

به نام خدا

سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه

بهین گستر گیتی

سامانه ارزیابی عملکرد سازمانی BSCMaster

12.0



شرکت تحقیق در عملیات
بهین گستر گیت

BEHIN GOSTAR GITI operations research co.

۱۴۰۱،۰۴

نسخه ۵،۰

پیشگفتار

در نظام ارزیابی امنیتی محصولات فتا، یکی از اسناد مورد نیاز برای انجام آزمون امنیتی، سند هدف امنیتی است. بر اساس استاندارد معیار مشترک (CC) سند هدف امنیتی مبتنی بر اسنادی که پروفایل حفاظتی نام دارند، 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 برای تولیدکننده کاری زمان‌بر 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.

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.

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- معرفی محصول
۴	۱-۱- ویژگی‌های فنی محصول
۴	۲-۱- معماری محصول
۶	۲- الزامات امنیتی
۶	۱-۲- ممیزی امنیت (Log)
۱۰	۲-۲- رمزنگاری
۱۲	۳-۲- شناسایی و احراز هویت
۱۶	۴-۲- حفاظت از داده‌ی کاربری
۲۰	۵-۲- مدیریت امنیت
۲۳	۶-۲- حفاظت از توابع امنیتی محصول
۲۵	۷-۲- تخصیص منابع
۲۶	۸-۲- دسترسی به محصول
۲۸	۹-۲- کانال‌ها/مسیرهای مورد اعتماد
۲۹	۳- الزامات امنیتی مبتنی بر انتخاب
۲۹	۱-۳- پروتکل HTTPS
۳۰	۲-۳- پروتکل TLS Client
۳۳	۳-۳- پروتکل TLS Server
۳۶	۴-۳- پروتکل TLS مشترک کلاینت و سرور
۳۷	۵-۳- اعتبارسنجی گواهی‌نامه
۳۹	۳-۶- پروتکل SSH

۱- معرفی محصول

نرم افزار BSCMaster یک نرم افزار ارزیابی عملکرد شاخصهای سازمانی است . شرکت یا سازمان مصرف کننده، برای تعیین خط مشی مدیریتی سازمان استراتژی های آینده خود را تعیین و تصویب و ابلاغ می کند.

این سیستم با هدف ایجاد بستر مناسب برای پیاده سازی متدولوژی ارزیابی متوازن در سازمان طراحی و تولید شده است. با در اختیار داشتن این سیستم سازمان می تواند عملکرد خود را به صورت مستمر ارزیابی کند، میزان تحقق استراتژی ها را پایش نموده و تصمیمات لازم جهت ارتقای سطح عملکرد را اتخاذ نماید.

این نرم افزار یک نرم افزار تحت وب و متمرکز می باشد که فقط در یک سرور Application Server نصب شده و کاربران فقط نیاز به یک مرورگر استاندارد دارند.

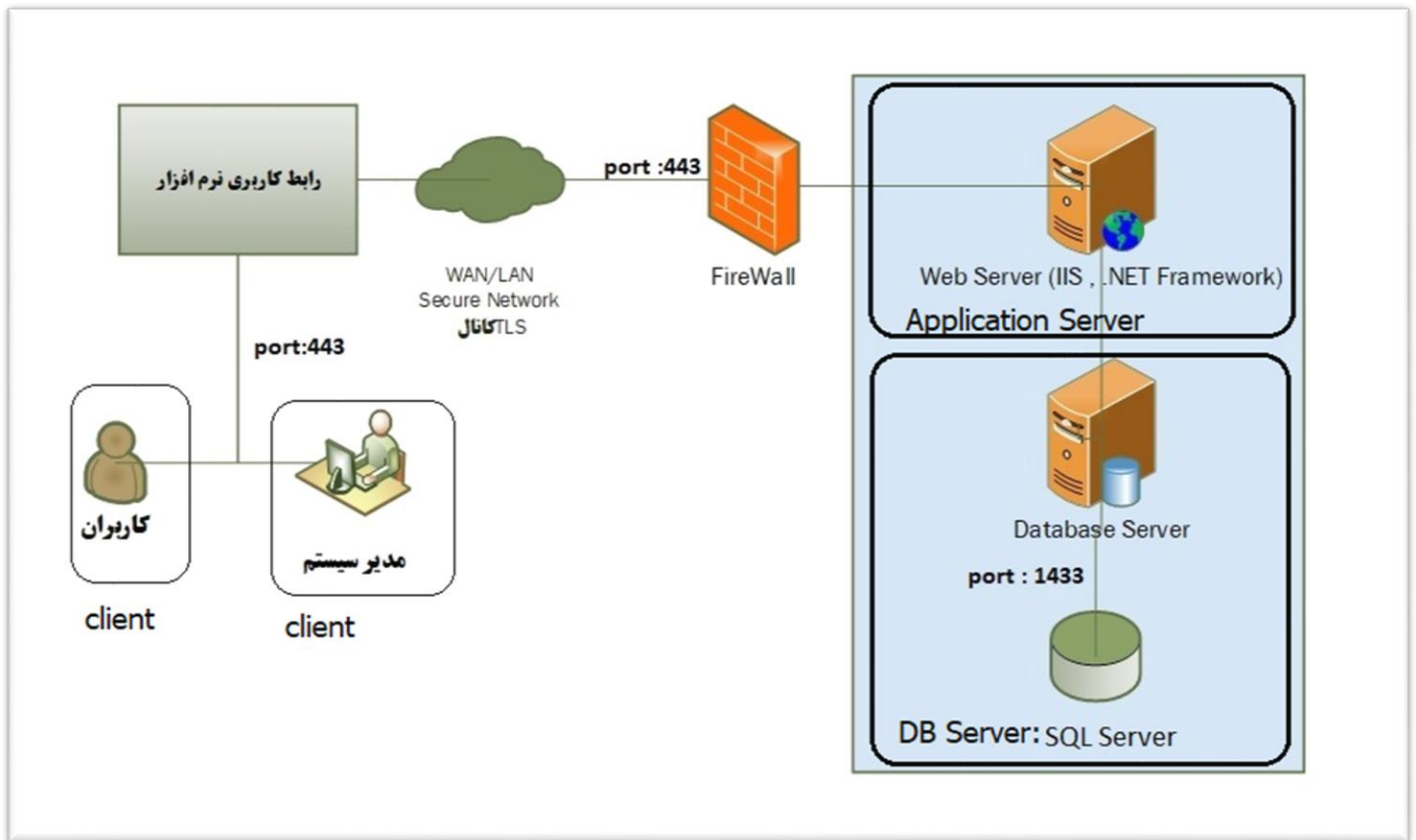
۱-۱- ویژگی‌های فنی محصول

نسخه‌ی نرم‌افزار/میان‌افزار	۱۲,۰
مدل و نسخه سیستم‌عامل	Windows server 2019
مدل و نسخه وب‌سرور	IIS over windows 2019
مدل و نسخه پایگاه داده	SQL Server 2019
زبان برنامه‌نویسی	C# Web Form

۱-۲- معماری محصول

در سامانه BSCMaster ، یک دیتابیس مرکزی SQL Server وجود دارد و همه کدهای برنامه نویسی شده و فایلها و عکسها در یک Application Server روی IIS نصب می شود. ارتباط بین دیتابیس و سامانه از طریق ConnectionString در فایل web.config تنظیم می شود. همه کاربران از طریق آدرس اینترنتی مربوطه و از طریق مرورگر استاندارد به سامانه متصل می شوند.

در شکل زیر نحوه قرار گیری محصول در محیط عملیاتی و پیکربندی آن نمایش داده شده است.



شکل ۱: نحوه قرار گیری محصول در محیط عملیاتی و پیکربندی

۲- الزامات امنیتی

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

۲-۱- ممیزی امنیت (Log)

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

توضیحات	رده ممیزی امنیت (Log)	شماره الزام																						
	<table border="1"> <tr> <td data-bbox="875 708 915 821"><input checked="" type="checkbox"/></td> <td data-bbox="915 708 1948 821">محصول باید برای موارد مشخص شده که در زیر آمده است، ثبت‌نشان^۲ تولید کند (Log) ثبت نماید).</td> </tr> <tr> <td data-bbox="875 821 915 870"><input checked="" type="checkbox"/></td> <td data-bbox="915 821 1948 870">شروع و اتمام توابع</td> </tr> <tr> <td data-bbox="875 870 915 919"><input checked="" type="checkbox"/></td> <td data-bbox="915 870 1948 919">تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها</td> </tr> <tr> <td data-bbox="875 919 915 967"><input checked="" type="checkbox"/></td> <td data-bbox="915 919 1948 967">خواندن اطلاعات از ثبت‌نشان‌ها</td> </tr> <tr> <td data-bbox="875 967 915 1016"><input checked="" type="checkbox"/></td> <td data-bbox="915 967 1948 1016">تمامی تغییرات در پیکربندی ثبت‌نشان‌ها</td> </tr> <tr> <td data-bbox="875 1016 915 1065"><input checked="" type="checkbox"/></td> <td data-bbox="915 1016 1948 1065">عملیات انجام شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه</td> </tr> <tr> <td data-bbox="875 1065 915 1114"><input checked="" type="checkbox"/></td> <td data-bbox="915 1065 1948 1114">عملیات انجام شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها</td> </tr> <tr> <td data-bbox="875 1114 915 1162"><input checked="" type="checkbox"/></td> <td data-bbox="915 1114 1948 1162">تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.</td> </tr> <tr> <td data-bbox="875 1162 915 1211"><input checked="" type="checkbox"/></td> <td data-bbox="915 1162 1948 1211">تمام کاربردهای سازوکار احراز هویت</td> </tr> <tr> <td data-bbox="875 1211 915 1260"><input checked="" type="checkbox"/></td> <td data-bbox="915 1211 1948 1260">نتایج نهایی عملیات احراز هویت</td> </tr> <tr> <td data-bbox="875 1260 915 1321"><input checked="" type="checkbox"/></td> <td data-bbox="915 1260 1948 1321">تلاش موفق و ناموفق هر گذرواژه بررسی شده توسط محصول</td> </tr> </table>	<input checked="" type="checkbox"/>	محصول باید برای موارد مشخص شده که در زیر آمده است، ثبت‌نشان ^۲ تولید کند (Log) ثبت نماید).	<input checked="" type="checkbox"/>	شروع و اتمام توابع	<input checked="" type="checkbox"/>	تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها	<input checked="" type="checkbox"/>	خواندن اطلاعات از ثبت‌نشان‌ها	<input checked="" type="checkbox"/>	تمامی تغییرات در پیکربندی ثبت‌نشان‌ها	<input checked="" type="checkbox"/>	عملیات انجام شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه	<input checked="" type="checkbox"/>	عملیات انجام شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها	<input checked="" 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 گذرواژه بررسی شده توسط محصول	<p>۱</p> <p>رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.</p>
<input checked="" type="checkbox"/>	محصول باید برای موارد مشخص شده که در زیر آمده است، ثبت‌نشان ^۲ تولید کند (Log) ثبت نماید).																							
<input checked="" type="checkbox"/>	شروع و اتمام توابع																							
<input checked="" type="checkbox"/>	تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها																							
<input checked="" type="checkbox"/>	خواندن اطلاعات از ثبت‌نشان‌ها																							
<input checked="" type="checkbox"/>	تمامی تغییرات در پیکربندی ثبت‌نشان‌ها																							
<input checked="" type="checkbox"/>	عملیات انجام شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه																							
<input checked="" type="checkbox"/>	عملیات انجام شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها																							
<input checked="" 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 گذرواژه بررسی شده توسط محصول																							

^۱ Profile

^۲ Log

	<input checked="" type="checkbox"/>	شکست و موفقیت انتساب ویژگی‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال)												
	<input checked="" type="checkbox"/>	تمامی تغییرات بر روی مقادیر ویژگی‌های امنیتی												
	<input checked="" type="checkbox"/>	تمامی درخواست‌ها (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 ویژگی‌های امنیتی)												
	<input checked="" type="checkbox"/>	همه تلاش‌ها برای خارج کردن اطلاعات از محصول												
	<input checked="" 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 checked="" type="checkbox"/>	شکست در کارکردهای امنیتی محصول												
	<input checked="" type="checkbox"/>	تمامی قابلیت‌هایی از محصول که به دلیل شکست (خرابی یا مشکل کارکرد)، نمی‌توانند عملیات مورد نظر را انجام دهند.												
	<input checked="" type="checkbox"/>	تلاش موفق یا ناموفق برای برقراری نشست.												
	<input checked="" type="checkbox"/>	ایجاد نشدن نشست به دلیل محدودیت نشست‌های همزمان (حداقل)												
	<input checked="" type="checkbox"/>	خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست												
	<input type="checkbox"/>	خاتمه به نشست غیرفعال توسط مدیر سیستم												
	<input type="checkbox"/>	سایر موارد												
	<input checked="" type="checkbox"/>	<p>محصول باید برای هر ثبت‌نشان تولیدشده، ویژگی‌هایی که در زیر آمده است را ثبت نماید.</p> <table border="1" data-bbox="961 1218 1711 1466"> <tr> <td data-bbox="961 1218 1045 1273"><input checked="" type="checkbox"/></td> <td data-bbox="1045 1218 1711 1273">تاریخ و زمان رویداد</td> <td data-bbox="1711 1218 2030 1466" rowspan="5">و ویژگی‌هایی که در ثبت‌نشان‌ها وجود دارد مشخص شود.</td> </tr> <tr> <td data-bbox="961 1273 1045 1328"><input checked="" type="checkbox"/></td> <td data-bbox="1045 1273 1711 1328">نوع رویداد</td> </tr> <tr> <td data-bbox="961 1328 1045 1383"><input checked="" type="checkbox"/></td> <td data-bbox="1045 1328 1711 1383">هویت ایجادکننده رویداد</td> </tr> <tr> <td data-bbox="961 1383 1045 1438"><input checked="" type="checkbox"/></td> <td data-bbox="1045 1383 1711 1438">نتیجه رویداد</td> </tr> <tr> <td data-bbox="961 1438 1045 1466"><input checked="" type="checkbox"/></td> <td data-bbox="1045 1438 1711 1466">آدرس IP ایجادکننده رویداد</td> </tr> </table>	<input checked="" type="checkbox"/>	تاریخ و زمان رویداد	و ویژگی‌هایی که در ثبت‌نشان‌ها 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	۲
<input checked="" type="checkbox"/>	تاریخ و زمان رویداد	و ویژگی‌هایی که در ثبت‌نشان‌ها 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													

در رویدادهای مهم User Agent هم نگهداری می شود	<input checked="" type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	محصول باید ثبت‌نشان‌ها را در برابر دسترسی غیرمجاز محافظت نماید.	
	<input checked="" type="checkbox"/>	ثبت‌نشان‌هایی که محصول تولید می‌نماید باید برای کاربر ساده و قابل فهم باشند.	
	<input checked="" type="checkbox"/>	نبود داده نامفهوم در رکوردها	مواردی که در
	<input checked="" type="checkbox"/>	نبود بخش‌های نامرتب	ثبت‌نشان‌ها وجود
	<input checked="" type="checkbox"/>	وجود داده معتبر و مناسب در هر بخش	دارند، مشخص شوند.
	<input checked="" type="checkbox"/>	محصول باید امکان انتخاب و مرتب‌سازی برای ثبت‌نشان‌های تولیدشده را بر اساس بخش‌ها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید.	
	<input checked="" type="checkbox"/>	هویت موجودیت فعال	مواردی که بر اساس
	<input type="checkbox"/>	نوع حساب کاربری	آنها مرتب‌سازی وجود
	<input checked="" type="checkbox"/>	تاریخ/زمان	دارد، مشخص شود.
	<input type="checkbox"/>	روش اتصال کاربر	
	<input checked="" type="checkbox"/>	نوع رخداد	
	<input checked="" type="checkbox"/>	مکان رویداد	
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	محصول باید هرگونه حذف و تغییر غیرمجاز در ثبت‌نشان‌ها را تشخیص دهد و در صورت امکان جلوگیری نماید.	
	<input type="checkbox"/>	استفاده از درهم‌سازی (Hash) برای تشخیص تغییرات	روش‌های تشخیص
	<input type="checkbox"/>	پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)	مشخص شود. (وجود)
همه کاربران حتی admin فقط اجازه خواندن ثبت‌نشان‌ها را دارند	<input checked="" type="checkbox"/>	فقط خواندنی کردن ثبت‌نشان‌ها در محصول	یک مورد لازم و کافی
	<input type="checkbox"/>	سایر موارد	(است)

	<input checked="" type="checkbox"/>	<p>محصول باید وقتی که حجم ثبت‌نشان‌ها، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.</p>	۷
<p>به مدیر سیستم در صفحه اصلی هشدار عبور از حد آستانه را نمایش می‌دهد</p>	<input type="checkbox"/>	<p>روش‌های اطلاع‌رسانی استفاده از یک کانال ارتباطی</p>	
	<input type="checkbox"/>	<p>ارسال پیام</p>	<p>مشخص شود (وجود)</p>
	<input checked="" type="checkbox"/>	<p>از طریق واسط کاربر مجاز</p>	<p>یک مورد لازم و کافی</p>
	<input type="checkbox"/>	<p>سایر موارد</p>	<p>(است)</p>
<p>دادها های ثبت نشان ها در زمان پر شدن محدودیت ثبت نشان ها کماکان ذخیره می شود وبه کاربر مدیر سیستم هشدار مناسب می دهد</p>	<input checked="" type="checkbox"/>	<p>محصول باید توانایی تولید ثبت‌نشان (ثبت Log) هنگام از کار افتادن محصول و/یا پر شدن حافظه ثبت‌نشان‌ها را داشته باشد و برای این کار از رویکردهای بیان‌شده استفاده نماید.</p>	۸
	<input type="checkbox"/>	<p>نادیده گرفتن ثبت‌نشان‌ها</p>	<p>رویکرد های مورد</p>
	<input type="checkbox"/>	<p>ذخیره‌سازی محدود ثبت‌نشان‌ها (آنهايي که توسط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند)</p>	<p>استفاده در محصول</p>
	<input type="checkbox"/>	<p>بازنویسی روی قدیمی‌ترین ثبت‌نشان‌های ذخیره‌شده</p>	<p>مشخص گردد (وجود)</p>
	<input checked="" type="checkbox"/>	<p>سایر موارد</p>	<p>یک مورد لازم و کافی (است)</p>

۲-۲- رمزنگاری

در این رده، توانایی محصول در پیاده‌سازی یا به‌کارگیری واحدهای^۳ رمزنگاری، بررسی می‌گردد. برای حفظ محرمانگی داده، از رمزنگاری استفاده می‌شود و این رمزنگاری‌ها می‌توانند 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 روش‌های مختلفی (مد عملیاتی) به رمزگذاری و رمزگشایی داده بپردازند که در این رده، توانایی محصول از این جهت مورد بررسی قرار گرفته است. در رده رمزنگاری همچنین الگوریتم‌های درهم‌سازی (Hash) برای برقراری جامعیت داده استفاده می‌گردد.

شماره الزام	رده رمزنگاری	توضیحات	
۱	<input checked="" type="checkbox"/> محصول باید قابلیت رمزنگاری یا واحد رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف‌شده 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 (تعریف‌شده در NIST SP 800-38A)	مد عملیاتی که الگوریتم از آن استفاده می‌کند را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)
		<input checked="" type="checkbox"/> مد عملیاتی GCM و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در NIST SP 800-38D)	طول بیت ۱۲۸ و ۲۵۶
		<input type="checkbox"/> مد عملیاتی CTR و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در ISO10116)	
۲	<input checked="" type="checkbox"/> محصول باید بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب می‌نماید، توانایی تولید داده درهم‌سازی شده (Hash) را داشته باشد؛ بنابراین باید برای تولید درهم‌سازی از موارد زیر بر اساس ISO/IEC 10118-3:2004 استفاده نماید.		
		<input type="checkbox"/> الگوریتم SHA-1 با اندازه خلاصه پیام ۱۶۰ بیت	الگوریتم و اندازه خلاصه پیام مورد استفاده را
		<input checked="" type="checkbox"/> الگوریتم SHA-256 با اندازه خلاصه پیام ۲۵۶ بیت	

^۳ Modules

	<input checked="" type="checkbox"/>	الگوریتم SHA-384 با اندازه خلاصه پیام ۳۸۴ بیت	انتخاب نمایید. (وجود
	<input type="checkbox"/>	الگوریتم SHA-512 با اندازه خلاصه پیام ۵۱۲ بیت	یک مورد لازم و کافی است.)
	<input checked="" type="checkbox"/>	در صورتی که تولید کلید رمزنگاری در محصول وجود دارد، نیاز است که تخریب کلید رمزنگاری نیز بر اساس موارد زیر صورت پذیرد. (اختیاری)	
	<input type="checkbox"/>	نابودی با استفاده از بازنویسی ساده (بازنویسی با صفرها، یک‌ها، مقدار تصادفی، مقدار جدیدی از کلید)	روش نابودی کلید مشخص گردد. (وجود
	<input type="checkbox"/>	نابودی با استفاده از یک واسط مشخص	یک مورد لازم و کافی است)
	<input checked="" type="checkbox"/>	از طریق توابع امنیتی محصول	
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	در صورتی که امضای دیجیتال در محصول پشتیبانی می‌شود، نیاز است که سرویس‌های امضای رمزنگاری (تولید و تأیید) بر اساس الگوریتم‌های رمزنگاری زیر انجام گیرد. (اختیاری)	
	<input checked="" type="checkbox"/>	الگوریتم‌های امضای دیجیتال RSA با کلیدهای رمزنگاری ۲۰۴۸ بیت و بزرگتر (بر اساس FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS) بخش ۵،۵،	الگوریتم و اندازه کلیدهای مورد استفاده را انتخاب نمایید.
	<input checked="" type="checkbox"/>	الگوی امضای RSASSA-PSS نسخه ۲.۱ v2.1 PKCS #1 و یا RSASSA-ISO/IEC 9796-2؛ PKCS1v_5، الگوی امضای دیجیتال ۲ و یا الگوی امضای دیجیتال (۳)	
	<input checked="" type="checkbox"/>	الگوریتم‌های امضای 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)	(وجود یک مورد لازم و کافی است)

۲-۳- شناسایی و احراز هویت

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

توضیحات	رده شناسایی و احراز هویت		شماره الزام
	<input checked="" type="checkbox"/>	محصول باید بتواند تعداد تلاش‌های ناموفقی را که برای احراز هویت صورت گرفته است (در هر بخش یا قسمتی که نیاز به احراز هویت وجود دارد)، بر اساس موارد زیر مشخص نماید.	۱
	<input type="checkbox"/>	مقدار یا یازهی مورد استفاده در هر یک باید یک عدد مثبت ثابت	مشخص گردد. (وجود یک مورد لازم و کافی است)
	<input checked="" type="checkbox"/>	یک عدد مثبت قابل تنظیم توسط مدیر	
<p>کاربر به مدت زمان تنظیم شده توسط مدیر سیستم Lock می‌شود و بعد از آن اجازه ورود به سیستم خواهد داشت</p> <p>سامانه همواره از Captcha استفاده می‌کند حتی اگر کاربر تلاش ناموفق قبلی نداشته باشد</p>	<input checked="" type="checkbox"/>	<p>محصول باید هنگامی 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> <p>غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)</p> <p>غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)</p> <p>استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت «توضیحات» بیان شود)</p>	۲
	<input type="checkbox"/>	روش استفاده شده برای پیچیده‌تر کردن احراز هویت را انتخاب	نمایند. (وجود یک مورد لازم و کافی است). لازم به ذکر است روش‌های فوق با توجه به نوع کاربرد می‌تواند از حالت انتخایی به حالت الزامی تغییر یابد.
	<input checked="" type="checkbox"/>	غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)	

	<input type="checkbox"/>	سایر موارد	برای مثال غیرفعال کردن حساب کاربری در تمامی کاربردها مفید نیست.	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	محصول باید برای هر کاربر، ویژگی‌های امنیتی را که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت می‌باشند، نگهداری نماید.		
		<input checked="" type="checkbox"/>	ویژگی‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند.	
		<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، مسدود شده و غیره)
		<input type="checkbox"/>		نقش کاربر سایر موارد
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	محصول باید قابلیت مدیریت گذرواژه را فراهم آورد.		
		<input checked="" type="checkbox"/>	موارد نیاز که باید در تعریف گذرواژه استفاده شوند.	
		<input checked="" type="checkbox"/>		استفاده از حروف کوچک
		<input checked="" type="checkbox"/>		استفاده از حروف بزرگ
		<input checked="" type="checkbox"/>		استفاده از اعداد
		<input checked="" type="checkbox"/>		استفاده از کاراکترهای خاص («@»، «#»، «\$»، «%»، «^»، «&»، «*»، «.»، «>» و «<»)
		<input checked="" type="checkbox"/>		حداقل طول ۸ یا بیشتر (قابل تنظیم)
<input type="checkbox"/>	سایر موارد			
<input checked="" type="checkbox"/>	<input type="checkbox"/>	محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید.		
		<input type="checkbox"/>	اقدامات عمومی که	
		<input type="checkbox"/>	کاربر می‌تواند قبل از بازیابی گذرواژه	

	<input checked="" type="checkbox"/>	هیچ اقدامی	احراز هویت انجام دهد،
	<input type="checkbox"/>	سایر موارد	انتخاب شود.
۶	<input checked="" type="checkbox"/>	محصول باید از سازوکار احراز هویت پشتیبانی نماید (برای احراز هویت کاربران راه‌دور، باید بیش از یک سازوکار احراز هویت در محصول به کار رفته باشد).	
	<input checked="" type="checkbox"/>	نام کاربری و گذرواژه	سازوکارهای احراز هویت موجود در محصول مشخص شوند.
	<input type="checkbox"/>	امضای دیجیتال	
	<input type="checkbox"/>	سامانه‌های احراز هویت مرکزی (مانند Active Directory و ...)	
	<input type="checkbox"/>	OTP یا توکن	
	<input checked="" type="checkbox"/>	احراز هویت دو فاکتوری	
	<input type="checkbox"/>	سایر موارد	
۷	<input checked="" type="checkbox"/>	محصول باید برای هر کاربر فعال، ویژگی‌های امنیتی را نگهداری نماید.	
	<input checked="" type="checkbox"/>	شناسه کاربر	ویژگی‌هایی 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).
	<input checked="" type="checkbox"/>	نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمت‌های مختلف برنامه	
	<input 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	
۸	<input checked="" type="checkbox"/>	محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.	

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

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 رده، توانایی محصول در حفاظت از این داده‌ها مورد بررسی قرار می‌گیرد.

توضیحات	رده حفاظت از داده‌ی کاربری		شماره الزام
	<input checked="" type="checkbox"/>	محصول باید برای موجودیت‌ها و عملیات، خطمشی‌های کنترل دسترسی اعمال نماید.	۱
	<input checked="" type="checkbox"/>	مدیر سیستم	موجودیت‌های فعالی که خطمشی‌های
	<input checked="" type="checkbox"/>	کاربر عادی	کنترل دسترسی در مورد آنها اعمال
	<input type="checkbox"/>	سایر موارد	می‌شوند، مشخص گردد.
	<input checked="" type="checkbox"/>	سوابق، مستندات و فراداده	موجودیت‌های غیرفعال که خطمشی‌های
	<input checked="" type="checkbox"/>	داده متعلق به کاربران	کنترل دسترسی در مورد آنها اعمال
	<input checked="" type="checkbox"/>	داده احراز هویت	می‌شوند، مشخص
	<input type="checkbox"/>	سایر موارد	گردد.
	<input checked="" type="checkbox"/>	ایجاد موجودیت غیرفعال جدید	عملیاتی که خطمشی‌های کنترل دسترسی در رابطه با
	<input checked="" type="checkbox"/>	حذف موجودیت غیرفعال	
	<input checked="" type="checkbox"/>	تغییر دسترسی‌ها به موجودیت غیرفعال	
	<input checked="" type="checkbox"/>	عملیات بر روی فراداده وابسته به موجودیت غیرفعال	

	<input type="checkbox"/>	سایر موارد	آنها اعمال می‌شوند، مشخص گردد.
	<input checked="" type="checkbox"/>	محصول باید بر اساس ویژگی‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.	
	<input checked="" type="checkbox"/>	نقش‌ها و مجوزهای کاربر مجاز	و ویژگی‌هایی که بر اساس آن خط‌مشی‌ها تعریف می‌شوند،
	<input checked="" type="checkbox"/>	اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند.	انتخاب گردد.
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	محصول باید بر اساس قاعده‌ای عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل شده را مجاز نماید (این قاعده می‌تواند بدین شکل باشد که در فهرست کنترل دسترسی، سابقه (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 checked="" type="checkbox"/>	محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.	
هر کاربر فقط مجاز به برقراری یک نشست است و در صورت ورود به سیستم نشست های دیگر خاتمه می‌یابد.	<input checked="" type="checkbox"/>	عبور تعداد نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف شده	قوانین ممانعت از دسترسی مشخص شوند (در صورت اعمال قوانین بیشتر توسط محصول، در «سایر موارد» بیان شود).
	<input type="checkbox"/>	سایر موارد	
داده های کاربر در صورت آزادسازی در دیتابیس delete می شود همچنین فایل‌های آپلود شده کاربران در دیتابیس نگهداری می شود (نه در سیستم فایل) بنابراین هنگام حذف ، رکورد مربوطه حذف می شود.	<input checked="" type="checkbox"/>	محصول باید تضمین نماید تمام اطلاعات قبلی منابع یا در هنگام تخصیص و یا در هنگام آزادسازی آنها، غیرقابل دسترس می‌گردد و یا سازوکاری امن برای دسترسی به منابع قبلی وجود دارد.	
	<input checked="" type="checkbox"/>	محصول باید هنگام دریافت داده کاربری خط‌مشی کنترل دسترسی را اعمال و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.	

<p>داده های کاربر از نظر نوع عددی و متنی کنترل می شود</p>	<input checked="" type="checkbox"/>	<p>نوع داده</p>	<p>ویژگی های امنیتی مرتبط با داده کاربری</p>
<p>در مورد فایلها ، امکان تنظیم حداکثر حجم در Web.config وجود دارد در حال حاضر ۲ مگابایت است</p>	<input checked="" type="checkbox"/>	<p>حجم و اندازه</p>	<p>که در هنگام ورود آن به محصول استفاده می شوند، مشخص شود</p>
<p>کاربر در زمان آپلود ، فایل های با پسوند مجاز زیر قابلیت آپلود دارند. فایل انتخابی فقط باید از نوع .pdf, .jpg, .png, .docx, .xlsx, .zip, .rar باشد</p>	<input checked="" type="checkbox"/>	<p>فرمت</p>	<p>(در صورتی که کنترل دسترسی برای موارد دیگری نیز صورت می گیرد، در قسمت</p>
	<input type="checkbox"/>	<p>تعداد دفعات Import</p>	<p>«سایر موارد» بیان گردد).</p>
	<input type="checkbox"/>	<p>سایر موارد</p>	
<p>از آنجا که پروتکل ارتباطی بین کاربر و سرور از طریق مرورگر استاندارد و از طریق TLS انجام می شود. تمام Form Data ها در بستر امن انتقال داده می شوند. و امکان شنود و گم شدن آنها وجود ندارد.</p>	<input checked="" type="checkbox"/>	<p>محصل باید از یک پروتکل امن برای انتقال داده استفاده نماید. این پروتکل ارتباط و همبستگی شفاف را بین داده کاربری دریافت شده و ویژگی های امنیتی آن فراهم و همچنین از شنود و گم شدن داده حین انتقال جلوگیری می کند.</p>	
	<input checked="" type="checkbox"/>	<p>محصل باید هنگام انتقال داده به بیرون از محصول، خط مشی کنترل دسترسی اعمال نماید و برای این کار از ویژگی های امنیتی مرتبط با داده کاربری استفاده کند.</p>	
	<input checked="" type="checkbox"/>	<p>نوع داده</p>	
	<input type="checkbox"/>	<p>حجم و اندازه</p>	<p>ویژگی های امنیتی مرتبط با داده کاربری</p>
<p>۱- دانلود فایل های خروجی با استفاده از دکمه های "خروج به اکسل" پسوند .xlsx می باشد</p>	<input checked="" type="checkbox"/>	<p>فرمت</p>	<p>که در هنگام خروج آن از محصول استفاده می شوند، مشخص شوند</p>
<p>۲- دانلود فایل های ضمیمه همان فایل های قبلی آپلود شده برای ضمیمه اطلاعات است که توسط خود کاربر آپلود شده و در زمان آپلود فرمت های مجاز برابر با د از نوع .pdf, .jpg, .png, .docx, .xlsx, .zip, .rar بوده است</p>	<input checked="" type="checkbox"/>		
	<input type="checkbox"/>	<p>سایر موارد</p>	

	<input checked="" type="checkbox"/>	محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.		۹
	<input checked="" type="checkbox"/>	مدیر سیستم باید خروج داده‌ها را محدود نماید، به طوریکه کاربران محصول، قادر به خروج بدون هدف داده به خارج از محصول نباشند.	قوانینی که در هنگام خروج داده از محصول اعمال می‌شوند،	
	<input type="checkbox"/>	سایر موارد	مشخص شوند	
	<input checked="" type="checkbox"/>	محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره‌شده در محصول تشخیص دهد.		۱۰
در داده‌های ثبت‌نشده همه جداول حاوی ثبت‌نشده دارای فیلد checksum هستند و صحت آنها با checksum کنترل می‌شود.	<input type="checkbox"/>	مقدار درهم‌سازی شده داده‌های کاربری ذخیره‌شده، نگهداری می‌شود.	چگونگی تشخیص تغییر در داده‌های کاربری حساس،	
	<input type="checkbox"/>	سایر موارد	مشخص شود.	
	<input checked="" type="checkbox"/>	محصول باید در صورت تشخیص خطای صحت در داده‌ها، اقدامات مقابله‌ای زیر را انجام دهد.		۱۱
مدیر سیستم هنگام مشاهده داده‌های حساس ثبت‌نشده رکوردهای خطای صحت را مشاهده می‌کند	<input checked="" type="checkbox"/>	ایجاد هشدار/اخطار برای نقش‌های مجاز	اقدام مقابله‌ای در صورت تشخیص خطا،	
	<input type="checkbox"/>	تصحیح داده بر اساس مقادیر قبل	مشخص شود (وجود یک مورد لازم و کافی	
	<input type="checkbox"/>	سایر موارد	است)	

۲-۵- مدیریت امنیت

در این رده 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	رده مدیریت امنیت	شماره الزام												
	<table border="1"> <tr> <td data-bbox="875 537 961 649"><input checked="" type="checkbox"/></td> <td data-bbox="961 537 1948 649">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> </tr> <tr> <td data-bbox="875 649 961 706"><input checked="" type="checkbox"/></td> <td data-bbox="961 649 1948 706">تعیین و تغییر رفتار</td> </tr> <tr> <td data-bbox="875 706 961 755"><input checked="" type="checkbox"/></td> <td data-bbox="961 706 1948 755">غیرفعال نمودن</td> </tr> <tr> <td data-bbox="875 755 961 803"><input checked="" type="checkbox"/></td> <td data-bbox="961 755 1948 803">فعال نمودن</td> </tr> <tr> <td data-bbox="875 803 961 852"><input type="checkbox"/></td> <td data-bbox="961 803 1948 852">سایر موارد</td> </tr> </table>	<input checked="" 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.	<input checked="" type="checkbox"/>	تعیین و تغییر رفتار	<input checked="" type="checkbox"/>	غیرفعال نمودن	<input checked="" type="checkbox"/>	فعال نمودن	<input type="checkbox"/>	سایر موارد	۱		
<input checked="" 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.													
<input checked="" type="checkbox"/>	تعیین و تغییر رفتار													
<input checked="" type="checkbox"/>	غیرفعال نمودن													
<input checked="" type="checkbox"/>	فعال نمودن													
<input type="checkbox"/>	سایر موارد													
	<table border="1"> <tr> <td data-bbox="875 852 961 1015"><input checked="" type="checkbox"/></td> <td data-bbox="961 852 1948 1015">محصول باید با اعمال خط‌مشی کنترل دسترسی، امکان تغییر پیش‌فرض و عملیات زیر را بر روی ویژگی‌های امنیتی الزام ۷ از رده (Class) شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.</td> </tr> <tr> <td data-bbox="875 1015 961 1063"><input checked="" type="checkbox"/></td> <td data-bbox="961 1015 1948 1063">پرس‌وجو</td> </tr> <tr> <td data-bbox="875 1063 961 1112"><input checked="" type="checkbox"/></td> <td data-bbox="961 1063 1948 1112">تغییر</td> </tr> <tr> <td data-bbox="875 1112 961 1161"><input type="checkbox"/></td> <td data-bbox="961 1112 1948 1161">حذف</td> </tr> <tr> <td data-bbox="875 1161 961 1209"><input type="checkbox"/></td> <td data-bbox="961 1161 1948 1209">تغییر پیش‌فرض</td> </tr> <tr> <td data-bbox="875 1209 961 1263"><input type="checkbox"/></td> <td data-bbox="961 1209 1948 1263">سایر موارد</td> </tr> </table>	<input checked="" type="checkbox"/>	محصول باید با اعمال خط‌مشی کنترل دسترسی، امکان تغییر پیش‌فرض و عملیات زیر را بر روی ویژگی‌های امنیتی الزام ۷ از رده (Class) شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.	<input checked="" type="checkbox"/>	پرس‌وجو	<input checked="" type="checkbox"/>	تغییر	<input type="checkbox"/>	حذف	<input type="checkbox"/>	تغییر پیش‌فرض	<input type="checkbox"/>	سایر موارد	۲
<input checked="" type="checkbox"/>	محصول باید با اعمال خط‌مشی کنترل دسترسی، امکان تغییر پیش‌فرض و عملیات زیر را بر روی ویژگی‌های امنیتی الزام ۷ از رده (Class) شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.													
<input checked="" type="checkbox"/>	پرس‌وجو													
<input checked="" type="checkbox"/>	تغییر													
<input type="checkbox"/>	حذف													
<input type="checkbox"/>	تغییر پیش‌فرض													
<input type="checkbox"/>	سایر موارد													
	<table border="1"> <tr> <td data-bbox="875 1263 961 1380"><input checked="" type="checkbox"/></td> <td data-bbox="961 1263 1948 1380">محصول باید برای داده‌های محصول، امکان کارکردهای زیر را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.</td> </tr> <tr> <td data-bbox="875 1380 961 1424"><input checked="" type="checkbox"/></td> <td data-bbox="961 1380 1948 1424">تغییر پیش‌فرض</td> </tr> </table>	<input checked="" 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 پیش‌فرض	۳								
<input checked="" 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 پیش‌فرض													

	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	حذف نمودن پرس‌وجو مقاردهی ایجاد مشاهده سایر موارد	عملیات بر روی داده‌های محصول که در محصول پشتیبانی می‌شوند، مشخص شود.
هیچ کاربری حتی admin اجازه ویرایش ندارد	<input checked="" type="checkbox"/>	محصول باید توانایی انجام کارکردهای زیر را داشته باشد. پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات ثبت‌نشده پشتیبانی از مجوزهای مشاهده/ویرایش ثبت‌نشده پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ثبت‌نشده مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول انتخاب زمان اجرای حفاظت از اطلاعات باقیمانده که می‌تواند در محصول قابل پیکربندی باشد. (برای مثال، زمان تخصیص و یا زمان آزادسازی منابع) ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول در نظر گرفتن یک عملیات از پیش تعیین شده پس از تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی نیز باشد. ۱. مدیریت حد آستانه برای تلاش‌های ناموفق ۲. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد. مدیریت معیارها برای تنظیم گذرواژه‌ها ۱. مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مربوطه ۲. مدیریت یک‌سری عملیاتی که قبل از احراز شدن هویت کاربر انجام می‌شوند.	۴ 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"/>	<p>۱. مدیریت سازوکارهای احراز هویت</p> <p>۲. مدیریت قوانین مرتبط با احراز هویت</p>													
	<input checked="" type="checkbox"/>	<p>مدیریت تغییرات و فرآیندهایی مانند (اختصاص آدرس IP برای عملیات شناسایی کاربر خاص و از این قبیل موارد) که مدیر مجاز می‌تواند قبل از شناسایی کاربر انجام دهد.</p>													
	<input checked="" type="checkbox"/>	<p>مدیر مجاز می‌تواند ویژگی‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد.</p>													
	<input checked="" type="checkbox"/>	<p>مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول</p>													
	<input checked="" type="checkbox"/>	<p>مدیریت نقش‌ها در محصول</p>													
	<input checked="" type="checkbox"/>	<p>مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر</p>													
	<input checked="" type="checkbox"/>	<p>مدیریت شرایط آغاز نشست توسط مدیر مجاز</p>													
	<input checked="" type="checkbox"/>	<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 checked="" type="checkbox"/>	<p>محصول باید توانایی تعریف نقش‌های مختلف را داشته باشد.</p> <table border="1" data-bbox="961 1015 2016 1214"> <tr> <td data-bbox="961 1015 1711 1068"><input checked="" type="checkbox"/></td> <td data-bbox="1711 1015 2016 1068">مدیر سیستم</td> <td data-bbox="961 1015 1711 1068">نقش‌هایی که در</td> </tr> <tr> <td data-bbox="961 1068 1711 1122"><input type="checkbox"/></td> <td data-bbox="1711 1068 2016 1122">کاربر پیشرفته</td> <td data-bbox="961 1068 1711 1122">محصول پشتیبانی</td> </tr> <tr> <td data-bbox="961 1122 1711 1175"><input checked="" type="checkbox"/></td> <td data-bbox="1711 1122 2016 1175">کاربر عادی</td> <td data-bbox="961 1122 1711 1175">می‌شوند، مشخص</td> </tr> <tr> <td data-bbox="961 1175 1711 1214"><input type="checkbox"/></td> <td data-bbox="1711 1175 2016 1214">سایر موارد</td> <td data-bbox="961 1175 1711 1214">گردد.</td> </tr> </table>	<input checked="" type="checkbox"/>	مدیر سیستم	نقش‌هایی که در	<input type="checkbox"/>	کاربر پیشرفته	محصول پشتیبانی	<input checked="" type="checkbox"/>	کاربر عادی	می‌شوند، مشخص	<input type="checkbox"/>	سایر موارد	گردد.	۵
<input checked="" type="checkbox"/>	مدیر سیستم	نقش‌هایی که در													
<input type="checkbox"/>	کاربر پیشرفته	محصول پشتیبانی													
<input checked="" type="checkbox"/>	کاربر عادی	می‌شوند، مشخص													
<input type="checkbox"/>	سایر موارد	گردد.													
	<input checked="" type="checkbox"/>	<p>محصول باید قادر باشد کاربران را به نقش‌های تعریف‌شده یا قابل تعریف مرتبط نماید، همچنین لازم است هر حساب کاربری تنها به یک نقش مرتبط شده باشد، اما ممکن است نقش‌ها تنها به یک کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند.</p>	۶												

۲-۶- حفاظت از توابع امنیتی محصول

در این رده، 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	رده حفاظت از توابع امنیتی محصول		شماره الزام
	<input checked="" type="checkbox"/>	محصول باید هنگام رخ دادن هرگونه خرابی، اشکال یا شکست مانند از کار افتادن محصول، قطع شدن ارتباط محصول با پایگاه داده و یا اختلال در کارکردهای محصول، در وضعیت امنی قرار گرفته، صحت داده‌ها و خط‌مشی کنترل دسترسی را حفظ نماید.	۱
	<input checked="" type="checkbox"/>	خرابی‌های نرم‌افزاری	هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول
	<input checked="" type="checkbox"/>	خرابی‌های سخت‌افزاری	حفظ می‌شود، مشخص گردد.
	<input checked="" type="checkbox"/>	محصول باید از طریق فراهم نمودن بستر و زیرساخت امن، توانایی جلوگیری از افشاء یا تغییر داده، هنگام انتقال بین بخش‌های مجزای خود را داشته باشد.	
	<input checked="" type="checkbox"/>	در صورتی که محصول از محصولات امن IT استفاده می‌کند، باید تفسیر سازگار و یکسانی را از داده امنیتی در زمان اشتراک‌گذاری آن بین خود و دیگر محصولات امن IT، فراهم آورد.	
	<input checked="" type="checkbox"/>	داده‌های احراز هویت	داده امنیتی قابل
	<input type="checkbox"/>	کلید	اشتراک‌گذاری که در
	<input type="checkbox"/>	امضای دیجیتال	محصول پشتیبانی
	<input checked="" type="checkbox"/>	ثبت‌نشان‌ها (داده‌های ممیزی)	می‌شوند، مشخص
	<input type="checkbox"/>	سایر موارد	گردد.

<p>از طریق مهر زمانی سرور Database که توسط هیچ کس قابل تغییر نیست.</p>	<input checked="" type="checkbox"/>	<p>محصل باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهرهای زمانی^۴ معتبر را تولید یا از آن‌ها استفاده نماید.</p>	<p>۴</p>
	<input type="checkbox"/>	گرفتن مهرهای زمانی از سرور NTP	روش‌های ایجاد مهرهای زمانی معتبر انتخاب شود. (دیگر
	<input type="checkbox"/>	تنظیم مهرهای زمانی از طریق اینترنت	رو شهای موجود در محصول، در قسمت «سایر موارد» بیان شود).
	<input checked="" type="checkbox"/>	تنظیم مهرهای زمانی به صورت پیش فرض (معتبر و عدم امکان دستکاری غیرمجاز)	
	<input type="checkbox"/>	سایر موارد	
<p>بروز رسانی نرم افزار فقط توسط کاربر فنی پشتیبانی شرکت به صورت دستی انجام می شود</p>	<input checked="" type="checkbox"/>	<p>محصل باید امکان بروزرسانی نرم افزار و میان افزار محصول را برای مدیر سیستم فراهم نماید.</p>	<p>۵</p>
	<input checked="" type="checkbox"/>	بروزرسانی دستی	روش بروزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).
	<input type="checkbox"/>	جستجوی خودکار بروزرسانی‌ها	
	<input type="checkbox"/>	بروزرسانی‌های خودکار	
	<input type="checkbox"/>	بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی	
	<input type="checkbox"/>	<p>در صورت استفاده از بروزرسانی به روش خودکار، محصول باید پیش از نصب بروزرسانی‌های نرم افزاری و میان‌افزاری، امکان احراز اصالت میان‌افزار یا نرم‌افزار را فراهم نماید.</p>	<p>۶</p>
	<input type="checkbox"/>	امضای دیجیتال	سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی) به‌روزرسانی‌ها انتخاب گردد.
	<input type="checkbox"/>	درهم‌ساز منتشرشده	

^۴ Time stamp

۲-۷- تخصیص منابع

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

توضیحات	رده تخصیص منابع	شماره الزام
	<input checked="" type="checkbox"/> محصول باید در زمان رخداد هرگونه اشکال و خرابی (شکست) نرم‌افزاری، از عملکرد کارکردهای اصلی محصول اطمینان حاصل نماید.	۱

۲-۸- دسترسی به محصول

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

شماره الزام	رده دسترسی به محصول	توضیحات
۱	محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.	<input checked="" type="checkbox"/> هر کاربر حتی admin فقط یک نشست فعال می‌تواند داشته باشد
۲	محصول باید کلیه نشست‌های تعاملی راه‌دور 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 checked="" type="checkbox"/>
		<input checked="" type="checkbox"/> روز
		<input checked="" type="checkbox"/> زمان
		<input type="checkbox"/> سایر موارد
۵	در صورت برقراری نشست به طور موفقیت‌آمیز، 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.	<input checked="" type="checkbox"/>
		<input checked="" type="checkbox"/> روز
		<input checked="" type="checkbox"/> زمان
		<input type="checkbox"/> سایر موارد

	<input checked="" type="checkbox"/>	محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.		۶
	<input checked="" type="checkbox"/>	محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.		۷
منظور IP کاربر است	<input checked="" type="checkbox"/>	مکان	پارامترهای موجود برای	
	<input type="checkbox"/>	شماره پورت	جلوگیری از نشست،	
روز هفته مثلا از یکشنبه تا سه شنبه	<input checked="" type="checkbox"/>	روز	مشخص شوند (وجود)	
	<input checked="" type="checkbox"/>	زمان	یک مورد لازم و کافی	
	<input type="checkbox"/>	سایر موارد	است).	

۲-۹- کانال‌ها/مسیرهای مورد اعتماد

در این رده 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	رده کانال‌ها/مسیرهای مورد اعتماد		شماره الزام
	<input checked="" type="checkbox"/>	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 دهد و از تغییر و افشای داده تبادلی حفاظت نماید و تغییرات را تشخیص دهد. در صورت انتخاب مورد HTTPS، رعایت الزام ۱-۳- و ۳-۳- و در صورت انتخاب TLS، رعایت الزامات ۳-۲- تا ۳-۴- که در بخش ۳- بیان گردیده است، الزامی است.	۱
	<input checked="" type="checkbox"/>	HTTPS	پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد.
	<input checked="" type="checkbox"/>	TLS	
	<input type="checkbox"/>	SSH	
	<input checked="" type="checkbox"/>	محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه دور را از طریق کانال امن آغاز کنند.	
	<input checked="" type="checkbox"/>	محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.	

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 رده کانال امن، پروتکل HTTPS انتخاب شود، آنگاه رعایت الزامات HTTPS که در این بخش بیان شده است، اجباری می‌گردد.

۳-۱- پروتکل HTTPS

توضیحات	پروتکل HTTPS	شماره الزام
	<input checked="" type="checkbox"/> محصول باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کند.	۱
	<input checked="" type="checkbox"/> محصول باید پروتکل HTTPS را با استفاده از TLS اجرا کند.	۲
	<input checked="" 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.	۳
	<input checked="" type="checkbox"/> اتصال را برقرار نکند.	محصول تنها از موارد بیان شده می‌تواند استفاده نماید.
	<input type="checkbox"/> برای برقراری اتصال درخواست مجوز کند.	

۲-۲- پروتکل TLS Client

توضیحات	پروتکل TLS Client		شماره الزام														
	<input checked="" type="checkbox"/>	<p>محصول باید (TLS 1.2 (RFC 5246 را پیاده‌سازی و دیگر نسخه‌های TLS و SSL را رد کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.</p> <table border="1" data-bbox="961 553 1728 1437"> <tr> <td data-bbox="961 553 1024 678"> <input type="checkbox"/> </td> <td data-bbox="1024 553 1728 678"> TLS_AES_256_GCM_SHA384 0x1302 مطابق با RFC 8446 </td> </tr> <tr> <td data-bbox="961 678 1024 803"> <input type="checkbox"/> </td> <td data-bbox="1024 678 1728 803"> TLS_AES_128_GCM_SHA256 0x1301 مطابق با RFC 8446 </td> </tr> <tr> <td data-bbox="961 803 1024 928"> <input type="checkbox"/> </td> <td data-bbox="1024 803 1728 928"> TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 0x009F مطابق با RFC 5288 </td> </tr> <tr> <td data-bbox="961 928 1024 1053"> <input type="checkbox"/> </td> <td data-bbox="1024 928 1728 1053"> TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 0x009E مطابق با RFC 5288 </td> </tr> <tr> <td data-bbox="961 1053 1024 1179"> <input checked="" type="checkbox"/> </td> <td data-bbox="1024 1053 1728 1179"> TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 0xC02F مطابق با RFC 5289 </td> </tr> <tr> <td data-bbox="961 1179 1024 1304"> <input checked="" type="checkbox"/> </td> <td data-bbox="1024 1179 1728 1304"> TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 0xC030 مطابق با RFC 5289 </td> </tr> <tr> <td data-bbox="961 1304 1024 1437"> <input checked="" type="checkbox"/> </td> <td data-bbox="1024 1304 1728 1437"> TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 0xC02C مطابق با RFC 5289 </td> </tr> </table> <p>مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.</p>	<input type="checkbox"/>	TLS_AES_256_GCM_SHA384 0x1302 مطابق با RFC 8446	<input type="checkbox"/>	TLS_AES_128_GCM_SHA256 0x1301 مطابق با RFC 8446	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 0x009F مطابق با RFC 5288	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 0x009E مطابق با RFC 5288	<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 0xC02F مطابق با RFC 5289	<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 0xC030 مطابق با RFC 5289	<input checked="" type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 0xC02C مطابق با RFC 5289	۱
<input type="checkbox"/>	TLS_AES_256_GCM_SHA384 0x1302 مطابق با RFC 8446																
<input type="checkbox"/>	TLS_AES_128_GCM_SHA256 0x1301 مطابق با RFC 8446																
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 0x009F مطابق با RFC 5288																
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 0x009E مطابق با RFC 5288																
<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 0xC02F مطابق با RFC 5289																
<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 0xC030 مطابق با RFC 5289																
<input checked="" type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 0xC02C مطابق با RFC 5289																

	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 0xC02B مطابق با RFC 5289		
	<input checked="" type="checkbox"/>	TLS_RSA_WITH_AES_256_GCM_SHA384 0x009D مطابق با RFC 5288		
	<input type="checkbox"/>	TLS_RSA_WITH_AES_128_GCM_SHA256 0x009C مطابق با RFC 5288		
	<input type="checkbox"/>	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 0xC02E مطابق با RFC 5288		
	<input type="checkbox"/>	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 0xC02D مطابق با RFC 5289		
	<input type="checkbox"/>	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 0xC032 مطابق با RFC 5289		
	<input type="checkbox"/>	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 0xC031 مطابق با RFC 5289		
	<input type="checkbox"/>	TLS_DH_RSA_WITH_AES_256_GCM_SHA384 0x00A1 مطابق با RFC 5288		
	<input type="checkbox"/>	TLS_DH_RSA_WITH_AES_128_GCM_SHA256 0x00A0 مطابق با RFC 5288		
	<input checked="" type="checkbox"/>	محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ۶ از RFC 6125، تأیید نماید.		۲

	<input checked="" type="checkbox"/>	<p>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.</p>	۳
	<input checked="" type="checkbox"/>	ارتباط را برقرار نکند	در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.
	<input type="checkbox"/>	برای برقراری ارتباط درخواست مجوز کند	
	<input type="checkbox"/>	سایر موارد	
	<input checked="" type="checkbox"/>	محصول باید در پیام ClientHello برای استفاده از خم‌های بیضوی، بر اساس موارد زیر عمل نماید.	۴
	<input type="checkbox"/>	Supported Elliptic Curves Extension را ارائه نکند.	در صورتی که محصول از خم‌های بیضوی استفاده می‌نماید، نوع خم باید مشخص گردد.
Curve های secp256r1 یا secp384r1 ارائه می‌شوند	<input checked="" type="checkbox"/>	Supported Elliptic Curves Extension را به همراه NIST Curve های secp256r1 یا secp384r1 یا secp521r1 ارائه نماید.	

۳-۳- پروتکل TLS Server

توضیحات	پروتکل TLS Server		شماره الزام															
	<input checked="" type="checkbox"/>	<p>محصول باید TLS 1.2 (RFC 5246) را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.</p> <table border="1" data-bbox="961 553 1728 1437"> <tr> <td data-bbox="961 553 1024 678" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1024 553 1728 678"> TLS_AES_256_GCM_SHA384 0x1302 مطابق با RFC 8446 </td> <td data-bbox="1728 553 1948 1437" rowspan="8" style="vertical-align: middle;">مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.</td> </tr> <tr> <td data-bbox="961 678 1024 803" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1024 678 1728 803"> TLS_AES_128_GCM_SHA256 0x1301 مطابق با RFC 8446 </td> </tr> <tr> <td data-bbox="961 803 1024 928" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1024 803 1728 928"> TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 0x009F مطابق با RFC 5288 </td> </tr> <tr> <td data-bbox="961 928 1024 1053" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1024 928 1728 1053"> TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 0x009E مطابق با RFC 5288 </td> </tr> <tr> <td data-bbox="961 1053 1024 1179" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1024 1053 1728 1179"> TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 0xC02F مطابق با RFC 5289 </td> </tr> <tr> <td data-bbox="961 1179 1024 1304" style="text-align: center;"><input checked="" type="checkbox"/></td> <td data-bbox="1024 1179 1728 1304"> TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 0xC030 مطابق با RFC 5289 </td> </tr> <tr> <td data-bbox="961 1304 1024 1429" style="text-align: center;"><input type="checkbox"/></td> <td data-bbox="1024 1304 1728 1429"> TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 0xC02C مطابق با RFC 5289 </td> </tr> </table>	<input type="checkbox"/>	TLS_AES_256_GCM_SHA384 0x1302 مطابق با RFC 8446	مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.	<input type="checkbox"/>	TLS_AES_128_GCM_SHA256 0x1301 مطابق با RFC 8446	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 0x009F مطابق با RFC 5288	<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 0x009E مطابق با RFC 5288	<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 0xC02F مطابق با RFC 5289	<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 0xC030 مطابق با RFC 5289	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 0xC02C مطابق با RFC 5289	۱
<input type="checkbox"/>	TLS_AES_256_GCM_SHA384 0x1302 مطابق با RFC 8446	مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.																
<input type="checkbox"/>	TLS_AES_128_GCM_SHA256 0x1301 مطابق با RFC 8446																	
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 0x009F مطابق با RFC 5288																	
<input type="checkbox"/>	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 0x009E مطابق با RFC 5288																	
<input type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 0xC02F مطابق با RFC 5289																	
<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 0xC030 مطابق با RFC 5289																	
<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 0xC02C مطابق با RFC 5289																	

	<input type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 0xC02B مطابق با RFC 5289		
	<input checked="" type="checkbox"/>	TLS_RSA_WITH_AES_256_GCM_SHA384 0x009D مطابق با RFC 5288		
	<input type="checkbox"/>	TLS_RSA_WITH_AES_128_GCM_SHA256 0x009C مطابق با RFC 5288		
	<input type="checkbox"/>	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 0xC02E مطابق با RFC 5288		
	<input type="checkbox"/>	TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 0xC02D مطابق با RFC 5289		
	<input type="checkbox"/>	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 0xC032 مطابق با RFC 5289		
	<input checked="" type="checkbox"/>	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 0xC031 مطابق با RFC 5289		
	<input type="checkbox"/>	TLS_DH_RSA_WITH_AES_256_GCM_SHA384 0x00A1 مطابق با RFC 5288		
	<input type="checkbox"/>	TLS_DH_RSA_WITH_AES_128_GCM_SHA256 0x00A0 مطابق با RFC 5288		
	<input checked="" type="checkbox"/>	TLS1.1 و TLS1.0, SSL3.0, SSL2.0, SSL1.0 که درخواست کاربرانی که در صورت اتصال باید اتصال‌های کاربرانی که درخواست TLS1.1 و TLS1.0, SSL3.0, SSL2.0, SSL1.0 دارند را رد نماید.		۲

	<input checked="" type="checkbox"/>	محصول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید.		۳	
طول بیت ۲۰۴۸	<input checked="" type="checkbox"/>	استفاده از RSA با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ یا ۴۰۹۶ بیت	طول کلید یا نوع خم مورد استفاده باید مشخص گردد.		
خم های secp256r1 یا secp384r1 ارایه می شوند	<input checked="" type="checkbox"/>	پارامترهای ECDH(E) با استفاده از NIST Curve های secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگر			
	<input type="checkbox"/>	پارامترهای دیفی-هلمن با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ بیت			

۳-۴- 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 checked="" type="checkbox"/>	محصول باید احراز هویت دوطرفه کلاینت‌ها/سرورهای TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید.	۱
	<input checked="" type="checkbox"/>	در صورت مطابقت نداشتن نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه از شناساننده کلاینت مورد انتظار بوده است، محصول نباید کانال امن را برقرار سازد.	۲

۳-۵- اعتبارسنجی گواهی نامه

توضیحات	اعتبارسنجی گواهی نامه	شماره الزام
	<input checked="" type="checkbox"/> محصول باید گواهی نامه‌ها را بر اساس قوانین زیر تأیید کند.	۱
	<input checked="" type="checkbox"/> تأیید گواهی نامه RFC 5280 و تأیید مسیر گواهی نامه که از حداقل طول مسیر دو گواهی نامه پشتیبانی می‌کند.	
	<input checked="" type="checkbox"/> مسیر گواهی نامه باید با یک گواهی نامه CA امن پایان یابد.	
	<input checked="" type="checkbox"/> محصول باید برای تأیید مسیر یک گواهی نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی نامه‌های CA به حالت «TRUE» تنظیم شده است.	
	<input type="checkbox"/> پروتکل وضعیت گواهی نامه آنلاین (OCSP) مشخص شده در RFC 696	
	<input type="checkbox"/> لیست فسخ گواهی نامه (CRL) مشخص شده در RFC 5280 بخش ۳، ۶	روش‌های تأیید وضعیت
	<input type="checkbox"/> لیست فسخ گواهی نامه (CRL) مشخص شده در RFC 5759 بخش ۵	فسخ گواهی نامه
	<input checked="" type="checkbox"/> هیچ روش فسخ دیگری	
	<input type="checkbox"/> گواهی نامه‌های مورد استفاده برای تأیید بروزرسانی‌های امن و اعتبارسنجی صحت کدهای اجرایی باید هدف «Code Signing» (id-kp3 با OID) extendedKeyUsage خود داشته باشند.	قوانین تأیید بخش extendedKeyUsage
	<input checked="" type="checkbox"/> گواهی نامه‌های سرور ارائه شده برای TLS باید هدف «Server Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در بخش extendedKeyUsage خود داشته باشند.	

		<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 بخش 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 بخش extendedKeyUsage خود داشته باشند.</p>													
	<input checked="" 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>	۲												
	<input checked="" type="checkbox"/>	<p>محصول باید برای پشتیبانی از احراز هویت برای موارد زیر، از گواهی‌نامه‌های X509v3 تعریف شده در RFC 5280 استفاده کند.</p> <table border="1" data-bbox="961 722 1711 1021"> <tr> <td data-bbox="961 722 1018 771" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="1018 722 1711 771">HTTPS</td> </tr> <tr> <td data-bbox="961 771 1018 820" style="text-align: center;"> <input checked="" type="checkbox"/> </td> <td data-bbox="1018 771 1711 820">TLS</td> </tr> <tr> <td data-bbox="961 820 1018 868" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="1018 820 1711 868">SSH</td> </tr> <tr> <td data-bbox="961 868 1018 917" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="1018 868 1711 917">امضای کد برای بروزرسانی‌های نرم‌افزار سیستم</td> </tr> <tr> <td data-bbox="961 917 1018 966" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="1018 917 1711 966">امضای کد برای تأیید یکپارچگی</td> </tr> <tr> <td data-bbox="961 966 1018 1021" style="text-align: center;"> <input type="checkbox"/> </td> <td data-bbox="1018 966 1711 1021">سایر موارد</td> </tr> </table> <p>در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.</p>	<input checked="" type="checkbox"/>	HTTPS	<input checked="" type="checkbox"/>	TLS	<input type="checkbox"/>	SSH	<input type="checkbox"/>	امضای کد برای بروزرسانی‌های نرم‌افزار سیستم	<input type="checkbox"/>	امضای کد برای تأیید یکپارچگی	<input type="checkbox"/>	سایر موارد	۳
<input checked="" type="checkbox"/>	HTTPS														
<input checked="" type="checkbox"/>	TLS														
<input type="checkbox"/>	SSH														
<input type="checkbox"/>	امضای کد برای بروزرسانی‌های نرم‌افزار سیستم														
<input type="checkbox"/>	امضای کد برای تأیید یکپارچگی														
<input type="checkbox"/>	سایر موارد														

۳-۶- پروتکل SSH

توضیحات	پروتکل SSH		شماره الزام																
	<input type="checkbox"/>	محصول باید پروتکل SSH را مطابق با RFCهای ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۵۶۵۶ و ۶۶۶۸ پیاده‌سازی نماید.	۱																
	<input type="checkbox"/>	<p>محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4252، از روش‌های احراز هویت زیر پشتیبانی نماید.</p> <table border="1" data-bbox="961 667 1713 769"> <tr> <td data-bbox="961 667 1024 716"><input type="checkbox"/></td> <td data-bbox="1024 667 1713 716">احراز هویت مبتنی بر کلید عمومی</td> </tr> <tr> <td data-bbox="961 716 1024 769"><input type="checkbox"/></td> <td data-bbox="1024 716 1713 769">احراز هویت مبتنی بر گذرواژه</td> </tr> </table>	<input type="checkbox"/>	احراز هویت مبتنی بر کلید عمومی	<input type="checkbox"/>	احراز هویت مبتنی بر گذرواژه	۲												
<input type="checkbox"/>	احراز هویت مبتنی بر کلید عمومی																		
<input type="checkbox"/>	احراز هویت مبتنی بر گذرواژه																		
	<input type="checkbox"/>	محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4253، بسته‌های بزرگتر از مقدار مشخصی (در بخش «توضیحات» ذکر شود) را کنار بگذارد.	۳																
	<input type="checkbox"/>	<p>محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های رمزنگاری زیر استفاده نماید.</p> <table border="1" data-bbox="961 997 1713 1364"> <tr> <td data-bbox="961 997 1024 1045"><input type="checkbox"/></td> <td data-bbox="1024 997 1713 1045">AES128-CBC</td> </tr> <tr> <td data-bbox="961 1045 1024 1094"><input type="checkbox"/></td> <td data-bbox="1024 1045 1713 1094">AES192-CBC</td> </tr> <tr> <td data-bbox="961 1094 1024 1143"><input type="checkbox"/></td> <td data-bbox="1024 1094 1713 1143">AES256-CBC</td> </tr> <tr> <td data-bbox="961 1143 1024 1192"><input type="checkbox"/></td> <td data-bbox="1024 1143 1713 1192">AES128-CTR</td> </tr> <tr> <td data-bbox="961 1192 1024 1240"><input type="checkbox"/></td> <td data-bbox="1024 1192 1713 1240">AES192-CTR</td> </tr> <tr> <td data-bbox="961 1240 1024 1289"><input type="checkbox"/></td> <td data-bbox="1024 1240 1713 1289">AES256-CTR</td> </tr> <tr> <td data-bbox="961 1289 1024 1338"><input type="checkbox"/></td> <td data-bbox="1024 1289 1713 1338">AEAD_AES_128_GCM</td> </tr> <tr> <td data-bbox="961 1338 1024 1364"><input type="checkbox"/></td> <td data-bbox="1024 1338 1713 1364">AEAD_AES_256_GCM</td> </tr> </table>	<input type="checkbox"/>	AES128-CBC	<input type="checkbox"/>	AES192-CBC	<input type="checkbox"/>	AES256-CBC	<input type="checkbox"/>	AES128-CTR	<input type="checkbox"/>	AES192-CTR	<input type="checkbox"/>	AES256-CTR	<input type="checkbox"/>	AEAD_AES_128_GCM	<input type="checkbox"/>	AEAD_AES_256_GCM	۴
<input type="checkbox"/>	AES128-CBC																		
<input type="checkbox"/>	AES192-CBC																		
<input type="checkbox"/>	AES256-CBC																		
<input type="checkbox"/>	AES128-CTR																		
<input type="checkbox"/>	AES192-CTR																		
<input type="checkbox"/>	AES256-CTR																		
<input type="checkbox"/>	AEAD_AES_128_GCM																		
<input type="checkbox"/>	AEAD_AES_256_GCM																		

	<p><input type="checkbox"/> محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های کلید عمومی زیر استفاده نماید.</p> <table border="1" data-bbox="919 266 1713 867"> <tr><td><input type="checkbox"/></td><td>ssh-ed25519</td></tr> <tr><td><input type="checkbox"/></td><td>ssh-ed448</td></tr> <tr><td><input type="checkbox"/></td><td>rsa-sha2-512</td></tr> <tr><td><input type="checkbox"/></td><td>rsa-sha2-256</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha2-nistp521</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha2-nistp384</td></tr> <tr><td><input type="checkbox"/></td><td>ecdsa-sha2-nistp256</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-ecdsa-sha2-nistp521</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-ecdsa-sha2-nistp384</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-ecdsa-sha2-nistp256</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-rsa2048-sha256</td></tr> <tr><td><input type="checkbox"/></td><td>ssh-rsa</td></tr> <tr><td><input type="checkbox"/></td><td>x509v3-ssh-rsa</td></tr> </table>	<input type="checkbox"/>	ssh-ed25519	<input type="checkbox"/>	ssh-ed448	<input type="checkbox"/>	rsa-sha2-512	<input type="checkbox"/>	rsa-sha2-256	<input type="checkbox"/>	ecdsa-sha2-nistp521	<input type="checkbox"/>	ecdsa-sha2-nistp384	<input type="checkbox"/>	ecdsa-sha2-nistp256	<input type="checkbox"/>	x509v3-ecdsa-sha2-nistp521	<input type="checkbox"/>	x509v3-ecdsa-sha2-nistp384	<input type="checkbox"/>	x509v3-ecdsa-sha2-nistp256	<input type="checkbox"/>	x509v3-rsa2048-sha256	<input type="checkbox"/>	ssh-rsa	<input type="checkbox"/>	x509v3-ssh-rsa	۵
<input type="checkbox"/>	ssh-ed25519																											
<input type="checkbox"/>	ssh-ed448																											
<input type="checkbox"/>	rsa-sha2-512																											
<input type="checkbox"/>	rsa-sha2-256																											
<input type="checkbox"/>	ecdsa-sha2-nistp521																											
<input type="checkbox"/>	ecdsa-sha2-nistp384																											
<input type="checkbox"/>	ecdsa-sha2-nistp256																											
<input type="checkbox"/>	x509v3-ecdsa-sha2-nistp521																											
<input type="checkbox"/>	x509v3-ecdsa-sha2-nistp384																											
<input type="checkbox"/>	x509v3-ecdsa-sha2-nistp256																											
<input type="checkbox"/>	x509v3-rsa2048-sha256																											
<input type="checkbox"/>	ssh-rsa																											
<input type="checkbox"/>	x509v3-ssh-rsa																											
	<p><input type="checkbox"/> محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های MAC صحت داده‌های زیر استفاده نماید.</p> <table border="1" data-bbox="919 980 1713 1260"> <tr><td><input type="checkbox"/></td><td>AEAD_AES_256_GCM</td></tr> <tr><td><input type="checkbox"/></td><td>AEAD_AES_128_GCM</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha2-512</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha2-256</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha1-96</td></tr> <tr><td><input type="checkbox"/></td><td>hmac-sha1</td></tr> </table>	<input type="checkbox"/>	AEAD_AES_256_GCM	<input type="checkbox"/>	AEAD_AES_128_GCM	<input type="checkbox"/>	hmac-sha2-512	<input type="checkbox"/>	hmac-sha2-256	<input type="checkbox"/>	hmac-sha1-96	<input type="checkbox"/>	hmac-sha1	۶														
<input type="checkbox"/>	AEAD_AES_256_GCM																											
<input type="checkbox"/>	AEAD_AES_128_GCM																											
<input type="checkbox"/>	hmac-sha2-512																											
<input type="checkbox"/>	hmac-sha2-256																											
<input type="checkbox"/>	hmac-sha1-96																											
<input type="checkbox"/>	hmac-sha1																											
	<p><input type="checkbox"/> محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های تبادل کلید زیر استفاده نماید.</p> <table border="1" data-bbox="919 1373 1713 1463"> <tr><td><input type="checkbox"/></td><td>curve25519-sha256</td></tr> <tr><td><input type="checkbox"/></td><td>curve448-sha512</td></tr> </table>	<input type="checkbox"/>	curve25519-sha256	<input type="checkbox"/>	curve448-sha512	۷																						
<input type="checkbox"/>	curve25519-sha256																											
<input type="checkbox"/>	curve448-sha512																											

	<input type="checkbox"/>	diffie-hellman-group-exchange-sha256 diffie-hellman-group18-sha512 diffie-hellman-group17-sha512 diffie-hellman-group16-sha512 diffie-hellman-group15-sha512 ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 rsa2048-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256		
	<input type="checkbox"/>	محصول باید اطمینان پیدا کند که در یک ارتباط SSH، کلیدهای نشست یکسانی برای حد آستانه (طول نشست بیشتر از یک ساعت و حجم داده مبادله شده بیشتر از ۱ گیگابایت نباشد) استفاده گردد. در صورت پر شدن حد آستانه برای هر کدام از موارد ذکر شده، باید تجدید کلید صورت بگیرد.	۸	
	<input type="checkbox"/>	محصول باید اطمینان حاصل نماید که کلاینت SSH، سرور SSH را احراز هویت می‌کند. سرور SSH از یک پایگاه داده محلی که نام هر میزبان را با کلید عمومی متناظر آن (تشریح شده در RFC 4251 بخش ۱.۷) همراه می‌کند، استفاده می‌نماید.	۹	