به نام خدا

سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه

ایده پردازان الکترونیک البرز
دهکده هوشمند(بهروب)
2.5.0

۱۴۰۱ ۰۶
نسخه۲.۵

پیشگفتار

در نظام ارزیابی امنیتی محصولات فتا، یکی از اسناد مورد نیاز برای انجام آزمون امنیتی، سند هدف امنیتی است. بر اساس استاندارد معیار مشترك (CC) سند هدف امنیتی مبتنی بر اسنادی که پروفایل حفاظتی نام دارند، تهیه و تدوین می‌گردد. پروفایل‌های حفاظتی حاوی الزامات امنیتی هستند که در یك 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 یك 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 چابك‌سازی 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 کمك 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

۱ـ معرفی محصول

دهکده هوشمند (بهروب) بخشی از سامانه مدیریت شهری است که بهروب مختص خرید پسماند قابل بازیافت از مبدا(منازل و اصناف) است.

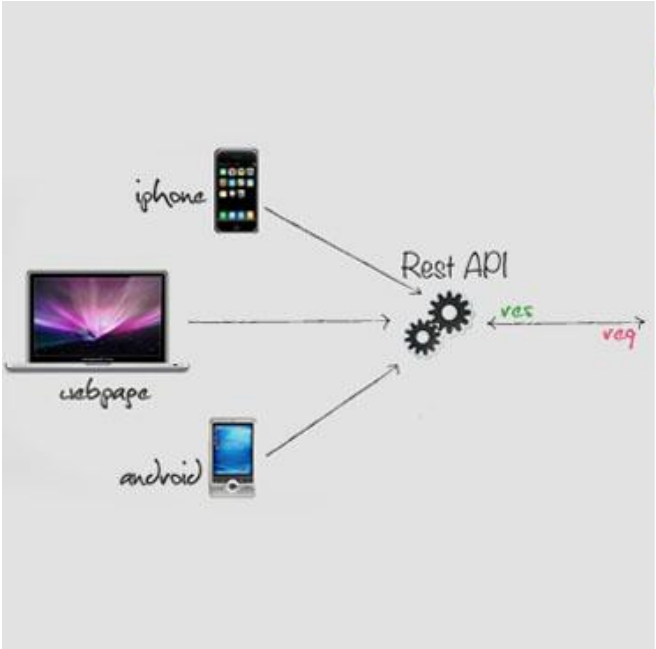
۱ـ۱ـ ویژگی‌های فنی محصول

نسخه‌ی نرم‌افزار/میان‌افزار	۲,۰,۱
مدل و نسخه سیستم‌عامل	لینوکس اوبونتو
مدل و نسخه وب‌سرور	Nginx 1.21.1
مدل و نسخه پایگاه داده	5.7.36 Mysql
زبان برنامه‌نویسی	Php Laravel 5.6

۱ـ۲ـ معماری محصول

<این نمودار چگونگی انجام رویدادها در یک گردش اطلاعات را نشان می دهد. این نمودارنرم‌افزارها، سخت‌افزارها و زیرسیستم‌ها و مؤلفه‌هایی که درگیر این گردش اطلاعات می‌شوند را در قالب ماژولها و مؤلفه‌های اصلی، مؤلفه‌های امنیتی، مؤلفه‌های سمت کلاینت (درصورت وجود)، مؤلفه یکپارچگی با سامانه خارجی (در صورت وجود) و اینکه چه اطلاعاتی جابه‌جا می‌شود؟ چه مؤلفه‌هایی این اطلاعات را دریافت می‌کنند؟ چه فرآیندهای عمومی‌ای رخ می‌دهد؟ و ... را در سسیستم مشخص می‌کند.>

مثالی از نمای کلی معماری یک برنامه کاربردی تحت شبکه {لطفا این متن و تصویر را با معماری محصول خود جایگزین نمایید.}



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 رده در پروفایل حفاظتی مربوطه، یك 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.

شماره الزام	رده ممیزی امنیت (Log)				توضیحات
۱	**محصول باید برای موارد مشخص‌شده که در زیر آمده است، ثبت‌نشان[1] تولید کند (Log ثبت نماید).**			☐	لاگهای کاربری(در منوی اصلی فعالیت کاربران – لاگهای سیستمی Laravel.logs لاگهای پکیج:
	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.	شروع و اتمام توابع	☑		
		تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها	☑		
		خواندن اطلاعات از ثبت‌نشان‌ها	☑		
		تمامی تغییرات در پیکربندی ثبت‌نشان‌ها	☐		لاگها پیکره بندی ندارند.
		عملیات انجام‌شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه	☑		
		عملیات انجام‌شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها	☑		
		تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.	☑		
		تمام کاربردهای سازوکار احراز هویت	☑		
		نتایج نهایی عملیات احراز هویت	☑		
		تلاش موفق و ناموفق هر گذرواژه بررسی‌شده توسط محصول	☑		
		شکست و موفقیت انتساب ویژگی‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال)	☑		لاگهای کاربری
		تمامی تغییرات بر روی مقادیر ویژگی‌های امنیتی	☑		در لاگهای کاربری
		تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یك موجودیت غیرفعال محصول	☑		در لاگهای کاربری

[1] Log

		تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه ویژگی‌های امنیتی)	☑	در لاگهای کاربری
		همه تلاش‌ها برای خارج کردن اطلاعات از محصول	☑	در لاگهای کاربری
		تمامی تغییرات در رفتارهای توابع کارکردی محصول	☑	*در لاگهای کاربری
		استفاده از کارکردهای مدیریتی	☑	*لاگ پکیج
		تغییرات در گروه کاربران	☑	گروه کاربران موجود نیست
		شکست در کارکردهای امنیتی محصول	☑	در لاگهای سیستمی ذخیره می شوند. Laravel.logs
		تمامی قابلیت‌هایی از محصول که به دلیل شکست (خرابی یا مشکل کارکرد)، نمی‌توانند عملیات مورد نظر را انجام دهند.	☑	در لاگهای سیستمی ذخیره می شوند. Laravel.logs
		تلاش موفق یا ناموفق برای برقراری نشست.	☑	در لاگهای سیستمی ذخیره می شوند. Laravel.logs
		ایجاد نشدن نشست به دلیل محدودیت نشست‌های همزمان (حداقل)	☑	محدودیت نشست همزمان نداریم
		خاتمه دادن به یك نشست غیرفعال توسط سازوکار قفل نشست	☑	
		خاتمه به نشست غیرفعال توسط مدیر سیستم	☑	
		سایر موارد	☐	
۲	**محصول باید برای هر ثبت‌نشان تولیدشده، ویژگی‌هایی که در زیر آمده است را ثبت نماید.**		☐	
	ویژگی‌هایی که در ثبت‌نشان‌ها وجود دارد مشخص شود.	تاریخ و زمان رویداد	☑	
		نوع رویداد	☑	
		هویت ایجادکننده رویداد	☑	
		نتیجه رویداد	☑	
		آدرس IP ایجادکننده رویداد	☑	
		سایر موارد	☐	
۳	**محصول باید ثبت‌نشان‌ها را در برابر دسترسی غیرمجاز محافظت نماید.**		☑	
٤	**ثبت‌نشان‌هایی که محصول تولید می‌نماید باید برای کاربر ساده و قابل فهم باشند.**		☑	
	مواردی که در ثبت‌نشان‌ها وجود دارند، مشخص شوند.	نبود داده نامفهوم در رکوردها	☑	
		نبود بخش‌های نامرتبط	☑	
		وجود داده معتبر و مناسب در هر بخش	☑	

٥	**محصول باید امکان انتخاب و مرتب‌سازی برای ثبت‌نشان‌های تولیدشده را بر اساس بخش‌ها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید.**		☑	
	موارد که بر اساس آنها مرتب‌سازی وجود دارد، مشخص شود.	هویت موجودیت فعال	☑	
		نوع حساب کاربری	☑	
		تاریخ/زمان	☑	
		روش اتصال کاربر	☐	
		نوع رخداد	☑	
		مکان رویداد	☑	
		سایر موارد	☐	
٦	**محصول باید هرگونه حذف و تغییر غیرمجاز در ثبت‌نشان‌ها را تشخیص دهد و در صورت امکان جلوگیری نماید.**		☑	
	روش‌های تشخیص مشخص شود. (وجود یک مورد لازم و کافی است)	استفاده از درهم‌سازی (Hash) برای تشخیص تغییرات	☐	
		پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)	☑	
		فقط خواندنی کردن ثبت‌نشان‌ها در محصول	☑	
		سایر موارد	☐	
۷	**محصول باید وقتی که حجم ثبت‌نشان‌ها، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید.**		☑	
	روش‌های اطلاع‌رسانی مشخص شود (وجود یک مورد لازم و کافی است)	استفاده از یک کانال ارتباطی	☐	
		ارسال پیام	☐	
		از طریق واسط کاربر مجاز	☐	
		سایر موارد	☑	لاگ ها به صورت ماهانه حذف می شوند
۸	**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.**		☑	
	رویکردهای مورد استفاده در محصول مشخص گردد (وجود یک مورد لازم و کافی است)	نادیده گرفتن ثبت‌نشان‌ها	☐	
		ذخیره‌سازی محدود ثبت‌نشان‌ها (آنهایی که توسط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند)	☐	
		بازنویسی روی قدیمی‌ترین ثبت‌نشان‌های ذخیره‌شده	☐	
		سایر موارد	☑	لاگ ها به صورت ماهانه حذف می شوند

۲-۲- رمزنگاری

در این رده، 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 یك کلید مشترك برای رمزگذاری و رمزگشایی، استفاده می‌شود ولی در رمزنگاری نامتقارن این کار با استفاده از یك 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 رده، توانایی محصول از این حیث مورد بررسی قرار گرفته است. در رده رمزنگاری همچنین از الگوریتمهای درهم‌سازی (هش) برای برقراری جامعیت داده استفاده می‌گردد.

شماره الزام	رده رمزنگاری			توضیحات
۱	**محصول باید قابلیت رمزنگاری یا واحد[2] رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف‌شده ISO 18033-3) با توجه به موارد زیر انجام دهد.**		☑	
	مد عملیاتی که الگوریتم از آن استفاده می‌کند را انتخاب نمایید. (وجود یك مورد لازم و کافی است.)	مد عملیاتی CBC و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵٦ بیتی (تعریف‌شده در NIST SP 800-38A)	☐	
		مد عملیاتی GCM و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵٦ بیتی (تعریف‌شده در NIST SP 800-38D)	☑	۲۵٦ و ۱۲۸ بیتی
		مد عملیاتی CTR و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵٦ بیتی (تعریف‌شده در ISO10116)	☐	
۲	**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.**		☑	
	الگوریتم و اندازه خلاصه پیام مورد استفاده را انتخاب نمایید. (وجود یك	الگوریتم SHA-1 با اندازه خلاصه پیام ۱٦۰ بیت	☐	
		الگوریتم SHA-256 با اندازه خلاصه پیام ۲۵٦ بیت	☑	
		الگوریتم SHA-384 با اندازه خلاصه پیام ۳۸٤ بیت	☑	

[2] Module

	مـــورد لازم و کـــافی است.)	الگوریتم SHA-512 با اندازه خلاصه پیام ۵۱۲ بیت	☐		
۳	**در صورتی که تولید کلید رمزنگاری در محصول وجود دارد، نیاز است که تخریب کلید رمزنگاری نیز بر اساس موارد زیر صورت پذیرد. (اختیاری)**			☑	
	روش نـــابودی کلیـــد مشخص گردد. (وجود یـــک مـــورد لازم و کافی است)	نابودی با استفاده از بازنویسی ساده (بازنویسی با صفرها، یکها، مقدار تصادفی، مقدار جدیدی از کلید)	☐		
		نابودی با استفاده از یك واسط مشخص	☐		
		از طریق توابع امنیتی محصول	☑		
		سایر موارد	☐		
٤	**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)**			☑	
	الگـــوریتم و انـــدازه کلیدهای مورد استفاده را انتخـــاب نماییـــد. (وجـــود یـــک مـــورد لازم و کافی است)	الگوریتم‌های امضای دیجیتال RSA با کلیدهای رمزنگاری ۲۰٤۸ بیت و بزرگتر (بر اساس FIPS PUB 186-4، استاندارد امضای 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)	☐		
		الگوریتم‌های امضای دیجیتال ECDSA با کلیدهای رمزنگاری ۲۵٦ بیت یا بزرگتر (بر اساس ISO/IEC 14888-3 بخش ٦,٤، استاندارد امضای دیجیتال (DSS) بخش ٦ و پیوست D، با استفاده از منحنی P-256 یا P-384 یا P-521)	☑		

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.

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

	توجه به نوع کاربرد می‌تواند از حالت انتخابی به حالت الزامی تغییر یابد. برای مثال غیرفعال کردن حساب کاربری در تمامی کاربردها مفید نیست.	☐	استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود)		
		☐	سایر موارد		
۳	**محصول باید برای هر کاربر، ویژگی‌های امنیتی را که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت باشند، نگهداری نماید.**			☑	
	ویژگی‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند.	☑	شناسه کاربر		
		☐	روش احراز هویت مورد استفاده		
		☑	داده احراز هویت		
		☑	وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره)		
		☑	نقش کاربر		
		☐	سایر موارد		
٤	**محصول باید قابلیت مدیریت گذرواژه را فراهم آورد.**			☑	
	موارد نیاز که باید در تعریف گذرواژه استفاده شوند.	☑	استفاده از حروف کوچك		
		☑	استفاده از حروف بزرگ		
		☑	استفاده از اعداد		
		☑	استفاده از کاراکترهای خاص ("@"، "#"، "$"، "٪"، "^"، "!" "&"، "*"، "(" , ")" و ...)		
		☑	حداقل طول ۸ یا بیشتر (قابل تنظیم)		
		☐	سایر موارد		
٥	**محصول باید پیش از احراز هویت موفق یك کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید.**			☑	
	اقدامات عمومی که کاربر می‌تواند قبل از احراز هویت انجام	☐	مشاهده راهنمای نحوه ورود به سیستم		
		☑	بازیابی گذرواژه		
		☐	هیچ اقدامی		

	دهد، انتخاب شود.	سایر موارد	☐	
٦	**محصول باید از سازوکار احراز هویت پشتیبانی نماید (برای احراز هویت کاربران راه‌دور، باید بیش از یك سازوکار احراز هویت در محصول به کار رفته باشد).**		☐	
	سازوکارهای احراز هویت موجود در محصول مشخص شوند.	نام کاربری و گذرواژه	☑	
		امضای دیجیتال	☐	
		Active Directory	☐	
		OTP یا توکن	☐	
		احراز هویت دو فاکتوری	☑	
		سایر موارد	☐	
۷	**محصول باید برای هر کاربر فعال، ویژگی‌های امنیتی را نگهداری نماید.**		☑	
	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).	شناسه کاربر	☑	
		نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمتهای مختلف برنامه	☑	
		جزئیات واسط کلاینت	☐	
		پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)	☑	
		سایر موارد	☐	
۸	**محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید.**		☑	
	در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این	از بین رفتن اعتبار نشستهای قبلی هنگام برقراری یك 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.)	☑	
		بروزرسانی اطلاعات پیشینه احراز هویت	☑	

	قوانین در «سایر موارد» بیان می‌شوند).	سایر موارد	☐		
۹	**محصول باید بر روی تغییرات ویژگی‌های امنیتی کاربر فعال قوانینی را اعمال نماید.**			☑	
	قوانینی که در صورت تغییر ویژگی‌های امنیتی کاربر فعال، اعمال می‌شود، مشخص گردد.	غیرمجاز بودن هرگونه تغییر در طول نشست فعال	☑		
		سایر موارد	☐		

۲-٤- حفاظت از داده‌ی کاربری

داده کاربری در واقع هر نوع داده‌ای است که کاربر تولید می‌کند یا مالك 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.

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

۲	**محصول باید بر اساس ویژگی‌های زیر، برای موجودیت‌های غیرفعال خطمشی‌های کنترل دسترسی اعمال نماید.**		☑	
	ویژگی‌هایی که بر اساس آن خطمشی‌ها تعریف می‌شوند، انتخاب گردد.	نقش‌ها و مجوزهای کاربر مجاز	☑	
		اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند.	☑	
		سایر موارد	☐	
۳	**محصول باید بر اساس قاعده‌ای عملیات بین موجودیت فعال تحت کنترل و موجودیت غیرفعال کنترل‌شده را مجاز نماید (این قاعده می‌تواند بدین شکل باشد که در لیست کنترل دسترسی، سابقه (رکوردی) وجود داشته باشد که به کاربر با شناسه کاربری یا شناسه گروه مربوطه یا نقش کاربری تعریف‌شده حق دسترسی به موجودیت غیرفعال را بدهد.)**		☑	
٤	**محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.**		☑	
	قوانین ممانعت از دسترسی مشخص شوند (در صورت اعمال قوانین بیشتر توسط محصول، در «سایر موارد» بیان شود).	عبور تعداد نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف‌شده	☑	
		سایر موارد	☐	
٥	**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.**		☑	
٦	**محصول باید هنگام دریافت داده کاربری خطمشی کنترل دسترسی را اعمال و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.**		☐	
	ویژگی‌های امنیتی مرتبط با داده کاربری	نوع داده	☐	

	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).	حجم و اندازه	☐		
		فرمت	☐		
		تعداد دفعات Import	☐		
		سایر موارد	☐		
۷	**محصول باید از یك پروتکل امن برای انتقال داده استفاده نماید. این پروتکل ارتباط و همبستگی شفافی را بین داده کاربری دریافت‌شده و ویژگی‌های امنیتی آن فراهم و همچنین از شنود و گم‌شدن داده حین انتقال جلوگیری می‌کند.**			☑	
۸	**محصول باید هنگام انتقال داده به بیرون از محصول، خطمشی کنترل دسترسی اعمال نماید و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند.**			☑	
	ویژگی‌های امنیتی مرتبط با داده کاربری که در هنگام خروج آن از محصول استفاده می‌شوند، مشخص شوند	نوع داده	☑		
		حجم و اندازه	☑		
		فرمت	☑		
		سایر موارد	☐		
۹	**محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید.**			☑	
	قوانینی که در هنگام خروج داده از محصول اعمال می‌شوند، مشخص شوند	مدیر سیستم باید خروج داده‌ها را محدود نماید، به طوریکه کاربران محصول، قادر به خروج بدون هدف داده به خارج از محصول نباشند.	☑		
		سایر موارد	☐		

۱۰	**محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره‌شده در محصول تشخیص دهد.**		☑	
	چگونگی تشخیص تغییر در داده‌های کاربری حساس، مشخص شود.	مقدار درهم‌سازی‌شده داده‌های کاربری ذخیره‌شده، نگهداری می‌شود.	☑	
		سایر موارد	☐	
۱۱	**محصول باید در صورت تشخیص خطای صحت در داده‌ها، اقدامات مقابله‌ای زیر را انجام دهد.**		☑	
	اقدام مقابله‌ای در صورت تشخیص خطا، مشخص شود (وجود یك مورد لازم و کافی است)	ایجاد هشدار/اخطار برای نقش‌های مجاز	☐	
		تصحیح داده بر اساس مقادیر قبل	☐	
		سایر موارد	☑	دادههای حساس توسط سیستم احراز هویت کنترل میگردد. با استفاده از تعریف دسترسیها در سامانه، امکان تغییر غیر مجاز وجود ندارد.

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.

شماره الزام	رده مدیریت امنیت			توضیحات
۱	**محصول باید برای مدیر سیستم و هر کاربری که مجوز لازم را دارد، امکان فعالیت‌های مدیریتی زیر را بر روی توابع و تمام کارکردهای مربوط به مدیریت محصول فراهم آورد.**		☑	
	فعالیت‌های مدیریتی که محصول پشتیبانی می‌کند، مشخص شوند.	تعیین و تغییر رفتار	☑	
		غیرفعال نمودن	☑	
		فعال نمودن	☑	
		سایر موارد	☐	
۲	**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.**		☑	
	عملیات بر روی ویژگی‌های امنیتی که در محصول پشتیبانی می‌شوند، مشخص گردد.	پرس‌وجو	☑	
		تغییر	☑	
		حذف	☑	
		تغییر پیش‌فرض	☐	
		سایر موارد	☐	
۳	**محصول باید برای داده‌های محصول، امکان کارکردهای زیر را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.**		☑	
	عملیات بر روی داده‌های محصول که در محصول پشتیبانی	تغییر پیش‌فرض	☐	
		حذف نمودن	☑	
		پرس‌وجو	☑	

	می‌شوند، مشخص شود.	مقداردهی	☑		
		ایجاد	☑		
		مشاهده	☑		
		سایر موارد	☐		
٤	**محصول باید توانایی انجام کارکردهای زیر را داشته باشد.**			☑	
	در صورتی که هرکدام از موارد مطرح‌شده، توسط محصول قابل اجرا نیست، در قسمت توضیحات باید دلایل مطرح گردد.	پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات ثبت‌نشان‌ها	☑		
		پشتیبانی از مجوزهای مشاهده/ویرایش ثبت‌نشان‌ها	☑		
		پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ثبت‌نشان‌ها	☑		
		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 یك عملیات از پیش تعیین‌شده پس از تشخیص یك 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.	☑		
		۱. مدیریت سازوکارهای احراز هویت ۲. مدیریت قوانین مرتبط با احراز هویت	☑		
		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.	☑		
		مدیر مجاز می‌تواند ویژگی‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد.	☑		
		مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول	☑		

		مدیریت نقش‌ها در محصول	☑	
		مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر	☑	
		مدیریت شرایط آغاز نشست توسط مدیر مجاز	☑	
		۱. تعیین زمان غیرفعال بودن برای یك کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد. ۲. تعیین زمان پیش‌فرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد.	☑	
٥	**محصول باید توانایی تعریف نقش‌های مختلف را داشته باشد.**		☑	
	نقش‌هایی که در محصول پشتیبانی می‌شوند، مشخص گردد.	مدیر سیستم	☑	
		کاربر پیشرفته	☐	
		کاربر عادی	☑	
		سایر موارد	☐	
٦	**محصول باید قادر باشد کاربران را به نقش‌های تعریف‌شده یا قابل تعریف مرتبط نماید، همچنین لازم است هر حساب کاربری تنها به یك نقش مرتبط شده باشد، اما ممکن است نقش‌ها تنها به یك کاربر محدود نشوند و چندین کاربر نقش مشابهی داشته باشند.**		☑	

۲-٦- 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.

شماره الزام	رده حفاظت از توابع امنیتی محصول				توضیحات
۱	**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.**			☑	
	هر یکی از مواردی که در صورت رخداد آن، وضعیت امن محصول حفظ می‌شود، مشخص گردد.	خرابی‌های نرم‌افزاری	☑		
		خرابی‌های سخت‌افزاری	☑		
۲	**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.**			☑	
۳	**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.**			☑	
	داده امنیتی قابل اشتراک‌گذاری که در محصول پشتیبانی می‌شوند، مشخص گردد.	داده‌های احراز هویت	☐		
		کلید	☐		
		امضای دیجیتال	☐		
		ثبت‌نشان‌ها (داده‌های ممیزی)	☐		
		سایر موارد	☐		

٤	**محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهرهای زمانی[3] معتبر را تولید یا از آن‌ها استفاده نماید.**		☑	
	روش‌های ایجاد مهرهای زمانی معتبر انتخاب شود. (دیگر روشهای موجود در محصول، در قسمت «سایر موارد» بیان شود).	گرفتن مهرهای زمانی از سرور NTP	☐	
		تنظیم مهرهای زمانی از طریق اینترنت	☐	
		تنظیم مهرهای زمانی به صورت پیش‌فرض (معتبر و عدم امکان دستکاری غیرمجاز)	☑	
		سایر موارد	☐	
٥	**محصول باید امکان بروزرسانی نرم‌افزار و میان‌افزار محصول را برای مدیر سیستم فراهم نماید.**		☑	
	روش بروزرسانی مورد استفاده در محصول، مشخص گردد (حداقل یک مورد لازم و کافی است).	بروزرسانی دستی	☑	
		جستجوی خودکار بروزرسانی‌ها	☐	
		بروزرسانی‌های خودکار	☐	
		بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی	☐	
٦	**در صورت استفاده از بروزرسانی به روش خودکار، محصول باید پیش از نصب بروزرسانی‌های نرم‌افزاری و میان‌افزاری، امکان احراز اصالت میان‌افزار یا نرم‌افزار را فراهم نماید.**		☐	
	سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی) به‌روزرسانی‌ها انتخاب گردد.	امضای دیجیتال	☐	
		درهم‌ساز منتشرشده	☐	

[3] 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.

شماره الزام	رده تخصیص منابع		توضیحات
۱	محصول باید در زمان رخداد هرگونه اشکال و خرابی (شکست) نرم‌افزاری، از عملکرد کارکردهای اصلی محصول اطمینان حاصل نماید.	☑	

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 یك کاربر را محدود نماید.**	☑	
۲	**محصول باید کلیه نشست‌های تعاملی راه‌دور را پس از مدت زمانی که غیرفعال هستند (و می‌بایست توسط مدیر قابل تنظیم باشد)، خاتمه دهد.**	☑	
۳	**محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.**	☑	
٤	**در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس موارد زیر باشد.**	☑	
	انتخاب یك مورد لازم و کافی است.		
	☑ روز		
	☑ زمان		
	☐ سایر موارد		
٥	**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 یك مورد لازم و کافی است.		
	☑ روز		
	☑ زمان		
	☐ سایر موارد		

٦	**محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاك نماید.**		☑	
۷	**محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.**		☑	
	پارامترهای موجود برای جلوگیری از نشست، مشخص شوند (وجود یك مورد لازم و کافی است).	مکان	☐	
		شماره پورت	☐	
		روز	☐	
		زمان	☐	
		سایر موارد	☑	با غیر فعال کردن کاربر می توان از ایجاد نشست جلوگیری کرد.

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.

شماره الزام	رده کانال‌ها/مسیرهای مورد اعتماد			توضیحات
۱	**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 افشاء 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 ۲-۳- تا ٤-۳- که در بخش ۳- بیان گردیده است، الزامی است.		☐	
	پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد.	HTTPS	☑	
		TLS	☑	
		SSH	☐	
۲	**محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانال امن آغاز کنند.**		☑	
۳	**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

شماره الزام	پروتکل HTTPS			توضیحات
۱	**محصول باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کند.**		☑	
۲	**محصول باید پروتکل HTTPS را با استفاده از TLS اجرا کند.**		☑	
۳	**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 ۵-۳- انجام می‌شود که در این صورت الزامات بخش ۵-۳- الزامی است.		☑	
	محصول تنها از موارد بیان‌شده می‌تواند استفاده نماید.	اتصال را برقرار نکند.	☑	
		برای برقراری اتصال درخواست مجوز کند.	☐	

۳-۲- پروتکل TLS Client

شماره الزام	پروتکل TLS Client				توضیحات
۱	**محصول باید TLS 1.2 (RFC 5246) و/یا TLS 1.1 (RFC 4346) را پیاده‌سازی و دیگر نسخه‌های TLS و SSL را رد کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.**			☑	
	مجموعه رمز مورد استفاده و پیاده‌سازی‌شده محصول، انتخاب گردد.	TLS_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	☐		
		TLS_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268	☐		
		TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	☐		
		TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	☐		
		TLS_DHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 3268	☐		
		TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	☐		
		TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	☐		
		TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492	☐		
		TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	☐		
		TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	☐		
		TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA مطابق با RFC 4492	☐		

		☐	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492		
		☐	TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246		
		☐	TLS_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246		
		☐	TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246		
		☐	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246		
		☐	TLS_DHE_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5246		
		☐	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246		
		☑	TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288		
		☐	TLS_RSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5288		
		☑	TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288		
		☐	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA384 مطابق با RFC 5289		
		☑	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256 مطابق با RFC 5289		
		☑	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289		
		☑	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256		

			مطابق با RFC 5289		
		☑	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289		
		☐	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289		
۲	**محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش ٦ از RFC 6125، تأیید نماید.**			☑	
۳	**محصول باید کانال امن را فقط در صورت معتبر بودن گواهی‌نامه سرور برقرار سازد؛ بنابراین اگر گواهی‌نامه سرور غیرمعتبر به نظر رسید، محصول باید بر اساس موارد زیر رفتار نماید.**			☑	
	در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.	☑	ارتباط را برقرار نکند		
		☐	برای برقراری ارتباط درخواست مجوز کند		
		☐	سایر موارد		
٤	**محصول باید در پیام ClientHello برای استفاده از خم‌های بیضوی، بر اساس موارد زیر عمل نماید.**			☑	
	در صورت که محصول از منحنی استفاده می‌نماید، طول کلید باید مشخص گردد.	☐	Supported Elliptic Curves Extension را ارائه نکند.		
		☑	Supported Elliptic Curves Extension را به همراه NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 ارائه نماید.		Secp384r1

۳-۳- پروتکل TLS Server

شماره الزام	پروتکل TLS Server				توضیحات
۱	**محصول باید TLS 1.2 (RFC 5246) را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید.**			☑	
	مجموعه رمز مورد استفاده و پیاده‌سازی شده محصول، انتخاب گردد.	TLS_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	☐		
		TLS_DHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 3268	☐		
		TLS_DHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 3268	☐		
		TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	☐		
		TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	☐		
		TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	☐		
		TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA مطابق با RFC 4492	☐		
		TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA مطابق با RFC 4492	☐		
		TLS_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246	☑		
		TLS_RSA_WITH_AES_256_CBC_SHA256 مطابق با RFC 5246	☑		
		TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5246	☐		
		TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	☐		

			مطابق با RFC 5246		
		☐	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289		
		☐	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289		
		☐	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289		
۲	**محصول باید اتصال‌های کاربرانی که درخواست SSL1.0، SSL2.0، SSL3.0، TLS1.0 و TLS1.1دارند را رد نماید.**			☑	
۳	**محصول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید.**			☑	
	در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.	☐	استفاده از RSA با اندازه کلید ۲۰٤۸ یا ۳۰۷۲ یا ٤۰۹٦ بیت		secp256r1
		☑	پارامترهای ECDH با استفاده از NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگر		
		☐	پارامترهای دیفی-هلمن با اندازه کلید ۲۰٤۸ یا ۳۰۷۲ بیت		

۳-٤- پروتکل TLS مشترک کلاینت و سرور

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

شماره الزام	پروتکل TLS مشترک کلاینت و سرور		توضیحات
۱	**محصول باید احراز هویت دوطرفه کلاینت‌ها/سرورهای TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید.**	☐	
۲	**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.**	☐	

۳-۵- اعتبارسنجی گواهی‌نامه

شماره الزام	اعتبارسنجی گواهی‌نامه				توضیحات
۱	**محصول باید گواهی‌نامه‌ها را بر اساس قوانین زیر تأیید کند.**			☑	
		تأیید گواهی‌نامه RFC 5280 و تأیید مسیر گواهی‌نامه که از حداقل طول مسیر دو گواهی‌نامه پشتیبانی می‌کند.	☑		
		مسیر گواهی‌نامه باید با یک گواهی‌نامه CA امن پایان یابد.	☑		
		محصول باید برای تأیید مسیر یک گواهی‌نامه، اطمینان حاصل نماید که افزونه basicConstraints وجود دارد و پرچم CA برای تمام گواهی‌نامه‌های CA به حالت «TRUE» تنظیم شده است.	☑		
	روش‌های تأیید وضعیت فسخ گواهی‌نامه	پروتکل وضعیت گواهی‌نامه آنلاین (OCSP) مشخص‌شده در RFC 696	☐		
		لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5280 بخش ۶,۳	☐		
		لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش ۵	☐		
		هیچ روش فسخ دیگری	☑		
	قوانین تأیید بخش extendedKeyUsage	گواهی‌نامه‌های مورد استفاده برای تأیید بروزرسانی‌های 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 بخش extendedKeyUsage خود داشته باشند.	☐		
		گواهی‌نامه‌های سرور ارائه شده برای TLS باید هدف « Server Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در بخش extendedKeyUsage خود داشته باشند.	☑		
		گواهی‌نامه‌های کلاینت ارائه شده برای TLS باید هدف « Client Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در بخش extendedKeyUsage خود داشته باشند.	☐		
		گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ OCSP باید « OCSP Signing» (id-pk9 با OID 1.3.6.1.5.5.7.3.9) را در بخش	☐		

			extendedKeyUsage خود داشته باشند.		
۲	**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.**			☑	
۳	**محصول باید برای پشتیبانی احراز هویت برای موارد زیر از گواهی‌نامه‌های X509v3 تعریف‌شده در RFC 5280 استفاده کند.**			☐	
	در صورت پشتیبانی از کارکردهای دیگر، در «سایر موارد» بیان گردد.		HTTPS	☑	
			TLS	☐	
			SSH	☐	
			امضای کد برای بروزرسانی‌های نرم‌افزار سیستم	☐	
			امضای کد برای تأیید یکپارچگی	☐	
			سایر موارد	☐	

۶-۳- پروتکل SSH

شماره الزام	پروتکل SSH		توضیحات
۱	**محصول باید پروتکل SSH را مطابق با RFCهای ٤٢٥١، ٤٢٥٢، ٤٢٥٣، ٤٢٥٤، ٥٦٥٦ و ٦٦٦٨ پیاده‌سازی نماید.**	☑	
۲	**محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4252، از روش‌های احراز هویت زیر پشتیبانی نماید.**	☑	
	احراز هویت مبتنی بر کلید عمومی	☑	
	احراز هویت مبتنی بر گذرواژه	☑	
۳	**محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4253، بسته‌های بزرگتر از مقدار مشخصی (در بخش «توضیحات» ذکر شود) را کنار بگذارد.**	☑	
٤	**محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های رمزنگاری زیر استفاده نماید.**	☑	
	AES128-CBC	☑	
	AES192-CBC	☑	
	AES256-CBC	☑	
	AES128-CTR	☑	
	AES192-CTR	☑	
	AES256-CTR	☑	
	AEAD_AES_128_GCM	☐	
	AEAD_AES_256_GCM	☐	

٥	**محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های کلید عمومی زیر استفاده نماید.**	☑	
	ssh-ed25519	☑	
	ssh-ed448	☐	
	rsa-sha2-512	☑	
	rsa-sha2-256	☑	
	ecdsa-sha2-nistp521	☐	
	ecdsa-sha2-nistp384	☐	
	ecdsa-sha2-nistp256	☑	
	x509v3-ecdsa-sha2-nistp521	☐	
	x509v3-ecdsa-sha2-nistp384	☐	
	x509v3-ecdsa-sha2-nistp256	☐	
	x509v3-rsa2048-sha256	☐	
	ssh-rsa	☑	
	x509v3-ssh-rsa	☐	
٦	**محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های MAC صحت داده‌های زیر استفاده نماید.**	☑	
	AEAD_AES_256_GCM	☐	
	AEAD_AES_128_GCM	☐	
	hmac-sha2-512	☑	
	hmac-sha2-256	☑	
	hmac-sha1-96	☑	
	hmac-sha1	☑	
۷	**محصول باید در پیاده‌سازی پروتکل SSH تنها از الگوریتم‌های تبادل کلید زیر استفاده نماید.**	☑	
	curve25519-sha256	☑	
	curve448-sha512	☐	

		☑	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	
۸	**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 می‌گردد. در صورت پر شدن حد آستانه برای هر کدام از موارد ذکر شده، باید تجدید کلید صورت بگیرد.**	☑		
۹	**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 (تشریح‌شده در RFC 4251 بخش ۱.۷) همراه می‌کند، استفاده می‌نماید.**	☑		