات پروتکلTLS Server/ احراز هویت ۱**	FCS_TLSS_EXT.1.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۸۵	**الزامات پروتکل TLS Server/ احراز هویت ۲**	FCS_TLSS_EXT.1.2
۸۶	**الزامات پروتکل TLS Server/ احراز هویت ۳**	FCS_TLSS_EXT.1.3
الزامات پیوست دو		

۶,۱ کلاس ممیزی امنیت

شماره الزام	نام الزام
۱	**تولید داده ممیزی ۱**

محصول باید بر اساس رخدادهای قابل ممیزی زیر، رکورد ممیزی تولید نماید:

- آغاز و اتمام توابع ممیزی؛
- تمامی رویدادهای قابل ممیزی که در جدول زیر آمده است،

مؤلفه	رویداد قابل ممیزی	جزئیات
بازبینی داده ممیزی ۳	تلاش‌های ناموفق برای خواندن اطلاعات از رکوردهای ممیزی (پایه)	
بازبینی داده ممیزی ۱	خواندن اطلاعات از رکوردهای ممیزی (پایه)	
صحت داده‌های کاربری ذخیره‌شده ۲	تلاش‌های موفقیت‌آمیز برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (حداقل) تمامی تلاش‌ها برای بررسی صحت داده کاربری، شامل نمایش نتایج بررسی (پایه)	
احراز هویت کاربر ۱	ثبت کاربرد ناموفق از سازوکار احراز هویت (حداقل) ثبت تمام کاربردهای سازوکار احراز هویت (پایه)	
احراز هویت کاربر ۷	ثبت نتایج احراز هویت (حداقل) ثبت هر سازوکار احراز هویت فعال همراه با نتیجه نهائی (پایه)	
شناسایی کاربر ۱	تمامی کاربردهای سازوکارها برای شناسایی کاربر (موفق و ناموفق)	شناسه کاربر شامل آدرس مبداء، شناسایی نقطه پایانی اتصال
مدیریت کلمه عبور	ثبت رد هر کلمه عبور آزمون شده توسط محصول (حداقل) ثبت تلاش موفق و ناموفق هر کلمه عبور آزمون شده توسط محصول (پایه)	برای مثال، رد و یا قبول کلمه عبور کاربر
انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر	ثبت شکست انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند، ایجاد موجودیت فعال) (حداقل)	

	شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند، شکست و موفقیت ایجاد موجودیت فعال) (پایه)	
مدیریت مشخصه‌های امنیتی ۱	تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی (پایه)	
مدیریت داده‌های محصول ۱-مدیر سیستم	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
مدیریت داده‌های محصول ۱-کاربر عادی، واردکننده داده	تمامی تغییرات بر روی مقادیر داده‌های امنیتی محصول (پایه)	تغییرات در مجوز دسترسی به رکوردها و اسناد باید ثبت شود.
حفظ وضعیت امن در زمان شکست ۱	ثبت شکست در محصول (پایه)	
تحمل خطا ۱	ثبت هر شکست شناسایی‌شده توسط محصول (حداقل) ثبت تمامی قابلیت‌های در حال قطع شدن محصول که به دلیل شکست است (پایه)	
برقراری نشست ۱	ثبت منع آغاز نشست به دلیل مکانیزم آغاز نشست (حداقل) ثبت تمامی تلاش‌ها در آغاز نشست کاربر (پایه)	
پروتکل TLS	ثبت شکست در برقراری یک نشست/برقراری یا پایان یک نشست	ارتباط نقطه پایانی غیر محصول (آدرس IP)، علت شکست

- [انتخاب: رویدادهای قابل ممیزی در سطح پایه (این رویدادها در «پیوست دو» آمده است)]،
- [اختصاص: دیگر رویدادهای ممیزی برای کارکردهای مدیریتی محصول]

نکته کاربردی ۱:

نویسنده‌ی سند هدف امنیتی ممکن است بر اساس کارکرد امنیتی محصول از برخی الزامات اختیاری و انتخابی ذکرشده در «پیوست دو» این سند استفاده نموده و به سند هدف امنیتی محصول اضافه نماید. در این صورت لازم است رویدادهای ممیزی دیگر با توجه به این الزامات نیز اضافه گردند.

اقدامات ارزیابی:

- **بخش خلاصه مشخصات محصول**[۲]

توسعه‌گر محصول باید قالب و نحوه ذخیره‌سازی رکوردهای ممیزی را در بخش «خلاصه مشخصات محصول» از سند هدف امنیتی بیان نماید؛ همچنین لازم است چگونگی استخراج رکوردهای ممیزی توسط مدیر سیستم یا ارزیاب به منظور تحلیل داده‌ها، در این بخش توضیح داده شود.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی نموده تا اطمینان حاصل نماید فهرستی از رویدادهای قابل ممیزی در محل ذخیره‌سازی به شکل مناسب و قابل درک فراهم کرده است.

- **آزمون‌ها**

ارزیاب باید آزمون‌های زیر را برای هر کدام از انواع رویدادها انجام دهد:

آزمون اول: ارزیاب باید یک نشست با سرور ایجاد و درخواستی را به سمت آن ارسال نماید. سپس باید تولید لاگ در سمت سرور برای درخواست ارسال‌شده را بررسی نماید.

آزمون دوم: ارزیاب باید عملیاتی را انجام دهد که منجر به ثبت هر کدام از رویدادهای قابل ممیزی می‌شود. سپس ثبت و یا عدم ثبت آن‌ها را بررسی نماید. به عنوان مثال، ارزیاب باید در سمت کلاینت اقداماتی مانند ایجاد فایل و یا تغییر نام انجام دهد و تولید لاگ در سمت سرور را بررسی نماید.

آزمون سوم: ارزیاب باید یک عمل غیرمجاز را انجام دهد و سپس بررسی کند که لاگی برای این عمل تولیدشده باشد.

۲	**تولید داده ممیزی ۲**

محصول باید برای هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت نماید:

تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال (در صورتی که کاربرد داشته باشد) و نتیجه (موفقیت یا شکست) رویداد

[اختصاص: تولیدکننده محصول، اطلاعات دیگری را که برای هر نوع رکورد ممیزی ذخیره می‌نماید را اعلام نماید.]

نکته کاربردی ۲:

به عنوان مثال می‌توان اطلاعات دیگری از قبیل آدرس IP و اطلاعات خاص یک کاربر را نیز ذخیره نمود.

[۲] TOE Summory Specification (TSS)

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی و تأیید نماید که در سند مذکور، نحوه نمایش لاگ‌های ممیزی ذخیره‌شده در شکل و فرمت مناسب را شرح داده‌شده است.

- **آزمون‌ها**

ارزیاب باید آزمون زیر را برای هر کدام از انواع رویدادها انجام دهد:

آزمون اول: ارزیاب باید بررسی کند که اطلاعات ذکرشده در این الزام برای لاگ ثبت‌شده در سرور وجود دارد یا خیر.

۳	**تولید داده ممیزی ۳**

برای رویدادهای ممیزی حاصل از اقدامات کاربران شناسایی‌شده، محصول باید بتواند هویت کاربری که باعث ایجاد آن رویداد شده است را شناسایی و ثبت نماید.

اقدامات ارزیابی:

- **بخش خلاصه مشخصات محصول**

در این بخش از سند هدف امنیتی باید در صورت امکان، روش‌هایی که باعث عدم انقیاد رویداد مرتبط با کاربری که آن را ایجاد کرده است، توضیح داده شود.

۴	**بازبینی داده ممیزی ۱**

محصول باید امکان خواندن/مشاهده [اختصاص: **فهرستی از اطلاعات ممیزی**] از کل رکوردهای ممیزی را برای [اختصاص: **کاربران مجاز**] فراهم نماید.

نکته کاربردی ۲:

- در این الزام در اولین «اختصاص» می‌توان به جای فهرستی از اطلاعات ممیزی، با توجه به سازوکار کنترل دسترسی در محصول، نوع اطلاعات ممیزی که کاربر مجاز قابلیت خواندن آن‌ها را دارد را اعلام نمایید.

- در این الزام در دومین «اختصاص» می‌توان به جای کاربران مجاز، با توجه به سازوکار کنترل دسترسی در محصول، کاربران و یا گروه کاربرانی که مجاز به قابلیت خواندن اطلاعات ممیزی هستند را اعلام نمود.

اقدامات ارزیابی:

- **بخش خلاصه مشخصات محصول**

در این بخش از سند هدف امنیتی باید توضیح داده شود که چه مواقعی کاربر قادر به خواندن داده ممیزی است.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند و اطمینان حاصل نماید در خصوص زمان امکان‌پذیر بودن خواندن رکورد ممیزی داده برای کاربر و همچنین واسط‌های فراهم‌کننده‌ی این امکان توضیحاتی ارائه‌شده است.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بررسی کند که تنها کاربر با دسترسی مجاز قادر به خواندن رکوردهای ممیزی در فرمت مناسب و قابل درک است.

آزمون دوم: ارزیاب باید بررسی کند که کاربران با توجه به نوع دسترسی تعریف‌شده، قادر به خواندن اطلاعات و رکوردهای ممیزی مناسب و خاص خود هستند.

۵	**بازبینی داده ممیزی ۲**

محصول باید رکوردهای ممیزی را به شکل خوانا و قابل درک برای کاربر نمایش دهد.

اقدامات ارزیابی:

آزمون این الزام وابسته به الزام شماره‌ی ۴: «بازبینی ممیزی امنیت ۱» است.

۶	**بازبینی داده ممیزی ۳**

محصول باید از دسترسی کلیه کاربران نسبت به خواندن رکوردهای ممیزی ممانعت نماید؛ بجز کاربرانی که به آن‌ها مجوز دسترسی خواندن داده‌شده باشد (الزام شماره ۴).

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند و اطمینان حاصل نماید در خصوص زمان امکان‌پذیر بودن خواندن رکورد ممیزی داده برای کاربر و همچنین واسط‌های فراهم‌کننده‌ی این امکان توضیحاتی ارائه‌شده است.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بررسی کند که کاربر غیرمجاز قادر به خواندن رکوردهای ممیزی است یا خیر.

۷	**بازبینی داده ممیزی ۴**

محصول باید امکان انجام [اختصاص: متدهای انتخاب و مرتب‌سازی] رکوردهای ممیزی را به نحوی فراهم نماید که کاربر مجاز بتواند آن رکوردها را بر اساس [اختصاص: حساب کاربری، تاریخ/زمان، نوع رخداد و [اختصاص: دیگر موارد]] مرتب نماید.

اقدامات ارزیابی:

- **راهنما**

ارزیاب باید سند راهنمای محصول را بررسی کند تا اطمینان حاصل نماید توضیحاتی در خصوص چگونگی مرتب‌سازی داده‌های ممیزی و همچنین واسط‌های فراهم‌کننده‌ی این امکان بیان‌شده است.

- **آزمون‌ها**

ارزیاب باید بتواند بر اساس یکی از داده‌های ممیزی مرتب‌سازی نماید.

۸	**ذخیره‌سازی رویدادهای ممیزی ۱**

محصول باید رکوردهای ممیزی ذخیره‌شده در محل ذخیره‌سازی را از حذف غیرمجاز حفاظت نماید.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید اطمینان حاصل نماید که در بخش «خلاصه مشخصات محصول» از سند هدف امنیتی مقدار حجم ذخیره‌سازی رکوردهای ممیزی به صورت محلی بیان‌شده است.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی نماید تا اطمینان حاصل نماید توضیحاتی در خصوص رابطه بین رکوردهای ممیزی محلی و رکوردهای ممیزی ارسالی به لاگ سرور ممیزی بیان‌شده است. برای مثال، اگر رکورد ممیزی تولیدشده باشد، به‌طور هم‌زمان هم در سرور خارجی و هم در محل ذخیره‌سازی محلی ذخیره شود، یا محل ذخیره‌سازی محلی به عنوان بافر مورد استفاده قرار گیرد و با ارسال داده‌ها به طور دوره‌ای به سرور ممیزی، داده‌ها از محل ذخیره‌سازی محلی پاک گردد.

۹	**ذخیره‌سازی رویدادهای ممیزی ۲**

محصول باید قادر به تشخیص تغییرات غیرمجاز در رکوردهای ممیزی ذخیره‌شده در محل ذخیره‌سازی آن‌ها باشد.

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند و اطمینان حاصل نماید در خصوص زمان امکان‌پذیر بودن حذف و یا تغییر رکورد ممیزی داده برای کاربر و همچنین واسط فراهم‌کننده‌ی این امکان توضیحاتی ارائه‌شده است.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بررسی کند که کاربر غیرمجاز قادر به تغییر و یا حذف رکوردهای ممیزی است یا خیر. آزمون دوم: ارزیاب باید بررسی کند که در صورت تلاش کاربر غیرمجاز برای حذف و یا اعمال تغییرات بر روی رکوردهای ممیزی، در لاگ ذخیره شود.	
۱۰	**ذخیره‌سازی رویدادهای ممیزی ۶**

محصول در صورت تجاوز دنباله ممیزی از [اختصاص: یک محدودیت از پیش تعریف‌شده] باید با استفاده از [اختصاص: یک کانال ارتباطی، پیام کوتاه یا معادل آن، از طریق واسط‌های محصول کاربران مربوطه را] مطلع نماید.

نکته کاربردی ۳:

برای اجرایی نمودن این الزام می‌توان تنظیمات لازم را در پایگاه داده‌ها اعمال کرد.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید اطمینان حاصل نماید که در بخش «خلاصه مشخصات محصول» از سند هدف امنیتی توضیحاتی در خصوص مقدار حجم ذخیره‌سازی رکوردهای ممیزی به صورت محلی، همچنین نوع رویدادی که در صورت پر شدن محل ذخیره‌سازی رخ می‌دهد و چگونگی محافظت از رکوردهای ممیزی در برابر دسترسی‌های غیرمجاز بیان‌شده است.

در این بخش باید ذکر گردد چه عملیاتی بعد از پر شدن محل ذخیره‌سازی ممیزی صورت می‌گیرد و چه نوع اطلاعاتی ممکن است از بین برود. همچنین چه تنظیماتی را مدیر سیستم باید بر روی محصول پیکربندی کند تا عملیات مورد نظر فعال گردند.

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند تا اطمینان حاصل نماید توضیحاتی در خصوص رویداد رخداده برای پیشگیری از دست رفتن رکوردهای ممیزی در صورت پر شدن محل ذخیره‌سازی بیان‌شده است.

ارزیاب باید سند راهنمای محصول را بررسی نماید تا اطمینان حاصل نماید در مورد رابطه بین رکوردهای ممیزی محلی و رکوردهای ممیزی ارسالی به لاگ سرور ممیزی توضیحاتی بیان‌شده است. برای مثال، اگر رکورد ممیزی تولیدشده باشد، به‌طور هم‌زمان هم در سرور خارجی و هم در محل ذخیره‌سازی محلی ذخیره شود، یا محل ذخیره‌سازی محلی به عنوان بافر مورد استفاده قرار گیرد و با ارسال داده‌ها به طور دوره‌ای به سرور ممیزی، داده‌ها از محل ذخیره‌سازی محلی پاک گردد.

- **آزمون‌ها**

ارزیاب باید مقدار حد آستانه ذخیره‌سازی رکورد ممیزی را به گونه‌ای انتخاب کند که محل ذخیره‌سازی پر شود و بررسی نماید که در این شرایط رویدادهای ادعاشده صورت می‌گیرد.

۱۱	**ذخیره‌سازی رویدادهای ممیزی ۷**

محصول در صورت پر شدن دنباله ممیزی، باید [انتخاب: «رویدادهای ممیزی را نادیده بگیرد»، «از ذخیره رویدادهای قابل ممیزی، به جز آن‌هایی که توسط کاربر مجاز و تحت حقوق خاص رخ می‌دهند، جلوگیری نماید»، «روی قدیمی‌ترین رکوردهای ممیزی ذخیره‌شده دوباره‌نویسی نماید»] و [اختصاص: یا دیگر اقدامات برای هشدار از پر شدن فضای ذخیره‌سازی] ارسال نمایند.

نکته کاربردی ۴:

برای اجرایی نمودن این الزام می‌توان تنظیمات لازم را در پایگاه داده‌ها اعمال کرد.

۱۲	**انتخاب داده ممیزی ۱**

محصول باید قادر به انتخاب مجموعه‌ای از رخدادها جهت ممیزی شدن، از مجموعه تمام رخدادهای قابل ممیزی بر اساس مشخصه‌های زیر باشد:

- [انتخاب: هویت موجودیت فعال، نوع رخداد]
- [اختصاص: معیارهای انتخاب دیگر بیان شوند]

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی کند تا نسبت به وجود فهرستی از انواع رویدادها و خصیصه‌های قابل ممیزی که بتوان انتخاب کرد، اطمینان حاصل نماید.

• **آزمون‌ها** ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید بررسی نماید که هریک از خصیصه‌ها و رویدادهای ذکرشده در فهرست، قابل انتخاب برای ممیزی شدن است. آزمون دوم: ارزیاب باید چندین آیتم از فهرست را برای ممیزی انتخاب و بررسی کند که با اضافه شدن چندین نوع خصیصه و رویداد، عمل به‌درستی اجرا می‌شود.

۶,۲ کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۱۳	**عملیات رمزنگاری ۱ (۱)**
محصول باید [اختصاص: برای وارسی صحت داده‌های ممیزی و داده‌های رکورد] بر اساس یک الگوریتم رمزنگاری مشخص [اختصاص: الگوریتم رمزنگاری] و اندازه کلید رمزنگاری [اختصاص: اندازه‌های کلید رمزنگاری]اجرا شود که مطابق با [اختصاص: فهرستی از استانداردها]باشد. **نکته کاربردی ۵:** روش‌های اطمینان از صحت داده‌ی رکوردها و داده‌ی ممیزی بر عهده نویسنده سند هدف امنیتی است. نویسنده در صورت استفاده از مؤلفه‌های اضافی به منظور صحت داده‌ها باید آن‌ها را در سند هدف امنیتی اضافه نماید. ممکن است با توجه به روش بررسی صحت داده نیاز به الزامات ذکرشده در پیوست یک (شماره‌های ۸۲ تا ۸۶) باشد لذا لازم است نویسنده سند هدف امنیتی الزامات مرتبط را از پیوست انتخاب نموده و به صورت تکمیل‌شده در سند هدف امنیتی ذکر نماید.	
۱۴	**عملیات رمزنگاری ۱(۲)**

شماره الزام	نام الزام
محصول باید [اختصاص: تولید داده درهم‌سازی] بر اساس یک الگوریتم رمزنگاری مشخص [اختصاص: الگوریتم رمزنگاری] و اندازه کلید رمزنگاری [اختصاص: هیچ‌کدام]اجرا شود که مطابق با [اختصاص: فهرستی از استانداردها] باشد. **نکته کاربردی ۶:** با توجه به آنکه الگوریتم رمزنگاری نیازی به کلید ندارد، لذا محدودیتی برای اختصاص وجود ندارد. در صورت استفاده از کلید رمزنگاری در محصول لازم است نویسنده سند هدف امنیتی الزامات مرتبط از «پیوست یک» را انتخاب نموده و به صورت تکمیل‌شده در سند بیان نماید.	
۱۵	**ذخیره‌سازی اسرار ۱**
محصول در فضای حافظه‌ی غیر فرّار باید [انتخاب: هیچ‌گونه اطلاعات کاربری را ذخیره نکند، از عملکردهای ارائه‌شده در پلت‌فرم برای ذخیره‌ی امن [اختصاص: فهرست اعتبارنامه‌ها] استفاده کند، عملکردی را برای ذخیره‌ی امن [اختصاص: فهرست اعتبارنامه‌ها]، پیاده‌سازی کند.] **نکته کاربردی ۷:** این الزام، در سمت سرور تضمین می‌کند که امنیت مشخصات دائمی حساب کاربری (کلیدهای مخفی، کلیدهای خصوصی PKI، گذرواژه‌ها) در هنگام استفاده نشدن نیز حفظ می‌گردد.	

۶,۳ کلاس شناسایی و احراز هویت

شماره الزام	نام الزام
۱۶	**مدیریت کلمه عبور ۱**

محصول باید امکان مدیریت رمز عبور را که در زیر ذکرشده‌اند برای رمزهای عبور مدیریتی فراهم نماید:

۱. رمزهای عبور باید بتوانند هر ترکیبی از حروف کوچک و بزرگ، اعداد و کاراکترهای خاص: [انتخاب: "@"، "#"، "$"، "٪"، "^"، "!"، "&"، "*"، "(" ، ")" [اختصاص: کاراکتر دیگر]] باشند.

۲. حداقل طول رمز عبور باید توسط مدیر امنیت، قابل تنظیم بوده و ۱۵ کاراکتر یا بیشتر باشد.

نکته کاربردی ۸:

نویسنده‌ی سند هدف امنیتی، کاراکترهای خاصی را که توسط محصول پشتیبانی می‌گردند انتخاب می‌نماید. نویسنده این اختیار را دارد تا کاراکترهای خاص بیشتری را با استفاده از عبارت «اختصاص» فهرست نماید.

«رمز عبور مدیریتی» به آن دسته از رمز عبورهایی اشاره دارد که مدیران از آن‌ها در کنسول محلی یا پروتکل‌هایی که از «رمز عبور» پشتیبانی می‌نمایند (همچون HTTPS, SSH)، استفاده می‌کنند.

اقدامات ارزیابی:

- **سند راهنمای محصول**

ارزیاب باید راهنمای محصول را بررسی کند تا اطمینان حاصل نماید که برای مدیران امنیتی در مورد ایجاد رمز عبورهای قوی و همچنین تنظیمات طول رمز عبور راهنمایی‌هایی ارائه‌شده باشد.

- **آزمون‌ها**

ارزیاب باید هم رمز عبورهای ضعیف و هم قوی ایجاد نماید و عکس‌العمل محصول را بررسی کند که آیا از هر دو رمز عبور پشتیبانی می‌شود؟ ارزیاب باید اطمینان حاصل نماید که تمام کاراکترها، قوانین و حداقل طول کلمه عبور که در راهنمای محصول آمده است را پشتیبانی می‌کند.

شماره الزام	نام الزام
۱۷	**مدیریت کلمه عبور ۲**

در عملیات تغییر کلمه عبور محصول باید، کلمه عبور قدیمی، کلمه عبور جدید و تائیدیه کلمه عبور جدید وجود داشته باشد.	
۱۸	**مدیریت کلمه عبور ۳**
محصول باید هنگام بازیابی کلمه عبور نباید کلمه عبور جاری را افشاء نماید و کلمه عبور جدید را به صورت متن آشکار به کاربر ارسال نماید.	
۱۹	**مدیریت کلمه عبور ۴**
محصول باید اطمینان دهد که از کلمه عبور پیش‌فرض در محصول و یا مؤلفه‌های آن فقط یکبار هنگام ایجاد کاربر استفاده می‌شود. **نکته کاربردی ۹:** کلمه عبور پیش فرض مانند (admin/password)	
۲۰	**مدیریت کلمه عبور ۵**
محصول باید برای بازیابی کلمه عبور با استفاده از [انتخاب: تعیین کلمه عبور جدید، ارسال کلمه عبور جاری به ایمیل کاربر] هویت کاربر را از طریق [اختصاص: ایمیل ثانویه، سوالات امنیتی] وارسی نماید.	
۲۱	**مدیریت احراز هویت ناموفق ۱**
محصول، باید بتواند با استفاده از [انتخاب: [اختصاص: یک عدد مثبت]، یک عدد مثبت قابل تنظیم توسط مدیر [اختصاص: بازه قابل قبولی از مقادیر]] تلاش ناموفق احراز هویت مرتبط با [اختصاص: فهرستی از رویدادهای احراز هویت] را تشخیص دهد. **نکته کاربردی ۹:** به عنوان مثال در سومین اختصاص می‌توان به وارد نمودن کلمه عبور توسط کاربر برای احراز هویت شدن اشاره نمود. **اقدامات ارزیابی:** • **خلاصه مشخصات محصول**	

ارزیاب باید «خلاصه مشخصات محصول» از سند هدف امنیتی را بررسی کند تا اطمینان حاصل نماید توضیحاتی در خصوص روش‌های مورد پشتیبانی برای عملیات مدیریتی از راه دور و همچنین چگونگی تشخیص تلاش‌های موفق و ناموفق احراز هویت ارائه‌شده است. • **سند راهنمای محصول** ارزیاب باید راهنمای محصول را بررسی کند تا اطمینان حاصل نماید توضیحاتی در خصوص دستورات پیکربندی تعداد تلاش‌های موفق و ناموفق احراز هویت و همچنین روش‌های مختلف احراز هویت از راه دور مانند SSH شرح داده‌شده است. • **آزمون‌ها** ارزیاب باید بر اساس حد آستانه تلاش موفق و ناموفق در احراز هویت در راهنما، محصول را پیکربندی نماید و هنگامی که تعداد تلاش احراز هویت به مقدار حد آستانه رسید با نام کاربری و کلمه عبور معتبر احراز هویت را بررسی کند که در این صورت نباید اجازه ورود دهد.
۲۲ مدیریت احراز هویت ناموفق ۲
زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت [انتخاب: به حد تعیین‌شده رسید و یا از آن بیشتر شد]، محصول باید [اختصاص: فهرستی از اقدامات مقابله‌ای] را اجرا نماید که باعث پیچیده‌تر کردن عمل احراز هویت مجدد کاربر شود. **اقدامات ارزیابی:** • **راهنما** ارزیاب باید راهنمای محصول را بررسی کند و اطمینان حاصل نماید، توضیحاتی در خصوص نحوه‌ی مدیریت احراز هویت در شرایطی که تعداد تلاش‌های ناموفق احراز هویت به بیش از حد آستانه رسید بیان‌شده باشد.
۲۳ تعریف مشخصات کاربر ۱
محصول باید مشخصه‌های امنیتی زیر را برای هر کاربر نگهداری نماید: [انتخاب: • شناسه کاربر • متد احراز هویت مورد استفاده • داده‌های احراز هویت

- نقش کاربر
- وضعیت حساب کاربری (فعال، غیرفعال، بلوکه‌شده و غیره)
- [اختصاص: **هر مشخصه امنیتی دیگر**]

]

نکته کاربردی ۱۰:

حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت باید وجود داشته باشد. این اطلاعات شامل نگهداری نمودن از هر مجوزی است که یک کاربر ممکن است دارا باشد.

اقدامات ارزیابی

- **خلاصه مشخصات محصول**

ارزیاب باید مشخصه‌های امنیتی نگهداری شده برای هر کاربر تعریف‌شده در فصل خلاصه مشخصات محصول را پیدا کند. البته ممکن است این فهرست با فهرستی که در الزام تعریف مشخصات کاربر ۱ آمده است، متفاوت باشد. در این صورت، باید در فصل "خلاصه مشخصات محصول" مشخصه‌های امنیتی مهم کاربر را تحت پوشش قرار دهد.

- **سند راهنمای محصول**

ارزیاب باید بخش راهنمای مدیریتی از سند راهنمای محصول را بررسی نماید تا اطمینان حاصل نماید توضیحاتی در خصوص ایجاد، مشاهده، تغییر و یا حذف مشخصه‌های امنیتی کاربر (به عنوان مثال، تغییر کلمه عبور) ارائه‌شده است.

- **آزمون‌ها**

ارزیاب باید واسط‌های مرتبط با مشخصه‌های امنیتی کاربر را بررسی و آزمون کند.

۲۴	**احراز هویت کاربر ۷**

محصول باید اقدامات زیر را برای احراز هویت مدیر سیستم فراهم آورد:

[اختصاص:

- نام کاربری و کلمه عبور

- [انتخاب: امضای دیجیتال، یا هر متد احراز هویت جایگزین دیگر برای فراهم آوردن امنیت بهتر]

]

نکته کاربردی ۱۱:

برای احراز هویت کاربر باید بیش از یک سازوکار احراز هویت در محصول به‌کاررفته باشد. به عنوان مثال از نام کاربری، کلمه عبور و گواهی دیجیتال برای احراز هویت در محصول استفاده گردد.

اقدامات ارزیابی:

- **خلاصه مشخصات محصول**

ارزیاب باید بخش «خلاصه مشخصات محصول» از سند هدف امنیتی را بررسی کند تا اطمینان حاصل نماید سازوکار احراز هویت معرفی‌شده باشد.

- **آزمون‌ها**

برای آزمون این الزام، ابتدا باید الزام «احراز هویت کاربر ۱» به طور کامل مورد تائید قرارگرفته باشد. ارزیاب باید تمام سازوکارهای احراز هویت قابل دسترس را پیکربندی نموده و واسط‌های پشتیبان همه سازوکارهای احراز هویت را بررسی کند.

۲۵	**احراز هویت کاربر ۸**

محصول باید برای [اختصاص: مدیر سیستم، فهرستی از مدیران گروه‌ها]احراز هویت را مطابق [**اختصاص: مدیر سیستم باید علاوه بر بررسی نام کاربری و کلمه عبور از روش احراز هویت چندگانه که در بالا تعریف‌شده استفاده کند،** [اختصاص: قوانینی که نحوه سازوکار احراز هویت چندگانه را شرح می‌دهد]] احراز هویت نماید.

۲۶	**احراز هویت کاربر ۱۰**

هنگامی‌که فرایند احراز هویت در حال جریان است، محصول مورد ارزیابی تنها باید بازخورد مبهم را در اختیار مدیر سیستم قرار دهد.

نکته کاربردی ۱۲:

«بازخورد مبهم» به معنی بازخوردی است که در آن محصول مورد ارزیابی داده‌های احراز هویت واردشده توسط کاربر را به‌صورت واضح و قابل‌خواندن نشان نمی‌دهد؛ البته ممکن است روند پیشرفت به شکل مبهم نشان داده شود (مانند یک ستاره برای هر کاراکتر). بازخورد مبهم همچنین نشان می‌دهد که محصول مورد ارزیابی در جریان احراز هویت هیچ اطلاعاتی را که ممکن است نشان‌دهنده داده‌های احراز هویت باشد، نمایش نمی‌دهد.
۲۷ سازوکار احراز هویت بر اساس رمز عبور۳
محصول باید تضمین کند که تمام عملیات احراز هویت در سمت سرور انجام می‌گیرد.
۲۸ سازوکار احراز هویت بر اساس رمز عبور ۴
محصول باید اطمینان دهد که بعد از تغییر یافتن کلمه عبور توسط کاربر به تمام نشست‌ها خاتمه داده و کاربر را مجددا احراز هویت نماید.
۲۹ انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱
محصول باید مشخصه‌های امنیتی زیر را برای کاربر فعال نگهداری نماید: [انتخاب: • شناسه کاربر • نقش‌های کاربر • جزئیات واسط کلاینت • پیشینه احراز هویت (زمان آخرین تلاش احراز هویت موفق و ناموفق) • [اختصاص: فهرست دیگر مشخصه‌های کاربری]] **اقدامات ارزیابی** • **خلاصه مشخصات محصول** ارزیاب باید مشخصه‌های امنیتی کاربر که در «خلاصه مشخصات ارزیابی» آمده است را با مشخصاتی که در واسط محصول وجود دارد مطابقت دهد که الزام انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر را پشتیبانی می‌کند. • **سند راهنمای محصول**

ارزیاب باید بخش راهنمای مدیریتی از سند راهنمای محصول را بررسی نماید تا نسبت به ارائه توضیحات در خصوص چگونگی ایجاد موجودیت فعال و امکان تغییر مشخصه‌های امنیتی آن اطمینان حاصل نماید.

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب باید بتواند مشخصه‌های امنیتی را برای اجرای عملیات با توجه به راهنمای محصول مقداردهی و یا ویرایش نماید. سپس بررسی کند که این تغییرات به طور موفقیت‌آمیز اعمال‌شده است. در برخی موارد باید این آزمون را همراه با کنترل دسترسی، محدودیت‌های مدیریتی امنیتی و یا در ممیزی انجام شود.

آزمون دوم: ارزیاب باید بتواند مشخصه‌های امنیتی را با توجه به راهنمای مدیریتی محصول برای اجرای عملیات، با تمامی حداقل شرایط، مقداردهی و یا ویرایش کند. در این صورت عملیات باید با یک پیغام خطا با شکست مواجه شود. سپس ارزیاب با استفاده از واسط باید بررسی کند که تغییرات مشخصه‌های امنیتی اعمال نشده است. در برخی موارد باید این آزمون همراه با کنترل دسترسی، محدودیت‌های مدیریتی امنیتی و یا در ممیزی بررسی شود.

۳۰	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۲**

محصول باید قوانین زیر را بر روی اتصال اولیه مشخصه‌های امنیتی کاربر با موجودیت فعالی که از طرف کاربر فعالیت می‌کند، اعمال نماید:

[انتخاب:

- زمانی که یک نشست جدید برقرار می‌شود، اطلاعات موجود از نشست‌های قبلی باید حذف گردد
- اطلاعات پیشینه احراز هویت باید بروزرسانی گردد
- [اختصاص: دیگر قوانین برای اتصال اولیه مشخصه‌ها]

]

اقدامات ارزیابی

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی و اطمینان حاصل نماید در خصوص چگونگی ایجاد موجودیت‌های فعال و اعمال تغییر در مشخصه‌های امنیتی مرتبط با موجودیت‌های فعال توضیحاتی ارائه‌شده است.

- **آزمون‌ها**

ارزیاب ابتدا نشستی را با محصول آغاز نماید و سپس از محصول خارج شود، ممکن است اطلاعات نشست به درستی منقضی نشده باشد؛ لذا در صورت ورود مجدد به سیستم ارزیاب باید بررسی کند که آیا از شناسه نشست قبلی استفاده می‌شود یا خیر.

۳۱	**انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۳**

محصول باید قوانین زیر را که حاکم بر تغییرات است به مشخصه‌های امنیتی کاربر فعال اعمال نماید:

[انتخاب: هیچ تغییری در طول نشست فعال مجاز نمی‌باشد، [اختصاص: دیگر قوانین حاکم بر تغییرات مشخصه‌ها]]

نکته کاربردی ۱۳:

منظور از تغییرات، به این معناست که هیچ مشخصه‌های امنیتی کاربر که در الزام شماره ۳۰ «انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر ۱» تعریف‌شده است در طول نشست، تغییر نکند.

اقدامات ارزیابی

- **آزمون‌ها**

ارزیاب باید اقدامات زیر را انجام دهد:

آزمون اول: ارزیاب ابتدا نشستی را با محصول با یک نام کاربری مشخص آغاز نماید، سپس یکی از مشخصه‌های امنیتی کاربر مانند آدرس IP سیستم را تغییر دهد در این صورت باید نشست غیرفعال و خاتمه یابد.

آزمون دوم: ارزیاب ابتدا نشستی را با محصول با یک نام کاربری مشخص آغاز نماید، سپس اطلاعات نشست را به سیستم دیگر انتقال داده و سعی کند با همان اطلاعات نشست اتصال با محصول ادامه داشته باشد. در این صورت به دلیل تغییر آدرس فیزیکی سیستم کاربر، باید نشست خاتمه یابد و مجددا احراز هویت صورت گیرد.

آزمون سوم: ارزیاب ابتدا با استفاده از یک نام کاربری و مرورگر مشخص، نشستی با محصول آغاز نماید، سپس با مرورگر دیگر همان اطلاعات نشست را وارد و تلاش نماید با همان اطلاعات نشست اتصال با محصول ادامه داشته باشد. در این صورت باید نشست خاتمه یابد و مجددا احراز هویت صورت گیرد.

۶,۴ کلاس حفاظت از داده‌های کاربری

شماره الزام	نام الزام
۳۲	**حفاظت از اطلاعات باقیمانده در منابع ۲**

محصول باید تضمین کند هرگونه محتوی اطلاعات قبلی یک منبع را هنگام [انتخاب: تخصیص منابع به، آزادسازی منابع از] تمام موجودیت‌های غیرفعال استفاده‌شده، غیرقابل دسترس کند.

اقدامات تضمینی

- **راهنما**

در صورت وجود امکانات برای پیکربندی و مدیریت کارکردهای منابع در محصول انتظار می‌رود که توضیحاتی در مورد نحوه پیکربندی مدیریت منابع و نحوه استفاده مجدد آن‌ها در راهنمای مدیریتی محصول آمده باشد.

- **آزمون‌ها**

ارزیاب باید تمام واسط‌هایی که از منابع استفاده می‌کنند، آزمون و بررسی نماید هنگام استفاده مجدد منابع، توسط موجودیت فعال دیگر (یک کاربر دیگر) اطلاعات قبلی قابل‌دسترسی است یا خیر.

شماره الزام	نام الزام
۳۳	**ورود داده‌های کاربری به محصول ۴**

محصول باید هنگام دریافت داده کاربری، [اختصاص: خط‌مشی کنترل دسترسی] را اعمال نماید.

اقدامات ارزیابی

- **سند راهنمای محصول**

ارزیاب باید سند راهنمای محصول را بررسی نموده تا اطمینان حاصل نماید توضیحاتی در خصوص چگونگی کنترل و ورود داده کاربری ارائه‌شده است.

- **آزمون‌ها**

ارزیاب باید با توجه به پیکربندی و کنترل دسترسی که در راهنمای مدیریتی محصول آمده است، یکبار با استفاده از حساب کاربری با مجوز ورود داده به داخل سیستم و بار دیگر با حساب کاربری بدون مجوز، درستی انجام عملیات را بررسی و تائید نماید.

شماره الزام	نام الزام
۳۴	**ورود داده‌های کاربری به محصول ۵**
محصول باید در هنگام ورود داده‌ها از مشخصه‌های امنیتی مرتبط با داده‌های کاربری استفاده نماید. **نکته کاربردی ۱۴:** مشخصه‌های امنیتی داده‌های کاربری می‌تواند شامل نوع داده، اندازه و غیره باشد. **اقدامات ارزیابی** • **آزمون‌ها** این آزمون وابسته به الزام شماره ۳۳: «ورود داده‌های کاربری به محصول ۴» است. ارزیاب هنگام ورود داده به سیستم باید اطمینان حاصل نماید که تمامی مشخصه‌های امنیتی کاربر ذکرشده در سند راهنما همچون نام کاربری و یا امضاء دیجیتال و غیره در نظر گرفته می‌شود. این بررسی در عملیاتی همانند ثبت رکورد ممیزی عملیات ورود با مشخصه امنیتی کاربر، ذخیره داده وارده با مشخصه امنیتی نیز باید در نظر گرفته شود.	
۳۵	**ورود داده‌های کاربری به محصول ۶**
محصول باید اطمینان دهد که پروتکل مورد استفاده برای انتقال، ارتباط و همبستگی بین مشخصه‌های امنیتی و داده کاربری دریافت شده را فراهم می‌نماید. **اقدامات ارزیابی** • **آزمون‌ها** ارزیاب باید اطمینان حاصل کند که هنگام ورود داده به داخل محصول، مطابق پروتکل ادعاشده در راهنما عملیات صورت می‌گیرد و حین انتقال شنود و گم‌شدن داده وجود ندارد.	
۳۶	**ورود داده‌های کاربری به محصول ۷**
محصول باید اطمینان دهد که تفسیر مشخصه‌های امنیتی داده‌های کاربری دریافت شده همانند، آنچه که فرستنده داده کاربری در نظر گرفته، است.	

شماره الزام	نام الزام
اقدامات ارزیابی • **آزمون‌ها** ارزیاب باید داده‌ای را مطابق آنچه که در راهنما گفته‌شده به محصول وارد نماید و بررسی نماید که تمام اطلاعات و داده‌ها به طور صحیح و کامل انتقال داده‌شده است.	
۳۷	**ورود داده‌های کاربری به محصول ۸**
محصول باید هنگام ورود داده کاربری از بیرون (خارج از محصول)، قوانین تحت کنترل خط‌مشی امنیتی زیر را اعمال نماید: [اختصاص: قوانین کنترلی اضافی هنگام ورود داده کاربری.] **نکته کاربردی ۱۵:** هدف عناصر ورود داده‌های کاربری به محصول، ارائه کارکردهایی به منظور بررسی و صحت داده ورودی است. به عنوان مثال، برای کنترل داده‌های ورودی می‌توان در هنگام ورود رکوردهای الکترونیکی، محصول صحت رکوردها را از طریق سازوکاری (همچون امضاء دیجیتال) بررسی نماید، یا از مشخصه‌های امنیتی رکوردهای الکترونیکی، مانند خصیصه نوشتنی، خواندنی و غیره محافظت نماید. **اقدامات ارزیابی** این الزام وابسته به ورود داده‌های کاربری به محصول ۴ و ورود داده‌های کاربری به محصول ۵ است.	
۳۸	**صحت داده‌های کاربری ذخیره‌شده ۲**
محصول باید داده کاربری ذخیره‌شده در مکان تحت کنترل خود را برای [اختصاص: خطاهای صحت داده] داده‌های رکورد و داده‌های ممیزی را بر اساس مشخصه‌های [اختصاص: درهم شده[۳] داده‌های کاربری ذخیره‌شده] پایش نماید. **اقدامات ارزیابی** • **خلاصه مشخصات محصول**	

[۳] Hash

شماره الزام	نام الزام
در این بخش باید در مورد پیاده‌سازی تشخیص خطای صحت توضیحاتی بیان‌شده باشد.	
۳۹	**صحت داده‌های کاربری ذخیره‌شده ۳**
هنگام تشخیص خطای صحت داده، محصول باید [اختصاص: اقدام لازم] را صورت دهد. **نکته کاربردی ۱۶:** مشخصه‌های داده کاربری می‌تواند انواع فایل‌ها، اندازه فایل و محتوای فایل باشد. محصول به منظور شناسایی خطای صحت داده‌ها باید مشخصه‌های داده‌های کاربری را مانیتور کند تا در صورت تغییر و یا حذف، هشدار دهد. می‌توان برای تشخیص صحت داده‌ها از روش‌های HMAC و یا ECC Checksum و دیگر روش‌های درهم‌سازی استفاده نمود.	
۴۰	**خط‌مشی کنترل دسترسی ۱**
محصول باید [اختصاص: **خط‌مشی‌های کنترل دسترسی**] را بر روی موارد زیر اعمال نماید: [اختصاص: • موجودیت فعال: [اختصاص: مدیر سیستم، کاربر عادی، [اختصاص: دیگر موجودیت‌های فعال] • موجودیت غیرفعال: o رکوردها، مستندات o داده‌های متعلق به کاربر o داده احراز هویت o داده با این معیارها: [اختصاص: معیارهای داده] o [اختصاص: دیگر موجودیت‌های غیرفعال که شامل خط مش کنترل دسترسی می‌باشند]	

شماره الزام	نام الزام

- عملیات:
  - ایجاد موجودیت غیرفعال جدید
  - حذف موجودیت غیرفعال
  - تغییر دسترسی‌ها به موجودیت غیرفعال
  - عملیات بر روی فرداده‌های وابسته به موجودیت غیرفعال
  - [اختصاص: دیگر عملیات]

]

اقدامات ارزیابی

- **خلاصه مشخصات محصول**

در این بخش، باید سازوکار کنترل دسترسی محصول و مشخصه‌های امنیتی مورد استفاده در خط‌مشی کنترل دسترسی به طور خلاصه توضیح داده شود.

- **سند راهنمای محصول**

ارزیاب باید راهنمای محصول را بررسی کرده و تائید نماید که توضیحاتی در مورد خط مش کنترل دسترسی و قوانین کنترل دسترسی برای مدیریت مشخصه‌های امنیتی آمده باشد. همچنین ارزیاب باید در مورد نحوه پیکربندی خط مش کنترل دسترسی شامل مقداردهی پیش فرض مشخصه‌های امنیتی و انتساب مجوزهای موردنیاز برای عملیات مدیریتی بررسی نماید.

- **آزمون‌ها**

ارزیاب باید موارد زیر برای این الزام بررسی کند:

- ✓ همه الگوریتم‌های کنترل دسترسی ذکرشده در سند هدف امنیتی
- ✓ برای هر الگوریتم کنترل دسترسی همه شرایط آمده در سند هدف امنیتی باید سنجیده شود (مانند شرایط منتهی شده به "yes" یا "no")
- ✓ مجموعه ترکیباتی از تنظیمات مشخصه‌های امنیتی مورد استفاده در الگوریتم‌های کنترل دسترسی

شماره الزام	نام الزام
همچنین باید برای این الزام کارکردهای مدیریتی مورد استفاده برای مدیریت مشخصه‌های امنیتی (مشخصه‌های امنیتی که در الگوریتم کنترل دسترسی استفاده می‌شوند) باید آزمون و بررسی شوند.	
۴۱	**عملیات کنترل دسترسی ۱**
محصول باید [اختصاص: **خط‌مشی‌های کنترل دسترسی**] را با توجه به موارد زیر بر روی موجودیت‌های غیرفعال اعمال نماید: [اختصاص: • هویت کاربر • نقش‌ها و مجوزهای کاربر مجاز • اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند • [اختصاص: دیگر مشخصه‌های موجودیت فعال]] **اقدامات ارزیابی** الزامات **عملیات** کنترل دسترسی به الزام خط‌مشی کنترل دسترسی ۱ وابسته هستند و همراه با آن الزام بررسی می‌شوند.	
۴۲	**عملیات کنترل دسترسی ۲**
محصول باید قوانین زیر را اجرا نمایند تا عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل‌شده را مجاز نمایند: [اختصاص: عملیات تنها به شرطی مجاز است که در فهرست کنترل دسترسی، رکوردی وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف‌شده حق دسترسی به موجودیت غیرفعال را بدهد.]	
۴۳	**عملیات کنترل دسترسی ۳**

شماره الزام	نام الزام
محصول باید بر اساس قوانین زیر، دسترسی مجازی از موجودیت فعال به موجودیت غیرفعال داشته باشد: • کاربران با مجوز مدیر سیستم به هر رکورد و روش ارائه‌شده توسط محصول دسترسی دارند. • کاربران غیر مجاز بدون نیاز به فرآیند احراز هویت، به اطلاعات قابل دسترس عموم، دسترسی دارند. • [اختصاص: دیگر قوانین]]	
۴۴	**عملیات کنترل دسترسی ۴**
محصول باید صراحتاً بر اساس قوانین زیر از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید: [اختصاص: • تجاوز چندین نشست آغازشده با نام کاربری مشابه از مقدار آستانه[۴] از پیش تعریف‌شده، • [اختصاص: دیگر قوانین]] **اقدامات ارزیابی** وابسته به الزام قبلی است.	
۴۵	**حفاظت از منابع و داده‌ها ۱**
محصول باید از دسترسی تجمیعی و مستمر به [اختصاص: فهرستی از کارکردها، منابع و داده‌ها] با استفاده از [اختصاص: فهرست محدودیت زمانی/تعداد] محافظت نماید.	

[۴] Threshold

شماره الزام	نام الزام

نکته کاربردی ۱۷:

برای استفاده از منابع و داده باید محدودیتی قائل شد. برای مثال، ویرایش داده در هر ساعت به تعداد مشخصی محدود گردد و یا یک کاربر نباید قادر به حذف کل پایگاه داده‌ها شود.

۴۶	انتقال امن کوکی‌ها ۱

محصول باید اطمینان حاصل نماید که کوکی‌های دارای مشخصه «امن» در سرآیند تنظیم کوکی[۵]، از طریق HTTPS ارسال می‌شوند.

نکته کاربردی ۱۸:

کارکرد سرآیند تنظیم کوکی در *RFC 6265*، تحت عنوان «مکانیسم مدیریت وضعیت HTTP» تشریح شده است.

اقدامات تضمینی:

- **شرح خلاصه هدف ارزیابی**

ارزیاب باید فصل «شرح خلاصه هدف ارزیابی» از سند هدف امنیتی را بررسی کند تا اطمینان حاصل نماید که هدف ارزیابی بر اساس RFC 6265، از مشخصه «امن» از سرآیند تنظیم کوکی پشتیبانی می‌کند. همچون الزام ارسال کوکی‌ها شامل این مشخصه بر روی پروتکل HTTPS اشاره نمود.

- **آزمون‌ها**

ارزیاب باید آزمون‌های زیر را انجام دهد:

[۵] *Set-cookie header*

شماره الزام	نام الزام
آزمون اول: ارزیاب باید هدف ارزیابی را به یک وب‌سایت آزمون متصل کند که کوکی‌های آن فعال‌شده‌اند و پروتکل HTTPS را اجرا می‌کند. سپس ارزیاب باید کاری کند که وب‌سایت، کوکی امن را در اختیار هدف ارزیابی قرار دهد. ارزیاب باید حافظه نهان کوکی هدف ارزیابی را بررسی و تأیید نماید که این حافظه شامل کوکی امن است. آزمون دوم: ارزیاب باید بار دیگر از طریق یک کانال غیر امن به وب‌سایت مذکور متصل شود و تأیید نماید که هیچ کوکی امنی ارسال نشده است.	
۴۷	**رمزگذاری داده‌های حساس برنامه کاربردی ۱**
محصول باید [انتخاب: • از عملکرد ارائه‌شده توسط پلت‌فرم برای رمزگذاری داده‌های حساس استفاده کند، • عملکردی برای رمزگذاری داده‌های حساس پیاده‌سازی کند، • هیچ گونه داده‌های حساسی را در حافظه غیرفرار ذخیره نکند.] **نکته کاربردی ۱۹:** هر فایلی که ممکن است حاوی داده‌های حساس باشد (به طور موقت شامل آن‌ها باشد) باید مورد حفاظت قرار گیرد. مگر آنکه کاربر از روی عمد داده‌های حساس را به یک فایل حفاظت نشده منتقل نماید.	

۶,۵ کلاس مدیریت امنیت

شماره الزام	نام الزام
۴۸	**مدیریت کارکرد در محصول ۱**

شماره الزام	نام الزام
محصول باید توانایی [انتخاب: تعیین رفتار، فعال نمودن، غیرفعال نمودن، تغییر رفتار] کارکرد [اختصاص: **تمام کارکردهای مربوط به مدیریت محصول**] را به [اختصاص: **مدیر سیستم،** [اختصاص: دیگر نقش‌ها]] محدود نماید. **نکته کاربردی ۲۰:** مثالی از این اختصاص: محصول باید قابلیت تغییر رفتار کارکرد جمع‌آوری داده‌های سیستم، آنالیز و عکس‌العمل را تنها به مدیران مجاز سیستم محدود نمایند. **اقدامات ارزیابی** • **خلاصه مشخصات محصول** ارزیاب باید در «خلاصه مشخصات محصول»، هر کارکرد مدیریتی معرفی‌شده در راهنما (که از طریق واسط قابل‌دسترسی هستند) را بررسی و تائید کند. • **سند راهنمای محصول** ارزیاب باید فهرست کارکردهای محصول را در راهنمای مدیریتی بررسی و تائید کند و همچنین باید در مورد نحوه پیکربندی و تنظیمات کارکردها در محصول توضیحاتی داده شود. • **آزمون‌ها** ارزیاب باید یکبار با مجوز مدیر سیستم سعی در تغییر پیکربندی کارکردهای محصول مطابق راهنمای محصول کند و بار دیگر با یک کاربر غیرمجاز تلاش به غیرفعال نمودن و یا تغییر تنظیمات اعمال‌شده در کارکردها را انجام دهد.	
۴۹	**مدیریت مشخصه‌های امنیتی ۱**

شماره الزام	نام الزام
محصول باید با اعمال [اختصاص: خط‌مشی کنترل دسترسی]، توانایی [انتخاب: تغییر پیش‌فرض، پرس و جو، تغییر، حذف، [اختصاص: دیگر عملیات]] مشخصه‌های امنیتی [اختصاص: فهرستی از مشخصه‌های امنیتی تعریف‌شده در الزام انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر۱] را به [مدیر سیستم،[اختصاص: دیگر نقش‌ها]] محدود نماید. **اقدامات ارزیابی** • **سند راهنمای محصول** ارزیاب باید راهنمای محصول را بررسی کند و شرایطی که یک کاربر اجازه مدیریت مشخصه‌های امنیتی موجودیت‌های غیرفعال را دارد اطمینان حاصل نماید. • **آزمون‌ها** ارزیاب باید تمامی واسط‌های مرتبط با مدیریت مشخصه‌های امنیتی موجودیت‌های غیرفعال و همه مشخصه‌های امنیتی موجودیت‌های غیرفعال با مقداردهی آن‌ها (البته به عنوان بخشی از آزمون الگوریتم کنترل دسترسی در الزام قبل بررسی می‌شوند) را آزمون نماید.	
۵۰	**مدیریت مشخصه‌های امنیتی ۳**
محصول برای مشخصه‌های امنیتی که برای اعمال[اختصاص: خط‌مشی] استفاده می‌شوند، باید مقادیر پیش فرض محدودشده‌ای در نظر بگیرد. **اقدامات ارزیابی** به الزام مدیریت کارکرد در محصول ۱ وابسته است.	
۵۱	**مدیریت مشخصه‌های امنیتی ۴**

شماره الزام	نام الزام
محصول برای تعیین مقادیر اولیه پیشنهادی باید به [اختصاص: مدیر سیستم] اجازه دهد تا هنگام ایجاد اطلاعات یا موجودیت غیرفعال، مقادیر پیش‌فرض را لغو و تغییر دهد.	
۵۲	**مدیریت داده‌های محصول ۱-مدیر سیستم**
محصول باید توانایی [انتخاب: تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک نمودن، [اختصاص: **دیگر کارکردها**]] [اختصاص: **فهرستی از داده‌های محصول**] به [اختصاص: مدیر سیستم،[اختصاص: دیگر نقش‌ها]] محدود نماید. **نکته کاربردی ۲۱:** داده‌های محصول می‌تواند شامل داده‌های ممیزی، کلیدها و داده‌های احراز هویت و از این نوع داده‌ها باشد. مثالی از این الزام: محصول باید توانایی **مدیریت** داده‌های خود را تنها به مدیر امنیتی محدود نماید. «**مدیریت**» در این الزام می‌تواند شامل موارد زیر باشد: ایجاد، مقداردهی، مشاهده، تغییر پیش‌فرض، تغییر دادن، حذف ، پاک کردن و اضافه کردن **اقدامات ارزیابی** به الزام مدیریت کارکرد در محصول وابسته است.	
۵۳	**مدیریت داده‌های محصول ۱-کاربر عادی، واردکننده داده**
محصول باید توانایی [انتخاب: تغییر پیش‌فرض، پرس‌وجو، تغییر، حذف، پاک کردن، [اختصاص: **دیگر کارکردها**]] [اختصاص: **داده‌های تحت مالکیت کاربر عادی**] به [اختصاص: کاربر عادی] محدود نماید.	

شماره الزام	نام الزام

اقدامات ارزیابی

به الزام مدیریت کارکرد در محصول وابسته است. همچنین ارزیاب باید حداقل یک کارکرد محصول را با کاربر غیرمجاز این الزام را آزمون نماید.

۵۴	**کارکردهای مدیریتی محصول ۱**

محصول باید قادر به انجام [اختصاص: کارکردهای مدیریتی که در جدول زیر آمده است] باشد:

مؤلفه	عملیات مدیریتی
بازبینی داده ممیزی ۱	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی
انتخاب داده ممیزی ۱	پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی
ذخیره‌سازی رویدادهای ممیزی	پشتیبانی از عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی
عملیات کنترل دسترسی ۱	مدیریت مشخصه‌های مورد استفاده برای ایجاد دسترسی و یا منع
ورود داده‌های کاربری به محصول	ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول
صحت داده‌های کاربری ذخیره‌شده ۲	عملیاتی برای تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی باشد.
مدیریت احراز هویت ناموفق ۱	مدیریت حد آستانه برای تلاش‌های ناموفق مدیریت عملیاتی که هنگام رویداد شکست احراز هویت باید صورت گیرد.
تعریف مشخصات کاربر ۱	مدیر مجاز باید قادر به تعریف مشخصه‌های امنیتی بیشتر برای کاربران باشد.
مدیریت کلمه عبور ۱	مدیریت معیارها برای بررسی کلمه عبورها
انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر۱	مدیر مجاز می‌تواند مشخصه‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف و یا تغییر دهد
مدیریت مشخصه‌های امنیتی 1	مدیریت گروهی از نقش‌هایی که با مشخصه‌های امنیتی در تعامل هستند.
مدیریت مشخصه‌های امنیتی ۳	مدیریت گروهی از نقش‌هایی که مقادیر اولیه را مشخص می‌کنند. مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول

شماره الزام	نام الزام

مدیریت داده‌های محصول ۱-مدیر سیستم	مدیریت گروهی از قوانینی مرتبط با داده‌های محصول
مدیریت داده‌های محصول ۱-کاربر عادی، واردکننده داده	مدیریت گروهی از قوانینی مرتبط با داده‌های محصول
نقش‌های امنیتی ۱	مدیریت گروهی از کاربرانی که بخشی از یک نقش هستند.
محدودیت بر روی چندین نشست هم‌زمان ۱	مدیریت حداکثر نشست مجاز کاربران به طور هم‌زمان توسط مدیر
برقراری نشست ۱	مدیریت شرایط آغاز نشست توسط مدیر مجاز
قفل‌کردن و خاتمه دادن به نشست‌ها ۵	تعیین زمان غیرفعال بودن کاربر که نشست آن کاربر خاتمه یابد. تعیین زمان پیش‌فرض غیرفعال بودن کاربر که نشست خاتمه یابد.

اقدامات ارزیابی

- **خلاصه مشخصات محصول**

تمام کارکردهای امنیتی محصول به طور خلاصه باید در این بخش توضیح داده شود.

۵۵	**نقش‌های امنیتی ۱**

نقش‌های زیر در محصول باید تعریف‌شده باشد:

[اختصاص: مدیر سیستم،

کاربر عادی،

[اختصاص: دیگر **نقش‌های مجاز معرفی‌شده**]]

نکته کاربردی ۲۲:

از جمله نقش‌های مجاز می‌توان به «مدیر مجاز»، «مدیر تحلیلگر مجاز»، «اپراتورها» اشاره نمود، نویسنده سند هدف امنیتی در این الزام می‌تواند از نقش‌های مجاز دیگر نیز استفاده نماید.

اقدامات ارزیابی

شماره الزام	نام الزام
• **خلاصه مشخصات محصول** ارزیاب باید توضیحاتی در مورد نقش مدیریتی و نقش‌هایی با دسترسی پایین را در این بخش پیدا نماید. • **سند راهنمای محصول** ارزیاب باید راهنمای مدیریتی محصول را مطالعه و اطمینان حاصل کند که دستورالعمل‌هایی برای مدیریت محصول هم به‌طور محلی و از راه دور وجود دارد و شامل پیکربندی‌هایی موردنیاز برای مدیریت راه دور است. • **آزمون‌ها** ارزیاب باید اطمینان حاصل نماید که نقش مدیریتی می‌تواند تمامی کارکردهای امنیتی محصول که در هدف امنیتی ذکرشده را مدیریت نماید. ارزیاب باید نقش مدیریتی و یا کاربر با یک نقش محدود را به طور محلی و یا از راه دور بر روی محصول آزمون نماید.	
۵۶	**نقش‌های امنیتی ۲**
محصول، باید قادر به مرتبط کردن کاربران با نقش‌های مجاز تعریف‌شده باشد. **نکته کاربردی ۲۳:** 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. **اقدامات ارزیابی** این الزام وابسته به الزام قبلی است.	

۶,۶ کلاس حفاظت از توابع امنیتی محصول

شماره الزام	عنصر امنیتی
۵۷	**حفظ وضعیت امن در زمان شکست ۱**
محصول باید در زمان رخداد انواع شکست‌های زیر، وضعیت امن را حفظ نمایند: [اختصاص: شکست‌های نرم‌افزاری، شکست‌های کاربری] **نکته کاربردی ۲۴:** شکست نرم‌افزاری به معنی از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول است که در این صورت محصول باید در وضعیت امنی قرارگرفته و صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ نماید. **اقدامات ارزیابی** • **خلاصه مشخصات محصول** ارزیاب باید در خلاصه مشخصات محصول، مستند پیاده‌سازی شکست امن محصول را بررسی و مشاهده نماید. همچنین باید انواع مدهای شکست محصول باید در سند هدف امنیتی توضیح داده شود و وضعیت امن هرکدام از شکست‌ها نیز باید آمده باشد. • **آزمون‌ها** ارزیاب باید انواع شکست‌ها را ایجاد و با وضعیت امن مقایسه و بررسی کند.	
۵۸	**سازگاری داده‌های امنیتی بین محصول و موجودیت امن ۱**
محصول در صورت استفاده از محصولات امن IT، باید تفسیر سازگار [اختصاص: فهرستی از انواع داده‌های امنیتی محصول] را در زمان اشتراک‌گذاری داده‌های امنیتی بین خود و دیگر محصولات امن IT، فراهم آورد. **نکته کاربردی ۲۵:**	

شماره الزام	عنصر امنیتی
منظور از داده‌های امنیتی محصول، داده‌های احراز هویت، کلید، امضای دیجیتال، داده‌های ممیزی و از این نوع داده‌ها است. **اقدامات ارزیابی** • **سند راهنمای محصول** در راهنمای مدیریتی محصول باید توضیحاتی درباره انواع داده‌های امنیتی محصول و داده‌های دریافتی از دیگر محصولات امن IT آمده باشد.	
۵۹	**سازگاری داده‌های امنیتی بین محصول و موجودیت امن ۲**
محصول باید هنگام تفسیر داده‌های دریافتی از دیگر محصولات IT امن، [اختصاص: فهرستی از قوانین تفسیر که در محصول به کار می‌روند] استفاده نماید. **اقدامات ارزیابی** • **آزمون‌ها** ارزیاب باید داده‌های دریافتی از دیگر محصولات را در داخل محصول مشاهده نماید و باید مطابق با آنچه که ادعای محصول است، باشد.	
۶۰	**انتقال داده امنیتی در داخل محصول ۱**
محصول باید هنگام انتقال داده‌ها بین بخش‌های مجزای خود، در برابر افشاء یا تغییر محافظت نماید. **نکته کاربردی ۲۶:** منظور از بخش‌های مجزا به این معنی است که بخش‌های محصول برروی دو سیستم مجزا قرارگرفته باشد، مانند وب سرور بر روی یک سیستم و بانک اطلاعاتی روی سیستم دیگر در یک شبکه عمومی باشد و یا دو بخش مجزای محصول یکی بر روی وب سرور و دیگری بر روی کلاینت باشد. **اقدامات ارزیابی**	

شماره الزام	عنصر امنیتی
	• **خلاصه مشخصات محصول** ارزیاب باید در خلاصه مشخصات محصول بررسی کند که روش و یا پروتکل‌هایی را برای انتقال داده بین اجزای توزیع‌شده محصول باشد. • **سند راهنمای محصول** ارزیاب باید در راهنمای محصول، توضیحاتی در مورد روش و یا پروتکل ارتباطی بین اجزای محصول پیدا کند. • **آزمون‌ها** ارزیاب باید اقدامات زیر را انجام دهد: آزمون اول: ارزیاب باید از روش ارتباطی آمده در راهنما را آزمون کند. آزمون دوم: ارزیاب باید اطمینان حاصل نماید که داده‌ها بین اجزای محصول به‌صورت آشکار نمایش داده نشود. آزمون سوم: ارزیاب باید اطمینان حاصل نماید که ویرایش داده‌ها حین انتقال توسط محصول تشخیص داده شود.
۶۱	**مهرهای زمانی ۱**
	محصول، باید قادر به ایجاد مهره‌های زمانی قابل اطمینان باشند. **اقدامات ارزیابی** • **خلاصه مشخصات محصول** ارزیاب باید اطمینان حاصل نماید در خلاصه مشخصات محصول که هر کارکرد امنیتی که از زمان استفاده می‌کند فهرست شده باشد. • **سند راهنمای محصول** ارزیاب باید در راهنمای محصول، دستورالعمل‌هایی در مورد تنظیمات و پیکربندی زمان توضیحاتی پیدا کند. • **آزمون‌ها** ارزیاب باید اقدامات زیر را اجرا کند:

شماره الزام	عنصر امنیتی
آزمون اول: ارزیاب باید مطابق راهنمای محصول زمان را پیکربندی نموده و سپس با توجه به واسط مربوطه از درست کار کردن آن اطمینان حاصل نماید. آزمون دوم: ارزیاب باید سعی کند توسط کاربر غیرمجاز با استفاده از واسط مربوط تلاش در تغییر پیکربندی زمان نماید. آزمون سوم: اگر محصول از سرور NTP پشتیبانی می‌کند باید کلاینت NTP را بر روی محصول پیکربندی نماید و زمان سرور و کلاینت را بررسی کند.	
۶۲	**قابلیت‌های ضد اکسپلویت ۴**
برنامه کاربردی نباید فایل‌هایی که توسط کاربر قابل تغییر هستند را در دایرکتوری‌هایی بنویسد که حاوی فایل‌های اجرایی‌اند. **نکته کاربردی ۲۸:** فایل‌های اجرایی و فایل‌هایی که توسط کاربر قابل تغییر هستند، نباید از دایرکتوری والد[۶] مشابهی استفاده نمایند، اما ممکن است از دایرکتوری‌هایی بالاتر از دایرکتوری والد استفاده کنند.	
۶۳	**مدیریت داده‌های محصول ۱**
محصول باید بعد از اتمام تاریخ انقضاء هر نوع داده‌های حساس، روشی برای حذف آن‌ها داشته باشد. **نکته کاربردی ۲۹:** به عنوان مثال، بعد از ۳۰ روز کلمه عبور کاربران باید منقضی شود و کلمه عبور قبلی حذف گردد.	
۶۴	**مدیریت کلیدهای موجود در محصول ۱**
محصول باید اطمینان دهد که داده‌های حساس از قبیل کلمه عبور و کلید و اطلاعات شناسایی شخصی در سمت کلاینت نگهداری نمی‌شود.	

[۶] Parent Directory

۶,۷ کلاس دسترسی به محصول

شماره الزام	نام الزام
۶۵	**محدودیت بر روی چندین نشست هم‌زمان ۱**
محصول باید حداکثر تعداد نشست‌های هم‌زمان متعلق به یک کاربر را محدود نماید. **اقدامات ارزیابی** • **سند راهنمای محصول** ارزیاب باید توضیحاتی در مورد نحوه پیکربندی تعداد نشست هم‌زمان برای یک کاربر در راهنمای محصول پیدا نماید. • **آزمون‌ها** ارزیاب باید با توجه به راهنمای محصول حداکثر نشست یک کاربر را پیکربندی کند و سپس با همان کاربر از چند سیستم به طور هم‌زمان سعی در ایجاد نشست نماید. در این صورت اگر تعداد نشست بیش از مقدار مشخص‌شده باشد باید اجازه ایجاد نشست را ندهد.	
۶۶	**محدودیت بر روی چندین نشست هم‌زمان ۲**
محصول باید به صورت پیش‌فرض، [اختصاص: تعداد نشست هم‌زمان پیش‌فرض] برای هر کاربر در نظر بگیرد. **اقدامات ارزیابی** وابسته به الزام قبلی است.	
۶۷	**قفل‌کردن و خاتمه دادن به نشست‌ها ۵**

شماره الزام	نام الزام
محصول باید کلیه نشست‌های تعاملی راه دور[۷] را پس از مدت زمان [اختصاص: **بازه زمانی که توسط مدیر تنظیم می‌شود**] غیرفعال بودن، خاتمه دهد. **اقدامات ارزیابی** • **سند راهنمای محصول** در راهنمای محصول باید در مورد نحوه پیکربندی زمان غیرفعال بودن نشست را توضیحاتی بیان‌شده باشد. • **آزمون‌ها** ارزیاب باید مطابق راهنمای محصول، مقادیر مختلف برای زمان غیرفعال بودن نشست تنظیم و پیکربندی کند که این مقادیر شامل حداقل و حداکثر زمان غیرفعال بودن طبق راهنما باشند. سپس ارزیاب برای هر زمان تنظیم‌شده نشستی با از راه دور با محصول ایجاد و درستی زمان غیرفعال بودن نشست را بررسی نماید که باعث خاتمه یافتن نشست می‌شود.	
۶۸	**قفل‌کردن و خاتمه دادن به نشست‌ها ۶**
محصول باید اجازه خاتمه نشست، از سوی کاربری که خود آغازگر نشست بوده است را بدهد. **اقدامات ارزیابی** • **آزمون‌ها** ارزیاب باید اقدامات زیر را اجرا نماید: آزمون اول: ارزیاب باید نشست محلی با محصول ایجاد کند و سپس مطابق راهنما با استفاده از موارد "Exit" یا "Log out" از محصول خارج شود و بررسی کند که آیا نشست خاتمه یافته است. آزمون دوم: ارزیاب باید نشستی از راه دور با محصول ایجاد کند و سپس مطابق راهنما با استفاده از موارد "Exit" یا "Log out" از محصول خارج شود و بررسی کند که آیا نشست خاتمه یافته است.	

[۷] Remote

شماره الزام	نام الزام
۶۹	**سوابق دسترسی به محصول ۱**
در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش (موفق/ناموفق) برای ایجاد نشست بر اساس [انتخاب: روز، زمان، [اختصاص: دیگر مشخصه‌ها]] باشد.	
۷۰	**سوابق دسترسی به محصول ۲**
محصول باید قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست بر اساس [انتخاب: روز، زمان، [اختصاص: دیگر مشخصه‌ها]] و تعداد تلاش ناموفق تا آخرین ایجاد نشست موفقیت‌آمیز باشد. **اقدامات ارزیابی** • **سند راهنمای محصول** باید در این راهنما در مورد نحوه پیکربندی نمایش تعداد و آخرین تلاش ناموفق توضیحاتی آمده باشد. • **آزمون‌ها** ارزیاب چندین بار با استفاده از یک نام کاربری با شرایطی غیرمجاز (مانند کلمه عبور نادرست) تلاش به برقراری نشست با محصول نماید و سپس یک نشست موفقیت‌آمیزی را برقرار نماید و سپس بررسی کند که تعداد تلاش‌های ناموفق کاربر و زمان آخرین تلاش برای برقراری نشست در محصول ثبت‌شده باشد.	
۷۱	**سوابق دسترسی به محصول ۳**
محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر از واسط کاربری پاک نماید. **اقدامات ارزیابی** • **سند راهنمای محصول** در صورت وجود پیکربندی اطلاعات سوابق دسترسی باید در راهنمای مدیریتی محصول توضیحاتی آمده باشد.	

شماره الزام	نام الزام
۷۲	**برقراری نشست ۱**

محصول باید قادر به ممانعت از ایجاد نشست بر اساس [انتخاب: مکان، شماره پورت، روز، زمان، [اختصاص: دیگر مشخصه‌ها]] باشد.

اقدامات تضمینی

- **خلاصه مشخصات محصول**

ارزیاب باید در خلاصه مشخصات محصول باید بررسی کند که تمام مشخصه‌های کلاینتی که باید نشست آن منع شود، تعریف‌شده باشد.

- **راهنما**

ارزیاب باید در راهنمای محصول، توضیحاتی درباره پیکربندی هر مشخصه‌ای که در خلاصه مشخصات محصول آمده است (مشخصه‌هایی مانند آدرس IP ، زمان/تاریخ، آدرس فیزیکی و ...) پیدا کند.

- **آزمون‌ها**

ارزیاب باید برای هر یک از مشخصه‌ها آزمون زیر را انجام دهد:

آزمون اول: ارزیاب باید با یک کاربر یک نشست موفقیت‌آمیزی را ایجاد کند، سپس مطابق راهنما، مشخصه‌های کاربر را طوری پیکربندی کند که از دسترسی آن کاربر به محصول ممانعت شود. ارزیاب باید تلاش در برقراری نشستی باشد که مشخصه‌ای از آن (مانند آدرس IP و یا مکان کاربر) برای دسترسی منع شده باشد و تلاش ناموفق دسترسی کاربر را مشاهده کند.

۶,۸ کلاس کانال‌ها/مسیرهای مورد اعتماد

برای این کلاس، تعدادی الزام مبتنی بر انتخاب در پیوست یک ارائه‌شده است.

شماره الزام	نام الزام
۷۳	**کانال امن ۱**
محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل [انتخاب:TLS, HTTPS] میان خود و موجودیت IT معتبر همچون سامانه کاربر، سرور ممیزی، [انتخاب: سرور احراز هویت، اختصاص:[دیگر قابلیت‌ها]] که به طور منطقی از کانال‌های دیگر متمایز است فراهم نماید تا آن‌ها را احراز هویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد.	
۷۴	**کانال امن ۲**
محصول مورد ارزیابی باید اجازه داشته باشد به موجودیت‌های معتبرIT اجازه دهد که ارتباطات را از طریق کانال امن آغاز کنند.	
۷۵	**کانال امن ۳**
محصول مورد ارزیابی باید ارتباطات را از طریق کانال امن، برای [اختصاص: فهرست خدماتی که محصول مورد ارزیابی می‌تواند برای آن‌ها ارتباطات را آغاز کند] راه‌اندازی نماید. **نکته کاربردی ۳۰:** هدف از الزام حاضر این است که ابزاری را برای استفاده از پروتکل رمزنگاری جهت حفاظت از ارتباطات خارجی با موجودیت‌های معتبر IT کارکرد فراهم آورد. منظور از موجودیت‌های معتبر IT موجودیت‌هایی است که محصول مورد ارزیابی برای انجام کارکردهای خود با آن‌ها ارتباط برقرار می‌کند. محصول مورد ارزیابی دست کم از یکی از پروتکل‌های فهرست‌شده استفاده می‌کند تا با سرور جمع‌آوری اطلاعات ممیزی ارتباط برقرار کند. این الزام بیان می‌دارد که نه تنها ارتباطات در هنگام برقراری اولیه حفاظت می‌شوند، بلکه در حین برقراری مجدد ارتباط پس از یک قطعی نیز از آن‌ها محافظت می‌شود. ممکن است نیاز به تنظیم دستی کانال‌هایی برای حفاظت از سایر ارتباطات وجود داشته باشد. در صورتی که پس از یک قطعی، محصول مورد ارزیابی تلاش کند تا ارتباطات را به صورت خودکار و با دخالت عامل انسانی از سر گیرد، ممکن است پنجره‌ای باز شود که مهاجمان بتوانند از طریق آن به اطلاعات مهمی دست یابند یا ارتباط را در معرض خطر قرار دهند.	
۷۶	**مسیر امن ۱**

شماره الزام	نام الزام
محصول، باید مسیر ارتباطی امنی را با استفاده از پروتکل [انتخاب: SSH, TLS, HTTPS] برای ایجاد کانال ارتباطی امن بین خود و مدیر سیستم راه دور را داشته که به طور منطقی از کانال‌های دیگر متمایز است فراهم نماید تا آن را احراز هویت کرده و از داده‌های تبادلی در برابر تغییر و افشاء محافظت نموده و تغییرات را تشخیص دهد.	
۷۷	**مسیر امن ۲**
محصول مورد ارزیابی باید به مدیر سیستم معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.	
۷۸	**مسیر امن ۳**
محصول مورد ارزیابی باید استفاده از کانال امن را برای احراز هویت اولیه مدیر سیستم و تمام فعالیت‌های راه دور مدیر سیستم الزامی کند. **نکته کاربردی ۳۱:** این الزام اطمینان حاصل می‌نماید که مدیران سیستم معتبر ، تمام ارتباطات از راه دور را با محصول مورد ارزیابی، از طریق یک مسیر امن آغاز می‌کنند و در طی ارتباط با محصول مورد ارزیابی، همچنان از مسیر امن استفاده می‌نمایند. داده‌های منتقل‌شده از طریق این مسیر، با استفاده از پروتکل انتخاب‌شده در عبارت انتخاب، رمزگذاری می‌شوند.	

۶,۹ کلاس محرمانگی

شماره الزام	نام الزام
۷۹	**استفاده کاربر از یک سرویس بدون افشاء هویت ۴**
محصول باید [انتخاب: اطلاعات شناسایی شخصی (PII) را در شبکه به‌طور متن آشکار انتقال ندهد]. **نکته کاربردی ۳۲:**	

شماره الزام	نام الزام
این الزام تنها در مورد اطلاعات شناسایی شخصی صدق می‌کند که اختصاصاً توسط محصول درخواست شده است؛ و شامل مواقعی نمی‌شود که کاربر به صورت داوطلبانه و بدون درخواست محصول اطلاعات شناسایی شخصی خود را در یک صفحه عمومی (نامناسب) وارد می‌کند. باز شدن یک جعبه گفتگو[۸] حین آغاز محصول که قصد محصول را از ارسال اطلاعات شناسایی شخصی به کاربر اطلاع می‌دهد، اقدامی کافی برای تبعیت از این الزام است.	

۷ الزامات تضمین امنیت

اهداف امنیتی تعریف‌شده در بخش ۵ جهت مقابله نمودن با تهدیدات معرفی‌شده در بخش ۴ در نظر گرفته‌شده‌اند. الزامات کارکردی در بخش ۶ بیان رسمی و استانداردی از «اهداف امنیتی» است. الزامات تضمین امنیتی که برگرفته از استاندارد ارزیابی امنیتی معیار مشترک می‌باشند تا بر اساس این الزامات ارزیابی، مستندات را ارزیابی و آزمون مستقل برروی محصول انجام دهد.

مدل کلی ارزیابی محصول در برابر سند هدف امنیتی که مطابق این پروفایل حفاظتی است، به صورت زیر است:

پس از تائید سند هدف امنیتی برای ارزیابی، تولیدکننده محصول رادر اختیار آزمایشگاه قرار می‌دهد و محیط آزمون آن را فراهم می‌نماید؛ و سپس فعالیت‌های تضمین که در سند هدف امنیتی مطرح‌شده، توسط آزمایشگاه انجام می‌شود. نتایج این فعالیت‌ها مستند و برای اعتباربخشی به مرکز گواهی ارائه می‌شود.

نام کلاس	نام الزام	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری

[۸] Dialog Box

	AGD_PRE.1	راهنمای آماده‌سازی
Tests	ATE_IND.1	آزمون مستقل-منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری
Life cycle Support	ALC_CMC.1	برچسب‌گذاری محصول
	ALC_CMS.1	پوشش پیکربندی محصول

۷,۱ کلاس توسعه

اطلاعات محصول، از طریق «مستندات راهنمای کاربر» و بخش «مشخصات امنیتی محصول» از سند هدف امنیتی در اختیار کاربر نهایی قرار می‌گیرد. الزامی بر وجود بخش «مشخصات امنیتی محصول» در سند هدف امنیتی نمی‌باشد، اما در صورت وجود باید محتوای آن با الزامات کارکردی مرتبط بوده و مورد تائید توسعه‌دهندگان محصول باشد.

مشخصات کارکردی:

مشخصات کارکردی، واسطهای کارکرد امنیتی محصول را توصیف می‌نماید اما نیازی به شرح مفصل و کاملی از این واسطها نمی‌باشد. فعالیت‌های این خانواده باید بر روی شناخت واسطهای معرفی‌شده در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و «مستندات راهنما» متمرکز گردد.

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید مشخصات کارکردی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
	شماره مؤلفه: (ADV_FSP.1.2D) **شرح مؤلفه:** توسعه‌دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. **نکته کاربردی:** مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده‌سازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات محصول» سند هدف امنیتی ارائه‌شده است، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات محصول» وجود داشته باشند، الزامات کارکردی تضمین می‌گردند. از آنجا که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شده‌اند، بنابراین ارتباط مطرح‌شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نمی‌باشد.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجراکننده کارکرد امنیتی[۹] و پشتیبان کننده‌ی الزام کارکرد امنیتی[۱۰] توصیف نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.2C)** **شرح مؤلفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجراکننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.3C)** **شرح مؤلفه:** مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.4C)** **شرح مؤلفه:** ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسط‌های کارکرد امنیتی در سند مشخصات کارکردی باشد.

[۹]-SFR-enforcing TSFI

[۱۰]-SFR-supporting TSFI

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: مشخصات کارکرد ابتدایی۱ **شماره مؤلفه: (ADV_FSP.1.2E)** **شرح مؤلفه:** ارزیاب باید مشخص نماید که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشند.

مستندات «مشخصات کارکردی» جهت پشتیبانی از ارزیابی الزامات کارکردی و اقدامات لازم در کلاس‌های «راهنما»، «آزمون» و «آسیب‌پذیری» ارائه‌شده است.

۷,۲ کلاس راهنمای کاربر

مستندات راهنما همراه با سند هدف امنیتی برای استفاده کاربران ارائه خواهند شد. در این دسته از مستندات شرحی از مدل مدیریتی و نحوه بررسی محیط عملیاتی توسط مدیر (تا مشخص گردد که آیا می‌تواند نقش خود را برای کارکرد امنیتی ایفا نماید) ارائه می‌شود.

برای هر محیط عملیاتی که در سند هدف امنیتی ادعای پشتیبانی از آن شده باید مستند راهنما ارائه گردد. این راهنما شامل:

دستورالعمل نصب موفقیت‌آمیز محصول در محیط

دستورالعمل مدیریت امنیت محصول به عنوان یک محصول و به عنوان بخشی از یک محیط عملیاتی بزرگ‌تر

دستورالعمل‌هایی که ارائه‌دهنده قابلیت مدیریتی محافظت‌شده از طریق استفاده از قابلیت‌های محصول، محیط عملیاتی یا هر دو است.

۷,۲,۱ راهنمای کاربردی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید راهنمای کاربردی ارائه نماید.

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی را که باید در یک محیط پردازشی امن کنترل شوند توصیف نماید، همانند هشدارهای مناسب.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.2C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف نماید که چگونه از واسط‌های در دسترس ارائه‌شده توسط محصول به صورت امن استفاده می‌گردد.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.3C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسط‌های در دسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف نموده و مقادیر امن را به صورت مناسبی تعیین نماید.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.4C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هر نوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط نماید، همانند تغییر مشخصات امنیتی موجودیت-های تحت کنترل توابع امنیتی محصول.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.5C)** **شرح مؤلفه:** سند راهنمای کاربردی باید تمام مدهای عملیاتی محصول (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آن‌ها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
	نام عنصر: راهنمای کاربردی ۱

مؤلفه‌های محتوایی	
نام خانواده	**عنصر امنیتی**
	شماره مؤلفه: (AGD_OPE.1.6C) **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی را که توسط کاربر تبعیت می‌شوند توصیف نماید تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده‌شده‌اند، کاملاً اجرا گردند.
	نام عنصر: راهنمای کاربردی ۱ **شماره مؤلفه: (AGD_OPE.1.7C)** **شرح مؤلفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۷,۲,۲ راهنمای آماده‌سازی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید محصول را همراه با سند آماده‌سازی ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1C)** **شرح مؤلفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن محصول توسط مشتری را مطابق با رویه‌های تحویل توسعه‌دهنده شرح دهند.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مؤلفه: (AGD_PRE.1.2C)** **شرح مؤلفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن محصول و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکرشده در سند هدف امنیتی، شرح دهند.

مؤلفه‌های اقدامات ارزیاب	
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: راهنمای آماده‌سازی ۱ **شماره مؤلفه: (AGD_PRE.1.2E)** **شرح مؤلفه:** ارزیاب باید رویه‌های آماده‌سازی شرح داده‌شده در سند را بکار ببرد تا تائید نماید، محصول می‌تواند به صورت امن برای عمل نمودن آماده شود.

۷,۳ کلاس آزمون

آزمون محصول برای بررسی بخش‌های کارکردی سیستم و همچنین بخش‌هایی که طراحی و پیاده‌سازی آن‌ها برای سیستم دارای آسیب‌های امنیتی است، در نظر گرفته می‌شود. آزمون بخش‌های کارکردی سیستم از طریق خانواده ATE_IND؛ و آزمون بخش‌هایی که طراحی و پیاده‌سازی آسیب‌زایی دارند از طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL1) آزمون بر اساس کارکردی که برای محصول در نظر گرفته‌شده و واسط‌هایی که بر اساس اطلاعات طراحی در اختیار ارزیاب قرار می‌گیرد، انجام می‌گردد. نتایج آزمون و تحلیل آسیب‌پذیری باید در گزارش آزمون لحاظ شوند این مسئله در الزامات زیر در نظر گرفته‌شده است.

۷,۳,۱ آزمون مستقل

«آزمون مستقل» برای تائید کارکرد محصول که در بخش «مشخصات امنیتی محصول» از سند هدف امنیتی و مستندات «راهنمای مدیر» ارائه‌شده، صورت می‌گیرند. هدف اصلی آزمون اطمینان از برآورده شدن الزامات کارکردی مشخص‌شده در سند هدف امنیتی است. ارزیاب باید در سند «گزارش آزمون»، طرح آزمون و نتایج آن را مستند نماید.

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید برای آزمودن، محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1C)** **شرح مؤلفه:** محصول باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات ارزیاب	
آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1E)**

مؤلفه‌های اقدامات ارزیاب	
	شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آزمون مستقل ۱ **شماره مؤلفه: (ATE_IND.1.2E)** **شرح مؤلفه:** ارزیاب باید زیرمجموعه‌ای از توابع امنیتی محصول را آزمون نماید تا تائید نماید که توابع امنیتی محصول به صورت مشخص‌شده عمل می‌نمایند.

۷,۴ کلاس آسیب‌پذیری

۷,۴,۱ تحلیل آسیب‌پذیری

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید برای آزمودن، محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1C)** **شرح مؤلفه:** محصول باید مناسب آزمودن باشد.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده، تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: آسیب‌پذیری ۱ **شماره مؤلفه: (AVA_VAN.1.2E)** **شرح مؤلفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در محصول، در منابع عمومی جستجویی را انجام دهد.
	نام عنصر: آسیب‌پذیری ۱ **شماره مؤلفه: (AVA_VAN.1.3E)** **شرح مؤلفه:**

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
	ارزیاب باید بر اساس آسیب‌پذیری‌های بالقوه شناسایی‌شده، آزمون نفوذ انجام دهد تا مقاومت محصول را در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص نماید.

۷,۵ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه‌شده است (EAL1) کلاس پشتیبانی از چرخه حیات به ویژگی‌هایی از چرخه حیات محدود می‌گردد که توسط کاربر نهایی قابل مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه‌دهنده نقش کمرنگی در قابل اعتماد بودن محصول دارد، بلکه در این سطح اطمینان (EAL1) تنها به این اطلاعات نیاز است.

۷,۵,۱ قابلیت‌های پیکربندی

این مؤلفه جهت معرفی محصول به صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه‌شده، است (بدین معنی که جدا از برچسب‌گذاری محصول، محصول که ممکن است بخشی از یک محصول باشد به تنهایی، برچسب‌گذاری شود، نام محصول، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند محصولی را که توسط مرکز گواهی تائید شده است را به آسانی تشخیص دهد.

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید محصول و مرجع محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1C)** **شرح مؤلفه:** محصول باید با یک مرجع یکتا برچسب زده شود.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۷,۵,۲ حوزه پیکربندی

مؤلفه‌های اقدامات توسعه‌دهنده	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1D)** **شرح مؤلفه:** ارزیاب باید فهرست پیکربندی محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1C)** **شرح مؤلفه:** فهرست پیکربندی باید شامل خود محصول و مدارک موردنیاز توسط الزامات تضمین امنیتی باشد.
	نام عنصر: پوشش پیکربندی محصول ۱ **شماره مؤلفه: (ALC_CMS.1.1C)** **شرح مؤلفه:** فهرست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی نماید.

مؤلفه‌های اقدامات ارزیاب	
نام خانواده	**عنصر امنیتی**
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه‌شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

۸ پیوست یک: الزامات مبتنی بر انتخاب

۸,۱ الزامات کلاس پشتیبانی از رمزنگاری

شماره الزام	نام الزام
۸۰	**عملیات رمزنگاری ۱-رمزنگاری و رمزگشایی ۱(۲)**
محصول باید [رمزنگاری و رمزگشایی] را مطابق با الگوریتم رمزنگاری متقارن AES- XTSمطابق مستند,NIST SP 800- 38E AES-CBC مطابق سند NIST SP 800- 38A AES-CCMP مطابق سند FIPS PUB 197، NIST SP 800- 38C و IEEE 802.11 2012 و [انتخاب: AES Key Wrap (KW مطابق سند NIST SP 800-38F, AES Key Wrap with Paddi ng (KWP مطابق سند NIST SP 800-38F، AES- GCMمطابق سند NIST SP 800-38D, AES- CCMمطابق سند NIST SP 800-38C, AES-CCMP-256مطابق سند NIST SP800-38Cو IEEE 802.11 ac-2013, AES-GCMP-256مطابق سند NIST SP800-38Dو IEEE 802.11 ac-2013 و هیچ‌کدام] با اندازه کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی را انجام دهد.	

شماره الزام	نام الزام
۸۱	**عملیات رمزنگاری ۱ (۴)**

محصول مورد ارزیابی باید خدمات امضای دیجیتال (تولید و تأیید) را بر اساس الگوریتم‌های رمزنگاری زیر ارائه کند: [انتخاب:

- الگوی RSA: اندازه کلیدهای [انتخاب: ۲۰۴۸ بیتی یا بزرگ‌تر] و بر اساس FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS» بخش ۴
- در مورد الگوی دیجیتال بیضوی ECDSA: اندازه کلیدهای [انتخاب: ۲۵۶ بیتی یا بزرگ‌تر] با استفاده از منحنی‌های NISTP-256 و P-384 و [انتخاب: P-521، هیچ منحنی دیگر]؛ بر اساس FIPS PUB 186-4، «استاندارد امضای دیجیتال (DSS)»، بخش ۵]

نکته کاربردی ۳۳:

نویسنده هدف امنیتی باید الگوریتم مورد استفاده برای اجرای امضای دیجیتال را تعیین کند. برای الگوریتم‌های انتخاب‌شده، نویسنده هدف امنیتی باید انتخاب‌ها و اختصاص‌های مناسب را انجام دهد و پارامترهای الگوریتم‌ها را به شکل مناسب تعیین نماید.

شماره الزام	نام الزام
۸۲	**تولید کلید رمزنگاری ۱**

محصول باید کلیدهای رمزنگاری نامتقارن را مطابق با الگوریتم‌های تولید کلید استاندارد زیر تولید کنند.

[انتخاب:

- *استفاده از طرح RSA با اندازه کلید 2048 بیت یا بیشتر که از این اسناد پیروی می‌کند: FIPS PUB 186-4، "Digital Signature Standard (DSS)"، Appendix B.3*
- *استفاده از طرح ECC "NIST curves" [انتخاب: P-256، P-384 ، P-521] که از اسناد زیر پیروی می‌کند: FIPS PUB 186-4، "Digital Signature Standard (DSS)"، Appendix B.4*

نکته کاربردی ۳۴:

نویسنده سند هدف امنیتی تمام طرح‌های تولید کلید که برای استقرار و احراز هویت کاربران استفاده می‌شود را انتخاب می‌کند. وقتی کلید تولیدشده برای احراز هویت کاربران استفاده می‌شود، انتظار می‌رود کلید عمومی با یک گواهی X.509v3 مرتبط گردد.

در صورتی که محصول به عنوان یک گیرنده در طرح استقرار کلید RSA عمل نماید، نیاز به پیاده‌سازی تولید کلید RSA نمی‌باشد.

شماره الزام	نام الزام
۸۳	**مدیریت کلید رمزنگاری ۱**
محصول باید بر اساس متد تخریب کلید رمزنگاری [اختصاص: **متد تخریب کلید رمزنگاری**] که بر اساس استاندارد [اختصاص: **فهرستی از استانداردها**] باشد، کلیدهای رمزنگاری را از بین ببرد. **اقدامات تضمینی:** • **خلاصه مشخصات محصول** ارزیاب باید این بخش را بررسی کند که در مورد همه کلیدهای محرمانه توضیحاتی بیان‌شده باشد. همچنین در مورد روش رویه تخریب کلید در حافظه (به عنوان مثال، بازنویسی با صفر و غیره) توضیحاتی را بیان نماید.	

۸,۲ الزامات پروتکلTLS Server/احراز هویت

با استفاده از پروتکل‌های زیر می‌توان تهدیدات مرتبط با به خطر افتادن کانال ارتباطی بین مدیران و دیگر بخش‌های محصول یا موجودیت‌های IT خارجی را کاهش داد. برای حفاظت از اتصال سرور ممیزی و مدیران راه دور باید از یکی از پروتکل‌های ارتباطی امن (TLS، TLS/HTTPS) استفاده نمود.

شماره الزام	نام الزام
۸۴	**الزامات پروتکلTLS Server/ احراز هویت ۱**
محصول باید [انتخاب: TLS 1.2 (RFC5246)] با پشتیبانی از مجموعه‌های رمز زیر را پیاده‌سازی نماید: • مجموعه‌های رمز اجباری:	

- [TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268]
- [انتخاب: مجموعه‌های رمز اختیاری:
  - LS_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 3268
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 3268
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHAمطابق با RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHAمطابق با RFC 4492
  - TLS_RSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5246
  - TLS_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
  - TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256مطابق با RFC 5246
  - TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256مطابق با RFC 5246
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256مطابق با RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384مطابق با RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256مطابق با RFC 5289
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384مطابق با RFC 5289
- هیچ مجموعه رمز دیگری]].

نکته کاربردی ۳۵:

مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. مجموعه‌های رمز که باید در پیکربندی ارزیابی آزمون شوند، توسط این الزام محدودشده‌اند. توجه شود که به‌منظور اطمینان از مطابقت با RFC 5246، TLS_RSA_WITH_AES_128_CBC_SHA الزامی است.	
۸۵	**الزامات پروتکلTLS Server/ احراز هویت ۲**
محصول باید اتصال‌های کاربرانی را که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0و [انتخاب: TLS1.1، هیچ‌کدام] دارند، رد نماید. **نکته کاربردی ۳۶:** تمام نسخه‌های SSL و نسخه TLS 1.0 رد می‌شوند. توصیه می‌شود که هر نسخه TLS که در شماره الزام ۸۷ «الزامات پروتکلTLS Server/ احراز هویت ۱» انتخاب‌نشده است، در اینجا انتخاب شود.	
۸۶	**الزامات پروتکلTLS Server/ احراز هویت ۳**
محصول باید پارامترهای ساخت کلید را با استفاده از RSA با اندازه کلید ۲۰۴۸ بیت و [انتخاب: ۳۰۷۲ بیت، ۴۰۹۶ بیت، یا هیچ اندازه دیگری] و [انتخاب: منحنی‌های NIST [انتخاب: secp256r1, secp384r1] و هیچ منحنی دیگری] ،[انتخاب: ۳۰۷۲ بیت، هیچ اندازه دیگری]] ایجاد نماید. **نکته کاربردی ۳۷:** اگر در الزام شماره ۸۷ «الزامات پروتکلTLS Server/ احراز هویت ۱» سند هدف امنیتی مجموعه رمزهایDHE یا ECDHE فهرست شده باشند، سند ST باید شامل Diffie-Hellman یا منحنی‌هایNIST فهرست شده در این الزام باشد.	

۹ پیوست دو: الزامات کلاس ممیزی مبتنی بر انتخاب

جدول زیر مربوط به رویدادهای ممیزی مربوط به الزامات مبتنی بر انتخاب است. همانطور که در بخش‌های قبلی هم مطرح‌شده بود، در صورت نیاز باید به این جدول برای ثبت اطلاعات ممیزی مراجعه کرد.

مؤلفه	رویداد قابل ممیزی	جزئیات
انتخاب داده ممیزی ۱	ثبت تمام تغییراتی که در پیکربندی ممیزی اتفاق می‌افتد در حالی‌که توابع ممیزی در حال انجام عملیات باشند. (حداقل)	
ذخیره‌سازی رویدادهای ممیزی ۶	عملیات انجام‌شده به دلیل پر شدن حافظه ممیزی بیش از حد آستانه (پایه)	
ذخیره‌سازی رویدادهای ممیزی ۷	عملیات انجام‌شده به دلیل شکست ذخیره‌سازی ممیزی (پایه)	
عملیات رمزنگاری ۱(۱)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیرفعال (پایه)	
عملیات رمزنگاری ۱ (۲)	شکست و موفقیت و هر نوع عملیات رمزنگاری (حداقل) هر حالتی از عملیات رمزنگاری کاربردی، مشخصه‌های موجودیت‌های فعال و غیرفعال (پایه)	
عملیات کنترل دسترسی ۱	درخواست‌های موفقیت‌آمیز برای اجرای عملیات بر روی موجودیت غیرفعال محصول (حداقل) تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول (پایه)	شناسایی داده‌های موجودیت غیرفعال
ورود داده‌های کاربری به محصول ۴	ورود داده کاربری موفقیت‌آمیز، شامل هر گونه مشخصه‌های امنیتی (حداقل) تمامی تلاش‌ها برای وارد کردن داده‌های کاربری، شامل هر گونه مشخصه‌های امنیتی (پایه)	
مدیریت کارکرد در محصول ۱	تمامی تغییرات در رفتارهای کارکردی محصول	
کارکردهای مدیریتی محصول ۱	ثبت استفاده از کارکردهای مدیریتی (حداقل)	

مؤلفه	رویداد قابل ممیزی	جزئیات
نقش‌های امنیتی	ثبت تغییرات در گروه‌های کاربری که بخشی از یک نقش است (حداقل)	
سازگاری داده‌های امنیتی بین محصول و موجودیت امن	ثبت استفاده موفق از مکانیزم سازگاری داده‌های محصول (حداقل) ثبت استفاده از مکانیزم سازگاری داده‌های محصول (پایه)	
محدودیت بر روی چندین نشست هم‌زمان	ثبت رد یک نشست مبتنی بر محدودیت نشست‌های هم‌زمان (حداقل)	
قفل‌کردن و خاتمه دادن به نشست‌ها ۵	ثبت خاتمه دادن به یک نشست بیکار توسط مکانیزم قفل نشست (حداقل)	
قفل‌کردن و خاتمه دادن به نشست‌ها ۶	ثبت خاتمه به نشست بیکار توسط مدیر سیستم (حداقل)	