به نام خدا

سند خودارزیابی

نام متقاضی	Raymand Communications Naqsh Jahan
نام محصول	Raymand-CTI
نسخه محصول	2.0.3

<لوگوی شرکت>

تاریخ تکمیل 2026-09-16

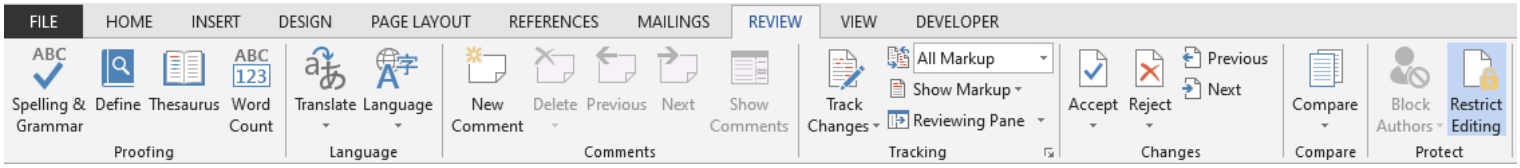
تهران، خیابان آزادی، دانشگاه صنعتی شریف، دانشکده مهندسی کامپیوتر، طبقه همکف، اتاق 007
تلفن: 021-66166660 فکس: 021-66072521 وب‌سایت: www.netel.org رایانامه: mail@netel.org

نسخه‌ی سند 1.0

پیش‌گفتار

سند «خودارزیابی» برای افزایش سرعت فرآیند ارزیابی آماده شده است. این سند شامل تمامی الزام‌های عملکردی مورد نیاز برای دریافت گواهی افتا است. در هر آزمون، موارد مورد نیاز برای برآورده شدن نیاز هر آزمون نیز به عنوان راهنما ارائه شده است. در این سند لازم است تصویری از پیاده‌سازی تمامی موارد خواسته شده (منطبق بر «پرسشنامه» تکمیل شده) در محصول ارائه شود. همچنین در مواردی که مربوط به پیکربندی است، لازم است محل دسترسی به بخش مورد نظر ذکر شود. همچنین در آزمون‌های مربوط به بخش «آسیب‌پذیری»، تصویری از پیکربندی انجام شده را ارائه نمایید.

برای جلوگیری از ایجاد تغییر ناخواسته در این فایل، تنها بخش‌هایی که نیاز به تکمیل دارند، قابل ویرایش هستند. برای مشاهده و تکمیل این بخش‌ها، در بخش «Review»، گزینه‌ی «Restrict Editing» را انتخاب نمایید. سپس با انتخاب « Find Next Region I Can Edit»، می‌توانید این بخش‌ها را مشاهده و تکمیل نمایید.



لازم به اشاره است که فرآیند ارزیابی و نصب محصول تنها هنگامی آغاز خواهد شد که این سند به طور کامل تکمیل شود. تأخیر در تکمیل این سند یا ناقص بودن اطلاعات آن منجر به تأخیر در فرآیند ارزیابی خواهد شد.

1- منابع مورد نیاز

لطفا منابع مورد نیاز جهت نصب و راه‌اندازی محصول را در جدول زیر مشخص نمایید.

سیستم‌عامل	نوع	GNU/Linux (Debian GNU/Linux 12 bookworm)
	نسخه	12 (bookworm)
تعداد هسته‌ی پردازنده		4
میزان RAM		8 GB
میزان حافظه		

با توجه به اینکه محصول در محیط آزمایشگاه زیر بار نخواهد بود، تا حد ممکن کمینه‌ی منابع مورد نیاز را اعلام نمایید.

در بخش «نوع سیستم‌عامل»، Windows یا GNU/Linux بودن سیستم‌عامل را مشخص نمایید. (توجه کنید که در صورتی که سیستم‌عامل بر پایه‌ی GNU/Linux است، نام «توزیع» مورد نیاز (Ubuntu، CentOS و ...) را درج نمایید.)

2- الزامات امنیتی

1- بند 1 جدول 2-1 (ممیزی امنیت (Log))

شناسه الزام	FAU_GEN.1.1	**نام الزام**	تولید داده ممیزی 1

متن الزام

محصول باید برای موارد مشخص‌شده که در زیر آمده است، ثبت‌نشان[1] تولید کند (Log ثبت نماید).

- شروع و اتمام توابع
- تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها
- خواندن اطلاعات از ثبت‌نشان‌ها
- تمامی تغییرات در پیکربندی ثبت‌نشان‌ها
- 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)
- تمامی تغییرات بر روی مقادیر ویژگی‌های امنیتی
- تمامی درخواست‌ها (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول
- تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه ویژگی‌های 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 (خرابی یا مشکل کارکرد)، نمی‌توانند عملیات مورد نظر را انجام دهند.
- تلاش موفق یا ناموفق برای برقراری نشست.
- ایجاد نشدن 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

راهنمایی

در این الزام تولید ثبت‌نشان (Log) برای رویدادهای مختلف بررسی می‌شود. محل تولید هر ثبت‌نشان نیز زیر آن درج شده است تا بتوانید درک بهتری از آن داشته باشید. برای ثبت‌نشان‌هایی که محل آن‌ها مشخص شده است، می‌توانید تصویر ثبت‌نشان را در الزام مرتبط نیز درج نمایید.

- شروع و اتمام توابع

- تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها
  - ✓ بند 3 جدول 2-1 (ممیزی امنیت (Log))

معتبر	عملیات غیرمجاز	لاگ های سیستمی		منشی	منشی	۱۳۹۹/۱۰/۰۶	۱۰:۳۲:۲۰	۱۹۲.۱۶۸.۳۵.۲۰۱	تلاش غیر مجاز جهت دسترسی به صفحه لاگ های سیستمی

- خواندن اطلاعات از ثبت‌نشان‌ها
  - ✓ بند 3 جدول 2-1 (ممیزی امنیت (Log))

لاگ های عملیاتی									
وضعیت رکورد	نوع عملیات	نام جدول	مقدار کلید	کاربر	نوع کاربر	تاریخ وقوع	زمان وقوع	آدرس ماشین	شرح عملیات
معتبر	مشاهده	لاگ های سیستمی		netel	مدیر	۱۳۹۹/۱۱/۰۵	۰۸:۵۵:۴۶	۱۹۲.۱۶۸.۳۵.۲۴۴	مشاهده اطلاعات ممیزی سیستم

- تمامی تغییرات در پیکربندی ثبت‌نشان‌ها
  - ✓ اگر امکان تغییر پیکربندی واحد رویدادنگاری (برای نمونه، تغییر ثبت شدن یا نشدن رویدادهای

[1] Log

مربوط به بخش‌های مختلف) وجود دارد؛ با تغییر در پیکربندی،
1 برای تغییر در پیکربندی ثبت‌نشان تولید شود
2 صحت عملکرد تغییرات بررسی گردد.



	کاربر	گروه	شعبه			تاریخ	زمان	عملیات	IP
۱	netel (آزمونگر)	مدیر سیستم	شرکت ایده	ارسال SMS - فعال	موارد رویدادنگاری	۱۳۹۹/۰۴/۰۸	۰۸:۳۶:۱۱	ویرایش	۱۹۲.۱۶۸.۳۵.۲۱۵
۲	netel (آزمونگر)	مدیر سیستم	شرکت ایده	ویرایش - فعال	موارد رویدادنگاری	۱۳۹۹/۰۴/۰۸	۰۸:۳۶:۱۰	ویرایش	۱۹۲.۱۶۸.۳۵.۲۱۵
۳	netel (آزمونگر)	مدیر سیستم	شرکت ایده	ورود ناموفق - غیرفعال	موارد رویدادنگاری	۱۳۹۹/۰۴/۰۸	۰۸:۳۵:۴۵	ویرایش	۱۹۲.۱۶۸.۳۵.۲۱۵

✓ تغییر حد آستانه برای سرریز (بند 7 جدول 2-1 (ممیزی امنیت (Log))

- عملیات انجام‌شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه
  ✓ بند 7 جدول 2-1 (ممیزی امنیت (Log)

- عملیات انجام‌شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها
  ✓ بند 8 جدول 2-1 (ممیزی امنیت (Log)

- تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.
  ✓ بند 11 جدول 2-4 (حفاظت از داده‌ی کاربری)

لاگ های عملیاتی

وضعیت رکورد	نوع عملیات	نام جدول	مقدار کلید	کاربر	نوع کاربر	تاریخ وقوع	زمان وقوع	آدرس ماشین	شرح عملیات
نامعتبر	خطا					۱۳۹۹/۰۹/۰۹	۱۲:۴۱:۳۹	۱۹۲.۱۶۸.۳۵.۲۵	Message : Value cannot be null, Parameter name: input
معتبر	خطا			netel	مدیر	۱۳۹۹/۱۱/۰۸	۱۵:۰۱:۵۳	۱۹۲.۱۶۸.۳۵.۲۴۴	Message : فایل مورد نظر به صورت غیرمجاز تغییر کرده و امکان دسترسی به آن وجود ندارد
معتبر	افزودن	ضمیمه	۰	netel	مدیر	۱۳۹۹/۱۱/۰۸	۱۴:۵۵:۵۳	۱۹۲.۱۶۸.۳۵.۲۴۴	AttachmentName: '۷۷۴ea۶۹۸-۴۲eb-۴ab۵-۸۰۵۲-c۳۹۹c۹۴۰a۷۷۶.xlsx' OrginalAttachmentName: 'iM.xlsx' TaskId: '۲۸۱۱۷' TaskRotationId: '۷۳۴۵۶' DocId: '۳۹۶۰۴' 'DocType: '۸' DocCount: '۱' DataType: '۱' IsAttached: 'True' Type: '۰

- تمام کاربردهای سازوکار احراز هویت
  ✓ بندهای 1، 2 و 6 جدول 2-3 (شناسایی و احراز هویت)

لاگ های عملیاتی

وضعیت رکورد	نوع عملیات	نام جدول	مقدار کلید	کاربر	نوع کاربر	تاریخ وقوع	زمان وقوع	آدرس ماشین	شرح عملیات
معتبر	ویرایش	کلید های پیکر بندی سیستم	۱۰۰۸۲	netel	مدیر	۱۳۹۹/۱۱/۰۵	۱۱:۵۳:۱۰	۱۹۲.۱۶۸.۳۵.۲۴۴	تعداد مجاز برای ورود اشتباه رمز عبور از ۵ به ۳ تغییر یافت

لاگ های عملیاتی

وضعیت رکورد	نوع عملیات	نام جدول	مقدار کلید	کاربر	نوع کاربر	تاریخ وقوع	زمان وقوع	آدرس ماشین	شرح عملیات
معتبر	ویرایش	کلید های پیکر بندی سیستم	۱۰۰۹۳	netel	مدیر	۱۳۹۹/۱۱/۰۵	۱۱:۵۴:۰۲	۱۹۲.۱۶۸.۳۵.۲۴۴	مدت زمان فعال شدن خودکار کاربر از ۵ به ۳ تغییر یافت
معتبر	ویرایش	کلید های پیکر بندی سیستم	۱۰۰۸۹	netel	مدیر	۱۴۰۰/۰۱/۲۴	۱۱:۵۴:۴۶	۱۹۲.۱۶۸.۳۵.۲۴۴	احراز هویت دو مرحله ای(۰:غیرفعال،۱:فعال) از ۱ به ۰ تغییر یافت
معتبر	ویرایش	کلید های پیکر بندی سیستم	۱۰۰۸۹	netel	مدیر	۱۴۰۰/۰۱/۲۴	۱۱:۵۴:۴۲	۱۹۲.۱۶۸.۳۵.۲۴۴	احراز هویت دو مرحله ای(۰:غیرفعال،۱:فعال) از ۰ به ۱ تغییر یافت

- نتایج نهایی عملیات احراز هویت
  ✓ بند 6 جدول 2-3 (شناسایی و احراز هویت)

لاگ های احراز هویت

وضعیت رکورد	کاربر	نوع کاربر	تاریخ وقوع	زمان وقوع	آدرس ماشین	شرح عملیات	نوع درخواست	نتیجه درخواست
معتبر	test	کارمند	۱۳۹۹/۱۱/۰۵	۰۹:۴۸:۰۳	۱۹۲.۱۶۸.۳۵.۲۴۴	کاربر موردنظر غیرفعال می باشد،لطفا در زمان دیگری مجددا تلاش کنید و یا جهت فعال سازی با مدیر سیستم تماس بگیرید.	ورود به سامانه	ناموفق
معتبر	test	کارمند	۱۳۹۹/۱۱/۰۵	۰۹:۴۷:۵۸	۱۹۲.۱۶۸.۳۵.۲۴۴	کاربر مورد نظر به علت تلاش غیر مجاز جهت ورود به سامانه غیر فعال شد.	ورود به سامانه	ناموفق
معتبر	test	کارمند	۱۳۹۹/۱۱/۰۵	۰۹:۴۷:۵۶	۱۹۲.۱۶۸.۳۵.۲۴۴	تلاش ناموفق جهت ورود به سامانه با نام کاربری 'test'	ورود به سامانه	ناموفق
معتبر	test	کارمند	۱۳۹۹/۱۱/۰۵	۰۹:۴۷:۵۳	۱۹۲.۱۶۸.۳۵.۲۴۴	تلاش ناموفق جهت ورود به سامانه با نام کاربری 'test'	ورود به سامانه	ناموفق

- تلاش موفق و ناموفق هر گذرواژه بررسی‌شده توسط محصول
  ✓ بند 4 جدول 2-3 (شناسایی و احراز هویت)

لاگ های عملیاتی

وضعیت رکورد	نوع عملیات	نام جدول	مقدار کلید	کاربر	نوع کاربر	تاریخ وقوع	زمان وقوع	آدرس ماشین	شرح عملیات
معتبر	ویرایش	کلید های پیکر بندی سیستم	۱۰۰۸۰	netel	مدیر	۱۳۹۹/۱۱/۰۵	۱۱:۵۵:۳۳	۱۹۲.۱۶۸.۳۵.۲۴۴	حداقل تعداد کاراکتر های رمز عبور از ۹ به ۸ تغییر یافت
معتبر	ویرایش	کلید های پیکر بندی سیستم	۱۰۰۸۱	netel	مدیر	۱۳۹۹/۱۱/۰۵	۱۱:۵۵:۲۷	۱۹۲.۱۶۸.۳۵.۲۴۴	کاراکترهای مورد نیاز برای رمز عبور از @%$&!# به @%$& تغییر یافت

- شکست و موفقیت انتساب ویژگی‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت

ایجاد موجودیت فعال)

✓ بند 7 جدول 2-3 (شناسایی و احراز هویت)

۱۵	۸۵۲۳۶۹۷۴۱۰	پرتال آموزش	نرم افزار	۱۳۹۹/۰۶/۱۲	۰۷:۳۰:۴۸	ثبت نام جدید	۱۹۲.۱۶۸.۳۵.۲۱۵	

- تمامی تغییرات بر روی مقادیر ویژگی‌های امنیتی

✓ بند 7 و 9 جدول 2-3 (شناسایی و احراز هویت)

معتبر	ویرایش	اشخاص حقوقی	۱۱۶۶۰	مدیر سیستم	مدیر	۱۴۰۰/۰۱/۲۹	۱۷:۱۰:۴۳	۱۹۲.۱۶۸.۳۵.۲۴۴	RegisterDate: تغییر یافت از '۳/۳۱/۲۰۲۱ ۱۲:۰۰:۰۰ AM' به '۳/۲۸/۲۰۲۱ ۱۲:۰۰:۰۰ AM' VATDate: تغییر یافت از " به "
معتبر	مشاهده	اشخاص حقوقی		مدیر سیستم	مدیر	۱۴۰۰/۰۱/۲۹	۱۷:۱۰:۲۴	۱۹۲.۱۶۸.۳۵.۲۴۴	مشاهده اطلاعات اشخاص حقوقی
معتبر	خطا			netel	مدیر	۱۳۹۹/۱۰/۰۶	۱۵:۱۸:۲۲	۱۹۲.۱۶۸.۳۵.۲۰۱	Message : کاربر مورد نظر در سامانه لاگین می باشد و امکان تغییر مشخصات آن وجود ندارد.

- تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول

✓ بند 2 جدول 2-4 (حفاظت از داده‌ی کاربری)

معتبر	حذف	گروههای کاربری	۱۰۹۲	netel	مدیر	۱۳۹۹/۱۰/۰۷	۱۶:۴۵:۰۴	۱۹۲.۱۶۸.۳۵.۲۰۱	Name: 'test' Icon: '' Description: 'dfgh'
معتبر	ویرایش	گروههای کاربری	۱۰۹۲	netel	مدیر	۱۳۹۹/۱۰/۰۷	۱۶:۴۵:۰۱	۱۹۲.۱۶۸.۳۵.۲۰۱	Description: تغییر یافت از '' به 'dfgh'
معتبر	افزودن	گروههای کاربری	۰	netel	مدیر	۱۳۹۹/۱۰/۰۷	۱۶:۴۴:۵۵	۱۹۲.۱۶۸.۳۵.۲۰۱	Name: 'test' Icon: '' Description: '' :

- تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه ویژگی‌های امنیتی)

✓ بند 6 جدول 2-4 (حفاظت از داده‌ی کاربری)

معتبر	افزودن	ضمیمه	۰	netel	مدیر	۱۳۹۹/۱۰/۰۷	۱۵:۵۹:۱۴	۱۹۲.۱۶۸.۳۵.۲۰۱	AttachmentName: 'obb۳۵۵a۶-cd۵b-۴۸۸۷-af۴d۳-۹۳۶d۹۱۰۴d۴b۷.xlsx' OrginalAttachmentName: 'IM.xlsx' TaskId: '۲۷۱۱۷' TaskRotationId: '۷۳۴۵۶' DocId: '۳۸۶۰۴' DocType: '۸' DocCount: '۱' DataType: '۱' IsAttached: 'True' Type: '۰
معتبر	حذف	ضمیمه	۲۵۱۳۷	netel	مدیر	۱۳۹۹/۱۰/۰۷	۱۵:۵۹:۰۱	۱۹۲.۱۶۸.۳۵.۲۰۱	AttachmentName: 'a۲۹c۹۸۸۱-۰۷۷۵-۴۵۸۱-a۳۱۰-f۸۹۴۳c۱۲۵۵۵۶.doc' OrginalAttachmentName: 'IM.doc' TaskId: '۲۷۱۱۷' TaskRotationId: '۷۳۴۵۶' DocId: '۳۸۶۰۴' DocType: '۸' DocCount: '۱' DataType: '۱' IsAttached: 'True' Type: '۰

- همه تلاش‌ها برای خارج کردن اطلاعات از محصول

✓ بند 8 جدول 2-4 (حفاظت از داده‌ی کاربری)

نام کاربری	نام و نام خانوادگی	قسمت/بخش	توضیحات	تاریخ	ساعت	IP کاربر	نوع فعالیت
netel	NETEL شریف	کتابخانه	نام فایل: add new source	۱۳۹۹/۰۴/۱۷	۱۵:۱۹:۴۲	۱۹۲.۱۶۸.۳۵.۲۱۵	دانلود فایل

- تمامی تغییرات در رفتارهای توابع کارکردی محصول

✓ بند 1 جدول 2-5 (مدیریت امنیت)

معتبر	ویرایش	کلید های پیکر بندی سیستم	۱۰۰۶۷	netel	مدیر	۱۳۹۹/۱۱/۰۵	۱۱:۵۱:۱۴	۱۹۲.۱۶۸.۳۵.۲۴۴	انتهای بازه زمانی مجاز برای ورود به سیستم از ۲۳:۳۰:۵۹ به ۲۳:۳۰ تغییر یافت
معتبر	ویرایش	کلید های پیکر بندی سیستم	۱۰۰۶۶	netel	مدیر	۱۳۹۹/۱۱/۰۵	۱۱:۵۱:۰۳	۱۹۲.۱۶۸.۳۵.۲۴۴	ابتدای بازه زمانی مجاز برای ورود به سیستم از ۰۶:۰۰ به ۰۷:۰۰ تغییر یافت

- استفاده از کارکردهای مدیریتی

✓ بند 4 جدول 2-5 (مدیریت امنیت)

معتبر	ویرایش	کلید های پیکر بندی سیستم	۱۱۰۲۹	netel	مدیر	۱۴۰۰/۰۱/۲۹	۱۷:۲۱:۱۷	۱۹۲.۱۶۸.۳۵.۲۴۴	آدرس ماشین های غیرمجاز سامانه از ۱۹۲.۱۶۸.۳۵.۲۴۴ به تغییر یافت
معتبر	ویرایش	کلید های پیکر بندی سیستم	۱۱۰۲۹,۱۱۰۳۰	netel	مدیر	۱۴۰۰/۰۱/۲۹	۱۷:۲۱:۱۳	۱۹۲.۱۶۸.۳۵.۲۴۴	آدرس ماشین های غیرمجاز سامانه از به ۱۹۲.۱۶۸.۳۵.۲۴۴ تغییر یافت آدرس ماشین های مجاز برای کاربران ارشد سامانه از ۱۹۲.۱۶۸.۳۵.۲۴۴ به تغییر یافت
معتبر	ویرایش	کلید های پیکر بندی سیستم	۱۱۰۳۰	netel	مدیر	۱۴۰۰/۰۱/۲۹	۱۷:۲۱:۰۱	۱۹۲.۱۶۸.۳۵.۲۴۴	آدرس ماشین های مجاز برای کاربران ارشد سامانه از به ۱۹۲.۱۶۸.۳۵.۲۴۴ تغییر یافت

- تغییرات در گروه کاربران

✓ بند 1 جدول 2-4 (حفاظت از داده‌ی کاربری)

معتبر	حذف	گروههای کاربری	۱۰۹۲	netel	مدیر	۱۳۹۹/۱۰/۰۷	۱۶:۴۵:۰۴	۱۹۲.۱۶۸.۳۵.۲۰۱	Name: 'test' Icon: '' Description: 'dfgh'
معتبر	ویرایش	گروههای کاربری	۱۰۹۲	netel	مدیر	۱۳۹۹/۱۰/۰۷	۱۶:۴۵:۰۱	۱۹۲.۱۶۸.۳۵.۲۰۱	Description: تغییر یافت از '' به 'dfgh'
معتبر	افزودن	گروههای کاربری	۰	netel	مدیر	۱۳۹۹/۱۰/۰۷	۱۶:۴۴:۵۵	۱۹۲.۱۶۸.۳۵.۲۰۱	Name: 'test' Icon: '' Description: '' :

- شکست در کارکردهای امنیتی محصول

✓ بند 1 جدول 2-6 (حفاظت از توابع امنیتی محصول)

```
#. error at 1/27/2021 3:53:12 PM.
Summary: System.Data.Entity.Core.EntityException: The underlying provider failed on Open. ---> System.Data.SqlClient.SqlException: SQL Server service has been paused.
```

- تمامی قابلیت‌هایی از محصول که به دلیل شکست (خرابی یا مشکل کارکرد)، نمی‌توانند عملیات مورد نظر را انجام دهند.

✓ بند 1 جدول 2-7 (تخصیص منابع)

```
#. error at 1/27/2021 3:53:12 PM.
Summary: System.Data.Entity.Core.EntityException: The underlying provider failed on Open. ---> System.Data.SqlClient.SqlException: SQL Server service has been paused.
```

- تلاش موفق یا ناموفق برای برقراری نشست.

✓ بند 7 جدول 2-8 (دسترسی به محصول) و بند 8 جدول 2-3 (شناسایی و احراز هویت)

لاگ های احراز هویت

وضعیت رکورد	کاربر	نوع کاربر	تاریخ وقوع	زمان وقوع	آدرس ماشین	شرح عملیات	نوع درخواست	نتیجه درخواست
معتبر	کاربر ارشد	مدیر	۱۳۹۹/۱۱/۰۵	۱۳:۴۵:۲۶	۱۹۲.۱۶۸.۳۵.۲۴	آدرس ماشین جاری جهت ورود کاربران ارشد مجاز نمی باشد	ورود به سامانه	ناموفق



لاگ های احراز هویت

وضعیت رکورد	کاربر	نوع کاربر	تاریخ وقوع	زمان وقوع	آدرس ماشین	شرح عملیات	نوع درخواست	نتیجه درخواست
معتبر	کاربر ارشد	مدیر	۱۳۹۹/۱۱/۰۵	۱۳:۵۴:۴۱	۱۹۲.۱۶۸.۳۵.۲۴	امکان ورود به سیستم در این بازه زمانی برای شما وجود ندارد.	ورود به سامانه	ناموفق

- ایجاد نشدن نشست به دلیل محدودیت نشست‌های همزمان (حداقل)
  - ✓ بند 1 جدول 2-8 (دسترسی به محصول)



لاگ های احراز هویت

وضعیت رکورد	کاربر	نوع کاربر	تاریخ وقوع	زمان وقوع	آدرس ماشین	شرح عملیات	نوع درخواست	نتیجه درخواست
معتبر	netel	مدیر	۱۳۹۹/۱۱/۰۵	۱۲:۱۴:۵۶	۱۹۲.۱۶۸.۳۵.۲۴۴	کاربر 'netel' با موفقیت وارد سیستم شد	ورود به سامانه	موفق
معتبر	netel	مدیر	۱۳۹۹/۱۱/۰۵	۱۲:۱۴:۵۶	۱۹۲.۱۶۸.۳۵.۲۴۴	کاربر 'netel:۱۹۲.۱۶۸.۳۵.۲۴۴' به علت برقرای نشست همزمان جدید از سامانه خارج شد	خروج از سامانه	موفق
معتبر	netel	مدیر	۱۳۹۹/۱۱/۰۵	۱۱:۳۶:۵۹	۱۹۲.۱۶۸.۳۵.۲۴۴	کاربر 'netel' با موفقیت وارد سیستم شد	ورود به سامانه	موفق
معتبر	کاربر ارشد	مدیر	۱۳۹۹/۱۰/۰۶	۱۵:۰۹:۳۳	۱۹۲.۱۶۸.۳۵.۲۴	حداکثر تعداد ارتباط همزمان برای این کاربر پر شده است،امکان ورود به سیستم وجود ندارد.		ناموفق
معتبر	کاربر ارشد	مدیر	۱۳۹۹/۱۰/۰۶	۱۵:۰۹:۱۸	۱۹۲.۱۶۸.۳۵.۲۰۱	کاربر 'کاربر ارشد' با موفقیت وارد سیستم شد		موفق
معتبر	کاربر ارشد	مدیر	۱۳۹۹/۱۰/۰۶	۱۵:۰۶:۲۸	۱۹۲.۱۶۸.۳۵.۲۰۱	کاربر 'کاربر ارشد' با موفقیت وارد سیستم شد		موفق

- خاتمه دادن به یك نشست غیرفعال توسط سازوکار قفل نشست
  - ✓ بند 2 جدول 2-8 (دسترسی به محصول)



معتبر	کاربر ارشد	مدیر	۱۳۹۹/۱۰/۰۶	۱۵:۴۰:۱۸	۱۹۲.۱۶۸.۳۵.۲۰۱	کاربر 'کاربر ارشد:۱۹۲.۱۶۸.۳۵.۲۰۱' به علت غیر فعال بودن نشست از سامانه خارج شد		موفق
معتبر	کاربر ارشد	مدیر	۱۳۹۹/۱۰/۰۶	۱۵:۳۸:۱۵	۱۹۲.۱۶۸.۳۵.۲۰۱	کاربر 'کاربر ارشد' با موفقیت وارد سیستم شد		موفق

- خاتمه به نشست غیرفعال توسط مدیر سیستم
  - ✓ بند 2 جدول 2-8 (دسترسی به محصول)



لاگ های احراز هویت

وضعیت رکورد	کاربر	نوع کاربر	تاریخ وقوع	زمان وقوع	آدرس ماشین	شرح عملیات	نوع درخواست	نتیجه درخواست
معتبر	منشی	منشی	۱۳۹۹/۱۱/۰۸	۱۰:۰۵:۴۹	۱۹۲.۱۶۸.۳۵.۲۴۴	کاربر 'منشی:۱۹۲.۱۶۸.۳۵.۲۴۴' توسط مدیر سیستم از سامانه خارج شد	خروج از سامانه	موفق

- سایر موارد

نحوه‌ی دسترسی

ثبت لاگ: کلاس UserLogger در بک‌اند (جدول tbl_user_logs). مشاهده: منوی مانیتورینگ ← گزارش لاگ سیستم (/endpoint، system-logs/index/ users/user-logs). لاگ فنی: فایل log/pline.log.

تصویر

تصویر صفحه گزارش لاگ سیستم و نمونه رکورد tbl_user_logs پیوست شود.

- شروع و اتمام توابع
- تلاش‌های ناموفق برای خواندن اطلاعات از ثبت‌نشان‌ها
  - ✓ بند 3 جدول 2-1 (ممیزی امنیت (Log)
- خواندن اطلاعات از ثبت‌نشان‌ها
  - ✓ بند 3 جدول 2-1 (ممیزی امنیت (Log)
- تمامی تغییرات در پیکربندی ثبت‌نشان‌ها
  - ✓ اگر امکان تغییر پیکربندی واحد رویدادنگاری (برای نمونه، تغییر ثبت شدن یا نشدن رویدادهای مربوط به بخش‌های مختلف) وجود دارد؛ با تغییر در پیکربندی،
    1. برای تغییر در پیکربندی ثبت‌نشان تولید شود
    2. صحت عملکرد تغییرات بررسی گردد.
  - ✓ تغییر حد آستانه برای سرریز (بند 7 جدول 2-1 (ممیزی امنیت (Log))
- عملیات انجام‌شده به دلیل سرریز حافظه ثبت‌نشان‌ها از حد آستانه
  - ✓ بند 7 جدول 2-1 (ممیزی امنیت (Log)
- عملیات انجام‌شده به دلیل شکست در ذخیره‌سازی ثبت‌نشان‌ها
  - ✓ بند 8 جدول 2-1 (ممیزی امنیت (Log)
- تلاش‌های موفقیت‌آمیز برای بررسی صحت داده‌ی کاربری، شامل نتایج بررسی.
  - ✓ بند 11 جدول 2-4 (حفاظت از داده‌ی کاربری)
- تمام کاربردهای سازوکار احراز هویت

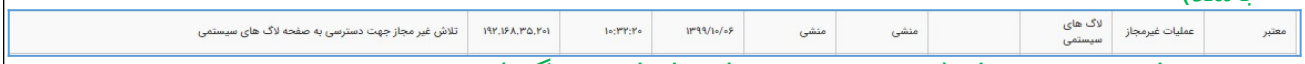
✓ بندهای 1، 2 و 6 جدول 2-3 (شناسایی و احراز هویت) • نتایج نهایی عملیات احراز هویت ✓ بند 6 جدول 2-3 (شناسایی و احراز هویت) • تلاش موفق و ناموفق هر گذرواژه بررسی‌شده توسط محصول ✓ بند 4 جدول 2-3 (شناسایی و احراز هویت) • شکست و موفقیت انتساب ویژگی‌های امنیتی کاربر به موجودیت فعال (مانند شکست و موفقیت ایجاد موجودیت فعال) ✓ بند 7 جدول 2-3 (شناسایی و احراز هویت) • تماتمامی تغییرات بر روی مقادیر ویژگی‌های امنیتی ✓ بند 7 و 9 جدول 2-3 (شناسایی و احراز هویت) • تمامی درخواست‌های (موفق و ناموفق) برای اجرای عملیات بر روی یک موجودیت غیرفعال محصول ✓ بند 2 جدول 2-4 (حفاظت از داده‌ی کاربری) • تمامی تلاش‌ها برای وارد کردن داده‌های کاربری (شامل هرگونه ویژگی‌های امنیتی) ✓ بند 6 جدول 2-4 (حفاظت از داده‌ی کاربری) • همه تلاش‌ها برای خارج کردن اطلاعات از محصول ✓ بند 8 جدول 2-4 (حفاظت از داده‌ی کاربری) • تمامی تغییرات در رفتارهای توابع کارکردی محصول ✓ بند 1 جدول 2-5 (مدیریت امنیت) • استفاده از کارکردهای مدیریتی ✓ بند 4 جدول 2-5 (مدیریت امنیت) • تغییرات در گروه کاربران ✓ بند 1 جدول 2-4 (حفاظت از داده‌ی کاربری) • شکست در کارکردهای امنیتی محصول ✓ بند 1 جدول 2-6 (حفاظت از توابع امنیتی محصول) • تمامی قابلیت‌هایی از محصول که به دلیل شکست (خرابی یا مشکل کارکرد)، نمی‌توانند عملیات مورد نظر را انجام دهند. ✓ بند 1 جدول 2-7 (تخصیص منابع) • تلاش موفق یا ناموفق برای برقراری نشست. ✓ بند 7 جدول 2-8 (دسترسی به محصول) و بند 8 جدول 2-3 (شناسایی و احراز هویت) • ایجاد نشدن نشست به دلیل محدودیت نشست‌های همزمان (حداقل) ✓ بند 1 جدول 2-8 (دسترسی به محصول) • خاتمه دادن به یک نشست غیرفعال توسط سازوکار قفل نشست ✓ بند 2 جدول 2-8 (دسترسی به محصول) • خاتمه به نشست غیرفعال توسط مدیر سیستم ✓ بند 2 جدول 2-8 (دسترسی به محصول)	

	▪ سایر موارد
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل رویدادهای ثبت‌شده فعلی: ورود موفق/ناموفق، حساب غیرفعال، تغییر گذرواژه، عملیات ایجاد/ویرایش/حذف موجودیت‌ها (کاربران، SIP، صف، IVR، مسیرها و ...) و اعمال تنظیمات سیستم. رویدادهای خواندن لاگ‌ها، تغییر پیکربندی لاگ، خروج داده و خاتمه نشست هنوز به‌طور کامل ثبت نمی‌شوند و در دستور کار اصلاح (NC-013 سند عدم‌انطباق) قرار دارند.

2- بند 2 جدول 2-1 (ممیزی امنیت (Log))

شناسه الزام	FAU_GEN.1.2 & FAU_GEN.2.1	**نام الزام**	تولید داده ممیزی2 و مرتبط نمودن هویت کاربر به رویداد 1
متن الزام	محصول باید برای هر ثبت‌نشان تولیدشده، ویژگی‌هایی که در زیر آمده است را ثبت نماید. - تاریخ و زمان رویداد - نوع رویداد - هویت ایجادکننده رویداد - نتیجه رویداد - آدرس IP ایجادکننده رویداد - سایر موارد		
راهنمایی	در ثبت‌نشان‌ها دست‌کم «تاریخ و زمان رویداد»، «نوع رویداد»، «هویت ایجادکننده رویداد» و «نتیجه‌ی رویداد» باید وجود داشته باشد. 		
نحوه‌ی دسترسی	رکوردهای لاگ از طریق صفحه گزارش لاگ سیستم (system-logs/index/) قابل مشاهده‌اند.		
تصویر	تصویر یک رکورد لاگ با جزئیات پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل هر رکورد در وضعیت فعلی شامل: کاربر ثبت‌کننده، شرح رویداد و تاریخ/زمان (createdAt) است. ثبت آدرس IP مبدأ و فیلد نتیجه (موفق/ناموفق) به‌صورت استاندارد در حال تکمیل است (NC-012).		

3- بند 3 جدول 2-1 (ممیزی امنیت (Log))

شناسه الزام	FAU_SAR.1.1 & FAU_SAR.2.1	**نام الزام**	بازبینی داده ممیزی 1 و بازبینی داده ممیزی محدود 1
متن الزام	محصول باید ثبت‌نشان‌ها را در برابر دسترسی غیرمجاز محافظت نماید.		
راهنمایی	کاربر مجاز باید قادر به مشاهده رویدادها باشد. باید از دسترسی کاربری که مجوز دسترسی به بخش «رویدادنگاری» ندارد جلوگیری شود. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان دسترسی / مشاهده برای کاربر مجاز  ✓ ثبت‌نشان جلوگیری از دسترسی کاربر غیرمجاز (بهتر است محل دسترسی غیرمجاز نیز مشخص باشد)  ✓ ثبت‌نشان حذف رویداد (در صورت پشتیبانی از این ویژگی)		
نحوه‌ی دسترسی	منوی مانیتورینگ ← گزارش لاگ سیستم (system-logs/index/) با مجوز منوی 5_6؛ endpoint بک‌اند: / users/user-logs با کنترل مجوز.		

تصویر	تصویر صفحه گزارش لاگ و پیام رد دسترسی برای کاربر فاقد مجوز پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی شده فقط کاربران دارای مجوز منو به بازبینی لاگ‌ها دسترسی دارند؛ درخواست بدون مجوز با کد 401/404 رد می‌شود. قابلیت حذف رکورد لاگ با مجوز ویژه و ثبت لاگ همراه است.

4- بند 4 جدول 2-1 (ممیزی امنیت (Log))

شناسه الزام	FAU_SAR.1.2	**نام الزام**	بازبینی داده ممیزی 2
متن الزام	ثبت‌نشان‌هایی که محصول تولید می‌نماید باید برای کاربر ساده و قابل فهم باشند. - نبود داده نامفهوم در رکوردها - نبود بخش‌های نامرتبط - وجود داده معتبر و مناسب در هر بخش		
راهنمایی	تمامی رویدادهای ثبت‌شده در هر آزمون باید به گونه‌ی صریحی، نمایانگر رخداد مربوط به آن باشند. همچنین اطلاعات نامرتبط، نامفهوم یا اضافی نیز نباید داشته باشند.		
نحوه‌ی دسترسی	نمایش لاگ‌ها در صفحه گزارش لاگ سیستم.		
تصویر	تصویر نمونه لاگ‌ها پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی شده لاگ‌ها به‌صورت متن ساده و قابل فهم (شرح رویداد، نام کاربر، تاریخ/زمان) ثبت و نمایش داده می‌شوند؛ بدون داده رمزنگاری‌شده یا بخش نامرتبط.		

5- بند 5 جدول 2-1 (ممیزی امنیت (Log))

شناسه الزام	FAU_SAR.3.1 & FAU_SEL.1.1	**نام الزام**	بازبینی داده ممیزی قابل انتخاب 1 و انتخاب داده ممیزی 1
متن الزام	محصول باید امکان انتخاب و مرتب‌سازی برای ثبت‌نشان‌های تولیدشده را بر اساس بخش‌ها و پارامترهای مختلف، برای کاربر مجاز فراهم نماید. - هویت موجودیت فعال - نوع حساب کاربری - تاریخ/زمان - روش اتصال کاربر - نوع رخداد - مکان رویداد - سایر موارد		
راهنمایی	در بخش «رویدادنگاری»، امکان «مرتب‌سازی» رویدادها (به صورت صعودی یا نزولی) و نیز امکان «غربال‌گری» رویدادها (نمایش رویدادها بر اساس شرایط مشخصی) بررسی شود.		
نحوه‌ی دسترسی	پنل فیلتر بالای صفحه /system-logs/index (فیلتر نام کاربری، بازه تاریخ، اندازه صفحه).		
تصویر	تصویر پنل فیلتر و نتیجه جستجو پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی شده جستجو و فیلتر لاگ‌ها بر اساس پارامترها در کوئری سمت سرور (endpoint /users/user-logs با		

	پارامترهای username، بازه تاریخ و sort) پیاده‌سازی شده است.

6- بند 6 جدول 2-1 (ممیزی امنیت (Log))

شناسه الزام	FAU_STG.1.1 & FAU_STG.1.2	**نام الزام**	ذخیره‌سازی رویدادهای ممیزی 1 و 2
متن الزام	محصول باید هرگونه حذف و تغییر غیرمجاز در ثبت‌نشان‌ها را تشخیص دهد و در صورت امکان جلوگیری نماید. - استفاده از درهم‌سازی (Hash) برای تشخیص تغییرات - پیکربندی امن پایگاه داده (کنترل دسترسی و رویدادنگاری) - فقط خواندنی کردن ثبت‌نشان‌ها در محصول - سایر موارد		
راهنمایی	[در صورت پشتیبانی]، کاربر مجاز باید قادر به حذف رویدادها باشد. [در صورت پشتیبانی]، کاربر غیرمجاز نباید بتواند رویدادها را حذف نماید. [در صورت پشتیبانی]، محصول برای حذف یا تغییر غیرمجاز [با دسترسی مستقیم به پایگاه داده] باید هشدار یا ثبت‌نشانی تولید نماید. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان حذف رویداد (در صورت پشتیبانی از این ویژگی) ✓ ثبت‌نشان تلاش ناموفق حذف توسط کاربر غیرمجاز (در صورتی که گزینه‌ی «حذف» برای کاربر غیرمجاز فعال باشد.)		
نحوه‌ی دسترسی	نگهداری لاگ در پایگاه‌داده (tbl_user_logs) و فایل لاگ (Logback). دسترسی مشاهده با مجوز منو محدود می‌شود.		
تصویر	تصویر مجوزهای مرتبط با لاگ و پیکربندی دسترسی فایل لاگ پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل دسترسی مشاهده لاگ محدود به کاربران دارای مجوز است. قابلیت حذف رکورد با مجوز ویژه وجود دارد؛ محدودسازی حذف غیرمجاز و افزودن سازوکار یکپارچگی (hash/append-only) در دستور کار (NC-012) است.		

7- بند 7 جدول 2-1 (ممیزی امنیت (Log))

شناسه الزام	FAU_STG.3.1	**نام الزام**	اقدامات لازم در زمان از دست رفتن داده ممیزی 1
متن الزام	محصول باید وقتی که حجم ثبت‌نشان‌ها، به حد آستانه تعریف شده برای ذخیره‌سازی می‌رسد، کاربر مجاز را مطلع نماید. - استفاده از یک کانال ارتباطی - ارسال پیام - از طریق واسط کاربر مجاز - سایر موارد		
راهنمایی	پس از رسیدن به و عبور از حد آستانه، نحوه‌ی اطلاع‌رسانی به کاربر باید – با ارائه‌ی تصویر - تشریح شود. ثبت‌نشان‌های مورد نیاز: ثبت‌نشان عملیات انجام شده (ارسال پیام، ارسال ایمیل، ارسال پیامک یا ...)		
نحوه‌ی دسترسی	پیکربندی: فایل application.properties (کلیدهای logging.logback.rollingpolicy.*).		
تصویر	تصویر فایل پیکربندی و فهرست فایل‌های چرخش‌شده در مسیر log پیوست شود.		

توضیحات بیشتر	وضعیت: پیاده‌سازی شده آستانه نگهداشت: حداکثر 100 مگابایت برای هر فایل لاگ و نگهداری 30 نسخه (پیکربندی چرخش خودکار Logback).

8- بند 8 جدول 2-1 (ممیزی امنیت (Log))

شناسه الزام	FAU_STG.4.1	**نام الزام**	پیشگیری از اتلاف و از دست رفتن داده ممیزی 1
متن الزام	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. - نادیده گرفتن ثبت‌نشان‌ها - ذخیره‌سازی محدود ثبت‌نشان‌ها (آنهایی که توسط کاربر مجاز و تحت حقوق خاصی رخ می‌دهند) - بازنویسی روی قدیمی‌ترین ثبت‌نشان‌های ذخیره‌شده - سایر موارد		
راهنمایی	رفتار محصول در مواجهه با رویدادهای جدید باید - با ارائه‌ی تصویر - تشریح شود. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان عملیات انجام‌شده در مواجهه با رویدادهای جدید. اگر گزینه‌ی «بازنویسی» انتخاب و پیاده‌سازی شده باشد، نیازی نیست که برای «بازنویسی»، ثبت‌نشان تولید کند.		
نحوه‌ی دسترسی	رفتار چرخش خودکار Logback در مسیر log/pline.log.		
تصویر	تصویر فایل‌های چرخش‌شده پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل در رسیدن به آستانه، چرخش خودکار انجام و نسخه‌های قدیمی تا سقف 30 نگهداری می‌شوند. رفتار در صورت شکست ذخیره‌سازی (مانند پرشدن دیسک پایگاه‌داده) در حال تعیین سیاست است (NC-014).		

9- بند 1 جدول 2-2 (رمزنگاری)

شناسه الزام	FAU_COP.1.1(1) & FCS_COP.1.1(3)	**نام الزام**	عملیات رمزنگاری 1 (1) و عملیات رمزنگاری 1 (3)
متن الزام	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. - مد عملیاتی CBC و طول کلید 128 یا 192 یا 256 بیتی (تعریف‌شده در NIST SP 800-38A) - مد عملیاتی GCM و طول کلید 128 یا 192 یا 256 بیتی (تعریف‌شده در NIST SP 800-38D) - مد عملیاتی CTR و طول کلید 128 یا 192 یا 256 بیتی (تعریف‌شده در ISO10116)		
راهنمایی	تنها الگوریتم‌هایی که در محصول وجود دارند باید انتخاب شوند.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات	وضعیت: پیاده‌سازی نشده — بدون ادعا		

بیشتر	در نسخه فعلی محصول سرویس رمزنگاری/رمزگشایی داده با AES ارائه نمی‌شود؛ بنابراین گزینه‌ای انتخاب نشده است.

10- بند 2 جدول 2-2 (رمزنگاری)

شناسه الزام	FAU_COP.1.1(2)	**نام الزام**	عملیات رمزنگاری 1 (2)
متن الزام	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 SHA-1 با اندازه خلاصه پیام 160 بیت - الگوریتم SHA-256 با اندازه خلاصه پیام 256 بیت - الگوریتم SHA-384 با اندازه خلاصه پیام 384 بیت - الگوریتم SHA-512 با اندازه خلاصه پیام 512 بیت			
راهنمایی	تنها الگوریتم‌هایی که در محصول وجود دارند باید انتخاب شوند.		
نحوه‌ی دسترسی	امضای توکن نشست: تولید و اعتبارسنجی JWT در UsersController و jwtAuthorizationCheck.		
تصویر	تصویر کد تولید/اعتبارسنجی JWT پس از اصلاح NC-003 پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل درهم‌سازی SHA-512 در قالب امضای JWT (HMAC-SHA512 / HS512) استفاده می‌شود. درهم‌سازی گذرواژه در وضعیت فعلی MD5 است که منسوخ محسوب می‌شود و مهاجرت به bcrypt در دستور کار اصلاح (NC-003) قرار دارد. همچنین کاربر پیش‌فرض admin با MD5("admin") در startup ساخته می‌شود که در دستور کار (NC-019) است.		

11- بند 3 جدول 2-2 (رمزنگاری)

شناسه الزام	FCS_CKM.4.1	**نام الزام**	تخریب کلید رمزنگاری 1
متن الزام	در صورتی که تولید کلید رمزنگاری در محصول وجود دارد، نیاز است که تخریب کلید رمزنگاری نیز بر اساس موارد زیر صورت پذیرد. (اختیاری) - 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		
راهنمایی	-		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: خارج از دامنه محصول کلید امضای توکن از پیکربندی خارجی (environment) خوانده می‌شود؛ سازوکار تخریب کلید در محصول تعبیه نشده است (الزام اختیاری).		

12- بند 4 جدول 2-2 (رمزنگاری)

شناسه الزام	FCS_CKM.1.1 & FCS_COP.1.1(4)	**نام الزام**	تولید کلید رمزنگاری 1 و عملیات رمزنگاری 1 (4)
متن الزام	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) - الگوریتم‌های امضای دیجیتال RSA با کلیدهای رمزنگاری 2048 بیت و بزرگتر (بر اساس FIPS PUB 186-4، استاندارد امضای دیجیتال (DSS) بخش 5.5، الگوی امضای RSASSA-PSS نسخه PKCS #1 v2.1 و/یا RSASSA-PKCS1v_5؛ ISO/IEC 9796-2، الگوی امضای دیجیتال 2 و یا الگوی امضای دیجیتال 3) - الگوریتم‌های امضای دیجیتال ECDSA با کلیدهای رمزنگاری 256 بیت یا بزرگتر (بر اساس ISO/IEC 14888-3 بخش 6.4، استاندارد امضای دیجیتال (DSS) بخش 6 و پیوست D، با استفاده از منحنی P-256 یا P-384 یا P-521)		
راهنمایی	تنها الگوریتم‌هایی که در محصول وجود دارند باید انتخاب شوند.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا امضای دیجیتال بسته‌های به‌روزرسانی هنوز پیاده‌سازی نشده است (NC-015)؛ گزینه‌ای انتخاب نشده.		

13- بند 1 جدول 2-3 (شناسایی و احراز هویت)

شناسه الزام	FIA_AFL.1.1	**نام الزام**	مدیریت احرازهویت ناموفق 1
متن الزام	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. - یک عدد مثبت ثابت - یک عدد مثبت قابل تنظیم توسط مدیر		
راهنمایی	نمایش پیام کاملا یکسان برای کاربرهای تعریف‌شده و تعریف‌نشده (جلوگیری از حمله‌ی Account Harvesting) ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان تغییر پیکربندی (در صورت پشتیبانی از این ویژگی) لاگ های عملیاتی وضعیت رکورد | نوع عملیات | نام جدول | مقدار کلید | کاربر | نوع کاربر | تاریخ وقوع | زمان وقوع | آدرس ماشین | شرح عملیات | ابزارها معتبر | ویرایش | کلید های پیکر بندی سیستم | ۱۰۰۸۲ | netel | مدیر | ۱۳۹۹/۱۱/۰۵ | ۱۱:۵۳:۱۰ | ۱۹۲.۱۶۸.۳۵.۲۴۴ | تعداد مجاز برای ورود اشتباه رمز عبور از ۵ به ۳ تغییر یافت ✓ ثبت‌نشان برای هر تلاش ناموفق باید ثبت گردد. (برای تمامی نام‌های کاربری، حتما باید نام کاربری واردشده ثبت شود.) لاگ های احراز هویت وضعیت رکورد | کاربر | نوع کاربر | تاریخ وقوع | زمان وقوع | آدرس ماشین | شرح عملیات | نوع درخواست | نتیجه درخواست | ابزارها معتبر | | | ۱۳۹۹/۱۱/۰۵ | ۰۹:۵۷:۴۱ | ۱۹۲.۱۶۸.۳۵.۲۴۴ | کاربر موردنظر غیرفعال می باشد،لطفا در زمان دیگری مجددا تلاش کنید و یا جهت فعال سازی با مدیر سیستم تماس بگیرید.'noname' | ورود به سامانه | ناموفق معتبر | | | ۱۳۹۹/۱۱/۰۵ | ۰۹:۵۷:۳۹ | ۱۹۲.۱۶۸.۳۵.۲۴۴ | کاربر مورد نظر به علت تلاش غیر مجاز جهت ورود به سامانه غیر فعال شد.'noname' | ورود به سامانه | ناموفق معتبر | | | ۱۳۹۹/۱۱/۰۵ | ۰۹:۵۷:۳۷ | ۱۹۲.۱۶۸.۳۵.۲۴۴ | تلاش ناموفق جهت ورود به سامانه با نام کاربری 'noname' | ورود به سامانه | ناموفق معتبر | | | ۱۳۹۹/۱۱/۰۵ | ۰۹:۵۷:۳۵ | ۱۹۲.۱۶۸.۳۵.۲۴۴ | تلاش ناموفق جهت ورود به سامانه با نام کاربری 'noname' | ورود به سامانه | ناموفق		
نحوه‌ی دسترسی	صفحه ورود: /login؛ endpoint /users/login.		
تصویر	پس از پیاده‌سازی NC-005، تصویر پیکربندی آستانه پیوست شود.		
توضیحات	وضعیت: پیاده‌سازی نشده — بدون ادعا		

بیشتر	آستانه تلاش ناموفق و قفل حساب در وضعیت فعلی پیاده‌سازی نشده است؛ هر تلاش ناموفق ثبت‌نشان می‌شود و پیام پاسخ برای کاربر تعریف‌شده و تعریف‌نشده یکسان است (جلوگیری از Account Harvesting). پیاده‌سازی آستانه قابل تنظیم توسط مدیر همراه با قفل موقت در دستور کار برنامه‌ریزی شده است. (NC-005)

14- بند 2 جدول 2-3 (شناسایی و احراز هویت)

شناسه الزام	FIA_AFL.1.2	**نام الزام**	مدیریت احرازهویت ناموفق 2
متن الزام	محصول باید هنگامی که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد تعیین‌شده رسید، برای پیچیده‌تر کردن احراز هویت از موارد زیر استفاده نماید. - 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) - استفاده از سازوکارهایی مانند کدهای CAPTCHA، گرفتن ایمیل و ... (در قسمت «توضیحات» بیان شود) - سایر موارد		
راهنمایی	نمایش پیام کاملا یکسان برای کاربرهای تعریف‌شده و تعریف‌نشده (جلوگیری از حمله‌ی Account Harvesting) بهتر است در زمان غیرفعال‌سازی کاربر به دلیل تلاش‌های ناموفق احراز هویت، از IP-Blocking در کنار Account-blocking استفاده شود. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان تغییر پیکربندی زمان غیرفعال شدن کاربر (در صورت پشتیبانی از این ویژگی)		

لاگ های عملیاتی

وضعیت رکورد	نوع عملیات	نام جدول	مقدار کلید	کاربر	نوع کاربر	تاریخ وقوع	زمان وقوع	آدرس ماشین	شرح عملیات
معتبر	ویرایش	کلید های پیکر بندی سیستم	۱۰۰۹۳	netel	مدیر	۱۳۹۹/۱۱/۰۵	۱۱:۵۴:۰۲	۱۹۲.۱۶۸.۳۵.۲۴۴	مدت زمان فعال شدن خودکار کاربر از ۵ به ۳ تغییر یافت

✓ ثبت‌نشان قفل شدن حساب کاربر یا مسدود شدن IP یا ... (برای تمامی نام‌های کاربری، باید نام کاربر ثبت شود)

لاگ های احراز هویت

وضعیت رکورد	کاربر	نوع کاربر	تاریخ وقوع	زمان وقوع	آدرس ماشین	شرح عملیات	نوع درخواست	نتیجه درخواست
معتبر	test	کارمند	۱۳۹۹/۱۱/۰۵	۰۹:۴۸:۰۳	۱۹۲.۱۶۸.۳۵.۲۴۴	کاربر موردنظر غیرفعال می باشد.لطفا در زمان دیگری مجددا تلاش کنید و یا جهت فعال سازی با مدیر سیستم تماس بگیرید.	ورود به سامانه	ناموفق
معتبر	test	کارمند	۱۳۹۹/۱۱/۰۵	۰۹:۴۷:۵۸	۱۹۲.۱۶۸.۳۵.۲۴۴	کاربر مورد نظر به علت تلاش غیر مجاز جهت ورود به سامانه غیر فعال شد.	ورود به سامانه	ناموفق
معتبر	test	کارمند	۱۳۹۹/۱۱/۰۵	۰۹:۴۷:۵۶	۱۹۲.۱۶۸.۳۵.۲۴۴	تلاش ناموفق جهت ورود به سامانه با نام کاربری 'test'	ورود به سامانه	ناموفق
معتبر	test	کارمند	۱۳۹۹/۱۱/۰۵	۰۹:۴۷:۵۳	۱۹۲.۱۶۸.۳۵.۲۴۴	تلاش ناموفق جهت ورود به سامانه با نام کاربری 'test'	ورود به سامانه	ناموفق

✓ ثبت‌نشان فعال‌سازی توسط مدیر (در صورت پشتیبانی از این ویژگی)

وضعیت رکورد	نوع عملیات	نام جدول	مقدار کلید	کاربر	نوع کاربر	تاریخ وقوع	زمان وقوع	آدرس ماشین	شرح عملیات
معتبر	ویرایش	کاربران	۱۷۴۹	netel	مدیر	۱۳۹۹/۱۱/۰۵	۰۹:۵۶:۰۹	۱۹۲.۱۶۸.۳۵.۲۴۴	فعالسازی کاربر مسدود شده با موفقیت انجام شد test

✓ ثبت‌نشان ارسال پیامک، ایمیل یا ... (در صورت پشتیبانی از این ویژگی)
✓ ثبت‌نشان ورود موفقیت‌آمیز کاربر

نحوه‌ی دسترسی	-
تصویر	پس از پیاده‌سازی، تصویر رفتار قفل حساب پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا وابسته به الزام قبل؛ پس از افزودن آستانه تلاش ناموفق، قفل موقت/غیرفعال‌سازی حساب و ثبت‌نشان آن اضافه می‌شود (NC-005).

15- بند 3 جدول 2-3 (شناسایی و احراز هویت)

شناسه الزام	FIA_ATD.1.1	**نام الزام**	تعریف مشخصات کاربر 1
متن الزام	محصول باید برای هر کاربر، ویژگی‌های امنیتی را که شامل حداقل اطلاعات کاربری لازم برای شناسایی و احراز هویت می‌باشند، نگهداری نماید. - شناسه کاربر - روش احراز هویت مورد استفاده - داده احراز هویت - وضعیت حساب کاربری (فعال، غیرفعال، مسدود شده و غیره) - نقش کاربر - سایر موارد		
راهنمایی	1 کاربر «غیرفعال» نباید بتواند وارد محصول گردد. (اگر محصول قرار است به کاربر اعلام کند که «غیرفعال» است، حتما باید پس از احراز هویت این پیام به کاربر نمایش داده شود.) 2 کاربر بدون سطح دسترسی [در صورتی که چنین شرایطی ممکن است]، نباید بتواند وارد محصول شود. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان تلاش کاربر غیرفعال ✓ ثبت‌نشان تلاش ناموفق ورود برای کاربر بدون سطح دسترسی [در صورتی پشتیبانی از این شرایط]		
نحوه‌ی دسترسی	صفحه کاربران (/users/index) — جداول tbl_pline_users و tbl_user_access.		
تصویر	تصویر فرم ایجاد/ویرایش کاربر و بخش دسترسی‌ها پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی شده ویژگی‌های امنیتی هر کاربر: شناسه یکتا، نام کاربری، نام کامل، نقش‌ها (ADMIN/CLIENT)، وضعیت فعال/غیرفعال و مجموعه مجوزهای منو/عملیات.		

16- بند 4 جدول 2-3 (شناسایی و احراز هویت)

شناسه الزام	FIA_PMG_EXT.1.1	**نام الزام**	مدیریت کلمه عبور
متن الزام	محصول باید قابلیت مدیریت گذرواژه را فراهم آورد. - استفاده از حروف کوچک - استفاده از حروف بزرگ - استفاده از اعداد - استفاده از کاراکترهای خاص («@»، «#»، «$»، «٪»، «^»، «!»، «&»، «*»، «(» , «)» و ...) - حداقل طول 8 یا بیشتر (قابل تنظیم) - سایر موارد		
راهنمایی	1 در پیکربندی «کمینه‌ی طول گذرواژه»، نباید بتوان عددی کمتر از 8 انتخاب نمود. 2 باید از انتخاب گذرواژه‌های کمتر از «طول کمینه‌ی گذرواژه» جلوگیری شود. 3 باید از انتخاب گذرواژه‌هایی با پیچیدگی کمتر از «پیچیدگی گذرواژه» جلوگیری شود. 4 اگر امکان «بازیابی گذرواژه» در محصول وجود دارد، باید پیچیدگی مناسب داشته باشد و کاربر به محض ورود مجبور به تغییر آن باشد. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان تغییر پیکربندی «کمینه‌ی طول گذرواژه» یا «پیچیدگی گذرواژه» (محصول می‌تواند این دو ویژگی را با عنوانی مانند «ویرایش قوانین انتخاب گذرواژه» یا عبارت‌های گویا و مشابهی ثبت نماید.)		

	لاگ های عملیاتی وضعیت رکورد | نوع عملیات | نام جدول | مقدار کلید | کاربر | نوع کاربر | تاریخ وقوع | زمان وقوع | آدرس ماشین | شرح عملیات معتبر | ویرایش | کلید های پیکر بندی سیستم | ۱۰۰۸۰ | netel | مدیر | ۱۳۹۹/۱۱/۰۵ | ۱۱:۵۵:۳۳ | ۱۹۲.۱۶۸.۳۵.۲۴۴ | حداقل تعداد کاراکتر های رمز عبور از ۹ به ۸ تغییر یافت معتبر | ویرایش | کلید های پیکر بندی سیستم | ۱۰۰۸۱ | netel | مدیر | ۱۳۹۹/۱۱/۰۵ | ۱۱:۵۵:۲۷ | ۱۹۲.۱۶۸.۳۵.۲۴۴ | کاراکترهای مورد نیاز برای رمز عبور از @$%$&! به @$%$& تغییر یافت ✓ ثبت‌نشان تغییر گذرواژه‌ی کاربر (توسط خود کاربر یا توسط کاربر مجاز دیگر) ✓ ثبت علت اجبار کاربر به تغییر گذرواژه [در صورتی که کاربر به دلیل ویژگی‌های خاص محصول (مانند «تاریخ انقضای گذرواژه»، «اعمال پیچیدگی برای گذرواژه‌های پیشین» یا ...) مجبور به تغییر گذرواژه می‌شود.]
نحوه‌ی دسترسی	فرم‌های ایجاد کاربر و تغییر گذرواژه (/change-password/index).
تصویر	پس از پیاده‌سازی NC-004، تصویر پیکربندی سیاست گذرواژه پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا سیاست پیچیدگی گذرواژه در وضعیت فعلی فقط در رابط کاربری (حداقل 6 کاراکتر) بررسی می‌شود و در سمت سرور enforce نمی‌گردد. پیاده‌سازی سیاست مرکزی قابل تنظیم توسط مدیر (حداقل طول، حروف بزرگ/کوچک، عدد، کاراکتر خاص) در دستور کار (NC-004) است.

17- بند 5 جدول 2-3 (شناسایی و احراز هویت)

شناسه الزام	FIA_UAU.1.1 & FIA_UAU.1.2 FIA_UID.1.1 & FIA_UID.1.2	**نام الزام**	احراز هویت کاربر 1 و 2 و شناسایی کاربر 1 و 2
متن الزام	محصول باید پیش از احراز هویت موفق یک کاربر، تنها اجازه انجام اقدامات محدودی را فراهم نماید. - مشاهده راهنمای نحوه ورود به سیستم - بازیابی گذرواژه - هیچ اقدامی - سایر موارد		
راهنمایی	در «صفحه‌ی ورود»، تنها باید ویژگی‌های مشخص‌شده، مشاهده شوند. در صورتی پشتیبانی از «بازیابی گذرواژه»، توجه نمایید که باید پیام کاملا یکسانی برای کاربرهای تعریف‌شده و تعریف‌نشده نمایش داده شود. (جلوگیری از حمله‌ی Account Harvesting) ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان فراموشی گذرواژه‌ی کاربر [در صورت پشتیبانی از این ویژگی] معتبر | ویرایش | کاربران | ۱۷۴۸ | ۱۳۹۹/۱۱/۰۵ | ۱۰:۳۳:۰۴ | ۱۹۲.۱۶۸.۳۵.۲۴۴ | بازیابی رمز عبور کاربر netel با موفقیت انجام شد معتبر | افزودن | کدهای پیامکی | ۰ | ۱۳۹۹/۱۱/۰۵ | ۱۰:۳۲:۳۷ | ۱۹۲.۱۶۸.۳۵.۲۴۴ | 'PhoneNumber: [redacted] Code: '۸۳۴۴۰' ExpireDate: '۱/۲۵/۲۰۲۱ ۱۰:۳۲:۳۷ AM ✓ ثبت‌نشان ثبت‌نام کاربر [در صورت پشتیبانی از این ویژگی]		
نحوه‌ی دسترسی	صفحه ورود (/login) — endpoint /users/login؛ احراز هویت درخواست‌ها: فیلتر jwtAuthorizationCheck.		
تصویر	تصویر صفحه ورود و پاسخ 401 برای درخواست بدون توکن پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی شده شناسایی و احراز هویت پیش از هر عملیات مجاز انجام می‌شود؛ همه مسیرها به‌جز مسیرهای عمومی (ورود، دریافت نسخه) نیازمند توکن معتبر (هدر Authorization: Bearer) هستند.		

18- بند 6 جدول 2-3 (شناسایی و احراز هویت)

شناسه الزام	FIA_UAU.5.1 & FIA_UAU.5.2	**نام الزام**	سازوکار احراز هویت چندگانه 1 و 2

متن الزام	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). - نام کاربری و گذرواژه - امضای دیجیتال - سامانه‌های احراز هویت مرکزی (مانند Active Directory و ...) - OTP یا توکن - احراز هویت دو فاکتوری - سایر موارد
راهنمایی	باید بتوان با تمامی سازوکارهای مشخص‌شده وارد محصول شد. ارتباط با سرور ایمیل، پنل پیامکی یا سرور احراز هویت باید با استفاده از یک پروتکل امن برقرار شود. پروتکل‌های احراز هویت مانند Kerberos، LDAP و ... نیز باید بر بستر TLS ارائه شوند. در صورتی که سامانه از احراز هویت دو مرحله‌ای استفاده می‌کند، در مرحله دوم احراز هویت، با اشتباه وارد کردن شناسه مورد نظر، یکی از موارد زیر باید اتفاق بیفتد: ا) کد کپچا فعال شود. ب) کاربر به مرحله اول احراز هویت هدایت شود. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان سازوکار احراز هویت مورد استفاده (در صورتی که از سازوکارهای مختلف به صورت موازی استفاده می‌شود. ✓ ثبت‌نشان ارسال ایمیل یا پیامک [در صورت پشتیبانی از این ویژگی]
نحوه‌ی دسترسی	صفحه ورود (/login).
تصویر	تصویر ورود موفق و کد تولید توکن پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی شده سازوکار احراز هویت: نام کاربری/گذرواژه (انتخاب شده). پس از ورود موفق، توکن JWT (HS512) با تاریخ انقضا ۳۱ روزه تولید و در سرور ذخیره می‌شود و در درخواست‌های بعدی به‌صورت Bearer ارسال می‌گردد. انقضای طولانی‌تر از استاندارد (۳۱ روز) در دستور کار (NC-020) برای کاهش به ۲ ساعت و پیاده‌سازی refresh token است. محصول به سامانه احراز هویت مرکزی، OTP یا ایمیل/پیامک متصل نیست.

معتبر	مشاهده	لاگ های احراز هویت		netel		مدیر	۱۳۹۹/۱۱/۰۵	۱۱:۳۸:۰۵	۱۹۲.۱۶۸.۳۵.۲۴۴	مشاهده اطلاعات ورود کاربران به سیستم
معتبر	افزودن	کدهای پیامکی	۰				۱۳۹۹/۱۱/۰۵	۱۱:۳۶:۵۹	۱۹۲.۱۶۸.۳۵.۲۴۴	'PhoneNumber: [redacted] Code: '۷۷۱۰۶' ExpireDate: '۱/۲۵/۲۰۲۱ ۱۱:۳۶:۵۹ AM

✓ ثبت‌نشان تعریف، ویرایش یا حذف یک سرور احراز هویت [در صورت پشتیبانی از این ویژگی]
✓ ثبت‌نشان پیکربندی سازوکار احراز هویت برای کاربر یا به صورت عمومی

19- بند 7 جدول 2-3 (شناسایی و احراز هویت)

شناسه الزام	FIA_USB.1.1	**نام الزام**	انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر 1
متن الزام	محصول باید برای هر کاربر فعال، ویژگی‌های امنیتی را نگهداری نماید. - 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		
راهنمایی	1 برای کاربرها باید این ویژگی‌ها را مشاهده نمود. 2 اگر هر یک از ویژگی‌های تعیین‌شده در این الزام وارد نشده باشد، نباید بتوان کاربر را ایجاد یا ویرایش نمود. ثبت‌نشان‌های مورد نیاز:		

	✓ ثبت‌نشان ایجاد کاربر ✓ ثبت‌نشان ویرایش کاربر ✓ ثبت‌نشان تلاش ناموفق برای ایجاد یا ویرایش کاربر ✓ ثبت‌نشان تغییر در ویژگی‌های امنیتی کاربر
نحوه‌ی دسترسی	صفحه کاربران و صفحه دسترسی‌ها؛ گزارش لاگ برای پیشینه احراز هویت.
تصویر	تصویر مشخصات کاربر و پیشینه ورود او پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل ویژگی‌های امنیتی نگهداری‌شده برای هر کاربر فعال: شناسه، نقش‌ها و مجموعه دسترسی منو/عملیات. پیشینه احراز هویت از طریق گزارش لاگ قابل مشاهده است. نمایش جزئیات کامل واسط کلاینت در حال بررسی است.

20- بند 8 جدول 2-3 (شناسایی و احراز هویت)

شناسه الزام	FIA_USB.1.2	**نام الزام**	انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر 2
متن الزام	محصول باید در زمان اتصال اولیه کاربر یا همان زمان برقراری نشست توسط کاربر، موارد زیر را اجرا نماید. - 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.) - بروزرسانی اطلاعات پیشینه احراز هویت - سایر موارد		
راهنمایی	- ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان جلوگیری از آغاز نشست جدید به علت رسیدن به حد آستانه [در صورت پشتیبانی از این ویژگی] ✓ ثبت‌نشان خاتمه به نشست قبلی به دلیل ایجاد نشست جدید [در صورت پشتیبانی از این ویژگی] ✓ ثبت‌نشان ورود موفقیت‌آمیز کاربر		
نحوه‌ی دسترسی	فرآیند ورود (/users/login).		
تصویر	تصویر رفتار ورود مجدد و ابطال نشست قبلی (کد) پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی شده با هر ورود موفق، توکن جدید تولید و جایگزین توکن قبلی در پایگاه‌داده می‌شود؛ در نتیجه نشست قبلی اعتبار خود را از دست می‌دهد و ثبت‌نشان ورود موفق (پیشینه احراز هویت) به‌روزرسانی می‌شود.		

21- بند 9 جدول 2-3 (شناسایی و احراز هویت)

شناسه الزام	FIA_USB.1.3	**نام الزام**	انقیاد مشخصه‌های امنیتی کاربر با موجودیت فعال متناظر 3
متن الزام	محصول باید بر روی تغییرات ویژگی‌های امنیتی کاربر فعال قوانینی را اعمال نماید. - غیرمجاز بودن هرگونه تغییر در طول نشست فعال - سایر موارد		
راهنمایی	-		

	ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان تغییر در ویژگی‌های امنیتی کاربر (شامل کاربر تغییردهنده و کاربری که اطلاعاتش تغییر یافته است) ✓ ثبت‌نشان خاتمه به نشست کاربر به دلیل ویرایش ویژگی‌های امنیتی توسط مدیر [در صورت پشتیبانی از این ویژگی] ✓ ثبت‌نشان تلاش ناموفق مدیر برای ویرایش کاربر فعال [در صورت پشتیبانی از این ویژگی]
نحوه‌ی دسترسی	صفحه کاربران (ویرایش توسط مدیر).
تصویر	تصویر ثبت‌نشان تغییر ویژگی‌های امنیتی پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل تغییرات ویژگی‌های امنیتی کاربر توسط مدیر انجام و ثبت‌نشان می‌شود. قاعده صریح «غیرمجاز بودن تغییر در طول نشست فعال کاربر» هنوز اعمال نمی‌شود و در حال بررسی است.

22- بند 1 جدول 2-4 (حفاظت از داده‌ی کاربری)

شناسه الزام	FDP_ACC.1.1	**نام الزام**	خط‌مشی کنترل دسترسی 1
متن الزام	محصول باید برای موجودیت‌ها و عملیات، خط‌مشی‌های کنترل دسترسی اعمال نماید. • موجودیت‌های فعال - مدیر سیستم - کاربر عادی - سایر موارد • موجودیت‌های غیرفعال - سوابق، مستندات و فراداده - داده متعلق به کاربران - داده احراز هویت - سایر موارد • عملیات - ایجاد موجودیت غیرفعال جدید - حذف موجودیت غیرفعال - تغییر دسترسی‌ها به موجودیت غیرفعال - عملیات بر روی فراداده وابسته به موجودیت غیرفعال - سایر موارد			
راهنمایی	توجه شود که هیچ الزامی مبنی بر وجود «گروه کاربری» یا «نقش» وجود ندارد، بلکه وجود «سطح دسترسی» کافی است. یعنی لزومی ندارد برای تعیین سطح دسترسی برای یک کاربر حتما گروه یا نقشی تعریف شود و سطح دسترسی برای آن تعریف شود. اگر بتوان دسترسی‌ها را به صورت فردی نیز تعریف کرد، کفایت می‌کند. نحوه‌ی تعیین سطوح دسترسی مختلف به‌طور کامل شرح داده شود. شامل اینکه 1) آیا سطوح دسترسی به صورت فردی تعیین می‌شود یا امکان تعریف نقش یا گروه کاربری وجود دارد. 2) همچنین اگر امکان تعیین سطوح دسترسی خاص برای کاربرهای عضو گروه نیز وجود دارد، مشخص گردد. تصویری از کلیات بخش «سطوح دسترسی» یا بخشی از جزئیات آن. در صورتی که تعیین سطوح دسترسی کاربر، با استفاده از تعریف نقش صورت می‌گیرد، نحوه‌ی تخصیص و نگاشت کاربرها و نقش‌ها نیز شرح داده شود.		
نحوه‌ی دسترسی	کنترل دسترسی منو/عملیات: صفحات کاربران ← دسترسی‌ها؛ جدول tbl_user_access و فیلتر jwtAuthorizationCheck.		
تصویر	تصویر صفحه تنظیم دسترسی کاربران پیوست شود.		

توضیحات بیشتر	وضعیت: پیاده‌سازی شده خط‌مشی کنترل دسترسی: هر منو/عملیات (خواندن، ایجاد، ویرایش، حذف) شناسه یکتای مجوز (Access Code) دارد؛ درخواست‌ها هدر Mid را حمل می‌کنند و فیلتر بک‌اند مجوز منو/عملیات کاربر را پیش از اجرا بررسی می‌کند. مشمولان: همه منوها و endpointهای مدیریتی.

23- بند 2 جدول 2-4 (حفاظت از داده‌ی کاربری)

شناسه الزام	FDP_ACF.1.1	**نام الزام**	عملیات کنترل دسترسی 1
متن الزام	محصول باید بر اساس ویژگی‌های زیر، برای موجودیت‌های غیرفعال خط‌مشی‌های کنترل دسترسی اعمال نماید. - نقش‌ها و مجوزهای کاربر مجاز - اطلاعات نشست کاربر و پارامترهایی که با درخواست فرستاده می‌شوند. - سایر موارد		
راهنمایی	- ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان دسترسی غیرمجاز کاربر (با ذکر محل دسترسی)		
نحوه‌ی دسترسی	همان ساختار مجوزهای منو/عملیات (tbl_user_access) و نقش‌های ADMIN/CLIENT.		
تصویر	تصویر پاسخ رد عملیات بدون مجوز پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی شده مجموعه قواعد امنیتی بر مبنای نقش و مجوز منو اعمال می‌شود: عملیات بدون مجوز با کد 401/404 رد می‌شود.		

24- بند 3 جدول 2-4 (حفاظت از داده‌ی کاربری)

شناسه الزام	FDP_ACF.1.2 & FDP_ACF.1.3	**نام الزام**	عملیات کنترل دسترسی 2 و 3
متن الزام	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 فهرست 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.)		
راهنمایی	در این الزام، وجود «سطح دسترسی» و «صحت عملکرد» آن مورد نظر است. اگر شرایط خاصی در تعیین و تعریف سطوح دسترسی وجود دارد، در این الزام تشریح شوند.		
نحوه‌ی دسترسی	صفحه کاربران ← دسترسی‌ها.		
تصویر	تصویر تخصیص مجوز پیش‌فرض پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی شده قواعد به‌ازای هر کاربر توسط مدیر تعیین می‌شود؛ توزیع پیش‌فرض بر اساس نقش (ADMIN/CLIENT) و مجوزهای منو.		

25- بند 4 جدول 2-4 (حفاظت از داده‌ی کاربری)

شناسه الزام	FDP_ACF.1.4	**نام الزام**	عملیات کنترل دسترسی 4
متن الزام	محصول باید بر اساس قوانینی، از دسترسی موجودیت فعال به موجودیت غیرفعال جلوگیری نماید. - عبور تعداد نشست آغاز شده با نام کاربری مشابه از مقدار آستانه از پیش تعریف‌شده - سایر موارد		
راهنمایی	-		
نحوه‌ی دسترسی	صفحه کاربران ← دسترسی‌ها.		
تصویر	تصویر ثبت‌نمان رد عملیات پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی شده قواعد: مجوز برای هر منو/عملیات لازم است؛ درخواست فاقد مجوز رد و در لاگ ثبت می‌شود.		

26- بند 5 جدول 2-4 (حفاظت از داده‌ی کاربری)

شناسه الزام	FDP_RIP.2.1	**نام الزام**	حفاظت کامل از اطلاعات باقی‌مانده در منابع 1
متن الزام	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.		
راهنمایی	1 شناسه نشست، یک شناسه یکتا می‌باشد که به هر نشست تعلق می‌گیرد و با خروج کاربر از نشست باید منقضی و مجدد مقداردهی شود. همچنین در صورتی که سامانه از احراز هویت دومرحله‌ای استفاده می‌کند در مورد شناسه نشست یکی از موارد زیر باید اجرا شود: ا) در هر مرحله از احراز هویت شناسه قبلی منقضی شده و مقدار جدید تولید و ارسال شود. ب) تا پایان موفقیت آمیز مرحله دوم احراز هویت، شناسه غیرمعتبر باشد. 2 با بستن مرورگر باید نشست کاربر خاتمه یافته و شناسه نشست منقضی شود. 3 ساختار تولید Session-ID را تشریح نمایید. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشانی با محتوایی مانند «حذف اطلاعات منابع هنگام تخصیص یا آزادسازی» [در صورت پشتیبانی از این ویژگی]		
نحوه‌ی دسترسی	عملیات حذف موجودیت‌ها (کاربران، SIP، صف و ...) از طریق UI و endpointهای DELETE.		
تصویر	تصویر ثبت‌نمان عملیات حذف پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل حذف موجودیت‌ها از پایگاه‌داده انجام می‌شود. تضمین صریح صفرسازی بلوک‌های حافظه ارائه نمی‌شود؛ زمان‌بندی اجرای حفاظت از اطلاعات باقی‌مانده در حال تعیین سیاست است.		

27- بند 6 جدول 2-4 (حفاظت از داده‌ی کاربری)

شناسه الزام	FDP_ITC.2.1 & FDP_ITC.2.2 FDP_ITC.2.4 & FDP_ITC.2.5	**نام الزام**	ورود داده کاربری به محصول با مشخصه امنیتی 1 و 2 و 4 و 5
متن الزام	محصول باید هنگام دریافت داده کاربری خط‌مشی کنترل دسترسی را اعمال و برای این کار از ویژگی‌های امنیتی مرتبط با داده کاربری استفاده کند. - نوع داده - حجم و اندازه		

	- فرمت - تعداد دفعات Import - سایر موارد
راهنمایی	کاربر مجاز باید بتواند داده‌هایی با مشخصات امنیتی مجاز (حجم، پسوند یا ...) به محصول وارد نماید. کاربر غیرمجاز نباید بتواند هیچ داده‌ای را وارد محصول نماید. کاربر مجاز نباید بتواند داده‌هایی با مشخصات امنیتی غیرمجاز را وارد محصول نماید. (از انتخاب، دریافت یا ... باید جلوگیری شود.) رویکرد محصول در جلوگیری از داده‌های غیرمجاز نیز باید در گزارش ذکر شود. اطمینان از وجود محدودیت‌هایی برای ورود اطلاعات در بخش‌های مختلف «ورود اطلاعات» (Input Validation) تمامی ورودی‌ها باید از لحاظ ساختار، سایز، فرمت و ...، هم در سمت کاربر و هم در سمت سرور بررسی شوند. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان ورود موفقیت‌آمیز داده به محصول (حاصل ورود داده مجاز توسط کاربر مجاز) ✓ ثبت‌نشان ورود ناموفق داده به محصول (حاصل ورود داده غیرمجاز) ✓ ثبت‌نشان ورود ناموفق داده به محصول (حاصل ورود داده توسط کاربر غیرمجاز)
نحوه‌ی دسترسی	صفحه پشتیبان‌گیری (Backup) و صفحات وارد کردن تنظیمات (Import).
تصویر	تصویر صفحه پشتیبان‌گیری/بارگذاری پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی شده داده واردشده: فایل پشتیبان پایگاه‌داده و فایل‌های تنظیمات/صدا. اقدامات مرتبط: اعتبارسنجی نوع و اندازه فایل در آپلود (سقف پیکربندی‌شده 1024MB).

28- بند 7 جدول 2-4 (حفاظت از داده‌ی کاربری)

شناسه الزام	FDP_ITC.2.3	**نام الزام**	ورود داده کاربری به محصول با مشخصه امنیتی 3
متن الزام	محصول باید از یک 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.		
راهنمایی	-		
نحوه‌ی دسترسی	همان صفحات آپلود/Import.		
تصویر	تصویر پیام رد فایل نامعتبر پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل فعالیت‌های مرتبط: اعتبارسنجی نوع و اندازه فایل انجام می‌شود؛ اعتبارسنجی معنایی کامل محتوای فایل‌های ورودی (مانند امضای دیجیتال) در دستور کار (NC-015) است.		

29- بند 8 جدول 2-4 (حفاظت از داده‌ی کاربری)

شناسه الزام	FDP_ETC.2.1 & FDP_ETC.2.2 & FDP_ETC.2.3	**نام الزام**	خروج داده کاربری به محصول با مشخصه امنیتی 1 و 2 و 3
متن الزام	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. - نوع داده		

	- حجم و اندازه - فرمت - سایر موارد
راهنمایی	کاربر مجاز باید بتواند داده‌هایی با مشخصات امنیتی مجاز (حجم، پسوند یا ...) را دریافت نماید. کاربر مجاز نباید بتواند داده‌هایی با مشخصات امنیتی غیرمجاز را دریافت نماید. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان خروج موفقیت‌آمیز داده از محصول (حاصل دریافت داده مجاز توسط کاربر مجاز) ✓ ثبت‌نشان خروج ناموفق داده از محصول (حاصل دریافت داده غیرمجاز)
نحوه‌ی دسترسی	خروجی‌های محصول: فایل‌های پشتیبان، خروجی CSV گزارش‌ها (مانند /sip-users/export)، فایل‌های ضبط مکالمات و فکس (صفحه دانلود).
تصویر	تصویر خروجی CSV و صفحه پشتیبان‌گیری پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی شده خروج داده کاربر از مسیرهای کنترل‌شده انجام می‌شود؛ تولید پشتیبان/CSV نیازمند احراز هویت و مجوز منو است.

30- بند 9 جدول 2-4 (حفاظت از داده‌ی کاربری)

شناسه الزام	FDP_ETC.2.4	**نام الزام**	خروج داده کاربری به محصول با مشخصه امنیتی 4
متن الزام	محصول باید هنگام خروج داده کاربری به خارج از محصول، قوانینی را اعمال نماید. - 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		
راهنمایی	کاربر غیرمجاز نباید بتواند هیچ داده‌ای را دریافت نماید. درصورتی که کاربر غیرمجاز امکان مشاهده‌ی بخش‌های مربوط به «خروجی داده» را ندارد، در گزارش ذکر شود. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان خروج ناموفق داده از محصول (حاصل دریافت داده توسط کاربر غیرمجاز)		
نحوه‌ی دسترسی	همان مسیرهای خروجی (پشتیبان، CSV، ضبط مکالمات).		
تصویر	تصویر پیکربندی مسیرهای دانلود پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل خروج داده با مجوز کنترل می‌شود؛ مسیرهای دانلود عمومی (/download/, /tmp/) در حال بازبینی و محدودسازی هستند (NC-010).		

31- بند 10 جدول 2-4 (حفاظت از داده‌ی کاربری)

شناسه الزام	FDP_SDI.2.1	**نام الزام**	صحت داده کاربری ذخیره‌شده 2
متن الزام	محصول باید تغییر غیرمجاز را در داده کاربری حساس ذخیره‌شده در محصول تشخیص دهد. - مقدار درهم‌سازی‌شده داده‌های کاربری ذخیره‌شده، نگهداری می‌شود. - سایر موارد		
راهنمایی	با توجه به تعریف نمایه حفاظتی از «درهم‌سازی/رمزنگاری داده حساس»، «مثالی از داده حساس		

	کلمه‌های عبور یا رکوردهای محرمانه می‌باشد.» گذرواژه‌ها باید به صورت درهم‌سازی‌شده (با استفاده از الگوریتم‌های مجاز ارائه‌شده در آزمون 10 (بند 2 جدول 2-2 (رمزنگاری))) نگهداری شوند. (معمولا پایگاه‌های داده به صورت پیش‌فرض این امکان را فراهم می‌کنند.) با دستکاری اطلاعات - و معمولا تلاش برای دسترسی به آنها - باید تولید ثبت‌نشان «خطای صحت داده» بررسی شود. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان نامعتبر بودن داده
نحوه‌ی دسترسی	ذخیره‌سازی داده در PostgreSQL؛ یکپارچگی با قیود پایگاه‌داده.
تصویر	بدون تصویر — شواهد پیکربندی پایگاه‌داده پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل یکپارچگی داده با قیود سطح پایگاه‌داده (کلید اصلی/خارجی) و اعتبارسنجی ورودی حفاظت می‌شود. سازوکار تشخیص تغییر ناخواسته (checksum/هش) برای رکوردها ارائه نمی‌شود.

32- بند 11 جدول 2-4 (حفاظت از داده‌ی کاربری)

شناسه الزام	FDP_SDI.2.2	**نام الزام**	صحت داده کاربری ذخیره‌شده 3
متن الزام	محصول باید در صورت تشخیص خطای صحت در داده‌ها، اقدامات مقابله‌ای زیر را انجام دهد. - ایجاد هشدار/اخطار برای نقش‌های مجاز - تصحیح داده بر اساس مقادیر قبل - سایر موارد		
راهنمایی	در صورتی که محصول پیام یا هشداری به کاربر مجاز ارسال می‌کند. بهتر است مشخص باشد که «خطای صحت داده» برای کدام داده رخ داده است. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان ارسال پیام به کاربر مجاز [در صورت پشتیبانی از این ویژگی] ✓ ثبت‌نشان اصلاح داده [در صورت پشتیبانی از این ویژگی]		
نحوه‌ی دسترسی	پاسخ‌های API در صورت خطای اعتبارسنجی.		
تصویر	تصویر پیام خطای اعتبارسنجی پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل در صورت تشخیص خطای صحت داده (نقض قیود یا اعتبارسنجی ورودی)، عملیات رد و پیام خطا به کاربر بازگردانده می‌شود؛ رفتار پیش‌فرض قابل پیکربندی نیست.		

33- بند 1 جدول 2-5 (مدیریت امنیت)

شناسه الزام	FMT_MOF.1.1 & FMT_MSA.3.1	**نام الزام**	مدیریت کارکرد در محصول 1 و مقداردهی اولیه مشخصه‌ها 1
متن الزام	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. - تعیین و تغییر رفتار - غیرفعال نمودن - فعال نمودن		

	- سایر موارد
راهنمایی	کارکردهای مدیریتی محصول و نیز نحوه‌ی انجام هر یک از موارد انتخاب شده روی آن‌ها را تشریح نمایید. توجه شود که نیازی نیست تمامی عملیات برای تمامی توابع قابل اجرا باشند. بنابراین تا حد امکان مشخص شود که انجام چه عملیاتی روی چه تابعی امکان‌پذیر است. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان فعال کردن توابع امنیتی (با ذکر نام تابع) ✓ ثبت‌نشان غیرفعال کردن توابع امنیتی (با ذکر نام تابع) ✓ ثبت‌نشان ویرایش کردن (تغییر رفتار) توابع امنیتی (با ذکر نام تابع)
نحوه‌ی دسترسی	صفحات تنظیمات سیستم و اعمال تنظیمات (Apply).
تصویر	تصویر منوی تنظیمات مخصوص مدیر پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی شده انجام/لغو/اصلاح عملیات: مدیریت توابع امنیتی (لاگ، احراز هویت، مجوزها) مختص نقش ADMIN است؛ تغییرات با ثبت‌نمان همراه است.

34- بند 2 جدول 2-5 (مدیریت امنیت)

شناسه الزام	FMT_MSA.1.1	**نام الزام**	مدیریت مشخصه‌های امنیتی 1
متن الزام	محصول باید با اعمال خط‌مشی کنترل دسترسی، امکان تغییر پیش‌فرض و عملیات زیر را بر روی ویژگی‌های امنیتی الزام 7 از رده (Class) شناسایی و احراز هویت، به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید. - پرس‌وجو - تغییر - حذف - تغییر پیش‌فرض - سایر موارد		
راهنمایی	باید توانایی انجام عملیات مشخص‌شده، روی «ویژگی‌های امنیتی» وجود داشته باشد. توجه شود که نیازی نیست تمامی عملیات برای تمامی ویژگی‌های قابل اجرا باشند. بنابراین تا حد امکان مشخص شود که انجام چه عملیاتی روی چه مشخصه‌ای امکان‌پذیر است. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان ویرایش (تغییر) ویژگی‌های امنیتی کاربر ✓ ثبت‌نشان حذف ویژگی‌های امنیتی کاربر		
نحوه‌ی دسترسی	صفحه کاربران ← دسترسی‌ها.		
تصویر	تصویر ویرایش مجوزهای نقش پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی شده مقادیر پیش‌فرض مجوزها برای نقش‌ها توسط مدیر قابل تعیین و تغییر است.		

35- بند 3 جدول 2-5 (مدیریت امنیت)

شناسه الزام	FMT_MSA.3.2 & FMT_MTD.1.1(1) & FMT_MTD.1.1(2)	**نام الزام**	مقداردهی اولیه مشخصه‌ها 2 و مدیریت داده محصول 1 - مدیر سیستم و مدیریت داده محصول 1 - کاربر عادی، واردکننده داده

متن الزام	محصول باید برای داده‌های محصول، امکان کارکردهای زیر را به مدیر سیستم و هر کاربری که مجوز لازم را دارد، محدود نماید. - تغییر پیش‌فرض - حذف نمودن - پرس‌وجو - مقداردهی - ایجاد - مشاهده - سایر موارد
راهنمایی	برای موجودیت‌های غیرفعال، باید عملیات مشخص‌شده قابل اجرا باشند. برای نمونه، بتوان در ثبت‌نشان‌ها، جستجو نمود، یا داده‌ای را حذف کرد. توجه شود که نیازی نیست تمامی عملیات برای تمامی داده‌ها قابل اجرا باشند. بنابراین تا حد امکان مشخص شود که انجام چه عملیاتی روی چه موجودیتی امکان‌پذیر است. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان حذف موجودیت غیرفعال ✓ ثبت‌نشان ویرایش موجودیت غیرفعال ✓ ثبت‌نشان مشاهده موجودیت غیرفعال (برای موجودیت‌های غیرفعال حساس، مانند رویدادهای ممیزی)
نحوه‌ی دسترسی	صفحات مدیریت داده (کاربران، SIP، صف، IVR و ...) و تغییر گذرواژه (/change-password/index).
تصویر	تصویر فرم تغییر گذرواژه پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی شده مدیر یا کاربر مربوطه می‌تواند داده‌های احراز هویت (گذرواژه) را تغییر دهد؛ تغییر گذرواژه با ثبت‌نمان همراه است.

36- بند 4 جدول 2-5 (مدیریت امنیت)

شناسه الزام	FMT_SMF.1.1	**نام الزام**	کارکردهای مدیریتی محصول 1
متن الزام	محصول باید توانایی انجام کارکردهای زیر را داشته باشد. - 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 یک عملیات از پیش تعیین‌شده پس از تشخیص یک خطای صحت داده که می‌تواند قابل پیکربندی نیز باشد. - 1. مدیریت حد آستانه برای تلاش‌های ناموفق 2. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد. - مدیریت معیارها برای تنظیم گذرواژه‌ها - 1. مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مربوطه 2. مدیریت یکسری عملیاتی که قبل از احراز شدن هویت کاربر انجام می‌شوند. - 1. مدیریت سازوکارهای احراز هویت 2. 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 - 1. تعیین زمان غیرفعال بودن برای یک کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد. 2. تعیین زمان پیش‌فرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد.
راهنمایی	در این الزام توانایی مدیریت کارکردهای مختلف بررسی می‌شود. محل هر کارکرد نیز زیر آن درج شده است تا بتوانید درک بهتری از آن داشته باشید. توجه شود که علاوه بر توانایی مدیریت هر کاربرد، برای تغییرات آن باید «ثبت‌نشان» تولید شود. ▪ پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات ثبت‌نشان‌ها ✓ بند 1 جدول 2-4 (حفاظت از داده‌ی کاربری) ▪ پشتیبانی از مجوزهای مشاهده/ویرایش ثبت‌نشان‌ها ✓ بند 3 جدول 2-1 (ممیزی امنیت (Log) ▪ پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ثبت‌نشان‌ها ✓ بند 7 جدول 2-1 (ممیزی امنیت (Log) ✓ بند 8 جدول 2-1 (ممیزی امنیت (Log) ▪ مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول ✓ بند 2 جدول 2-4 (حفاظت از داده کاربری) ▪ انتخاب زمان اجرای حفاظت از اطلاعات باقیمانده که می‌تواند در محصول قابل پیکربندی باشد. (برای مثال، زمان تخصیص و یا زمان آزادسازی منابع) ✓ بند 5 جدول 2-4 (حفاظت از داده کاربری) ▪ ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول ✓ بند 6 جدول 2-4 (حفاظت از داده‌ی کاربری) ▪ در نظر گرفتن یك عملیات از پیش تعیین‌شده پس از تشخیص یك خطای صحت داده که می‌تواند قابل پیکربندی نیز باشد. ✓ بند 11 جدول 2-4 (حفاظت از داده‌ی کاربری) ▪ 1. مدیریت حد آستانه برای تلاش‌های ناموفق 2. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد. ✓ بندهای 1 و 2 جدول 2-3 (شناسایی و احراز هویت) ▪ مدیریت معیارها برای تنظیم گذرواژه‌ها ✓ بند 4 جدول 2-3 (شناسایی و احراز هویت) ▪ 1. مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مربوطه 2. مدیریت یکسری عملیاتی که قبل از احراز شدن هویت کاربر انجام می‌شوند. ✓ بند 5 جدول 2-3 (شناسایی و احراز هویت) ▪ 1. مدیریت سازوکارهای احراز هویت 2. مدیریت قوانین مرتبط با احراز هویت ✓ بند 6 جدول 2-3 (شناسایی و 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. ✓ بند 7 جدول 2-8 (دسترسی به محصول) ▪ مدیر مجاز می‌تواند ویژگی‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد. ✓ بند 7 جدول 2-3 (شناسایی و احراز هویت) ▪ مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول ✓ بند 1 جدول 2-4 (حفاظت از داده‌ی کاربری) ▪ مدیریت نقش‌ها در محصول ✓ بند 2 جدول 2-5 (مدیریت امنیت)

	▪ مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر ✓ بند 1 جدول 2-8 (دسترسی به محصول) ▪ مدیریت شرایط آغاز نشست توسط مدیر مجاز ✓ بند 7 جدول 2-8 (دسترسی به محصول) ▪ 1. تعیین زمان غیرفعال بودن برای یك کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد. 2. تعیین زمان پیش‌فرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد. ✓ بند 2 جدول 2-8 (دسترسی به محصول) ✓ بند 3 جدول 2-8 (دسترسی به محصول) در هر یک از آزمون‌های مشخص‌شده، باید توانایی مدیریت معیارها، ویژگی‌ها یا توابع مورد نظر فراهم باشد. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان تغییر در عملکردهای مدیریتی ✓ (نیازی به تولید ثبت‌نشان در این الزام وجود نـدارد، امـا در الزام‌هـای مشخص‌شـده، لازم اسـت ثبت‌نشان مربوط به عملیات مدیریتی و نتایج آنها تولید گردد.)
نحوه‌ی دسترسی	منوهای مدیریت: کاربران، دسترسی‌ها، تنظیمات، پشتیبان‌گیری، به‌روزرسانی، شبکه، ذخیره‌سازی، گزارش‌ها و لاگ. ▪ پشتیبانی از (حذف، ویرایش، اضافه) گروهی از کاربران با مجوز دسترسی برای خواندن اطلاعات ثبت‌نشان‌ها ✓ بند 1 جدول 2-4 (حفاظت از داده‌ی کاربری) ▪ پشتیبانی از مجوزهای مشاهده/ویرایش ثبت‌نشان‌ها ✓ بند 3 جدول 2-1 (ممیزی امنیت (Log) ▪ پشتیبانی از حد آستانه و عملیات (حذف، ویرایش، اضافه) در زمان خرابی ذخیره‌سازی ثبت‌نشان‌ها ✓ بند 7 جدول 2-1 (ممیزی امنیت (Log) ✓ بند 8 جدول 2-1 (ممیزی امنیت (Log) ▪ مدیریت معیارها/پارامترهای مورد استفاده برای ایجاد و یا منع دسترسی به محصول ✓ بند 2 جدول 2-4 (حفاظت از داده کاربری) ▪ انتخاب زمان اجرای حفاظت از اطلاعات باقیمانده که می‌تواند در محصول قابل پیکربندی باشد. (برای مثال، زمان تخصیص و یا زمان آزادسازی منابع) ✓ بند 5 جدول 2-4 (حفاظت از داده کاربری) ▪ ویرایش قوانین کنترلی بیشتر برای وارد کردن داده به داخل محصول ✓ بند 6 جدول 2-4 (حفاظت از داده‌ی کاربری) ▪ در نظر گرفتن یك عملیات از پیش تعیین‌شده پس از تشخیص یك خطای صحت داده که می‌تواند قابل پیکربندی نیز باشد. ✓ بند 11 جدول 2-4 (حفاظت از داده‌ی کاربری) ▪ 1. مدیریت حد آستانه برای تلاش‌های ناموفق 2. مدیریت عملیاتی که هنگام شکست احراز هویت باید صورت گیرد. ✓ بندهای 1 و 2 جدول 2-3 (شناسایی و احراز هویت) ▪ مدیریت معیارها برای تنظیم گذرواژه‌ها ✓ بند 4 جدول 2-3 (شناسایی و احراز هویت) ▪ 1. مدیریت داده‌های احراز هویت توسط مدیر یا کاربر مربوطه 2. مدیریت یکسری عملیاتی که قبل از احراز شدن هویت کاربر انجام می‌شوند. ✓ بند 5 جدول 2-3 (شناسایی و احراز هویت)

	1. مدیریت سازوکارهای احراز هویت 2. مدیریت قوانین مرتبط با احراز هویت ✓ بند 6 جدول 2-3 (شناسایی و 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. ✓ بند 7 جدول 2-8 (دسترسی به محصول) مدیر مجاز می‌تواند ویژگی‌های امنیتی موجودیت‌های فعال پیش‌فرض را تعریف کند و تغییر دهد. ✓ بند 7 جدول 2-3 (شناسایی و احراز هویت) مدیریت مقادیر پیش‌فرض برای کنترل دسترسی محصول ✓ بند 1 جدول 2-4 (حفاظت از داده‌ی کاربری) مدیریت نقش‌ها در محصول ✓ بند 2 جدول 2-5 (مدیریت امنیت) مدیریت حداکثر تعداد مجاز نشست‌های همزمان کاربران توسط مدیر ✓ بند 1 جدول 2-8 (دسترسی به محصول) مدیریت شرایط آغاز نشست توسط مدیر مجاز ✓ بند 7 جدول 2-8 (دسترسی به محصول) 1. تعیین زمان غیرفعال بودن برای یك کاربر مشخص که پس از آن، نشست آن کاربر خاتمه یابد. 2. تعیین زمان پیش‌فرض غیرفعال بودن کاربران که پس از آن، نشست خاتمه یابد. ✓ بند 2 جدول 2-8 (دسترسی به محصول) ✓ بند 3 جدول 2-8 (دسترسی به محصول)
تصویر	تصویر فهرست کامل منوهای مدیریتی پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی شده هر یک از کارکردهای مدیریتی زیر از طریق منوها در دسترس است: مدیریت کاربران/مجوزها (شناسایی و احراز هویت)، فیلتر لاگ‌ها (ثبت‌نمان‌ها)، مدیریت مجوزهای منو/عملیات (کنترل دسترسی)، مدیریت پشتیبان/به‌روزرسانی (به‌روزرسانی امن در دستور کار NC-015)، مدیریت نقش‌ها.

37- بند 5 جدول 2-5 (مدیریت امنیت)

شناسه الزام	FMT_SMR.1.1	**نام الزام**	نقش‌های امنیتی 1
متن الزام	محصول باید توانایی تعریف نقش‌های مختلف را داشته باشد. - مدیر سیستم - کاربر پیشرفته - کاربر عادی - سایر موارد		
راهنمایی	در این الزام، بیشتر به بررسی ویژگی‌ها، شرایط یا نکات بیشتری که در ممکن است برای سطح دسترسی کاربر در نظر گرفته شده باشد پرداخته خواهد شد. برای نمونه، اگر گزینه‌ی وجود دارد که فارغ از سطح دسترسی تعیین‌شده، دسترسی به تمامی بخش‌ها را برای کاربر فعال می‌کند، یا گزینه‌ای که انتخاب آن سبب اعطای امتیازهای ویژه‌ای برای کاربر می‌شود. در صورتی که ویژگی‌ها، شرایط یا نکات بیشتری جهت مدیریت سطح دسترسی کاربرها وجود دارد، به تفصیل (شامل نحوه‌ی		

	عملکرد، امتیازها و ...) تشریح شوند.
نحوه‌ی دسترسی	صفحه کاربران با نقش‌های ADMIN و CLIENT.
تصویر	تصویر لیست نقش‌ها پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی شده نقش‌های امنیتی: مدیر (ADMIN) با دسترسی کامل و کاربر عادی (CLIENT) با مجوزهای تخصیصی؛ کاربران مجاز می‌توانند درخواست‌های تعریف‌شده را ارسال کنند.

38- بند 6 جدول 2-5 (مدیریت امنیت)

شناسه الزام	FMT_SMR.1.2	**نام الزام**	نقش‌های امنیتی 2
متن الزام	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.		
راهنمایی	توجه شود که هیچ الزامی مبنی بر وجود «گروه کاربری» یا «نقش» وجود ندارد، بلکه وجود «سطح دسترسی» کافی است. در صورت وجود شرایط خاصی در اعطای سطوح دسترسی (امکان تعیین چند نقش برای هر کاربر، امکان اعطای امتیاز ویژه به کاربرها (علاوه بر سطوح دسترسی مشخص‌شده در گروه) یـا ...)، این شرایط (شامل نحوه‌ی اعطای دسترسی خاص یا تعیین چند گروه و ...) تشریح شوند. در صورتی که به دلیل شرایط خاص محصول، امکان اعطای چندین نقش به یک کاربر وجـود داشـته باشد، لازم است مشخص شود که دسترسی کاربر در مواردی که بین نقش‌ها اختلاف وجود دارد چگونه است؟		
نحوه‌ی دسترسی	صفحه ورود و فیلتر jwtAuthorizationCheck.		
تصویر	تصویر رد درخواست کاربر غیرمجاز پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی شده کاربران مجاز: کاربران تعریف‌شده با نقش و مجوز فعال. درخواست‌های کاربران غیرمجاز/ناشناس با 401/404 رد می‌شود.		

39- بند 1 جدول 2-6 (حفاظت از توابع امنیتی محصول)

شناسه الزام	FPT_FLS.1.1	**نام الزام**	حفظ و امنیت وضعیت امن در زمان شکست 1
متن الزام	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. - خرابی‌های نرم‌افزاری - خرابی‌های سخت‌افزاری		
راهنمایی	هنگام شکست، محصول هرگز نباید اطلاعات محرمانه‌ای (مانند کد محصول) را فاش کند. همچنین در زمان شکست، باید سیاست‌های «سطح دسترسی» همچنان اجرا شوند. به این معنی که کاربری که به بخشی دسترسی نداشته باشد، در زمان شکست نیز نباید دسترسی داشته باشد. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان بروز شکست در محصول		
نحوه‌ی	لاگ فنی محصول (log/pline.log) و مانیتورینگ سرویس‌ها.		

دسترسی	
تصویر	تصویر لاگ خطای اتصال پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل حالات شکست (مانند قطعی اتصال Asterisk یا پایگاه‌داده) در لاگ فنی ثبت می‌شود. واردکردن محصول به حالت حفاظت‌شده ثابت (Fail-safe) به‌صورت مستند تعریف نشده و در حال بررسی است.

40- بند 2 جدول 2-6 (حفاظت از توابع امنیتی محصول)

شناسه الزام	FPT_ITT.1.1	**نام الزام**	انتقال داده امنیتی در داخل محصول
متن الزام	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.		
راهنمایی	در صورتی که محصول روی چند سرور (چند ماشین مجازی) به صورت توزیع‌شده کار می‌کند، لازم است ارتباط بین این ماشین‌ها امن باشد. به این معنی که حتما باید با استفاده از یک پروتکل امن، اطلاعات تبادل‌شده بین ماشین‌ها رمزشده جابجا گردد.		
نحوه‌ی دسترسی	معماری تک‌سروری: ارتباط داخلی با پایگاه‌داده (localhost) و Asterisk (AMI).		
تصویر	تصویر معماری استقرار پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی شده جریان داده کاربر بین اجزای روی یک میزبان (ویندوز/لینوکس سرور محصول) منتقل می‌شود؛ کانال‌های ارتباطی داخلی محدود به localhost است.		

41- بند 3 جدول 2-6 (حفاظت از توابع امنیتی محصول)

شناسه الزام	FPT_TDC.1.1 & FPT_TDC.1.2	**نام الزام**	سازگاری داده امنیتی بین محصول و موجودیت امن 1 و 2
متن الزام	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. - داده‌های احراز هویت - کلید - امضای دیجیتال - ثبت‌نشان‌ها (داده‌های ممیزی) - سایر موارد		
راهنمایی	در این الزام محصول باید درک درستی از اطلاعات تبادل‌شده بین خود و محصول‌های دیگر داشته باشد. (معمولا رفتار مناسب متناسب با اطلاعات تبادل‌شده، نشان‌دهنده‌ی درک صحیح دو طرف از اطلاعات است. برای نمونه، در ارتباط محصول به سرور احراز هویت، وقتی کاربر به درست احراز هویت می‌شود، نشان‌دهنده‌ی درک صحیح محصول و سرور احراز هویت از اطلاعات تبادل‌شده است.) همچنین ارتباط با سایر محصول‌ها باید به صورت امن انجام شود.		
نحوه‌ی دسترسی	داخل محصول: خواندن/نوشتن پیکربندی با سازوکار همزمانی و اعمال تنظیمات (Apply).		
تصویر	تصویر فرآیند اعمال تنظیمات (Apply) پیوست شود.		
توضیحات	وضعیت: پیاده‌سازی شده		

بیشتر	داده‌های همگام‌سازی‌شده بین اجزای داخلی: فایل‌های پیکربندی Asterisk (sip.conf، extensions.conf و ...) و پارامترهای صف؛ همگام‌سازی با تراکنش پایگاه‌داده و ثبت‌نمان انجام می‌شود.

42- بند 4 جدول 2-6 (حفاظت از توابع امنیتی محصول)

شناسه الزام	FPT_STM.1.1	**نام الزام**	مهرهای زمانی 1
متن الزام	محصول باید زمان و تاریخ معتبری داشته باشد، بنابراین باید مهرهای زمانی[2] معتبر را تولید یا از آن‌ها استفاده نماید. - 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		
راهنمایی	نحوه‌ی دریافت اطلاعات زمانی را توضیح دهید. در صورتی که امکان تعیین زمان یا تعیین سرور NTP در محصول وجود دارد، منحوه‌ی پیکربندی آن را شرح دهید. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان تغییر سرور NTP [در صورت پشتیبانی از این ویژگی] ✓ ثبت‌نشان تغییر زمان [در صورت پشتیبانی از این ویژگی]		
نحوه‌ی دسترسی	تنظیمات زمان سیستم در صفحه تنظیمات (سیستم/زمان؛ endpoint /app/ntp-check).		
تصویر	تصویر تنظیمات زمان و بررسی NTP پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل زمان سیستم از منبع زمان سیستم‌عامل گرفته می‌شود؛ قابلیت اطمینان منبع زمان (NTP) و جلوگیری از تغییر غیرمجاز در حال بررسی است (NC-016).		

43- بند 5 جدول 2-6 (حفاظت از توابع امنیتی محصول)

شناسه الزام	FPT_TUD_EXT.1.2	**نام الزام**	بروزرسانی امن 2
متن الزام	محصول باید امکان بروزرسانی نرم‌افزار و میان‌افزار محصول را برای مدیر سیستم فراهم نماید. - بروزرسانی دستی - جستجوی خودکار بروزرسانی‌ها - بروزرسانی‌های خودکار - بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایل بروزرسانی		
راهنمایی	درمورد انواع بروزرسانی، باید به نکات زیر توجه داشت: ▪ بروزرسانی دستی ✓ بروزرسانی دستی به دو روش انجام می‌شود. یکی بروزرسانی توسط کارشناس‌های شرکت توسعه‌دهنده و بارگذاری فایل‌های جدید روی سرور محصول، دیگری بروزرسانی توسط کاربر مجاز، که با نصب یک فایل (خودکار کردن عملیات بروزرسانی) صورت می‌پذیرد. ▪ جستجوی خودکار بروزرسانی‌ها ✓ این روش، تنها وجود بروزرسانی برای نسخه‌ی فعلی را بررسی می‌کند و در صورت وجود نسخه‌ی جدید، به کاربر مجاز اطلاع می‌دهد. (منبع بروزرسانی می‌تواند به صورت محلی		

[2] Timestamp

	یا خارجی باشد، اما ارتباط با سرور بروزرسانی باید به صورت امن انجام شود.) ▪ بروزرسانی خودکار ✓ بروزرسانی خودکار، به این معنی است که محصول بـه صـورت خودکـار بروزرسـانی را نصب می‌کند و نیازی به انجام اقدامی از سوی کاربر نیست. باید توجه داشت که در این این روش، لازم است محصول با یکی از روش‌های ارائه‌شده در بند 6 جدول 2-6 (حفاظت از توابع امنیتی محصول)، اعتبار و اصالت فایل بروزرسانی را بررسی نماید. ▪ بروزرسانی دستی پس از اطمینان از امنیت وصله و یا فایل بروزرسانی ✓ این روش، مانند «بروزرسانی دستی» است، با این تفاوت که قبل از پذیرفتن یا قبـل از اعمال فایل بروزرسانی، با استفاده از امضا، درهم‌سازی یا روش‌های احراز اصالت دیگر، از امنیت، اصالت و یکپارچگی فایل بروزرسانی اطمینان حاصل می‌کند. (طبیعتـا در این روش، بروزرسانی توسط کاربر صورت می‌پذیرد، نه شرکت توسعه‌دهنده) 1 در «بروزرسانی دستی» توضیح داده شود که توسط شرکت توسعه‌دهنده انجام می‌شود یا کاربر و اگر توسط کاربر انجام می‌شود، نحوه‌ی بروزرسانی تشریح شود. 2 در «بروزرسانی دستی بعد از اطمینان از امنیت وصله و یا فایـل بروزرسـانی»، حتمـا بایـد فایـل توسط محصول دریافت گردد و فایل توسط محصول اعتبارسنجی شود. ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان نتیجه‌ی بروزرسانی ✓ ثبت‌نشان تلاش کاربر برای بروزرسانی [در صورت پشتیبانی از این ویژگی] ✓ ثبت‌نشان وجود نسخه‌ی جدید (در صورت امکان) [در صورت پشتیبانی از این ویژگی] ✓ ثبت‌نشان تلاش برای بروزرسانی خودکار[در صورت پشتیبانی از این ویژگی] ✓ ثبت‌نشان اعتبارسنجی فایل بروزرسانی [در صورت پشتیبانی از این ویژگی]
نحوه‌ی دسترسی	صفحه به‌روزرسانی (Update) — endpointهای AppControllers.
تصویر	پس از پیاده‌سازی NC-015، تصویر فرآیند تأیید امضا پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل مکانیزم به‌روزرسانی وجود دارد؛ تأیید هویت سازنده/اعتبارسنجی امضای دیجیتال بسته به‌روزرسانی هنوز ارائه نمی‌شود (NC-015) و به‌عنوان نقص مستند شده است.

44- بند 6 جدول 2-6 (حفاظت از توابع امنیتی محصول)

شناسه الزام	FPT_TUD_EXT.1.3	**نام الزام**	بروزرسانی امن 3
متن الزام	در صورت استفاده از بروزرسـانی بـه روش خودکـار، محصـول بایـد پیش از نصـب بروزرسـانی‌های نرم‌افزاری و میان‌افزاری، امکان احراز اصالت میان‌افزار یا نرم‌افزار را فراهم نماید. - امضای دیجیتال - درهم‌ساز منتشرشده		
راهنمایی	در صورتی که محصول از «بروزرسانی خودکار» پشـتیبانی می‌کنـد، نحـوه‌ی اعتبارسـنجی فایل‌هـای بروزرسانی باید مشخص شود.		
نحوه‌ی دسترسی	صفحه به‌روزرسانی.		
تصویر	پس از پیاده‌سازی NC-015، تصویر پیکربندی به‌روزرسانی پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل به‌روزرسانی فقط از نسخه رسمی سازنده پشتیبانی می‌کند؛ الزامات اعتبارسنجی امضا در دستور کار (NC-015) است.		

45- بند 1 جدول 2-7 (تخصیص منابع)

شناسه الزام	FRU_FLT.1.1	**نام الزام**	تحمل خطا 1
متن الزام	محصول باید در زمان رخداد هرگونه اشکال و خرابی (شکست) نرم‌افزاری، از عملکـرد کارکردهـای اصلی محصول اطمینان حاصل نماید.		
راهنمایی	تمامی خطاهای داخلی محصول باید مدیریت شود و نباید به هیچ درخواستی با کد 5XX پاسخ داده شود. آیا توانایی تشخیص و اعلام خطا وجود دارد؟ آیا اطلاعاتی از شکست رخ داده، ثبت می‌شود؟ ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان بروز شکست		
نحوه‌ی دسترسی	مانیتورینگ سرویس‌ها و لاگ فنی (log/pline.log).		
تصویر	تصویر لاگ خطای سرویس پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی شده در صورت شکست اجزا (Asterisk/DB)، ثبت‌نمان خطا تولید می‌شود؛ در این حالت توابع وابسته در دسترس نیستند و این موضوع در لاگ منعکس می‌گردد.		

46- بند 1 جدول 2-8 (دسترسی به محصول)

شناسه الزام	FTA_MCS.1.1 & FTA_MCS.1.2	**نام الزام**	محدودیت بر روی چندین نشسـت همزمـان 1 و 2
متن الزام	محصول باید حداکثر تعداد نشست‌های همزمان متعلق به یک کاربر را محدود نماید.		
راهنمایی	- ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان جلوگیری از آغاز نشست جدید به علت رسیدن به حد آستانه [در صورت پشتیبانی از این ویژگی] ✓ ثبت‌نشان خاتمه به نشست قبلی به دلیل ایجاد نشست جدید [در صورت پشتیبانی از این ویژگی]		
نحوه‌ی دسترسی	فرآیند ورود؛ توکن در پایگاه‌داده.		
تصویر	تصویر رفتار ورود مجدد پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل حداکثر تعداد نشست همزمان قابل تعیین توسط مدیر نیست؛ در وضعیت فعلی با هر ورود جدید، توکن قبلی باطل می‌شود (عملاً یک نشست فعال به‌ازای هر کاربر). مدیریت سقف نشست همزمان در دستور کار (NC-007) است.		

47- بند 2 جدول 2-8 (دسترسی به محصول)

شناسه الزام	FTA_SSL.3.1	**نام الزام**	خاتمه دادن به نشست‌ها توسط محصول 1
متن الزام	محصول باید کلیه نشست‌های تعاملی راه‌دور را پس از مدت زمانی که غیرفعال هستند (و می‌بایست توسط مدیر قابل تنظیم باشد)، خاتمه دهد.		
راهنمایی	طبق متن الزام، لازم است زمان غیرفعال بودن نشست توسط کاربر مجاز قابل پیکربندی باشد.		

	ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان پیکربندی زمان خاتمه به نشست غیرفعال ✓ ثبت‌نشان خروج کاربر غیرفعال (با ذکر علت خروج (غیرفعال بودن))
نحوه‌ی دسترسی	فرآیند ورود و فیلتر نشست.
تصویر	پس از پیاده‌سازی NC-007، تصویر پیکربندی timeout پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل قفل/خاتمه نشست بر اساس مدت بی‌کاری (inactivity timeout) سمت سرور هنوز به‌صورت صریح و قابل پیکربندی اعمال نمی‌شود؛ در دستور کار (NC-007).

48- بند 3 جدول 2-8 (دسترسی به محصول)

شناسه الزام	FTA_SSL.4.1	**نام الزام**	خاتمه دادن به نشست‌ها توسط کاربر 1
متن الزام	محصول باید به کاربری که خود آغازگر نشست بوده است اجازه‌ی خاتمه نشست را بدهد.		
راهنمایی	- ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان خروج کاربر		
نحوه‌ی دسترسی	منوی کاربر ← خروج (LogOut).		
تصویر	تصویر منوی خروج پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی شده کاربر می‌تواند به‌طور خودانگیخته نشست را خاتمه دهد (خروج از سیستم). خروج کامل سمت سرور (ابطال توکن) در دستور کار (NC-008) است.		

49- بند 4 جدول 2-8 (دسترسی به محصول)

شناسه الزام	FTA_TAH.1.1	**نام الزام**	سوابق دسترسی به محصول 1
متن الزام	در صورت برقراری نشست به طور موفقیت‌آمیز، محصول باید قادر به نمایش آخرین تلاش موفق برای ایجاد نشست بر اساس موارد زیر باشد. - روز - زمان - سایر موارد		
راهنمایی	باید بتوان اطلاعاتی از نشست موفقیت‌آمیز قبلی را مشاهده نمود.		
نحوه‌ی دسترسی	فرآیند ورود.		
تصویر	پس از پیاده‌سازی، تصویر رفتار قفل نشست پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل قفل نشست پس از مدت تعیین‌شده بی‌کاری هنوز پیاده‌سازی نشده است (NC-007).		

50- بند 5 جدول 2-8 (دسترسی به محصول)

شناسه الزام	FTA_TAH.1.2	**نام الزام**	سوابق دسترسی به محصول 2
متن الزام	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. - روز - زمان - سایر موارد		
راهنمایی	باید بتوان اطلاعاتی تلاش‌های ناموفق برای ورود را مشاهده نمود.		
نحوه‌ی دسترسی	فرآیند ورود.		
تصویر	پس از پیاده‌سازی، تصویر احراز هویت مجدد پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل نیازمند احراز هویت دوباره پس از قفل نشست است؛ همراه با NC-007 تکمیل می‌شود.		

51- بند 6 جدول 2-8 (دسترسی به محصول)

شناسه الزام	FTA_TAH.1.3	**نام الزام**	سوابق دسترسی به محصول 3
متن الزام	محصول نباید اطلاعات سوابق دسترسی را بدون بازدید کاربر، از واسط کاربری پاک نماید.		
راهنمایی	باید مشخص شود که موارد خواسته شده در بندهای 4 و 5 جدول 2-8 (دسترسی به محصول) چگونه به کاربر نمایش داده می‌شوند. برای نمونه، آیا به صورت ثابت از در بخشی از محصول قابل دسترسی هستند یا به صورت Pop-up به کاربر نمیش داده می‌شود؟		
نحوه‌ی دسترسی	فرآیند ورود و گزارش لاگ.		
تصویر	پس از پیاده‌سازی، تصویر نمایش اطلاعات پیش از قفل پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل نمایش اطلاعات پیش از قفل (مانند پیام هشدار) و ثبت‌نمان قفل/خاتمه نشست بی‌کار هنوز کامل نیست؛ همراه با NC-007 تکمیل می‌شود.		

52- بند 7 جدول 2-8 (دسترسی به محصول)

شناسه الزام	FTA_TSE.1.1	**نام الزام**	برقراری نشست 1
متن الزام	محصول باید توانایی ممانعت از ایجاد نشست بر اساس پارامترهایی را داشته باشد. - مکان - شماره پورت - روز - زمان - سایر موارد		
راهنمایی	هر یک از گزینه‌های انتخاب شده باید از داخل محصول قابل پیکربندی باشند. در شرایطی که این ویژگی‌ها نقض می‌شوند، باید جلوی ورود کاربر محصول گرفته شود.		

	ثبت‌نشان‌های مورد نیاز: ✓ ثبت‌نشان جلوگیری از ورود کاربر (این ثبت‌نشان می‌تواند به عنوان ثبت‌نشان «تلاش ناموفق ورود» ثبت شود، اما باید دلیل ناموفق بودن تلاش به صورت واضح مشخص باشد. به عبارت دیگر، محصول باید بین تلاش ناموفق به دلیل ورود اطلاعات کاربری اشتباه یا تلاش ناموفق به دلیل نقض محدودیت‌های دسترسی تمایز قائل شود.)
نحوه‌ی دسترسی	مدیریت نشست‌ها توسط مدیر: صفحه کاربران (فعال/غیرفعال‌سازی حساب).
تصویر	تصویر عملیات غیرفعال‌سازی حساب پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل مدیر می‌تواند با غیرفعال‌سازی حساب، خاتمه دسترسی کاربر را اعمال کند. خاتمه نشست‌های فعال بر اساس شرایط تعریف‌شده (مانند timeout) هنوز کامل نیست (NC-007).

53- بند 1 جدول 2-9 (کانال‌ها/مسیرهای مورد اعتماد)

شناسه الزام	FTP_TRP.1.1	**نام الزام**	مسیر امن 1
متن الزام	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 دهـد و از تغییر و افشای داده تبادلی حفاظت نماید و تغییرات را تشخیص دهد. - HTTPS - TLS - SSH		
راهنمایی	باید تمامی ارتباط‌های خارجی محصول رمزشده و امن باشند. کاربرد هر یک از پرتکل‌ها را تشریح نمایید.		
نحوه‌ی دسترسی	ارتباط فرانت و بک‌اند: پنل وب روی پورت 8080 (HTTP)؛ WebSocket در مسیر /ws.		
تصویر	پس از فعال‌سازی NC-001، تصویر پیکربندی TLS پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل ارتباط بین کاربر و محصول از طریق مرورگر و HTTP انجام می‌شود. مسیر ارتباطی قابل اعتماد مبتنی بر HTTPS/TLS در وضعیت فعلی فراهم نیست و فعال‌سازی TLS در دستور کار (NC-001) قرار دارد.		

54- بند 2 جدول 2-9 (کانال‌ها/مسیرهای مورد اعتماد)

شناسه الزام	FTP_TRP.1.2	**نام الزام**	مسیر امن 2
متن الزام	محصول باید به کاربر/دیگر محصول IT معتبر اجازه دهد که ارتباطات راه‌دور را از طریق کانـال امن آغاز کنند.		
راهنمایی	-		
نحوه‌ی دسترسی	همان مسیر ارتباطی (HTTP/8080).		
تصویر	پس از فعال‌سازی NC-001، تصویر پیکربندی پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل		

	کاربر می‌تواند مسیر ارتباطی را مشخص کند (آدرس سرور در مرورگر)؛ در وضعیت فعلی تعیین‌کننده بودن امن بودن مسیر، تضمین نمی‌شود (NC-001).

55- بند 3 جدول 2-9 (کانال‌ها/مسیرهای مورد اعتماد)

شناسه الزام	FTP_TRP.1.3	**نام الزام**	مسیر امن 3
متن الزام	محصول باید استفاده از کانال امن را برای احراز هویت اولیه کاربر الزامی نماید.		
راهنمایی	-		
نحوه‌ی دسترسی	همان مسیر ارتباطی (HTTP/8080).		
تصویر	پس از فعال‌سازی NC-001، تصویر پیکربندی پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل اعمال نیازمندی‌های الزامات HTTPS (جدول 3-1) به محصول اعمال نمی‌شود تا زمان فعال‌سازی TLS (NC-001).		

56- بند 1 جدول 3-1 (پروتکل HTTPS)

شناسه الزام	FCS_HTTPS_EXT.1.1	**نام الزام**	الزامات پروتکل HTTPS (1)
متن الزام	محصول باید پروتکل HTTPS را مطابق با RFC 2818 اجرا کند.		
راهنمایی	-		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا محصول در وضعیت فعلی HTTPS ارائه نمی‌کند (سرویس روی HTTP/8080)؛ فعال‌سازی TLS در دستور کار اصلاح (NC-001) برنامه‌ریزی شده است.		

57- بند 2 جدول 3-1 (پروتکل HTTPS)

شناسه الزام	FCS_HTTPS_EXT.1.2	**نام الزام**	الزامات پروتکل HTTPS (2)
متن الزام	محصول باید پروتکل HTTPS را با استفاده از TLS اجرا کند.		
راهنمایی	تصویری از پیاده‌سازی HTTPS با استفاده از TLS ارائه نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا وابسته به الزام قبل (NC-001). پس از فعال‌سازی TLS مجموعه رمزهای مجاز اعلام می‌شود.		

58- بند 3 جدول 3-1 (پروتکل HTTPS)

شناسه الزام	FCS_HTTPS_EXT.1.3	نام الزام	الزامات پروتکل HTTPS (3)
متن الزام	در صورتی که گواهی‌نامه ارائه شده از سمت دیگر محصولات IT (درهنگام برقراری ارتباط) نامعتبر باشد، محصول باید بر اساس موارد زیر عمل نماید. - اتصال را برقرار نکند. - برای برقراری اتصال درخواست مجوز کند.		
راهنمایی	واکنش محصول هنگامی که گواهی‌نامه‌ی سرور (سروری که محصول می‌خواهد به آن متصل شود) نامعتبر باشد، را تشریح نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا وابسته به الزام قبل (NC-001).		

59- بند 1 جدول 3-2 (پروتکل TLS Client)

شناسه الزام	FCS_TLSC_EXT.1.1	نام الزام	الزامات پروتکل TLS Client (1)
متن الزام	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. - [0x1302] TLS_AES_256_GCM_SHA384 مطابق با RFC 8446 - [0x1301] TLS_AES_128_GCM_SHA256 مطابق با RFC 8446 - [0x009F] TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 - [0x009E] TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288 - [0xC02F] TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 - [0xC030] TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 - [0xC02C] TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 - [0xC02B] TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 - [0x009D] TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 - [0x009C] TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288 - [0xC02E] TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 - [0xC02D] TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 - [0xC032] TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 - [0xC031] TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 - [0x00A1] TLS_DH_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 - [0x00A0] TLS_DH_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288		
راهنمایی	باید مجموعه‌های رمز ارائه‌شده در پیام ClientHello، با مجموعه‌های رمز انتخاب‌شده مطابقت داشته باشند. تصویری از پیکربندی محصول ارائه نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا محصول در وضعیت فعلی کلاینت TLS ندارد (ارتباط با سرویس لایسنس در حال حاضر HTTP است		

	— (NC-002).

60- بند 2 جدول 3-2 (پروتکل TLS Client)

شناسه الزام	FCS_TLSC_EXT.1.2	نام الزام	الزامات پروتکل TLS Client (2)
متن الزام	محصول باید مطابقت شناسه ارائه‌شده با شناسه مرجع را با توجه به بخش 6 از RFC 6125، تأیید نماید.		
راهنمایی	-		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا وابسته به الزام قبل (NC-002).		

61- بند 3 جدول 3-2 (پروتکل TLS Client)

شناسه الزام	FCS_TLSC_EXT.1.3	نام الزام	الزامات پروتکل TLS Client (3)
متن الزام	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. - ارتباط را برقرار نکند - برای برقراری ارتباط درخواست مجوز کند - سایر موارد		
راهنمایی	واکنش محصول هنگامی که گواهی‌نامه‌ی سرور (سروری که محصول می‌خواهد به آن متصل شود یا سرور خود محصول هنگام ارتباط کلاینت‌های محصول با آن [در شرایطی که محصول نرم‌افزارهای ویندوزی و ... دارد]) نامعتبر باشد، را تشریح نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا وابسته به الزام قبل (NC-002).		

62- بند 4 جدول 3-2 (پروتکل TLS Client)

شناسه الزام	FCS_TLSC_EXT.1.4	نام الزام	الزامات پروتکل TLS Client (4)
متن الزام	محصول باید در پیام ClientHello برای استفاده از خم‌های بیضوی، بر اساس موارد زیر عمل نماید. - Supported Elliptic Curves Extension را ارائه نکند. - Supported Elliptic Curves Extension را به همراه NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 ارائه نماید.		
راهنمایی	تصویری از پیکربندی محصول ارائه نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		

توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا وابسته به الزام قبل (NC-002).

63- بند 1 جدول 3-3 (پروتکل TLS Server)

شناسه الزام	FCS_TLSS_EXT.1.1	**نام الزام**	الزامات پروتکل TLS Server (1)
متن الزام	محصول باید TLS 1.2 (RFC 5246) را پیاده‌سازی کند. همچنین محصول باید TLS را با پشتیبانی از مجموعه‌های رمز زیر پیاده‌سازی نماید. - [0x1302] TLS_AES_256_GCM_SHA384 مطابق با RFC 8446 - [0x1301] TLS_AES_128_GCM_SHA256 مطابق با RFC 8446 - [0x009F] TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 - [0x009E] TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288 - [0xC02F] TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 - [0xC030] TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 - [0xC02C] TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 - [0xC02B] TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 - [0x009D] TLS_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 - [0x009C] TLS_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288 - [0xC02E] TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 - [0xC02D] TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 - [0xC032] TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5289 - [0xC031] TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5289 - [0x00A1] TLS_DH_RSA_WITH_AES_256_GCM_SHA384 مطابق با RFC 5288 - [0x00A0] TLS_DH_RSA_WITH_AES_128_GCM_SHA256 مطابق با RFC 5288		
راهنمایی	باید مجموعه‌های رمز ارائه‌شده در پیام ServerHerllo، با مجموعه‌های رمز انتخاب‌شده مطابقت داشته باشند. تصویری از پیکربندی محصول ارائه نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا محصول در وضعیت فعلی سرور TLS ندارد (NC-001).		

64- بند 2 جدول 3-3 (پروتکل TLS Server)

شناسه الزام	FCS_TLSS_EXT.1.2	**نام الزام**	الزامات پروتکل TLS Server (2)
متن الزام	محصول باید اتصال‌های کاربرانی که درخواست TLS1.0، SSL3.0، SSL2.0، SSL1.0 و TLS1.1 دارند را رد نماید.		
راهنمایی	تصویری از پیکربندی محصول ارائه نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		

توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا وابسته به الزام قبل (NC-001).

65- بند 3 جدول 3-3 (پروتکل TLS Server)

شناسه الزام	FCS_TLSS_EXT.1.3	نام الزام	الزامات پروتکل TLS Server (3)
متن الزام	محصول باید پارامترهای ساخت کلید را بر اساس موارد زیر ایجاد نماید. - استفاده از RSA با اندازه کلید 2048 یا 3072 یا 4096 بیت - پارامترهای ECDH(E) با استفاده از NIST Curveهای secp256r1 یا secp384r1 یا secp521r1 و هیچ مورد دیگر - پارامترهای دیفی-هلمن با اندازه کلید 2048 یا 3072 بیت		
راهنمایی	تصویری از پیکربندی محصول ارائه نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا وابسته به الزام قبل (NC-001).		

66- بند 1 جدول 3-4 (پروتکل TLS مشترکت کلاینت و سرور)

شناسه الزام	FCS_TLSS_EXT.2.4	نام الزام	الزامات پروتکل TLS Server / احراز هویت (4)
متن الزام	محصول باید احراز هویت دوطرفه کلاینت‌ها/سرورهای TLS را با استفاده از گواهی‌نامه‌های X509v3 پشتیبانی نماید.		
راهنمایی	-		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا وابسته به الزام قبل (NC-001). احراز هویت متقابل TLS با گواهینامه X.509 در نسخه فعلی ارائه نمی‌شود.		

67- بند 2 جدول 3-4 (پروتکل TLS مشترکت کلاینت و سرور)

شناسه الزام	FCS_TLSS_EXT.2.6	نام الزام	الزامات پروتکل TLS Server / احراز هویت (5)
متن الزام	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.		
راهنمایی	-		
نحوه‌ی دسترسی	-		

تصویر	بدون ادعا — تصویری لازم نیست.
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا وابسته به الزام قبل (NC-001).

68- بند 1 جدول 3-5 (اعتبارسنجی گواهی‌نامه)

شناسه الزام	FIA_X509_EXT.1.1/Rev	**نام الزام**	الزامات پروتکل X509 (1) / ابطال
متن الزام	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 6.3 - لیست فسخ گواهی‌نامه (CRL) مشخص شده در RFC 5759 بخش 5 - 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.		
راهنمایی	تصویری از پیکربندی محصول یا مستندات ابزار مورد استفاده ارائه نمایید.		
نحوه‌ی دسترسی	صفحه مدیریت گواهینامه‌ها (/certificates/index).		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا رابط کاربری مدیریت گواهینامه وجود دارد، اما اعتبارسنجی کامل مطابق RFC 5280 (زنجیره گواهینامه، basicConstraints/CA، روش ابطال OCSP/CRL و extendedKeyUsage) در محصول اثبات/پیاده‌سازی نشده است (NC-017). گزینه‌ای انتخاب نشده.		

69- بند 2 جدول 3-5 (اعتبارسنجی گواهی‌نامه)

شناسه الزام	FIA_X509_EXT.1.2/Rev	**نام الزام**	الزامات پروتکل X509 (2) / ابطال
متن الزام	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.		
راهنمایی	تصویری از پیکربندی محصول یا مستندات ابزار مورد استفاده ارائه نمایید.		

نحوه‌ی دسترسی	-
تصویر	بدون ادعا — تصویری لازم نیست.
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا پذیرش گواهینامه به‌عنوان CA فقط با basicConstraints/CA=TRUE به‌صورت مستند اعمال نمی‌شود (NC-017).

70- بند 3 جدول 3-5 (اعتبارسنجی گواهی‌نامه)

شناسه الزام	FIA_X509_EXT.2.1	**نام الزام**	الزامات پروتکل X509 (3)
متن الزام	محصول باید برای پشتیبانی از احراز هویت برای موارد زیر، از گواهی‌نامه‌های X509v3 تعریف‌شده در RFC 5280 استفاده کند. - HTTPS - TLS - SSH - امضای کد برای بروزرسانی‌های نرم‌افزار سیستم - امضای کد برای تأیید یکپارچگی - سایر موارد		
راهنمایی	-		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا با توجه به عدم پشتیبانی HTTPS/TLS/SSH و امضای کد در نسخه فعلی، کاربرد گواهینامه X.509v3 در این موارد وجود ندارد؛ صفحه مدیریت گواهینامه (Certificates.tsx) برای کاربردهای احتمالی آینده است و مصرف امنیتی آن در حال بررسی است.		

71- بند 1 جدول 3-6 (پروتکل SSH)

شناسه الزام	FCS_SSH_EXT.1.1	**نام الزام**	الزامات پروتکل SSH (1)
متن الزام	محصول باید پروتکل SSH را مطابق با RFCهای 4251، 4252، 4253، 4254، 5656 و 6668 پیاده‌سازی نماید.		
راهنمایی	تصویری از پیکربندی محصول یا مستندات ابزار مورد استفاده ارائه نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: خارج از دامنه محصول محصول سرویس SSH ارائه نمی‌کند؛ SSH صرفاً ابزار مدیریتی سیستم‌عامل میزبان است و بخشی از محصول محسوب نمی‌شود.		

72- بند 2 جدول 3-6 (پروتکل SSH)

شناسه الزام	FCS_SSH_EXT.1.2	**نام الزام**	الزامات پروتکل SSH (2)
متن الزام	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		
راهنمایی	تصویری از پیکربندی محصول یا مستندات ابزار مورد استفاده ارائه نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: خارج از دامنه محصول خارج از دامنه محصول (بدون سرویس SSH).		

73- بند 3 جدول 3-6 (پروتکل SSH)

شناسه الزام	FCS_SSH_EXT.1.3	**نام الزام**	الزامات پروتکل SSH (3)
متن الزام	محصول باید در پیاده‌سازی پروتکل SSH مطابق RFC 4253، بسته‌های بزرگتر از مقدار مشخصی (در بخش «توضیحات» ذکر شود) را کنار بگذارد.		
راهنمایی	تصویری از پیکربندی محصول یا مستندات ابزار مورد استفاده ارائه نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: خارج از دامنه محصول خارج از دامنه محصول (بدون سرویس SSH).		

74- بند 4 جدول 3-6 (پروتکل SSH)

شناسه الزام	FCS_SSH_EXT.1.4	**نام الزام**	الزامات پروتکل SSH (4)
متن الزام	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		
راهنمایی	تصویری از پیکربندی محصول ارائه نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		

توضیحات بیشتر	وضعیت: خارج از دامنه محصول خارج از دامنه محصول (بدون سرویس SSH).

75- بند 5 جدول 3-6 (پروتکل SSH)

شناسه الزام	FCS_SSH_EXT.1.5	**نام الزام**	الزامات پروتکل SSH (5)
متن الزام	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			
راهنمایی	تصویری از پیکربندی محصول ارائه نمایید.			
نحوه‌ی دسترسی	-			
تصویر	بدون ادعا — تصویری لازم نیست.			
توضیحات بیشتر	وضعیت: خارج از دامنه محصول خارج از دامنه محصول (بدون سرویس SSH).			

76- بند 6 جدول 3-6 (پروتکل SSH)

شناسه الزام	FCS_SSH_EXT.1.6	**نام الزام**	الزامات پروتکل SSH (6)
متن الزام	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			
راهنمایی	تصویری از پیکربندی محصول ارائه نمایید.			
نحوه‌ی دسترسی	-			
تصویر	بدون ادعا — تصویری لازم نیست.			

توضیحات بیشتر	وضعیت: خارج از دامنه محصول خارج از دامنه محصول (بدون سرویس SSH).

77- بند 7 جدول 3-6 (پروتکل SSH)

شناسه الزام	FCS_SSH_EXT.1.7	**نام الزام**	الزامات پروتکل SSH (7)
متن الزام	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		
راهنمایی	تصویری از پیکربندی محصول ارائه نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: خارج از دامنه محصول خارج از دامنه محصول (بدون سرویس SSH).		

78- بند 8 جدول 3-6 (پروتکل SSH)

شناسه الزام	FCS_SSH_EXT.1.8	**نام الزام**	الزامات پروتکل SSH (8)
متن الزام	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 1 گیگابایت نباشد) استفاده گردد. در صورت پر شدن حد آستانه برای هر کدام از موارد ذکر شده، باید تجدید کلید صورت بگیرد.		
راهنمایی	تصویری از پیکربندی محصول یا مستندات ابزار مورد استفاده ارائه نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: خارج از دامنه محصول خارج از دامنه محصول (بدون سرویس SSH).		

79- بند 9 جدول 3-6 (پروتکل SSH)

شناسه الزام	FCS_SSH_EXT.1.9	**نام الزام**	الزامات پروتکل SSH (9)
متن الزام	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 ۷.1) همراه می‌کند، استفاده می‌نماید.		
راهنمایی	تصویری از پیکربندی محصول یا مستندات ابزار مورد استفاده ارائه نمایید.		
نحوه‌ی دسترسی	-		
تصویر	بدون ادعا — تصویری لازم نیست.		
توضیحات بیشتر	وضعیت: خارج از دامنه محصول خارج از دامنه محصول (بدون سرویس SSH).		

آزمون‌های آسیب‌پذیری

80- بروز بودن اجزای محصول

شناسه الزام		**نام الزام**	
متن الزام	تمامی ابزارها و چارچوب‌های مورد استفاده در محصول		
راهنمایی	لطفا ضمن اشاره به تمامی ابزارها، چارچوب‌ها و تکنولوژی‌های مورد استفاده، نسخه‌ی آن‌ها را بروزرسانی و اعلام نمایید. شامل وب‌سرور، CMS و ...		
نحوه‌ی دسترسی	بک‌اند: Java 17 (LTS)، Spring Boot 3.4.5، Hibernate، PostgreSQL؛ فرانت‌اند: React 18.3.1، TypeScript، Vite — فهرست کامل: package.json و pom.xml.		
تصویر	تصویر خروجی ابزارهای اسکن و نسخه‌ها پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل فهرست کامل اجزا و نسخه‌های آن‌ها در جدول ویژگی‌های فنی سند درج شده است. اجرای اسکن آسیب‌پذیری وابستگی‌ها (npm audit و OWASP Dependency-Check) و به‌روزرسانی اجزای دارای CVE قبل از ارزیابی توصیه و در دستور کار قرار دارد.		

81- سرآیندها

شناسه الزام		**نام الزام**	
متن الزام	فعال‌سازی و پیکربندی صحیح سرآیندهای (Header) - Strict Transport Security - Cache-Control - X-Content-Type-Options - X-Frame-Options - XSS-Protection		
راهنمایی	Strict-Transport-Security: max-age=<seconds>[; includeSubDomains] Cache-Control: no-cache, no-store, must-revalidate Pragma: no-store		

	X-Content-Type-Options: nosniff
نحوه‌ی دسترسی	-
تصویر	پس از پیاده‌سازی، تصویر خروجی ابزار بررسی هدرها پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا هدرهای امنیتی (Strict Transport Security، Cache-Control، X-Content-Type-Options، X-Frame-Options، XSS-Protection) در پاسخ‌های سرور فعلاً ست نمی‌شوند. افزودن این سرآیندها هم‌زمان با فعال‌سازی TLS (NC-001) در دستور کار اصلاح قرار دارد.

82- Cookie

شناسه الزام		نام الزام	
متن الزام	پیکربندی صحیح Cookie		
راهنمایی	برای Cookieها، ویژگی‌های زیر را فعال نمایید. Samesite, secure, Httponly, Hostonly		
نحوه‌ی دسترسی	-		
تصویر	پس از پیاده‌سازی، تصویر پیکربندی کوکی‌ها پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا توکن نشست در وضعیت فعلی در کوکی سمت کلاینت (بدون ویژگی‌های Secure، HttpOnly، SameSite) نگهداری می‌شود؛ مهاجرت به کوکی امن HttpOnly همراه با سایر اصلاحات نشست (NC-008) در دستور کار است.		

83- درگاه‌های (Ports) باز

شناسه الزام		نام الزام	
متن الزام	تمامی درگاه‌هایی که از آن‌ها ستفاده نمی‌شود باید بسته باشند.		
راهنمایی	اگر درگاهی باز است، حتما دلیل باز بودن آن را توضیح دهید.		
نحوه‌ی دسترسی	درگاه‌های مورد استفاده محصول: 8080 (سرویس CTI)، 5432 (PostgreSQL — فقط روی localhost)، 8684، 5038 (AMI Asterisk) (سرور به‌روزرسانی سازنده).		
تصویر	تصویر خروجی ss -tulpn / nmap پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل درگاه‌های ضروری سرویس محصول و اجزای وابسته اعلام شد؛ سایر درگاه‌ها وابسته به پیکربندی سیستم‌عامل است. خروجی پورت‌اسکن محیط نصب نهایی قبل از ارزیابی پیوست می‌شود.		

84- متدهای ناامن

شناسه الزام		نام الزام	

متن الزام	نباید از متدهای ناامن استفاده شود.
راهنمایی	نباید از متدهای زیر استفاده شود و محصول به این درخواست‌ها باید با کد 4XX پاسخ دهد. PUT DELETE CONNECT OPTIONS TRACE PATCH در صورتی که از این متدها استفاده شده است، لازم است: 1 علت استفاده از آن‌ها تشریح شود 2 کنترل دسترسی روی این متدها اعمال شود و توضیح داده شود.
نحوه‌ی دسترسی	-
تصویر	پس از پیاده‌سازی، تصویر پاسخ 4XX برای متد ناامن پیوست شود.
توضیحات بیشتر	وضعیت: پیاده‌سازی نشده — بدون ادعا سازوکار رد متدهای ناامن (مانند TRACE و متدهای غیراستاندارد) با پاسخ 4XX در فیلتر سرور فعلاً اعمال نشده است؛ افزودن فهرست مجاز متدها در دستور کار اصلاح است.

85- ارسال یا دسترسی به فرم‌های حساس

شناسه الزام		**نام الزام**	
متن الزام	در ارسال یا دسترسی به فرم‌های حساس باید از Anti-CSRF استفاده شود.		
راهنمایی	ضمن استفاده از Anti-CSRF، باید به درستی پیکربندی شود و با هر درخواست منقضی و مجدد مقداردهی شود.		
نحوه‌ی دسترسی	فرم‌های حساس: صفحه ورود (/login) و تغییر گذرواژه.		
تصویر	پس از پیاده‌سازی، تصویر توکن CSRF در فرم‌ها پیوست شود.		
توضیحات بیشتر	وضعیت: پیاده‌سازی جزئی — نیازمند تکمیل درخواست‌های API با هدر Authorization (Bearer) ارسال می‌شوند که درخواست‌های متقابل‌جعل (CSRF) را برای این مسیرها ذاتاً کاهش می‌دهد. سازوکار توکن Anti-CSRF مستقل برای فرم‌ها و کوکی‌های احراز هویت‌شده در دستور کار اصلاح است.		