به نام خدا

سند الزامات امنیتی برنامه‌های کاربردی تحت شبکه

شرکت مهندسی فناوری اطلاعات داده گستر آرشام

پرتال و وب سایت خبری شرکت آب و فاضلاب استان آذربایجان غربی

نسخه ۱.۰

اردیبهشت ۱۴۰۰
نسخه 1.8

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

۱- معرفی محصول

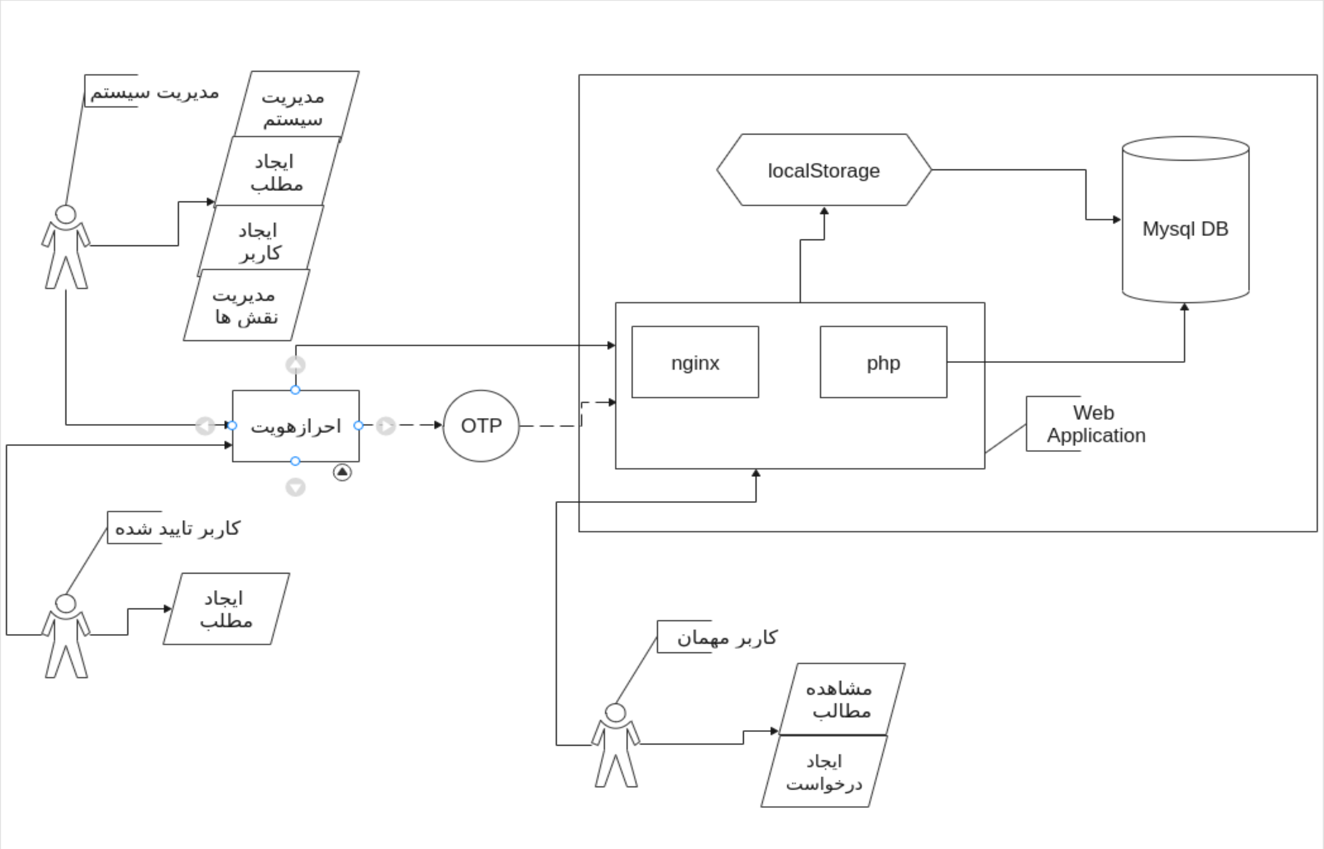
معرفی عملکرد محصول

۱-۱- مشخصات فنی محصول

نسخه‌ی نرم‌افزار/میان‌افزار	V1.0
مدل و نسخه سیستم‌عامل	Linux Ubuntu 18
مدل و نسخه وب‌سرور	Ngnix 1.14
مدل و نسخه پایگاه داده	MYSQL 5.7
زبان برنامه‌نویسی	Php 7.4

۱-۲- معماری محصول

محصول یک سامانه تحت وب می باشد . جهت اطلاع رسانی رویداد ها و اخبار های مربوط به سازمان ، این محصول به وسیله سیستم مدیریت دروپال و nginx, php,mariadb طراحی و پیاده سازی شده است . و سه نوع کابری دارد . "مدیریت " ، "کاربر تایید شده "، "کاربر مهمان " . که مدیریت میتواند کل سیستم را مدیریت کرده و نظارت داشته باشد . کابر تایید شده . فقط میتواند مطالب جدید ، ایجاد ، ویرایش و حذف نمایید . و کابر مهمان هم فقط میتواند مطالب سایت را مشاهده کرده و یا با مدیریت سایت از طریق فرم های طراحی شده تماس داشته باشد .



۲- الزامات امنیتی

الزامات امنیتی این سند بر اساس نسخه ۱.۱ پروفایل حفاظتی «برنامه‌های کاربردی تحت شبکه» تهیه شده است. ساختار این سند بدین صورت است که برای هر کلاس در پروفایل حفاظتی مربوطه، یک دسته الزام بیان شده است.

۲-۱- ممیزی امنیت (لاگ)

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

شماره الزام	کلاس ممیزی امنیت (لاگ)			توضیحات
۱	**محصول باید برای موارد مشخص‌شده که در ذیل آمده است، رکورد ممیزی تولید کند (لاگ ثبت نماید).**		■	
	رویدادهایی که برای آنها لاگ ثبت می‌شود را مشخص نمایید.	شروع و اتمام توابع	■	
		تلاش‌های ناموفق برای خواندن اطلاعات از رکوردهای لاگ	■	
		خواندن اطلاعات از رکوردهای لاگ	■	
		تمامی تغییرات در پیکربندی لاگ	■	
		عملیات انجام‌شده به دلیل سرریز حافظه لاگ از حد آستانه	■	
		عملیات انجام‌شده به دلیل شکست در ذخیره‌سازی لاگ‌ها	■	
		تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.	■	
		تمام کاربردهای سازوکار احراز هویت	■	
		نتایج نهایی عملیات احراز هویت	■	
		تلاش موفق و ناموفق هر کلمه عبور تست‌شده توسط محصول	■	
		شکست و موفقیت انقیاد مشخصه‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال)	■	
		تمامی تغییرات بر روی مقادیر مشخصه‌های امنیتی	■	

		تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول	■		
		تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه مشخصه‌های امنیتی)	■		
		همه تلاش‌ها برای خارج کردن اطلاعات از محصول	■		
		تمامی تغییرات در رفتارهای توابع کارکردی محصول	■		
		استفاده از کارکردهای مدیریتی	■		
		تغییرات در گروه کاربران	■		
		شکست در کارکردهای امنیتی محصول	■		
		تمامی قابلیت‌هایی از محصول که به دلیل شکست، نمی‌توانند عملیات مورد نظر را انجام دهند.	■		
		تلاش موفق یا ناموفق برای برقراری نشست.	■		
		عدم ایجاد نشست به دلیل محدودیت نشست‌های هم‌زمان (حداقل)	■		
		خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست	■		
		خاتمه به نشست غیرفعال توسط مدیر سیستم	■		
		سایر موارد	☐		
۲	**محصول باید برای هر رکورد ممیزی تولیدشده، مشخصاتی که در ذیل آمده است را ثبت نماید.**			■	
	مشخصاتی که در رکوردهای ممیزی وجود دارد مشخص شود.	تاریخ و زمان رویداد	■		
		نوع رویداد	■		
		هویت ایجادکننده رویداد	■		
		نتیجه رویداد	■		
		آدرس IP ایجادکننده رویداد	■		
		سایر موارد	☐		

۳	**محصول باید رکوردهای ممیزی را در برابر دسترسی غیرمجاز محافظت نماید.**			■	
۴	**رکوردهای ممیزی که محصول تولید می‌نماید باید برای کاربر ساده و قابل فهم باشند.**			■	
	مواردی که در رکوردهای ممیزی وجود دارند، مشخص شوند.	عدم وجود داده نامفهوم در رکوردها	■		
		عدم وجود فیلدهای نامرتبط	■		
		وجود داده معتبر و مناسب در هر فیلد	■		
۵	**محصول باید امکان انتخاب و مرتب‌سازی برای رکوردهای ممیزی تولید شده را بر اساس فیلدها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید.**			■	
	مواردی که بر اساس آنها مرتب‌سازی وجود دارد، مشخص شود.	هویت موجودیت فعال	☐		
		نوع حساب کاربری	■		
		تاریخ/زمان	■		
		روش اتصال کاربر	☐		
		نوع رخداد	■		
		مکان رویداد	☐		
		سایر موارد	☐		
۶	**محصول باید هرگونه حذف و تغییر غیرمجاز در رکوردهای ممیزی را تشخیص دهد و در صورت امکان جلوگیری نماید.**			■	
	روش‌های تشخیص مشخص شود. (وجود یک مورد لازم و کافی است)	استفاده از هش برای تشخیص تغییرات	■		
		پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری)	■		
		فقط خواندنی کردن ممیزی‌ها در محصول	■		
		سایر موارد	☐		

۷	**محصول باید وقتی که حجم داده‌های ممیزی، 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	☐		
۸	**محصول باید توانایی ممیزی (ثبت لاگ) هنگام از کار افتادن محصول و/یا پر شدن حافظه ممیزی را داشته باشد و برای این کار از رویکردهای بیان‌شده استفاده نماید.**			■	
	رویکردهای مورد استفاده در محصول مشخص گردد (وجود یک مورد لازم و کافی است)	نادیده گرفتن رویدادهای ممیزی	☐		
		ذخیره‌سازی محدود رویدادهای ممیزی، (آنهایی که توسط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند)	■		
		بازنویسی روی قدیمی‌ترین رکوردهای ممیزی ذخیره‌شده	■		
		سایر موارد	☐		

۲-۲- رمزنگاری

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

شماره الزام	کلاس رمزنگاری				توضیحات
۱	**محصول باید قابلیت رمزنگاری یا ماژول رمزنگاری داشته باشد، بنابراین باید رمزگذاری و رمزگشایی را بر اساس الگوریتم AES (تعریف‌شده ISO 18033-3) با توجه به موارد زیر انجام دهد.**			■	
	مد عملیاتی که الگوریتم از آن استفاده می‌کند را انتخاب نمایید. (وجود یک مورد لازم و کافی است.)	مد عملیاتی CBC و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در NIST SP 800-38A)	☐		
		مد عملیاتی GCM و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در NIST SP 800-38D)	■		با طول کلید ۲۵۶
		مد عملیاتی CTR و طول کلید ۱۲۸ یا ۱۹۲ یا ۲۵۶ بیتی (تعریف‌شده در ISO10116)	☐		
۲	**محصول باید بر اساس الگوریتم رمزنگاری و طول کلیدی که انتخاب می‌نماید، توانایی تولید داده درهم‌سازی شده (هش) را داشته باشد؛ بنابراین باید برای تولید درهم‌سازی از موارد زیر بر اساس ISO/IEC 10118-3:2004 استفاده نماید.**			■	با اندازه خلاصه پیام ۳۸۴
	الگوریتم و اندازه خلاصه پیام مورد استفاده را انتخاب نمایید. (وجود	الگوریتم SHA-1 با اندازه خلاصه پیام ۱۶۰	☐		
		الگوریتم SHA-256 با اندازه خلاصه پیام ۲۵۶	☐		
		الگوریتم SHA-384 با اندازه خلاصه پیام ۳۸۴	■		

	یک مورد لازم و کافی است.)	الگوریتم SHA-512 با اندازه خلاصه پیام ۵۱۲	☐		
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 نابودی کلید مشخص گردد. (وجود یک مورد لازم و کافی است)	نابودی با استفاده از بازنویسی ساده (بازنویسی با صفرها، یکها، مقدار تصادفی، مقدار جدیدی از کلید)	☐		
		نابودی با استفاده از یک واسط مشخص	☐		
		از طریق توابع امنیتی محصول	■		
		سایر موارد	☐		
۴	**در صورتی که امضاء دیجیتال در محصول پشتیبانی می‌شود، نیاز است که سرویس‌های امضاء رمزنگاری (تولید و تأیید) بر اساس الگوریتم‌های رمزنگاری زیر انجام گیرد. (اختیاری)**			☐	
	الگوریتم و اندازه کلیدهای مورد استفاده را انتخاب نمایید. (وجود یک مورد لازم و کافی است)	الگوریتم‌های امضاء دیجیتال RSA با کلیدهای رمزنگاری ۲۰۴۸ بیت و بزرگتر (بر اساس FIPS PUB 186-4، استاندارد امضاء دیجیتال (DSS) بخش ۵.۵، الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSA-PKCS1v_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال ۲ و یا الگوی امضای دیجیتال ۳)	■		
		الگوریتم‌های امضاء دیجیتال ECDSA با کلیدهای رمزنگاری ۲۵۶ بیت یا بزرگتر (بر اساس ISO/IEC 14888-3 بخش ۶.۴، استاندارد امضای دیجیتال (DSS) بخش ۶ و پیوست D، با استفاده از منحنی P-256 یا P-384 یا P-521)	☐		

۲-۳- شناسایی و احراز هویت

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

شماره الزام	کلاس 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 بازه‌ی مورد استفاده در هریک باید مشخص گردد. (وجود یک مورد لازم و کافی است)	یک عدد مثبت ثابت	■		به صورت پیش فرض عدد مثبت ۵ میباشد
		یک عدد مثبت قابل تنظیم توسط مدیر	■		
		یک 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 توجه به نوع کاربرد می‌توانند از حالت انتخابی به حالت الزامی تغییر یابد.	غیرفعال کردن حساب کاربری (فعال کردن به صورت دستی توسط مدیر صورت می‌گیرد)	■		در هر بار تلاش برای احرازهویت از کاربر captcha گرفته میشود . پس از ۵ بار تلاش ناموفق کاربر بلاک شده . پس از ۱ روز از بلاک خارج میشود .
		غیرفعال کردن حساب کاربری بر اساس مدت زمان معین (فعال کردن پس از زمان مذکور به صورت خودکار صورت می‌گیرد)	■		
		استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت توضیحات بیان شود)	■		

	برای مثال غیرفعال کردن حساب کاربری در تمامی کاربردها مفید نیست.	سایر موارد	☐		
۳	**محصول باید برای هر کاربر، مشخصه‌های امنیتی که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت باشند را نگهداری نماید.**			■	
	مشخصه‌های امنیتی مورد نیاز که باید برای هر کاربر نگهداری شوند.	شناسه کاربر	■		
		روش احراز هویت مورد استفاده	☐		
		داده احراز هویت	■		
		وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره)	■		
		نقش کاربر	■		
		سایر موارد	☐		
۴	**محصول باید قابلیت مدیریت کلمه عبور را فراهم آورد.**			■	
	موارد نیاز که باید در تعریف کلمه‌عبور استفاده شوند.	استفاده از حروف کوچک	■		
		استفاده از حروف بزرگ	■		
		استفاده از اعداد	■		
		استفاده از کاراکترهای خاص ("@"، "#"، "$"، "٪"، "^"، "!" "&"، "*"، "(" , ")" و ...)	■		
		حداقل طول ۸ یا بیشتر (قابل تنظیم)	■		
		سایر موارد	☐		
۵	**محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید.**			■	
	اقدامات عمومی که کاربر می‌تواند قبل از	مشاهده راهنمای نحوه ورود به سیستم	■		
		بازیابی کلمه‌عبور	■		

	احراز هویت انجام دهد، انتخاب شود.	هیچ اقدامی	☐		
		سایر موارد	☐		
۶	**محصول باید از سازوکار احراز هویت پشتیبانی نماید (برای احراز هویت کاربران راه‌دور، باید بیش از یک سازوکار احراز هویت در محصول به کار رفته باشد).**			■	
	سازوکارهای احراز هویت موجود در محصول مشخص شوند.	نام کاربری و کلمه‌عبور	■		
		امضاء دیجیتال	☐		
		Active Directory	☐		
		OTP یا توکن	■		
		احراز هویت دو فاکتوری	☐		
		سایر موارد	☐		
۷	**محصول باید برای هر کاربر فعال، مشخصه‌های امنیتی نگهداری نماید.**			■	
	مشخصه‌هایی امنیتی که محصول برای هر کاربر نگهداری می‌کند، مشخص گردد (در صورتی که محصول قوانین بیشتری هنگام برقراری نشست اعمال می‌نماید، این قوانین در «سایر موارد» بیان می‌شوند).	شناسه کاربر	■		
		نقش‌ها و یا مجموعه دسترسی‌های کاربر به قسمتهای مختلف برنامه	■		
		جزئیات واسط کلاینت	☐		
		پیشینه احراز هویت (جزئیات تلاش برای احراز هویت موفق و ناموفق)	■		
		سایر موارد	☐		
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 قوانین در «سایر موارد» بیان می‌شوند).	از بین رفتن اعتبار نشستهای قبلی هنگام برقراری یک نشست جدید (به جزء مواردی که فعال بودن همزمان چندین نشست 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	■		
		سایر موارد	☐		
۹	**محصول باید بر روی تغییرات مشخصه‌های امنیتی کاربر فعال قوانینی را اعمال نماید.**			■	
	قوانینی که در صورت تغییر مشخصه‌های امنیتی کاربر فعال، اعمال می‌شود، مشخص گردد.	غیرمجاز بودن هرگونه تغییر در طول نشست فعال	■		
		سایر موارد	☐		

۲-٤- حفاظت از داده‌ی کاربری

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

شماره الزام	کلاس حفاظت از داده‌ی کاربری			توضیحات
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.	رکوردها، مستندات و فراداده	■	
		داده متعلق به کاربران	■	
		داده احراز هویت	■	
		سایر موارد	☐	
	عملیاتی که خط‌مشی‌های کنترل دسترسی در رابطه با	ایجاد موجودیت غیرفعال جدید	■	
		حذف موجودیت غیرفعال	■	
		تغییر دسترسی‌ها به موجودیت غیرفعال	■	
		عملیات بر روی فراداده وابسته به موجودیت غیرفعال	■	

	آنها اعمال می‌شوند، مشخص گردد.	سایر موارد	☐		
۲	**محصول باید بر اساس مشخصه‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید.**			■	
	مشخصه‌هایی که بر اساس آن خط‌مشی‌ها تعریف می‌شوند، انتخاب گردد.	نقش‌ها و مجوزهای کاربر مجاز	■		
		اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند.	■		
		سایر موارد	☐		
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، 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.)**			■	
۴	**محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید.**			■	
	قوانین ممانعت از دسترسی مشخص شوند (در صورت اعمال قوانین بیشتر توسط محصول، در «سایر موارد» بیان شود).	تجاوز چندین نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف‌شده	■		
		سایر موارد	☐		
۵	**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.**			■	تخصیص و آزادسازی منابع به عهده پایگاه داده می باشد .
۶	**محصول باید هنگام دریافت داده کاربری خط‌مشی کنترل دسترسی را اعمال نماید و برای این کار از مشخصه‌های امنیتی مرتبط با داده کاربری استفاده کند.**			■	شرایط قابل قبول برای هر فیلد توسط مدیریت سیستم تعریف میشود . در حالت فعلی از فایل های txt,pdf,docx,png,jpg,xlsx با حجم کمتر از ۲۰ مگابایت تعریف شده است .

	مشخصه‌های امنیتی مرتبط با داده کاربری که در هنگام ورود آن به محصول استفاده می‌شوند، مشخص شود (در صورتی که کنترل دسترسی برای موارد دیگری نیز صورت می‌گیرد، در قسمت «سایر موارد» بیان گردد).	نوع داده	■		
		حجم و اندازه	■		
		فرمت	■		
		تعداد دفعات Import	☐		
		سایر موارد	☐		
۷	**محصول باید از یک پروتکل امن برای انتقال داده استفاده نماید. این پروتکل ارتباط و همبستگی شفافی را بین داده کاربری دریافت‌شده و مشخصه‌های امنیتی آن فراهم می‌کند و همچنین از شنود و گمشدن داده حین انتقال جلوگیری می‌کند.**			■	از متد postبرای ارسال فایل استفاده می شود . و همچنین از ssl استفاده می شود .
۸	**محصول باید هنگام انتقال داده به بیرون از محصول، خط‌مشی کنترل دسترسی اعمال نماید و برای این کار از مشخصه‌های امنیتی مرتبط با داده کاربری استفاده کند.**			■	در هنگام تعریف فیلد ، مدیریت مشخص میکند . که فایل باید به صورت عمومی منتشر شود یا خیر . اگر به صورت عمومی قایل انتشار باشد . هر شخص و کاربری قادر به بارگیری فایل ها خواهد بود . در غیر اینصورت با توجه به احراز هویت و داشتن دسترسی کاربر با توجه به نوع و حجم اندازه فایل قابل دسترس برای شخص خواهد بود .
	مشخصه‌های امنیتی مرتبط با داده کاربری که در هنگام خروج آن از محصول استفاده می‌شوند، مشخص شوند	نوع داده	■		
		حجم و اندازه	■		
		فرمت	■		
		سایر موارد	☐		

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 رکوردها 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.	درهم شده 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 یک مورد لازم و کافی است)	ایجاد هشدار/اخطار برای نقش‌های مجاز	■		
		تصحیح داده بر اساس مقادیر قبل	☐		
		سایر موارد	☐		

۲-۵- مدیریت امنیت

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

شماره الزام	کلاس مدیریت امنیت				توضیحات
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 سایر عملیات زیر را بر روی مشخصه‌های امنیتی الزام ۷ از کلاس شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید.**			■	
	عملیات بر روی مشخصه‌های امنیتی که در محصول پشتیبانی 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	تغییر پیش‌فرض	■		
		حذف نمودن	■		

	در محصول پشتیبانی می‌شوند، مشخص شود.	پرس‌وجو	■		
		مقداردهی	■		
		ایجاد	■		
		مشاهده	■		
		سایر موارد	☐		
۴	**محصول باید توانایی انجام کارکردهای زیر را داشته باشد.**			■	گزینه مدیریت حداکثر تعداد مجاز نشستهای همزمان کاربران مورد نیاز شرکت نبوده و در نرم افزار پیاده سازی نشده است .
	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 رکوردهای ممیزی	■		
		پشتیبانی از مجوزهای مشاهده/ویرایش رویدادهای ممیزی	■		
		پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ممیزی	■		
		مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول	■		انتخاب زمان اجرای حفاظت از اطلاعات باقیمانده به عهده پایگاه داده و سیستم عامل می باشد . و به وسیله cron مدیریت می شود .
		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 تعیین‌شده 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 کلمات عبور	■		
		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 مشخصه‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد.	■		
		مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول	■		
		مدیریت نقش‌ها در محصول	■		
		مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر	■		
		مدیریت شرایط آغاز نشست توسط مدیر مجاز	■		
		۱. تعیین زمان غیرفعال بودن برای یک 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.	■		
۵	**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	☐		
۶	**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.**			■	

۲-۶- حفاظت از توابع امنیتی محصول

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

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

۴	**محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهرهای زمانی معتبر، تولید یا استفاده نماید.**		■	
	روش‌های ایجاد مهرهای زمانی معتبر انتخاب شود. (دیگر روشهای موجود در محصول، در قسمت «سایر موارد» بیان شود).	گرفتن مهرهای زمانی از سرور NTP	☐	در داخل نرم افزار قابلیت تغییر موقعیت زمانی (timezone) وجود دارد
		تنظیم مهرهای زمانی از طریق اینترنت	■	
		تنظیم مهرهای زمانی به صورت پیش‌فرض (معتبر و عدم امکان دستکاری غیرمجاز)	■	
		سایر موارد	☐	
۵	**محصول باید امکان بروزرسانی نرم‌افزار و میان‌افزار محصول را برای مدیر سیستم فراهم نماید.**		■	نرم افزار مستقیما بروزرسانی ها را از سایت رسمی خود به آدرس drupal .org بررسی کرده و در صورت بروزرسانی ، هسته اصلی و ماژول ها را بروزرسانی می نمایید . تمام فایل های بروز رسانی توسط سایت مرجع و تیم امنیتی اعتبار سنجی و درجه بندی شده و سپس در سایت منتشر می شود . با توجه به درجه امنیتی داده شده به فایل های ماژول ، بروز رسانی انجام می شود .
	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	☐	
۶	**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.**		☐	محصول قادر به بروزرسانی خودکار نمی باشد .
	سازوکار مورد استفاده برای صحت‌سنجی (اصالت سنجی) به‌روزرسانی‌ها انتخاب گردد.	امضاء دیجیتال	☐	
		درهم‌ساز منتشرشده	☐	

۲-۷- تخصیص منابع

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

شماره الزام	کلاس تخصیص منابع		توضیحات
۱	محصول باید در زمان رخداد هرگونه شکست نرم‌افزاری؛ از عملکرد کارکردهای اصلی محصول اطمینان حاصل نماید.	■	

۲-۸- دسترسی به محصول

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

شماره الزام	کلاس دسترسی به محصول			توضیحات
۱	**محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.**		■	
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.**		■	
۴	**در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس موارد زیر باشد.**		■	
	انتخاب یک مورد لازم و کافی است.	روز	■	
		زمان	■	
		سایر موارد	☐	
۵	**در صورت برقراری نشست به طور موفقیت آمیز، محصول باید قادر به نمایش آخرین تلاش ناموفق برای ایجاد نشست بر اساس موارد زیر و تعداد تلاش‌های ناموفق تا آخرین ایجاد نشست موفقیت‌آمیز باشد.**		■	
	انتخاب یک مورد لازم و کافی است.	روز	■	
		زمان	■	
		سایر موارد	☐	

۶	**محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.**			■	
۷	**محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد.**			■	
	پارامترهای موجود برای جلوگیری از نشست، مشخص شوند (وجود یک مورد لازم و کافی است).	مکان	■		
		شماره پورت	☐		
		روز	☐		
		زمان	☐		
		سایر موارد	☐		

۲-۹- کانال‌ها/مسیرهای مورد اعتماد

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

شماره الزام	کلاس 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 داده و از تغییر و افشاء داده تبادلی حفاظت نموده 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 ۴-۳- که در بخش ۳- بیان گردیده است، الزامی است.		■	
	پروتکل مورد استفاده برای ایجاد کانال امن انتخاب گردد.	HTTPS	■	
		TLS	☐	
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 کلاس کانال امن، پروتکل HTTPS انتخاب شود، آنگاه رعایت الزامات HTTPS که در این بخش بیان شده است، اجباری می‌گردد.

۳-۱- پروتکل HTTPS

شماره الزام	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 کند 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 ۶ 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	☐		
۴	**محصول باید در پیام ClientHello برای استفاده از منحنی‌ها، بر اساس موارد زیر عمل نماید.**			■	
	در صورت که محصول از منحنی استفاده می‌نماید، طول کلید باید مشخص گردد.	Supported Elliptic Curves Extension را ارائه نکند	■		
		Supported Elliptic Curves Extension را به همراه NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 ارائه نماید	■		
		هیچ منحنی دیگری	☐		

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 TLS1.1 دارند را رد نماید.**			■	
۳	**محصول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید.**			■	secp384r1 خم اندازه کلید ۴۰۹۶ می باشد .
	در صورت پشتیبانی از اقدامات دیگر، در «سایر موارد» بیان گردد.	استفاده از RSA با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ یا ۴۰۹۶ بیت	☐		
		پارامترهای ECDH با استفاده را NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگری	■		
		پارامترهای دیفی-هلمن با اندازه کلید ۲۰۴۸ یا ۳۰۷۲ بیت	■		

۴-۳- پروتکل TLS مشترک کلاینت و سرور

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

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	**محصول در صورت مطابقت نداشتن نام متمایز یا نام دیگر فاعل موجود در گواهی‌نامه، با آنچه از شناساننده کلاینت مورد انتظار بوده است، نباید کانال امن را برقرار سازد.**	☐	

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 فیلد 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 فیلد extendedKeyUsage خود داشته باشند.	☐	
		گواهی‌نامه‌های سرور ارائه شده برای TLS باید هدف « Server Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.1) را در فیلد extendedKeyUsage خود داشته باشند.	■	

		گواهی‌نامه‌های کلاینت ارائه شده برای TLS باید هدف «Client Authentication» (id-kp1 با OID 1.3.6.1.5.5.7.3.2) را در فیلد extendedKeyUsage خود داشته باشند.	☐		
		گواهی‌نامه‌های OCSP مورد استفاده برای پاسخ OCSP باید «OCSP Signing» (id-pk9 با OID 1.3.6.1.5.5.7.3.9) را در فیلد extendedKeyUsage خود داشته باشند.	■		
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 جهت 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	☐		
		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 ۴۲۵۱، ۴۲۵۲، ۴۲۵۳، ۴۲۵۴، ۵۶۵۶ و ۶۶۶۸ پیاده‌سازی نماید.**		■	4251 , 4252 , 4253 , 4254 , 4256, 5656, 6668, 8308, 8332
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.**		■	بیشینه طول بسته ۲۵۶ کیلوبایت می باشد .
۴	**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	☐		
۵	**محصول باید در پیاده‌سازی پروتکل انتقال SSH تنها از الگوریتم‌های کلید عمومی زیر استفاده نماید.**		☐	

		ssh-rsa	■		
		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	☐		
		x509v3-ssh-rsa	☐		
۶	**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-group-exchange-sha1	☐		

	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-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 نباشد و حجم داده مخابره شده بیشتر از ۱ گیگابایت نباشد، استفاده می‌گردد. در صورت پر شدن حد آستانه هر کدام از موارد ذکر شده، مجددسازی کلید باید 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.**		■	