

به نام خدا

سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه

تیر ماه ۹۷

نسخه ۱,۰

پیشگفتار

در نظام ارزیابی امنیتی محصولات فتا، یکی از اسناد مورد نیاز برای انجام آزمون امنیتی، سند هدف امنیتی است. سند هدف امنیتی بر اساس اسنادی که پروفایل‌های حفاظتی نامیده می‌شوند، تهیه و تدوین می‌گردد. پروفایل‌های حفاظتی حاوی الزامات امنیتی هستند که در یک محصول افتایی می‌بایست رعایت گردد. از آنجا که متن این پروفایل‌ها پیچیده بوده، تهیه سند هدف امنیتی کاری زمان‌بر برای تولیدکننده است، ساده‌سازی الزامات امنیتی موجود در پروفایل‌های حفاظتی به نحوی که برای تولیدکننده مشخص شود که چه مواردی امنیتی باید در یک محصول خاص رعایت شود، بسیار مفید خواهد بود.

سند پیشرو حاوی الزامات امنیتی «پروفایل حفاظتی برنامه‌های کاربردی تحت شبکه» که سعی شده است تا حد ممکن ساده و قابل فهم گردد، است. این سند دو هدف را دنبال می‌کند. اول آنکه موارد امنیتی را که باید در محصول رعایت شود (تا منجر به دریافت گواهی امنیتی گردد) برای تولیدکننده مشخص نماید و ثانیاً، تدوین سند هدف امنیتی را که کاری زمان‌بر است را برای تولیدکننده سریع و آسان نماید.

فهرست

۳	فهرست.....
۴	۱- مقدمه
۵	۲- الزامات امنیتی
۵	۲-۱- ممیزی امنیت (لاگ).....
۱۰	۲-۲- رمزنگاری.....
۱۳	۲-۳- شناسایی و احراز هویت.....
۱۸	۲-۴- حفاظت از داده‌ی کاربری
۲۴	۲-۵- مدیریت امنیت
۲۸	۲-۶- حفاظت از توابع امنیتی محصول.....
۳۱	۲-۷- تخصیص منابع
۳۲	۲-۸- دسترسی به محصول.....
۳۴	۲-۹- کانال‌ها/مسیرهای مورد اعتماد.....
۳۵	۳- الزامات امنیتی مبتنی بر انتخاب.....
۳۵	۳-۱- پروتکل HTTPS.....
۳۶	۳-۲- پروتکل TLS Client.....
۴۰	۳-۳- پروتکل TLS Server.....
۴۳	۳-۴- پروتکل TLS مشترک کلاینت و سرور
۴۴	۳-۵- اعتبارسنجی گواهی‌نامه.....

۱- مقدمه

سند هدف امنیتی، یکی از اسنادی است که تولیدکننده می‌بایست قبل از شروع آزمون ارزیابی امنیتی تدوین نماید. بر اساس استاندارد معیار مشترک (CC) این سند مبتنی بر اسنادی که پروفایل حفاظتی نام دارند، تهیه می‌شود. متن پروفایل‌های حفاظتی اغلب ثقیل بوده و تسلط بر مفاهیم آنها زمان‌بر است. در این راستا مرکز افتا و سازمان فناوری اطلاعات ایران با همکاری آزمایشگاه‌های ارزیابی امنیتی، به منظور چابک‌سازی فرآیند ارزیابی امنیتی، «سند الزامات امنیتی» را جایگزین پروفایل‌های حفاظتی نموده است.

هدف از سند الزامات امنیتی، ساده‌سازی مفاهیم الزامات مطرح شده در پروفایل‌های حفاظتی و نیز کمک به تولیدکننده در جهت سرعت بخشیدن به تدوین سند هدف امنیتی است.

این سند مجموعه‌ای از الزامات امنیتی برای برنامه‌های کاربردی تحت شبکه را مطرح می‌کند. هر محصولی که ادعای انطباق با «سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه» را داشته باشد، می‌بایست الزامات مطرح شده در آن را پیاده‌سازی نماید.

۲- الزامات امنیتی

الزامات امنیتی این سند بر اساس نسخه ۱,۱ پروفایل حفاظتی «برنامه‌های کاربردی تحت شبکه» تهیه شده است. ساختار این سند بدین صورت است که برای هر کلاس در پروفایل حفاظتی مربوطه، یک دسته الزام بیان شده است.

۲-۱- ممیزی امنیت (لاگ)

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

توضیحات	کلاس ممیزی (لاگ)		شماره الزام															
	<input type="checkbox"/>	<p>محصول باید برای موارد مشخص شده که در ذیل آمده است، رکورد ممیزی تولید کند (لاگ ثبت نماید).</p> <table border="1" data-bbox="835 898 1833 1344"> <tr> <td data-bbox="835 898 892 954" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="892 898 1600 954">شروع و اتمام توابع</td> <td data-bbox="1600 898 1833 1344" rowspan="8" style="vertical-align: middle;">رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.</td> </tr> <tr> <td data-bbox="835 954 892 1011" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="892 954 1600 1011">تلاشهای ناموفق برای خواندن اطلاعات از رکوردهای لاگ</td> </tr> <tr> <td data-bbox="835 1011 892 1068" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="892 1011 1600 1068">خواندن اطلاعات از رکوردهای لاگ</td> </tr> <tr> <td data-bbox="835 1068 892 1125" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="892 1068 1600 1125">تمامی تغییرات در پیکربندی لاگ</td> </tr> <tr> <td data-bbox="835 1125 892 1182" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="892 1125 1600 1182">عملیات انجام شده به دلیل سرریز حافظه لاگ از حد آستانه</td> </tr> <tr> <td data-bbox="835 1182 892 1239" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="892 1182 1600 1239">عملیات انجام شده به دلیل شکست در ذخیره‌سازی لاگها</td> </tr> <tr> <td data-bbox="835 1239 892 1295" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="892 1239 1600 1295">تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.</td> </tr> </table>	<input type="checkbox"/>	شروع و اتمام توابع	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.	<input checked="" type="checkbox"/>	تلاشهای ناموفق برای خواندن اطلاعات از رکوردهای لاگ	<input checked="" type="checkbox"/>	خواندن اطلاعات از رکوردهای لاگ	<input checked="" type="checkbox"/>	تمامی تغییرات در پیکربندی لاگ	<input type="checkbox"/>	عملیات انجام شده به دلیل سرریز حافظه لاگ از حد آستانه	<input type="checkbox"/>	عملیات انجام شده به دلیل شکست در ذخیره‌سازی لاگها	<input type="checkbox"/>	تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.	۱
<input type="checkbox"/>	شروع و اتمام توابع	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.																
<input checked="" type="checkbox"/>	تلاشهای ناموفق برای خواندن اطلاعات از رکوردهای لاگ																	
<input checked="" type="checkbox"/>	خواندن اطلاعات از رکوردهای لاگ																	
<input checked="" type="checkbox"/>	تمامی تغییرات در پیکربندی لاگ																	
<input type="checkbox"/>	عملیات انجام شده به دلیل سرریز حافظه لاگ از حد آستانه																	
<input type="checkbox"/>	عملیات انجام شده به دلیل شکست در ذخیره‌سازی لاگها																	
<input type="checkbox"/>	تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.																	

<input checked="" type="checkbox"/>	تمام کاربردهای سازوکار احراز هویت
<input checked="" type="checkbox"/>	نتایج نهایی عملیات احراز هویت
<input checked="" type="checkbox"/>	تلاش موفق و ناموفق هر کلمه عبور تست شده توسط محصول
<input checked="" type="checkbox"/>	شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال)
<input checked="" type="checkbox"/>	تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی
<input checked="" type="checkbox"/>	تمامی درخواستهای (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول
<input checked="" type="checkbox"/>	تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه مشخصه‌های امنیتی)
<input checked="" type="checkbox"/>	همه تلاش‌ها برای خارج کردن اطلاعات از محصول
<input type="checkbox"/>	تمامی تغییرات در رفتارهای توابع کارکردی محصول
<input checked="" type="checkbox"/>	استفاده از کارکردهای مدیریتی
<input checked="" type="checkbox"/>	تغییرات در گروه کاربران
<input type="checkbox"/>	شکست در کارکردهای امنیتی محصول
<input checked="" type="checkbox"/>	تمامی قابلیت‌هایی از محصول که به دلیل شکست، نمی‌توانند عملیات موردنظر را انجام دهند.
<input checked="" type="checkbox"/>	تلاش موفق یا ناموفق برای برقراری نشست.
<input checked="" type="checkbox"/>	عدم ایجاد نشست به دلیل محدودیت نشست‌های هم‌زمان (حداقل)
<input checked="" type="checkbox"/>	خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست

		<input checked="" type="checkbox"/>	خاتمه به نشست غیرفعال توسط مدیر سیستم	
		<input checked="" type="checkbox"/>	سایر موارد	
	۲	<input checked="" type="checkbox"/>	محصول باید برای هر رکورد ممیزی تولید شده، مشخصاتی که در ذیل آمده است را ثبت نماید.	
		<input checked="" type="checkbox"/>	تاریخ و زمان رویداد	مشخصاتی که در رکوردهای ممیزی وجود دارد مشخص شود.
		<input checked="" type="checkbox"/>	نوع رویداد	
		<input checked="" type="checkbox"/>	هویت ایجادکننده رویداد	
		<input checked="" type="checkbox"/>	نتیجه رویداد	
		<input checked="" type="checkbox"/>	آدرس IP ایجادکننده رویداد	
		<input checked="" type="checkbox"/>	سایر موارد	
	۳	<input checked="" type="checkbox"/>	محصول باید رکوردهای ممیزی را در برابر دسترسی غیرمجاز محافظت نماید.	
		<input checked="" type="checkbox"/>	فقط به کاربرانی اجازه دسترسی به لاگ داده می شود که permission لازم را داشته باشند	
	۴	<input checked="" type="checkbox"/>	رکوردهای ممیزی که محصول تولید می نماید باید برای کاربر ساده و قابل فهم باشند.	
		<input checked="" type="checkbox"/>	عدم وجود داده نامفهوم در رکوردها	مواردی که در رکورد های ممیزی وجود دارند، مشخص شوند.
		<input checked="" type="checkbox"/>	عدم وجود فیلدهای نامرتبط	
		<input checked="" type="checkbox"/>	وجود داده معتبر و مناسب در هر فیلد	
	۵	<input checked="" type="checkbox"/>	محصول باید امکان انتخاب و مرتب سازی برای رکوردهای ممیزی تولید شده را بر اساس فیلدها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید.	
		<input checked="" type="checkbox"/>	هویت موجودیت فعال	

		<input checked="" type="checkbox"/>	نوع حساب کاربری	مواردی که بر اساس آنها مرتب‌سازی وجود دارد، مشخص شود.
		<input checked="" type="checkbox"/>	تاریخ/زمان	
		<input checked="" type="checkbox"/>	روش اتصال کاربر	
		<input checked="" type="checkbox"/>	نوع رخداد	
		<input type="checkbox"/>	مکان رویداد	
		<input type="checkbox"/>	سایر موارد	
	<input type="checkbox"/>	محصول باید هرگونه حذف و تغییر غیرمجاز در رکوردهای ممیزی را تشخیص دهد و در صورت امکان جلوگیری نماید.		۶
		<input type="checkbox"/>	استفاده از هش برای تشخیص تغییرات	روش‌های تشخیص مشخص شود. (وجود یک مورد لازم و کافی است)
		<input checked="" type="checkbox"/>	پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)	
		<input checked="" type="checkbox"/>	فقط خواندنی کردن ممیزی‌ها در محصول	
		<input type="checkbox"/>	سایر موارد	
<p>- چون داده‌های ممیزی نه به شکل مستقیم که با استفاده از صف بر روی پایگاه داده mongo و همچنین بصورت سریال شده روی file بر روی storage ذخیره سازی می‌شود لذا وظیفه مدیر سیستم تعریف شده است که هر هفته طی گزارشی از وضعیت صف و وضعیت فضای دیسک را به صورت دستی استخراج کرده و به مسئولان سامانه ارائه دهد</p>	<input type="checkbox"/>	محصول باید وقتی که حجم داده‌های ممیزی، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.		۷
		<input type="checkbox"/>	استفاده از یک کانال ارتباطی	روش‌های اطلاع رسانی مشخص شود (وجود یک مورد لازم و کافی است)
		<input type="checkbox"/>	ارسال پیام	
		<input type="checkbox"/>	از طریق واسط کاربر مجاز	
		<input checked="" type="checkbox"/>	سایر موارد	

<p>- داده های ممیزی بر روی پایگاه داده فقط برای مدت ۳ ماه ذخیره سازی می شود و پس از آن فقط به شکل بک آپ بر روی فایل storage قابل دسترس خواهد بود لذا امکان سرریز وجود ندارد.</p> <p>- حتی در صورتی که پایگاه داده گنجایش ۳ ماهه اش تمام شده باشد چون به صورت صف داده ها روی پایگاه داده ردیس ابتدا ذخیره می شوند لذا تا زمان نوشته نشدن روی پایگاه داده و فایل در صف باقی می مانند.</p>	<input type="checkbox"/>	<p>محصول باید توانایی ممیزی (ثبت لاگ) هنگام از کار افتادن محصول و/یا پر شدن حافظه ممیزی را داشته باشد و برای این کار از رویکردهای بیان شده استفاده نماید.</p>		<p>۸</p>	
		<input type="checkbox"/>	<p>نادیده گرفتن رویدادهای ممیزی</p>		<p>رویکردهای مورد استفاده در محصول مشخص گردد (وجود یک مورد لازم و کافی است)</p>
		<input type="checkbox"/>	<p>ذخیره سازی محدود رویدادهای ممیزی، (آنهايي که توسط کاربر مجاز و تحت حقوق خاصی رخ می دهند)</p>		
		<input type="checkbox"/>	<p>بازنویسی روی قدیمی ترین رکوردهای ممیزی ذخیره شده</p>		
		<input checked="" type="checkbox"/>	<p>سایر موارد</p>		

۲-۲- رمزنگاری

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

شماره الزام	کلاس رمزنگاری	توضیحات
۱	<input type="checkbox"/>	محصول باید قابلیت رمزنگاری یا ماژول رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف شده ISO 18033-3) با توجه به موارد زیر انجام دهد.
	<input type="checkbox"/>	مد عملیاتی CBC و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در NIST SP 800-38A)
	<input type="checkbox"/>	مد عملیاتی GCM و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در NIST SP 800-38D)
	<input type="checkbox"/>	مد عملیاتی CTR و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف شده در ISO10116)
		مد عملیاتی که الگوریتم از آن استفاده می‌کند را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)

	<input type="checkbox"/>	<p>محصول باید بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب می‌نماید، توانایی تولید داده درهم‌سازی شده (هش) را داشته باشد؛ بنابراین باید برای تولید درهم‌سازی از موارد زیر بر اساس ISO/IEC 10118-3:2004 استفاده نماید.</p>	<p>۲</p>
	<input type="checkbox"/>	<p>الگوریتم SHA-1 با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲</p>	<p>الگوریتم و اندازه خلاصه پیام مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)</p>
	<input type="checkbox"/>	<p>الگوریتم SHA-256 با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲</p>	
	<input type="checkbox"/>	<p>الگوریتم SHA-384 با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲</p>	
	<input type="checkbox"/>	<p>الگوریتم SHA-512 با اندازه خلاصه پیام ۱۶۰ یا ۲۵۶ یا ۳۸۴ یا ۵۱۲</p>	
	<input type="checkbox"/>	<p>در صورتی که تولید کلید رمزنگاری در محصول وجود دارد، نیاز است که تخریب کلید رمزنگاری نیز بر اساس موارد زیر صورت پذیرد. (اختیاری)</p>	<p>۳</p>
	<input type="checkbox"/>	<p>نابودی با استفاده از بازنویسی ساده (بازنویسی با صفرها، یکها، مقدار تصادفی، مقدار جدیدی از کلید)</p>	<p>روش نابودی کلید مشخص گردد. (وجود یک مورد لازم و کافی است)</p>
	<input type="checkbox"/>	<p>نابودی با استفاده از یک واسط مشخص</p>	
	<input type="checkbox"/>	<p>از طریق توابع امنیتی محصول</p>	
	<input type="checkbox"/>	<p>سایر موارد</p>	
	<input type="checkbox"/>	<p>در صورتی که امضاء دیجیتال در محصول پشتیبانی می‌شود، نیاز است که سرویس‌های امضاء رمزنگاری (تولید و تأیید) بر اساس الگوریتم‌های رمزنگاری زیر انجام گیرد. (اختیاری)</p>	<p>۴</p>

		<p><input type="checkbox"/> الگوریتم‌های امضاء دیجیتال RSA با کلیدهای رمزنگاری ۲۰۴۸ بیت و بزرگتر (بر اساس FIPS PUB 186-4، استاندارد امضاء دیجیتال (DSS) بخش ۵.۵، الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSA-PKCS1v_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال ۲ و یا الگوی امضای دیجیتال ۳)</p>	<p>الگوریتم و اندازه کلیدهای مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است)</p>	
		<p><input type="checkbox"/> الگوریتم‌های امضاء دیجیتال ECDSA با کلیدهای رمزنگاری ۲۵۶ بیت یا بزرگتر (بر اساس ISO/IEC 14888-3 بخش ۴.۶، استاندارد امضای دیجیتال (DSS) بخش ۶ و پیوست D، با استفاده از منحنی P-256 یا P-384 یا P-521)</p>		

۲-۳- شناسایی و احراز هویت

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

توضیحات	کلاس شناسایی و احراز هویت		شماره الزام									
	<input type="checkbox"/>	<p>محصول باید بتواند تعداد تلاش‌های ناموفقی را که برای احراز هویت شدن صورت گرفته است (در هر بخش یا قسمتی که نیاز به احراز هویت وجود دارد)، بر اساس موارد زیر مشخص نماید.</p> <table border="1" data-bbox="940 678 1602 979"> <tr> <td data-bbox="940 678 1003 776" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="1003 678 1602 776">یک عدد مثبت ثابت</td> <td data-bbox="1602 678 1835 776">مقدار یا یازهی مورد استفاده در هر یک باید مشخص گردد.</td> </tr> <tr> <td data-bbox="940 776 1003 873" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="1003 776 1602 873">یک عدد مثبت قابل تنظیم توسط مدیر</td> <td data-bbox="1602 776 1835 873">(وجود یک مورد لازم و کافی است)</td> </tr> <tr> <td data-bbox="940 873 1003 979" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="1003 873 1602 979">یک بازهی قابل قبولی از مقادیر</td> <td></td> </tr> </table>	<input checked="" type="checkbox"/>	یک عدد مثبت ثابت	مقدار یا یازهی مورد استفاده در هر یک باید مشخص گردد.	<input type="checkbox"/>	یک عدد مثبت قابل تنظیم توسط مدیر	(وجود یک مورد لازم و کافی است)	<input type="checkbox"/>	یک بازهی قابل قبولی از مقادیر		۱
<input checked="" type="checkbox"/>	یک عدد مثبت ثابت	مقدار یا یازهی مورد استفاده در هر یک باید مشخص گردد.										
<input type="checkbox"/>	یک عدد مثبت قابل تنظیم توسط مدیر	(وجود یک مورد لازم و کافی است)										
<input type="checkbox"/>	یک بازهی قابل قبولی از مقادیر											
	<input type="checkbox"/>	<p>محصول باید زمانی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین شده رسید، برای پیچیده‌تر کردن احراز هویت از موارد زیر استفاده نماید.</p> <table border="1" data-bbox="940 1079 1602 1287"> <tr> <td data-bbox="940 1079 1003 1287" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="1003 1079 1602 1287">غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)</td> <td data-bbox="1602 1079 1835 1287">روش استفاده شده برای پیچیده‌تر کردن احراز هویت را انتخاب نمایید.</td> </tr> </table>	<input type="checkbox"/>	غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)	روش استفاده شده برای پیچیده‌تر کردن احراز هویت را انتخاب نمایید.	۲						
<input type="checkbox"/>	غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)	روش استفاده شده برای پیچیده‌تر کردن احراز هویت را انتخاب نمایید.										

		<input checked="" type="checkbox"/>	غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)	(وجود یک مورد لازم و کافی است.) لازم به ذکر است روش های فوق با توجه به نوع کاربرد می‌تواند از حالت انتخابی به حالت الزامی تغییر یا بد. برای مثال غیرفعال کردن حساب کاربری در تمامی کاربردها مفید نیست.			
		<input checked="" type="checkbox"/>	استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود)				
		<input type="checkbox"/>	سایر موارد				
	<input type="checkbox"/>	محصول باید برای هر کاربر، مشخصه‌های امنیتی که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت باشند را نگهداری نماید.		مشخصه های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند.	۳		
		<input checked="" type="checkbox"/>	شناسه کاربر				
		<input checked="" type="checkbox"/>	روش احراز هویت مورد استفاده				
		<input checked="" type="checkbox"/>	داده احراز هویت				
		<input checked="" type="checkbox"/>	وضعیت حساب کاربری (فعال، غیرفعال، بلوکه شده و غیره)				
		<input checked="" type="checkbox"/>	نقش کاربر				
		<input type="checkbox"/>	سایر موارد				

<p>- برای دسترسی مدیران بالادستی به سرور مانند اتصال SSH از رمز عبور به همراه یک کلید خصوصی استفاده می‌شود</p>		<table border="1"> <tr> <td data-bbox="892 250 940 305"><input type="checkbox"/></td> <td data-bbox="940 250 1598 305">Active Directory</td> </tr> <tr> <td data-bbox="892 305 940 360"><input type="checkbox"/></td> <td data-bbox="940 305 1598 360">OTP یا توکن</td> </tr> <tr> <td data-bbox="892 360 940 415"><input type="checkbox"/></td> <td data-bbox="940 360 1598 415">احراز هویت دو فاکتوری</td> </tr> <tr> <td data-bbox="892 415 940 483"><input checked="" type="checkbox"/></td> <td data-bbox="940 415 1598 483">سایر موارد</td> </tr> </table>	<input type="checkbox"/>	Active Directory	<input type="checkbox"/>	OTP یا توکن	<input type="checkbox"/>	احراز هویت دو فاکتوری	<input checked="" type="checkbox"/>	سایر موارد	<p>در محصول مشخص شوند.</p>		
<input type="checkbox"/>	Active Directory												
<input type="checkbox"/>	OTP یا توکن												
<input type="checkbox"/>	احراز هویت دو فاکتوری												
<input checked="" type="checkbox"/>	سایر موارد												
	<input type="checkbox"/>	<p>محصول باید برای هر کاربر فعال، مشخصه‌های امنیتی نگهداری نماید.</p> <table border="1"> <tr> <td data-bbox="892 592 940 706"><input checked="" type="checkbox"/></td> <td data-bbox="940 592 1598 706">شناسه کاربر</td> </tr> <tr> <td data-bbox="892 706 940 820"><input checked="" type="checkbox"/></td> <td data-bbox="940 706 1598 820">نقشه‌ها و یا مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه</td> </tr> <tr> <td data-bbox="892 820 940 933"><input checked="" type="checkbox"/></td> <td data-bbox="940 820 1598 933">جزئیات واسط کلاینت</td> </tr> <tr> <td data-bbox="892 933 940 1047"><input checked="" type="checkbox"/></td> <td data-bbox="940 933 1598 1047">پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)</td> </tr> <tr> <td data-bbox="892 1047 940 1235"><input type="checkbox"/></td> <td data-bbox="940 1047 1598 1235">سایر موارد</td> </tr> </table>	<input checked="" type="checkbox"/>	شناسه کاربر	<input checked="" type="checkbox"/>	نقشه‌ها و یا مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه	<input checked="" type="checkbox"/>	جزئیات واسط کلاینت	<input checked="" type="checkbox"/>	پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)	<input type="checkbox"/>	سایر موارد	<p>۷</p> <p>مشخصه‌هایی امنیتی که محصول برای هر کاربر نگهداری می‌کند، مشخص گردد (در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین در «سایر موارد» بیان می‌شوند).</p>
<input checked="" type="checkbox"/>	شناسه کاربر												
<input checked="" type="checkbox"/>	نقشه‌ها و یا مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه												
<input checked="" type="checkbox"/>	جزئیات واسط کلاینت												
<input checked="" type="checkbox"/>	پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)												
<input type="checkbox"/>	سایر موارد												
	<input type="checkbox"/>	<p>محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.</p>	<p>۸</p>										

		<p>از بین رفتن اعتبار نشستهای قبلی هنگام برقراری یک نشست جدید</p> <p><input type="checkbox"/> (به جزء مواردی که فعال بودن همزمان چندین نشست موردنیاز کارکردی برنامه باشد. در این موارد، هنگام فعال شدن نشست‌های جدید، باید به صفحه کاربر اصلی (نشست اول) اطلاع داده شود).</p>	<p>در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین در «سایر موارد» بیان می‌شوند.</p>	
	<p><input type="checkbox"/></p>	<p>به‌روزرسانی اطلاعات پیشینه احراز هویت</p>	<p>محمول باید بر روی تغییرات مشخصه‌های امنیتی کاربر فعال قوانینی را اعمال نماید.</p>	<p>۹</p>
	<p><input type="checkbox"/></p>	<p>غیرمجاز بودن هرگونه تغییر در طول نشست فعال</p>	<p>قوانینی که در صورت تغییر مشخصه‌های امنیتی کاربر فعال، اعمال می‌شود، مشخص گردد.</p>	
	<p><input type="checkbox"/></p>	<p>سایر موارد</p>		

۴-۲- حفاظت از داده‌ی کاربری

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

توضیحات	کلاس حفاظت از داده‌ی کاربری		شماره الزام
<p>- در این سامانه دسترسی‌ها بر روی آدرس‌های URL و بر اساس permission‌های هر URL بررسی می‌شود برای همین مدیر سامانه میتواند به تعداد مورد نیاز و بر اساس دسترسی‌های مورد نیاز نقش ایجاد کرده و دسترسی‌های مورد نیاز هر نقش را تعریف نماید.</p> <p>- لازم بذکر است تغییرات در دسترسی‌های یک نقش بلافاصله بر روی همه موجودیت‌های فعال اعمال می‌شود</p>	<input type="checkbox"/>	<p>محصول باید برای موجودیتها و عملیات، خط‌مشی‌های کنترل دسترسی اعمال نماید.</p>	۱
		مدیر سیستم	موجودیت‌های فعالی که خط‌مشی‌های کنترل دسترسی در مورد آنها اعمال می‌شوند، مشخص گردد.
		کاربر عادی	
		سایر موارد	
		رکوردها، مستندات و فراداده	موجودیت‌های غیر فعالی که خط‌مشی‌های
		داده متعلق به کاربران	

^۱Metadata

		<input type="checkbox"/> داده احراز هویت	کنترل دسترسی در مورد آنها اعمال می‌شوند، مشخص گردد.
		<input type="checkbox"/> سایر موارد	
		<input checked="" type="checkbox"/> ایجاد موجودیت غیرفعال جدید	عملیاتی که خط‌مشی‌های کنترل دسترسی در رابطه با آنها اعمال می‌شوند، مشخص گردد.
		<input checked="" type="checkbox"/> حذف موجودیت غیرفعال	
		<input checked="" type="checkbox"/> تغییر دسترسیها به موجودیت غیرفعال	
		<input checked="" type="checkbox"/> عملیات بر روی فرا-داده وابسته به موجودیت غیرفعال	
		<input type="checkbox"/> سایر موارد	
	<input type="checkbox"/>	محصول باید بر اساس مشخصه‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.	
		<input checked="" type="checkbox"/> نقش‌ها و مجوزهای کاربر مجاز	مشخصه‌هایی که بر اساس آن خط‌مشی‌ها تعریف می‌شوند، انتخاب گردد.
		<input checked="" type="checkbox"/> اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند.	
		<input type="checkbox"/> سایر موارد	
	<input checked="" type="checkbox"/>	محصول باید بر اساس قاعده‌های عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نماید (این قاعده می‌تواند بدین شکل باشد که در لیست کنترل دسترسی، رکوردی وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف شده حق دسترسی به موجودیت غیرفعال را بدهد).	

	<input type="checkbox"/>	<p>محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.</p>	<p>۴</p>
	<input checked="" type="checkbox"/>	<p>تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه^۳ از پیش تعریف شده</p>	<p>قوانین ممانعت از دسترسی مشخص شوند (در صورت اعمال قوانین بیشتر توسط محصول، در «سایر موارد» بیان شود).</p>
	<input type="checkbox"/>	<p>سایر موارد</p>	
	<input checked="" type="checkbox"/>	<p>محصول باید تضمین نماید تمام اطلاعات قبلی منابع یا در هنگام آزادسازی آنها، غیرقابل دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد.</p>	<p>۵</p>
<p>- در این محصول دسترسی هر موجودیت فعال به هر فرم ورود اطلاعات بر اساس خود موجودیت فعال و دسترسی های همان موجودیت فعال بررسی و تایید می شود</p>	<input checked="" type="checkbox"/>	<p>محصول باید هنگام دریافت داده کاربری خطمشی کنترل دسترسی را اعمال نماید و برای این کار از مشخصه‌های امنیتی مرتبط با داده کاربری استفاده کند.</p>	<p>۶</p>
	<input checked="" type="checkbox"/>	<p>نوع داده</p>	<p>مشخصه‌های امنیتی مرتبط با</p>

^۳Threshold

		<input checked="" type="checkbox"/>	حجم و اندازه	<p>داده کاربری که در هنگام ورود آن به محصول استفاده می‌شوند، مشخص شود (در صورتی که کنترل دسترسی برای موارد دیگری نیز صورت می‌گیرد، در قسمت «سایر موارد» بیان گردد).</p>		
		<input checked="" type="checkbox"/>	فرمت			
		<input type="checkbox"/>	تعداد دفعات Import			
		<input checked="" type="checkbox"/>	سایر موارد			
<p>- محصول از پروتکل HTTPS برای برقراری اتصال امن بین کاربر و محصول بهره می‌برد</p>		<input checked="" type="checkbox"/>	<p>محصول باید از یک پروتکل امن برای انتقال داده استفاده نماید. این پروتکل ارتباط و همبستگی شفاف را بین داده کاربری دریافت شده و مشخصه‌های امنیتی آن فراهم می‌کند و همچنین از شنود و گمشدن داده حین انتقال جلوگیری می‌کند.</p>			
<p>- چون محصول یک وبسایت است کنترل دسترسی بر اساس URL و دسترسی‌های موجودیت فعال بر روی داده‌های خروجی بررسی می‌شود</p>		<input type="checkbox"/>	<p>محصول باید هنگام انتقال داده به بیرون از محصول، خط‌مشی کنترل دسترسی اعمال نماید و برای این کار از مشخصه‌های امنیتی مرتبط با داده کاربری استفاده کند.</p>			
		<input type="checkbox"/>	نوع داده	مشخصه‌های امنیتی مرتبط با داده کاربری که		
		<input type="checkbox"/>	حجم و اندازه	در هنگام خروج		
		<input type="checkbox"/>	فرمت			

	<input checked="" type="checkbox"/>	سایر موارد	آن از محصول استفاده می‌شوند، مشخص شوند
	<input type="checkbox"/>	محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.	
		<input type="checkbox"/>	مدیر سیستم باید خروج رکوردها را محدود نماید، به طوریکه کاربران محصول، قادر به خروج بدون هدف داده به خارج از محصول نباشند.
		<input type="checkbox"/>	سایر موارد
	<input type="checkbox"/>	قوانینی که در هنگام خروج داده از محصول اعمال می‌شوند، مشخص شوند	
		<input type="checkbox"/>	سایر موارد
		<input type="checkbox"/>	سایر موارد
	<input type="checkbox"/>	محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره شده در محصول تشخیص دهد.	
		<input type="checkbox"/>	چگونگی تشخیص تغییر در داده‌های کاربری حساس، مشخص شود.
		<input type="checkbox"/>	درهم شده داده‌های کاربری ذخیره شده، نگهداری می‌شود
	<input type="checkbox"/>	<input type="checkbox"/>	سایر موارد
		<input type="checkbox"/>	ایجاد هشدار/خطر برای نقش‌های مجاز

Hash

		<input type="checkbox"/>	تصحیح داده بر اساس مقادیر قبل	اقدام مقابله‌ای در صورت تشخیص خطا، مشخص شود (وجود یک مورد لازم و کافی است)
		<input type="checkbox"/>	سایر موارد	

۵-۲- مدیریت امنیت

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

توضیحات	کلاس مدیریت امنیت	شماره الزام											
	<table border="1"> <tr> <td data-bbox="842 630 884 727" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="884 630 1598 727">محصول باید برای مدیر سیستم و هر کاربری که مجوز لازم را دارد، امکان فعالیتهای مدیریتی زیر را بر روی توابع و تمام کارکردهای مربوط به مدیریت محصول فراهم آورد.</td> <td data-bbox="1598 630 1835 979" rowspan="5" style="text-align: center; vertical-align: middle;"> فعالیتهای مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند. </td> </tr> <tr> <td data-bbox="842 727 884 789" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="884 727 1598 789">تعیین و تغییر رفتار</td> </tr> <tr> <td data-bbox="842 789 884 850" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="884 789 1598 850">غیرفعال نمودن</td> </tr> <tr> <td data-bbox="842 850 884 912" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="884 850 1598 912">فعال نمودن</td> </tr> <tr> <td data-bbox="842 912 884 979"></td> <td data-bbox="884 912 1598 979">سایر موارد</td> </tr> </table>	<input type="checkbox"/>	محصول باید برای مدیر سیستم و هر کاربری که مجوز لازم را دارد، امکان فعالیتهای مدیریتی زیر را بر روی توابع و تمام کارکردهای مربوط به مدیریت محصول فراهم آورد.	فعالیتهای مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند.	<input checked="" type="checkbox"/>	تعیین و تغییر رفتار	<input checked="" type="checkbox"/>	غیرفعال نمودن	<input checked="" type="checkbox"/>	فعال نمودن		سایر موارد	۱
<input type="checkbox"/>	محصول باید برای مدیر سیستم و هر کاربری که مجوز لازم را دارد، امکان فعالیتهای مدیریتی زیر را بر روی توابع و تمام کارکردهای مربوط به مدیریت محصول فراهم آورد.	فعالیتهای مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند.											
<input checked="" type="checkbox"/>	تعیین و تغییر رفتار												
<input checked="" type="checkbox"/>	غیرفعال نمودن												
<input checked="" type="checkbox"/>	فعال نمودن												
	سایر موارد												
	<table border="1"> <tr> <td data-bbox="842 979 884 1130" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="884 979 1598 1130">محصول باید با اعمال خط‌مشی کنترل دسترسی؛ امکان تغییر پیش‌فرض و سایر عملیات زیر را بر روی مشخصه‌های امنیتی الزام ۷ از کلاس شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.</td> <td data-bbox="1598 979 1835 1359" rowspan="5" style="text-align: center; vertical-align: middle;"> عملیات بر روی مشخصه‌های امنیتی که در محصول پشتیبانی </td> </tr> <tr> <td data-bbox="842 1130 884 1192" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="884 1130 1598 1192">پرس‌وجو</td> </tr> <tr> <td data-bbox="842 1192 884 1253" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="884 1192 1598 1253">تغییر</td> </tr> <tr> <td data-bbox="842 1253 884 1315" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="884 1253 1598 1315">حذف</td> </tr> <tr> <td data-bbox="842 1315 884 1359" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="884 1315 1598 1359">تغییر پیش‌فرض</td> </tr> </table>	<input type="checkbox"/>	محصول باید با اعمال خط‌مشی کنترل دسترسی؛ امکان تغییر پیش‌فرض و سایر عملیات زیر را بر روی مشخصه‌های امنیتی الزام ۷ از کلاس شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.	عملیات بر روی مشخصه‌های امنیتی که در محصول پشتیبانی	<input type="checkbox"/>	پرس‌وجو	<input type="checkbox"/>	تغییر	<input type="checkbox"/>	حذف	<input type="checkbox"/>	تغییر پیش‌فرض	۲
<input type="checkbox"/>	محصول باید با اعمال خط‌مشی کنترل دسترسی؛ امکان تغییر پیش‌فرض و سایر عملیات زیر را بر روی مشخصه‌های امنیتی الزام ۷ از کلاس شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.	عملیات بر روی مشخصه‌های امنیتی که در محصول پشتیبانی											
<input type="checkbox"/>	پرس‌وجو												
<input type="checkbox"/>	تغییر												
<input type="checkbox"/>	حذف												
<input type="checkbox"/>	تغییر پیش‌فرض												

	<input type="checkbox"/>	سایر موارد	می شوند، مشخص گردد.	
	<input type="checkbox"/>	محصول باید برای داده‌های محصول، امکان کارکردهای زیر را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.		
		<input checked="" type="checkbox"/>	تغییر پیش فرض	عملیات بر روی داده‌های محصول که در محصول پشتیبانی می‌شوند، مشخص شود.
		<input checked="" type="checkbox"/>	حذف نمودن	
		<input checked="" type="checkbox"/>	پرس و جو	
		<input checked="" type="checkbox"/>	مقداردهی	
		<input checked="" type="checkbox"/>	ایجاد	
		<input checked="" type="checkbox"/>	مشاهده	
		<input type="checkbox"/>	سایر موارد	
	<input type="checkbox"/>	محصول باید توانایی انجام کارکردهای زیر را داشته باشد.		
		<input type="checkbox"/>	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات رکوردهای ممیزی	در صورتی که هر کدام از موارد مطرح شده، توسط محصول قابل اجرا نیست، در قسمت توضیحات باید دلایل مطرح گردد.
		<input checked="" type="checkbox"/>	پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی	
		<input type="checkbox"/>	پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی	
		<input type="checkbox"/>	مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول	
<input type="checkbox"/>				

		<input type="checkbox"/> انتخاب زمان اجرای حفاظت از اطلاعات باقیمانده که می‌تواند در محصول قابل پیکربندی باشد. (برای مثال، زمان تخصیص و یا زمان آزادسازی منابع)	
		<input type="checkbox"/> ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول	
		<input type="checkbox"/> در نظر گرفتن یک عملیات از پیش تعیین شده پس از تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی نیز باشد.	
		<input type="checkbox"/> ۱. مدیریت حد آستانه برای تلاش‌های ناموفق ۲. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد.	
		<input checked="" type="checkbox"/> مدیریت معیارها برای تنظیم کلمات عبور	
		<input type="checkbox"/> ۱. مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مربوطه ۲. مدیریت یکسری عملیاتی که قبل از احراز شدن هویت کاربر انجام میشوند.	
		<input checked="" type="checkbox"/> ۱. مدیریت سازوکارهای احراز هویت ۲. مدیریت قوانین مرتبط با احراز هویت	
		<input type="checkbox"/> مدیریت تغییرات و فرایندهایی مانند (اختصاص آدرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می‌تواند قبل از شناسایی کاربر انجام دهد.	
		<input type="checkbox"/> مدیر مجاز می‌تواند مشخصه‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد.	

		<table border="1"> <tr> <td data-bbox="884 248 940 305"><input type="checkbox"/></td> <td data-bbox="940 248 1600 305">مدیریت مقادیر پیشفرض برای کنترل دسترسی محصول</td> </tr> <tr> <td data-bbox="884 305 940 362"><input checked="" type="checkbox"/></td> <td data-bbox="940 305 1600 362">مدیریت نقشها در محصول</td> </tr> <tr> <td data-bbox="884 362 940 467"><input checked="" type="checkbox"/></td> <td data-bbox="940 362 1600 467">مدیریت حداکثر تعداد مجاز نشستهای همزمان کاربران توسط مدیر</td> </tr> <tr> <td data-bbox="884 467 940 524"><input type="checkbox"/></td> <td data-bbox="940 467 1600 524">مدیریت شرایط آغاز نشست توسط مدیر مجاز</td> </tr> <tr> <td data-bbox="884 524 940 727"></td> <td data-bbox="940 524 1600 727"> <p>۱. تعیین زمان غیرفعال بودن برای یک کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد.</p> <p>۲. تعیین زمان پیشفرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد.</p> </td> </tr> </table>	<input type="checkbox"/>	مدیریت مقادیر پیشفرض برای کنترل دسترسی محصول	<input checked="" type="checkbox"/>	مدیریت نقشها در محصول	<input checked="" type="checkbox"/>	مدیریت حداکثر تعداد مجاز نشستهای همزمان کاربران توسط مدیر	<input type="checkbox"/>	مدیریت شرایط آغاز نشست توسط مدیر مجاز		<p>۱. تعیین زمان غیرفعال بودن برای یک کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد.</p> <p>۲. تعیین زمان پیشفرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد.</p>		
<input type="checkbox"/>	مدیریت مقادیر پیشفرض برای کنترل دسترسی محصول													
<input checked="" type="checkbox"/>	مدیریت نقشها در محصول													
<input checked="" type="checkbox"/>	مدیریت حداکثر تعداد مجاز نشستهای همزمان کاربران توسط مدیر													
<input type="checkbox"/>	مدیریت شرایط آغاز نشست توسط مدیر مجاز													
	<p>۱. تعیین زمان غیرفعال بودن برای یک کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد.</p> <p>۲. تعیین زمان پیشفرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد.</p>													
	<input type="checkbox"/>	<p>محصول باید توانایی تعریف نقشهای مختلف را داشته باشد.</p> <table border="1"> <tr> <td data-bbox="884 833 940 889"><input checked="" type="checkbox"/></td> <td data-bbox="940 833 1600 889">مدیر سیستم</td> <td data-bbox="1600 833 1837 1068" rowspan="4">نقش هایی که در محصول پشتیبانی می شوند، مشخص گردد.</td> </tr> <tr> <td data-bbox="884 889 940 946"><input checked="" type="checkbox"/></td> <td data-bbox="940 889 1600 946">کاربر پیشرفته</td> </tr> <tr> <td data-bbox="884 946 940 1003"><input checked="" type="checkbox"/></td> <td data-bbox="940 946 1600 1003">کاربر عادی</td> </tr> <tr> <td data-bbox="884 1003 940 1068"><input type="checkbox"/></td> <td data-bbox="940 1003 1600 1068">سایر موارد</td> </tr> </table>	<input checked="" type="checkbox"/>	مدیر سیستم	نقش هایی که در محصول پشتیبانی می شوند، مشخص گردد.	<input checked="" type="checkbox"/>	کاربر پیشرفته	<input checked="" type="checkbox"/>	کاربر عادی	<input type="checkbox"/>	سایر موارد	۵		
<input checked="" type="checkbox"/>	مدیر سیستم	نقش هایی که در محصول پشتیبانی می شوند، مشخص گردد.												
<input checked="" type="checkbox"/>	کاربر پیشرفته													
<input checked="" type="checkbox"/>	کاربر عادی													
<input type="checkbox"/>	سایر موارد													
	<input checked="" type="checkbox"/>	<p>محصول باید قادر باشد کاربران را به نقش های تعریف شده یا قابل تعریف مرتبط نماید، همچنین لازم است هر حساب کاربری تنها به یک نقش مرتبط شده باشد، اما ممکن است نقش ها تنها به یک کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند.</p>	۶											

۶-۲- حفاظت از توابع امنیتی محصول

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

توضیحات	کلاس حفاظت از توابع امنیتی محصول		شماره الزام					
	<input type="checkbox"/>	<p>محصول باید هنگام رخ دادن هرگونه شکست مانند از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول، در وضعیت امنی قرار گرفته و صحت داده‌ها و خطمشی کنترل دسترسی را حفظ نماید.</p> <table border="1" data-bbox="884 792 1835 1136"> <tr> <td data-bbox="884 792 940 966" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="940 792 1600 966">شکست‌های نرم‌افزاری</td> <td data-bbox="1600 792 1835 1136" rowspan="2">هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول حفظ می‌شود، مشخص گردد.</td> </tr> <tr> <td data-bbox="884 966 940 1136" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="940 966 1600 1136">شکست‌های سخت‌افزاری</td> </tr> </table>	<input checked="" type="checkbox"/>	شکست‌های نرم‌افزاری	هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول حفظ می‌شود، مشخص گردد.	<input checked="" type="checkbox"/>	شکست‌های سخت‌افزاری	۱
<input checked="" type="checkbox"/>	شکست‌های نرم‌افزاری	هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول حفظ می‌شود، مشخص گردد.						
<input checked="" type="checkbox"/>	شکست‌های سخت‌افزاری							
	<input checked="" type="checkbox"/>	محصول باید از طریق فراهم نمودن بستر و زیرساخت امن، توانایی محافظت از افشاء یا تغییر داده، هنگام انتقال بین بخش‌های مجزای خود را داشته باشد.	۲					
	<input type="checkbox"/>	در صورتی که محصول از محصولات امن IT استفاده می‌کند، باید تفسیر سازگار و یکسانی را از داده امنیتی در زمان اشتراک گذاری آن بین خود و دیگر محصولات امن IT، فراهم آورد.	۳					

		<input type="checkbox"/> داده‌های احراز هویت <input type="checkbox"/> کلید <input type="checkbox"/> امضای دیجیتال <input type="checkbox"/> داده‌های ممیزی <input type="checkbox"/> سایر موارد	داده امنیتی قابل اشتراک گذاری که در محصول پشتیبانی می‌شوند، مشخص گردد.	
	<input type="checkbox"/>	محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهره‌های زمانی معتبر، تولید یا استفاده نماید.	روش‌های ایجاد مهره‌های زمانی معتبر انتخاب شود. (دیگر روش‌های موجود در محصول، در قسمت «سایر موارد» بیان شود).	۴
	<input type="checkbox"/>	<input type="checkbox"/> گرفتن مهره‌های زمانی از سرور NTP <input type="checkbox"/> تنظیم مهره‌های زمانی از طریق اینترنت <input checked="" type="checkbox"/> تنظیم مهره‌های زمانی به صورت پیشفرض (معتبر و عدم امکان دستکاری غیرمجاز) <input type="checkbox"/> سایر موارد		
	<input type="checkbox"/>	محصول باید امکان به‌روزرسانی نرم افزار و میان افزار محصول را برای مدیر سیستم فراهم نماید.	به‌روز رسانی دستی	۵

		<input type="checkbox"/> جستجوی خودکار به روزرسانی ها	روش به‌روزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).
		<input type="checkbox"/> به روزرسانی‌های خودکار	
		<input type="checkbox"/> به‌روزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل به‌روزرسانی	
	<input type="checkbox"/>	در صورت استفاده از به‌روزرسانی به روش خودکار، محصول باید پیش از نصب به‌روزرسانی‌های نرم‌افزاری و میان‌افزاری، امکان احراز اصالت میان‌افزار یا نرم‌افزار را فراهم نماید.	۶ سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی) به‌روزرسانی‌ها انتخاب گردد.
		<input type="checkbox"/> امضاء دیجیتال	
		<input type="checkbox"/> درهم‌ساز منتشرشده	

۲-۷- تخصیص منابع

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

توضیحات	کلاس تخصیص منابع		شماره الزام
	<input checked="" type="checkbox"/>	محصول باید در زمان رخداد هرگونه شکست نرم‌افزاری؛ از عملکرد کارکردهای اصلی محصول اطمینان حاصل نماید.	۱

۸-۲- دسترسی به محصول

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

شماره الزام	کلاس دسترسی به محصول	توضیحات
۱	محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.	<input checked="" type="checkbox"/>
۲	محصول باید کلیه نشست‌های تعاملی راه‌دور ^۴ را پس از مدت زمانی که غیرفعال هستند (و می‌بایست توسط مدیر قابل تنظیم باشد)، خاتمه دهد.	<input checked="" type="checkbox"/>
۳	محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.	<input checked="" type="checkbox"/>
۴	در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس موارد زیر باشد.	<input type="checkbox"/>
	روز	<input checked="" type="checkbox"/>
	زمان	<input checked="" type="checkbox"/>
	سایر موارد	<input type="checkbox"/>

انتخاب یک مورد لازم و کافی است.

^۴Remote

	<input type="checkbox"/>	در صورت برقراری نشست به طور موفقیت آمیز، محصول باید قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست بر اساس موارد زیر و تعداد تلاش‌های ناموفق تا آخرین ایجاد نشست موفقیت‌آمیز باشد.		انتخاب یک مورد لازم و کافی است.
		<input type="checkbox"/>	روز	
		<input type="checkbox"/>	زمان	
		<input type="checkbox"/>	سایر موارد	
	<input type="checkbox"/>	محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.		۶
	<input type="checkbox"/>	محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.		پارامترهای موجود برای جلوگیری از نشست، مشخص شوند (وجود یک مورد لازم و کافی است).
		<input type="checkbox"/>	مکان	
		<input checked="" type="checkbox"/>	شماره پورت	
		<input type="checkbox"/>	روز	
		<input type="checkbox"/>	زمان	
		<input type="checkbox"/>	سایر موارد	

۹-۲- کانال‌ها/مسیرهای مورد اعتماد

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

توضیحات	کلاس کانال‌ها/مسیرهای مورد اعتماد		شماره الزام					
	<input type="checkbox"/>	<p>محصول باید قادر باشد مسیر ارتباطی امنی بین خود، کاربران و دیگر محصولات IT فراهم نماید که به طور منطقی از دیگر کانال‌ها متمایز باشد. سپس از طریق این کانال احراز هویت را انجام داده و از تغییر و افشاء داده تبادلی حفاظت نموده و تغییرات را تشخیص دهد. در صورت انتخاب مورد HTTPS، رعایت الزام ۳-۱- و در صورت انتخاب TLS، رعایت الزامات ۳-۲- تا ۳-۴- که در بخش ۳- بیان گردیده است، الزامی است.</p> <table border="1" data-bbox="884 889 1835 1092"> <tr> <td data-bbox="884 889 940 987" style="text-align: center; vertical-align: top;"> <input checked="" type="checkbox"/> </td> <td data-bbox="940 889 1602 987">HTTPS</td> <td data-bbox="1602 889 1835 1092" rowspan="2" style="text-align: center; vertical-align: middle;"> پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد. </td> </tr> <tr> <td data-bbox="884 987 940 1092" style="text-align: center; vertical-align: top;"> <input type="checkbox"/> </td> <td data-bbox="940 987 1602 1092">TLS</td> </tr> </table>	<input checked="" type="checkbox"/>	HTTPS	پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد.	<input type="checkbox"/>	TLS	۱
<input checked="" type="checkbox"/>	HTTPS	پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد.						
<input type="checkbox"/>	TLS							
	<input checked="" type="checkbox"/>	<p>محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.</p>	۲					
	<input checked="" type="checkbox"/>	<p>محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.</p>	۳					

۳- الزامات امنیتی مبتنی بر انتخاب

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

۳-۱- پروتکل HTTPS

شماره الزام	کلاس کانال‌ها/مسیرهای مورد اعتماد	توضیحات
۱	<input checked="" type="checkbox"/> محصول باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کند.	
۲	<input checked="" type="checkbox"/> محصول باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	
۳	<input type="checkbox"/> در صورتی که گواهی‌نامه ارائه شده از سمت دیگر محصولات IT (درهنگام برقراری ارتباط) نامعتبر باشد، محصول باید بر اساس موارد زیر عمل نماید. اعتبارسنجی گواهی‌نامه بر اساس الزامات بخش ۳-۵-۳ انجام می‌شود که در این صورت الزامات بخش ۳-۵-۳ الزامی است.	
	<input checked="" type="checkbox"/> اتصال را برقرار نکنند.	محصول تنها از موارد بیان شده می‌تواند استفاده نماید.
	<input checked="" type="checkbox"/> برای برقراری اتصال درخواست مجوز کند.	

۳-۲- پروتکل TLS Client

توضیحات	پروتکل TLS Client		شماره الزام																	
	<input type="checkbox"/>	<p>محصول باید TLS 1.2 (RFC 5246) و/یا TLS 1.1 (RFC 4346) را پیاده‌سازی کند و دیگر نسخه‌های TLS و SSL را رد کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه رمزهای زیر پیاده‌سازی نماید.</p> <table border="1" data-bbox="882 634 1633 1338"> <tr> <td data-bbox="882 634 882 721"><input type="checkbox"/></td> <td data-bbox="882 634 1633 721"> TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 </td> <td data-bbox="1633 634 1837 1338" rowspan="8"> مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد. </td> </tr> <tr> <td data-bbox="882 721 882 807"><input type="checkbox"/></td> <td data-bbox="882 721 1633 807"> TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268 </td> </tr> <tr> <td data-bbox="882 807 882 893"><input type="checkbox"/></td> <td data-bbox="882 807 1633 893"> TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 </td> </tr> <tr> <td data-bbox="882 893 882 979"><input type="checkbox"/></td> <td data-bbox="882 893 1633 979"> TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 </td> </tr> <tr> <td data-bbox="882 979 882 1065"><input type="checkbox"/></td> <td data-bbox="882 979 1633 1065"> TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268 </td> </tr> <tr> <td data-bbox="882 1065 882 1151"><input type="checkbox"/></td> <td data-bbox="882 1065 1633 1151"> TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 </td> </tr> <tr> <td data-bbox="882 1151 882 1237"><input type="checkbox"/></td> <td data-bbox="882 1151 1633 1237"> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 </td> </tr> <tr> <td data-bbox="882 1237 882 1338"><input type="checkbox"/></td> <td data-bbox="882 1237 1633 1338"> TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492 </td> </tr> </table>	<input type="checkbox"/>	TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.	<input type="checkbox"/>	TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492	۱
<input type="checkbox"/>	TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.																		
<input type="checkbox"/>	TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268																			
<input type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268																			
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268																			
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268																			
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268																			
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492																			
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492																			

<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492		
<input type="checkbox"/>	TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246		
<input type="checkbox"/>	TLS_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246		
<input type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246		
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246		
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246		
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246		
<input type="checkbox"/>	TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288		
<input type="checkbox"/>	TLS_RSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5288		

<input type="checkbox"/>	TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA384 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289		
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289		

	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289		
۲	<input type="checkbox"/>	محصول باید مطابقت شناسه ارائه شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تأیید نماید.		
۳	<input type="checkbox"/>	محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد؛ بنابراین اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید بر اساس موارد زیر رفتار نماید.		
		<input checked="" type="checkbox"/>	ارتباط را برقرار نکند	در صورت پشتیبانی
		<input type="checkbox"/>	برای برقراری ارتباط درخواست مجوز کند	از اقدامات دیگر، در «سایر موارد»
		<input type="checkbox"/>	سایر موارد	بیان گردد.
۴	<input type="checkbox"/>	محصول باید در پیام ClientHello برای استفاده از منحنی‌ها، بر اساس موارد زیر عمل نماید.		
		<input type="checkbox"/>	Supported Elliptic Curves Extension را ارائه نکند	در صورت که محصول از
		<input type="checkbox"/>	Supported Elliptic Curves Extension را به همراه NIST Curve های secp256r1 یا secp384r1 یا secp521r1 ارائه نماید	منحنی استفاده می‌نماید، طول
		<input type="checkbox"/>	هیچ منحنی دیگری	کلید باید مشخص گردد.

۳-۳- پروتکل TLS Server

توضیحات	پروتکل TLS Server		شماره الزام																	
	<input type="checkbox"/>	<p>محصول باید (RFC 5246) TLS 1.2 را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه رمزهای زیر پیاده‌سازی نماید.</p> <table border="1" data-bbox="798 617 1837 1320"> <tr> <td data-bbox="798 617 850 1320" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="850 617 1606 706"> TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 </td> <td data-bbox="1606 617 1837 1320" rowspan="8" style="vertical-align: middle;"> مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد. </td> </tr> <tr> <td data-bbox="798 706 850 787" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="850 706 1606 787"> TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268 </td> </tr> <tr> <td data-bbox="798 787 850 868" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="850 787 1606 868"> TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268 </td> </tr> <tr> <td data-bbox="798 868 850 950" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="850 868 1606 950"> TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 </td> </tr> <tr> <td data-bbox="798 950 850 1031" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="850 950 1606 1031"> TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 </td> </tr> <tr> <td data-bbox="798 1031 850 1112"></td> <td data-bbox="850 1031 1606 1112"> TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 </td> </tr> <tr> <td data-bbox="798 1112 850 1193" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="850 1112 1606 1193"> TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492 </td> </tr> <tr> <td data-bbox="798 1193 850 1320" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="850 1193 1606 1320"> TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492 </td> </tr> </table>	<input type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492		TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	۵
<input type="checkbox"/>	TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.																		
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268																			
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268																			
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492																			
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492																			
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492																			
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492																			
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492																			

	<input type="checkbox"/> TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246	
	<input type="checkbox"/> TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246	
	<input type="checkbox"/> TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246	
	<input type="checkbox"/> TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246	
	<input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289	
	<input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289	
	<input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289	
	<input type="checkbox"/> TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289	
	<input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289	
	<input type="checkbox"/> TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289	
	<input type="checkbox"/> محصول باید اتصالاتی کاربرانی که درخواست TLS1.0 ، SSL3.0 ، SSL2.0 و SSL1.0 دارند را رد نماید.	۶
	<input type="checkbox"/> محصول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید.	۷

	<input type="checkbox"/>	استفاده از RSA با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ یا ۴۰۹۶ بیت	در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.
	<input type="checkbox"/>	پارامترهای ECDH با استفاده از NIST Curve های secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگری	
	<input type="checkbox"/>	پارامترهای دیفی-هلمن با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ بیت	

۴-۳- پروتکل TLS مشترک کلاینت و سرور

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

توضیحات	پروتکل TLS مشترک کلاینت و سرور	شماره الزام
	<input type="checkbox"/> محصول باید احراز هویت دوطرفه کلاینت‌ها/سرورهای TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید.	۱
	<input checked="" type="checkbox"/> محصول در صورت مطابقت نداشتن نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه از شناساننده کلاینت مورد انتظار بوده است، نباید کانال امن را برقرار سازد.	۲

 Identifier

۵-۳- اعتبارسنجی گواهی‌نامه

توضیحات	شناسایی و احراز هویت	شماره الزام																
	<table border="1"> <tr> <td data-bbox="785 508 821 613" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="821 508 1835 613">محصول باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند.</td> </tr> <tr> <td data-bbox="785 613 821 719" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="821 613 1835 719">تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.</td> </tr> <tr> <td data-bbox="785 719 821 776" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="821 719 1835 776">مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.</td> </tr> <tr> <td data-bbox="785 776 821 927" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="821 776 1835 927">محصول باید برای تأیید مسیر یک گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم شده است.</td> </tr> <tr> <td data-bbox="785 927 821 1032" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="821 927 1835 1032">پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص شده در RFC 696</td> </tr> <tr> <td data-bbox="785 1032 821 1138" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="821 1032 1835 1138">لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۳، ۶</td> </tr> <tr> <td data-bbox="785 1138 821 1243" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="821 1138 1835 1243">لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵</td> </tr> <tr> <td data-bbox="785 1243 821 1287" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="821 1243 1835 1287">هیچ روش فسخ دیگری</td> </tr> </table>	<input type="checkbox"/>	محصول باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند.	<input type="checkbox"/>	تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.	<input type="checkbox"/>	مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.	<input type="checkbox"/>	محصول باید برای تأیید مسیر یک گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم شده است.	<input type="checkbox"/>	پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص شده در RFC 696	<input type="checkbox"/>	لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۳، ۶	<input type="checkbox"/>	لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵	<input type="checkbox"/>	هیچ روش فسخ دیگری	۱
<input type="checkbox"/>	محصول باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند.																	
<input type="checkbox"/>	تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.																	
<input type="checkbox"/>	مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.																	
<input type="checkbox"/>	محصول باید برای تأیید مسیر یک گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم شده است.																	
<input type="checkbox"/>	پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص شده در RFC 696																	
<input type="checkbox"/>	لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۳، ۶																	
<input type="checkbox"/>	لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵																	
<input type="checkbox"/>	هیچ روش فسخ دیگری																	

	<input type="checkbox"/>	<p>گواهی‌نامه‌های مورد استفاده برای تأیید به‌روزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی باید هدف «Code Signing» (id-kp3 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.</p> <p>گواهی‌نامه‌های سرور ارائه شده برای TLS باید هدف «Server Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.</p> <p>گواهی‌نامه‌های کلاینت ارائه شده برای TLS باید هدف «Client Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.</p> <p>گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ OCSP باید «OCSP Signing» (id-pk9 با OID 1.3.6.1.5.5.7.3.9) را در فیلد extendedKeyUsage خود داشته باشند.</p>	<p>قوانین تأیید فیلد extendedKeyUsage</p>						
	<input type="checkbox"/>	<p>محصول باید تنها در صورتی که افزونه مربوط به basicConstraints از پیش تنظیم شده باشد و همچنین، پرچم CA به حالت «TRUE» تنظیم شده باشد، یک گواهی‌نامه را به عنوان گواهی‌نامه CA بپذیرد.</p>							
	<input type="checkbox"/>	<p>محصول باید جهت پشتیبانی احراز هویت برای موارد زیر از گواهی‌نامه‌های X509v3 تعریف شده در RFC 5280 استفاده کند.</p> <table border="1" data-bbox="829 1169 1596 1299"> <tr> <td data-bbox="829 1169 871 1234"> <input type="checkbox"/> </td> <td data-bbox="871 1169 1596 1234">HTTPS</td> <td data-bbox="1596 1169 1837 1234" rowspan="2"> <p>در صورت پشتیبانی از</p> </td> </tr> <tr> <td data-bbox="829 1234 871 1299"> <input type="checkbox"/> </td> <td data-bbox="871 1234 1596 1299">TLS</td> </tr> </table>			<input type="checkbox"/>	HTTPS	<p>در صورت پشتیبانی از</p>	<input type="checkbox"/>	TLS
<input type="checkbox"/>	HTTPS	<p>در صورت پشتیبانی از</p>							
<input type="checkbox"/>	TLS								

	<input type="checkbox"/>	امضای کد برای به‌روزرسانی‌های نرم‌افزار سیستم	کارکرد های دیگر، در «سایر موارد» بیان گردد.
	<input type="checkbox"/>	امضای کد برای تأیید یکپارچگی	
	<input type="checkbox"/>	سایر موارد	