

مستند جامع پروژه CRM آتش فراز

معماری، دیتابیس، پنل مدیریت، پنل بازاریاب و برنامه تست

هدف سند: این سند بر اساس مطالعه فایل‌های SQL، PHP، قالب‌های مشترک، اسکریپت‌های اصلی پنل بازاریاب و ساختار داریی‌های پروژه تهیه شده است. هدف آن این است که یک فرد فنی یا تستر بتواند بدون حدس‌زدن، سامانه را راه‌اندازی، بررسی و سناریوهای اصلی را اجرا کند.

مقدار	مشخصه
سامانه اختصاصی بازرگانی آتش فراز	نام سامانه
CRM و مدیریت مشتری، بازاریاب و توزیع	نوع پروژه
PHP سنتی، PDO، MySQL، HTML/CSS/JavaScript	فناوری اصلی
فارسی، راست‌به‌چپ، تاریخ شمسی در نمایش	زبان رابط
syspakhshdb	پایگاه داده پیش‌فرض
http://atashfaraz.localhost	نشانی محلی پیشنهادی
۰/۱	نسخه درج‌شده در تنظیمات
۲۲ مرداد ۱۴۰۵ / ۱۳ اوت ۲۰۲۶	تاریخ بررسی

راهنمای خواندن: در متن سند، عبارت «فعال» یعنی در کد مسیر و پردازش متناظر وجود دارد؛ عبارت «نیازمند بررسی» یعنی از روی ارجاع، ساختار یا رفتار فعلی احتمال نقص، ناسازگاری یا ریسک وجود دارد و باید در تست تأیید شود.

فهرست فصل‌ها

- ۱. خلاصه اجرایی و دامنه بررسی
- ۲. معماری و فناوری پروژه
- ۳. ساختار فایل‌ها و قراردادهای مشترک
- ۴. معماری احراز هویت و دسترسی
- ۵. مدل کامل دیتابیس و روابط
- ۶. پنل مدیریت
- ۷. پنل بازاریاب
- ۸. جریان‌های کاری و قواعد کسب‌وکار
- ۹. راهنمای راه‌اندازی و داده‌های تست
- ۱۰. برنامه تست جامع
- ۱۱. بررسی‌های امنیتی و کیفیتی
- ۱۲. نواقص، ریسک‌ها و موارد نیازمند تصمیم
- ۱۳. نقشه مسیرها و فایل‌ها
- ۱۴. جمع‌بندی عملیاتی

ترتیب پیشنهادی مطالعه: برای تست بهتر، فصل ۹ را ابتدا اجرا کنید، سپس فصل‌های ۶ و ۷ را به‌ترتیب بخوانید و در پایان فصل ۱۰ را به‌صورت چک‌لیست اجرا کنید.

۱. خلاصه اجرایی و دامنه بررسی

پروژه یک CRM سبک و اختصاصی برای مدیریت مشتریان، بازاریاب‌ها و بخشی از عملیات توزیع است. کد بدون فریم‌ورک نوشته شده و هر صفحه PHP بخشی از منطق دریافت داده، اعتبارسنجی، واکنشی از دیتابیس و نمایش را همزمان انجام می‌دهد. این روش برای پروژه کوچک و کنترل‌شده قابل استفاده است، اما باعث می‌شود مرز بین لایه نمایش، منطق کسب‌وکار و دسترسی به دیتابیس در برخی فایل‌ها کمرنگ باشد.

نتیجه	وضعیت پوشش	حوزه بررسی
مسیرهای API، CRUD، login داخلی و پردازش‌های اصلی مستند شده‌اند.	بررسی فایل‌های اجرایی پروژه	PHP و منطق سمت سرور
جدول، کلیدها، وضعیت‌ها، داده‌های پایه و داده تست استخراج شده‌اند.	بررسی ۰۰۱، initial_schema، ۰۰۲ required_data و ۰۰۳ test_data	SQL و دیتابیس
مسیرهای صفحه، دسترسی و رفتار عملیاتی ثبت شده است.	بررسی ماژول‌های مشتری، کاربران، نقش‌ها، مکان، ناوگان، زون و لاگ	پنل مدیریت
احراز هویت مستقل، مالکیت مشتری و پیگیری‌ها شرح داده شده است.	بررسی تمام فایل‌های marketer و اسکریپت مشترک	پنل بازاریاب
ساختار RTL، layout، تاریخ شمسی و AJAX شرح داده شده است.	بررسی قالب‌های مشترک و CSS/JS اختصاصی	قالب و دارایی‌های رابط
جزئیات همه پلاگین‌های غیرمرتبط با منطق کسب‌وکار در این سند تکرار نشده است.	فهرست‌برداری و بررسی وابستگی‌های مورد استفاده	فایل‌های vendor

۱.۱. نتیجه کلی

- مرکز داده مشتری جدول customers است و برای پنل بازاریاب جدول موازی وجود ندارد.
- بازاریاب با visitor_id در customers شناخته می‌شود و تاریخچه تغییر مالک در customer_assignments ثبت می‌گردد.
- چرخه CRM از customer_activities، customer_status_history، customer_statuses و follow_ups تشکیل شده است.
- پنل مدیریت و پنل بازاریاب از یک users، roles و permissions مشترک استفاده می‌کنند، اما session‌های جدا دارند.
- بخش ناوگان از vehicles، تخصیص راننده به ماشین و تخصیص ماشین به زون استفاده می‌کند.
- زیرساخت برای ثبت سفارش و حسابداری کامل هنوز در مخزن حاضر نیست؛ accounting_id فقط به‌عنوان شناسه نگهداری می‌شود.

۲. معماری و فناوری پروژه

۲.۱. پشته فنی

نقش	فناوری/فایل	لایه
-----	-------------	------

نقش	فناوری/فایل	لایه
vhost.txt دامنه محلی atashfaraz.localhost را به ریشه پروژه وصل می‌کند.	Apache / VirtualHost	وب‌سرور
صفحات وب، endpointهای POST و خروجی‌های JSON.	PHP سنتی	Backend
اتصال به syspakhshdb با utf8mb4 و prepared statement.	PDO با MySQL / MariaDB	Database
پوسته دسکتاپ و جدول‌های مدیریتی.	Bootstrap RTL، jQuery، DataTables، SweetAlert، MetisMenu	Frontend مدیریت
رابط موبایل‌محور و فرم‌های AJAX.	CSS اختصاصی marketer-panel.css و JS marketer-panel.js	Frontend بازاریاب
نمایش شمسی و تبدیل تاریخ شمسی/میلادی.	Persian Datepicker و JDF	تقویم
نمایش فارسی در پوسته‌های مختلف.	IranSans، Estedad، Yekan و فونت‌های پروژه	فونت
ذخیره تصویر فروشگاه مشتری با نام تصادفی.	uploads/shop_images	فایل و تصویر

۲.۲. الگوی اجرای درخواست

۱. کاربر یک URL صفحه یا endpoint را فراخوانی می‌کند.
۲. صفحه session را آغاز می‌کند و فایل‌های تنظیمات، اتصال دیتابیس و توابع مشترک را وارد می‌کند.
۳. در صفحات مدیریت، دسترسی با hasPermission یا requirePermission کنترل می‌شود.
۴. در پنل بازاریاب، bootstrap.php_ نشست helper، ATASH_MARKETER_SESSION، CSRF و layout را آماده می‌کند.
۵. داده از MySQL با PDO خوانده یا در تراکنش نوشته می‌شود.
۶. صفحات مدیریت معمولاً با redirect و query string پیام می‌دهند؛ پنل بازاریاب endpointهای عملیاتی را JSON پاسخ می‌دهد.
۷. تاریخ‌ها در دیتابیس میلادی هستند و هنگام نمایش به شمسی تبدیل می‌شوند.



۲.۳. تنظیمات اتصال

ملاحظات تست/استقرار	مقدار فعلی در کد	پارامتر
برای سرور واقعی باید از تنظیمات محیطی استفاده شود.	localhost	Host
در ADMIN/sql.php نیز همین نام استفاده شده است.	sypakhshdb	Database
برای تولید ناامن است؛ کاربر محدود دیتابیس ایجاد شود.	root	Username
ریسک جدی در محیط غیرمحلی.	خالی	Password
برای فارسی مناسب است.	utf8mb4	Charset
در برخی فایل‌ها به صورت ASIA/TEHRAN نیز نوشته شده؛ یکسان‌سازی توصیه می‌شود.	Asia/Tehran	Timezone

۳. ساختار فایل‌ها و قراردادهای مشترک

نقطه ورود/نقش	محتوا	مسیر
اتصال PDO و متغیرهای عمومی سامانه.	app_settings.php و db_settings.php	/app_config
توابع مشترک، permission، لاگ، تبدیل تاریخ و helperهای lookup.	function.php	/core
پوسته پنل مدیریت.	layout_start/end، navbar، sidebar، header، footer	/templates
احراز هویت و خروج پنل مدیریت.	logout.php و login.php	/pages
هسته CRM.	CRUD مشتری، پروفایل، پیگیری و تاریخچه بازاریاب	/modules/customers
مدیریت گروه‌های مشتری.	CRUD دسته‌بندی مشتری	/modules/customerscat
مدیریت کاربران، راننده و بازاریاب.	CRUD کاربر و پروفایل	/modules/users
مدیریت RBAC.	CRUD نقش و دسترسی	/modules/roles
داده‌های جغرافیایی.	CRUD استان و شهر	/modules/locations
ناوگان پخش.	CRUD ماشین، تخصیص راننده و تاریخچه	/modules/vehicles
مسیر/ناحیه توزیع.	CRUD زون، تخصیص ماشین و مشتریان زون	/modules/zones
حسابرسی رخدادهای.	صفحه و API DataTables	/modules/logs
امنیت حساب کاربری.	تغییر رمز پنل مدیریت	/modules/adminsetting
مشتریان خود، ثبت مشتری و پیگیری.	پنل موبایل بازاریاب	/marketer

نقطه ورود/نقش	محتوا	مسیر
نصب دیتابیس.	schema، داده پایه و داده تست	/ADMIN/sql
ابزار نصب/ریست؛ حساس و نیازمند حفاظت.	اجرای فایل SQL و حذف جدولها	ADMIN/sql.php
وابستگی‌های frontend.	JS، CSS، فونت، پلاگین و تصاویر	/assets
فایل‌های runtime؛ باید backup و محدودسازی شوند.	تصاویر آپلودی فروشگاه	/uploads/shop_images

۳.۱. قرارداد layout پنل مدیریت

- هر صفحه معمولاً متغیرهای custom_css و custom_js را تعریف می‌کند.
- متغیرهای menuname و pagename برای active شدن منوی sidebar استفاده می‌شوند.
- layout_start.php session را بررسی و navbar، header و sidebar را باز می‌کند.
- layout_end.php footer، modal جست‌وجوی مشتری و footer_js را وارد می‌کند.
- برخی فایل‌ها به \$_SERVER['DOCUMENT_ROOT'] متکی هستند؛ اجرای پروژه در subdirectory بدون VirtualHost ممکن است مسیرها را خراب کند.

۳.۲. قرارداد پنل بازاریاب

رفتار	فایل/تابع
session جدا، اتصال، CSRF، login/permission، escape، تاریخ و layout.	marketer/_bootstrap.php
قالب مشترک، topbar، تاریخ شمسی، bottom navigation و بارگذاری JS.	marketer_page_start/end
پاسخ JSON با UTF-۸ و status code.	marketer_json
بررسی hash_equals برای فرم‌های تغییردهنده.	marketer_check_csrf
کمترین due_at پیگیری pending را در customers.next_follow_up_at ذخیره می‌کند.	marketer_refresh_next_followup
فرم‌های data-marketer-ajax-form را با fetch ارسال و redirect/alert را مدیریت می‌کند.	assets/js/marketer-panel.js

۴. معماری احراز هویت و دسترسی

۴.۱. ورود پنل مدیریت

۱. pages/login.php نام کاربری را در users جست و جو می‌کند.
۲. password_verify رمز bcrypt را بررسی می‌کند.
۳. کاربر باید status برابر active داشته باشد؛ pending، blocked، inactive پیام متفاوت دارند.
۴. session_regenerate_id(true) اجرا می‌شود.
۵. نقش‌ها از user_roles و permissions از permissions → role_permissions → user_roles خوانده می‌شوند.
۶. در session کلیدهای permissions، role_slugs، roles، user_id، permission_slugs و ذخیره می‌شوند.
۷. last_login_at به‌روزرسانی و رخداد ورود در logs ثبت می‌شود.

یافته مهم: در کد فعلی ورود اصلی صرفاً به active بودن کاربر و صحت رمز متکی است و در خود login.php مجوز panel.login را enforce نمی‌کند. تست باید مشخص کند آیا این رفتار عمدی است یا باید اصلاح شود.

۴.۲. ورود پنل بازاریاب

۸. marketer/login.php فقط کاربری را می‌پذیرد که role با slug=visitor داشته باشد.
۹. همان کاربر باید permission با slug=marketer.panel.login داشته باشد.
۱۰. status کاربر باید active باشد.
۱۱. session با نام ATASH_MARKETER_SESSION ساخته و permission slugها در marketer_permission_slugs ذخیره می‌شوند.
۱۲. CSRF token مستقل برای session بازاریاب ساخته می‌شود.

۴.۳. نقش‌ها و دسترسی‌های پایه

کاربرد	وضعیت پیش‌فرض در SQL	slug	نقش
مدیریت کامل سامانه.	تمام دسترسی‌های پایه و مدیریتی	superadmin	مدیر سیستم
مدیریت عملیاتی CRM در نظر گرفته شده.	رکورد نقش وجود دارد؛ دسترسی‌ها باید بررسی/تخصیص داده شوند.	system_expert	کارشناس سیستم
نقش سازمانی پیشنهادی.	رکورد نقش وجود دارد؛ دسترسی پایه کامل در seed نیست.	supervisor	ناظر
نقش سازمانی پیشنهادی.	رکورد نقش وجود دارد؛ دسترسی‌ها باید تنظیم شوند.	accountant	حسابدار
نقش سازمانی پیشنهادی.	رکورد نقش وجود دارد؛ دسترسی‌ها باید تنظیم شوند.	assistant_accountant	کمک حسابدار
نقش سازمانی پیشنهادی.	رکورد نقش وجود دارد؛ دسترسی‌ها باید تنظیم شوند.	warehouse_keeper	انباردار

کاربرد	وضعیت پیش فرض در SQL	slug	نقش
مشاهده مشتری خود، ثبت مشتری و پیگیری.	permission های پنل بازاریاب	visitor	بازاریاب
انتساب به ماشین و عملیات توزیع.	رکورد نقش؛ دسترسی های صفحه ای باید تنظیم شوند.	driver	راننده

۴.۴. مدل RBAC

```
users —< user_roles >— roles —< role_permissions >— permissions
```

اصلی session :

```
user_id + role_slugs + permission_slugs
```

بازاریاب session :

```
marketer_user_id + marketer_permission_slugs + marketer_csrf
```

۵. مدل کامل دیتابیس و روابط

ترتیب نصب: ترتیب نصب رسمی فایل ها: ۰۰۱ initial_schema.sql سپس ۰۰۲ required_data.sql و در صورت نیاز ۰۰۳ test_data.sql. اجرای دوباره ۰۰۱ روی دیتابیس موجود به دلیل ALTER های بدون شرط می تواند خطا بدهد؛ برای نصب تکراری، دیتابیس را پاک یا migration را idempotent کنید.

۵.۱. نقشه روابط

```
provinces_list 1 —< provinces_cities
customers_cat 1 —< customers
zones 1 —< customers
users 1 —< customers (created_by / visitor_id)
users N —N roles via user_roles
roles N —N permissions via role_permissions
vehicles N —N users via vehicle_driver_assignments (history)
zones N —N vehicles via zone_vehicle_assignments (history)
zones N —N users via zone_drivers (legacy/direct driver history)
customers 1 —< customer_assignments
customers 1 —< customer_status_history
customers 1 —< customer_activities
customers 1 —< follow_ups
users 1 —< follow_ups (assigned_to / created_by / completed_by)
users 1 —< logs (nullable)
```

۵.۲. جدول‌های جغرافیا و دسته‌بندی

رفتار حذف	کلید/قید	ستون‌های مهم	جدول
حذف استان، شهرهای وابسته را CASCADE می‌کند؛ UI قبل از حذف وجود شهر/مشتری را می‌سنجد.	id روی PK	id, name, ordered	provinces_list
با حذف استان حذف می‌شود.	FK prov_id → provinces_list.id	id, prov_id, name, ordered	provinces_cities
به دلیل FK مشتری، دسته دارای مشتری حذف نمی‌شود.	PK؛ soft delete مفهومی	id, name, descri, status, soft_deleted	customers_cat

۵.۳. کاربران و RBAC

روابط	ستون‌های مهم	جدول
مرجع نقش، مشتری، راننده، لاگ و پیگیری.	username یکتا، password, full_name, status, last_login_at, mobile یکتا	users
N به N با users و permissions.	name یکتا، slug یکتا، description	roles
از طریق role_permissions به نقش متصل می‌شود.	name, slug یکتا، description	permissions
حذف کاربر/نقش CASCADE.	user_id, role_id	user_roles
حذف نقش/مجوز CASCADE.	role_id, permission_id	role_permissions
ON DELETE SET NULL با user_id.	user_id nullable, log_type, log_event, ip_address, created_at	logs

۵.۴. ناوگان و توزیع

قواعد عملیاتی	فیلدهای مهم	جدول
نام در process یکتا بررسی می‌شود؛ status عددی ۱/۰.	name, area_name, description, status	zones
وضعیت active/inactive/maintenance.	plate_number یکتا، vehicle_code یکتا، vehicle_type, ownership_type, status	vehicles
فقط یک تخصیص active فعلی از طریق process نگهداری می‌شود.	vehicle_id, driver_id, assigned_from, assigned_to, status	vehicle_driver_assignments
یک ماشین نمی‌تواند هم‌زمان در دو زون فعال باشد.	zone_id, vehicle_id, assigned_from, assigned_to, status	zone_vehicle_assignments
جدول قدیمی/سازگاری؛ UI جدید بیشتر از تخصیص ماشین استفاده می‌کند.	zone_id, driver_id, is_primary, status, assigned_from	zone_drivers

۵.۵. جدول customers

دسته اطلاعات	ستونها	قاعده/توضیح
هویت	shop_name, owner_name, national_code, economic_code, birthday, shop_image	owner_name و mobile در منطق برنامه ضروری هستند؛ national_code الگوریتمی بررسی می‌شود.
تماس	mobile, phone, alternative_mobile, phone_verified_at, password	mobile اصلی یکتا و با ۰۹ + ۹ رقم اعتبارسنجی می‌شود.
مکان	province_id, city_id, address, postal_code, latitude, longitude	city باید با province انتخاب شده هم‌خوان باشد.
دسته و وضعیت	customer_category_id, status, profile_status, lifecycle_status_id	status وضعیت دسترسی است؛ lifecycle_status وضعیت CRM است.
مالکیت CRM	visitor_id, created_by, lead_source, first_contact_at, first_purchase_at, last_activity_at, next_follow_up_at, lost_at, lost_reason	visitor_id مالک فعلی و customer_assignments تاریخچه است.
فروش و توزیع	zone_id, visit_days, delivery_note, payment_type, credit_limit, settlement_days, customer_grade	در پنل بازاریاب فقط بخشی از این فیلدها قابل ثبت است.
تجهیزات/یادداشت	has_company_equipment, equipment_note, notes	بخش توزیع/اطلاعات تکمیلی.

۵.۶. وضعیت‌های CRM

slug	عنوان	رنگ seed	رفتار فعلی
lead	سرنخ	secondary	برای توسعه چرخه اولیه.
potential	مشتری بالقوه	info	وضعیت پیش‌فرض ثبت مشتری از هر دو پنل.
customer	مشتری واقعی	success	هنگام انتخاب، first_purchase_at در ویرایش پر می‌شود.
inactive	کم‌فعال / نیازمند پیگیری	warning	فعلاً تغییر دستی؛ job خودکار وجود ندارد.
lost	از دست رفته	danger	دلیل از دست رفتن اجباری و lost_at ثبت می‌شود.

۵.۷. فعالیت و پیگیری

چرخه	فیلدهای مهم	جدول
با ثبت مشتری یک رکورد اولیه و با تغییر lifecycle یک رکورد جدید.	old_status_id, new_status_id, changed_by, reason, created_at	customer_status_history
ثبت ویزیت اولیه و فعالیت حاصل از complete پیگیری.	performed_by, activity_type, activity_at, result, note	customer_activities
pending یا cancelled در پنل مدیریت؛ پنل بازاریاب فقط done → pending.	assigned_to, due_at, follow_up_type, status, result, note, completed_at, completed_by, created_by	follow_ups

۵.۸. قواعد حذف و یکپارچگی

- customers_cat دارای مشتری قابل حذف نیست؛ FK نیز ON DELETE RESTRICT است.
- حذف استان در سطح DB می‌تواند شهرها را cascade کند، اما process برنامه وجود شهر/مشتری را بررسی و حذف را منع می‌کند.
- حذف کاربر از نظر دیتابیس روی برخی روابط CASCADE و روی برخی RESTRICT یا SET NULL است؛ قبل از حذف کاربر اثر آن بررسی شود.
- حذف مشتری، activity، status history، assignment و followup‌های وابسته را به‌صورت cascade حذف می‌کند؛ در محیط واقعی بهتر است حذف سخت محدود شود.
- تاریخچه تخصیص‌ها با پایان دادن رکورد قبلی و درج رکورد جدید حفظ می‌شود؛ قید یکتایی فعال در سطح دیتابیس وجود ندارد و process باید مرجع باشد.

۶. پنل مدیریت

اصل تست پنل مدیریت: پنل مدیریت از مسیر `pages/login.php` وارد می‌شود و صفحات اصلی در `modules` قرار دارند. نمایش منو با `permission` انجام می‌شود، اما برای تست باید هم پنهان شدن منو و هم جلوگیری سمت سرور با URL مستقیم بررسی شود.

۶.۱. داشبورد

تست	رفتار فعلی	مجوز	مسیر
ورود با کاربر مجاز/غیرمجاز و بررسی عدم نمایش اطلاعات <code>session</code> .	صفحه پایه؛ بخشی از خروجی فعلی چاپ <code>session</code> و متن تست <code>permission</code> است.	<code>dashboard.view</code>	<code>/modules/dashboard/</code>

۶.۲. مدیریت مشتریان

قابلیت	مجوز اصلی	صفحه
صفحه عملیات مشتریان و لینک‌های دسترسی‌محور.	<code>customers.modules</code>	<code>modules/customers/index.php</code>
لیست کامل، فیلتر دسته‌بندی، <code>DataTables</code> و <code>export</code> <code>Excel/PDF</code> .	<code>customers.fulllist</code>	<code>modules/customers/list.php</code>
فرم کامل مشتری؛ دسته، هویت، عکس، تماس، مکان، مالی، توزیع و <code>CRM</code> .	<code>customers.add</code>	<code>modules/customers/add.php</code>
فرم بخش‌بندی‌شده با قفل کردن فیلدها بر اساس <code>permission</code> .	مجوزهای جزئی	<code>modules/customers/edit.php</code>
نمایش مشخصات، تاریخچه، <code>CRM</code> ، <code>assignment</code> ، <code>activities</code> و <code>followups</code> .	<code>customers.profile</code>	<code>modules/customers/profile.php</code>
لیست، فیلتر، ایجاد، انجام و لغو پیگیری.	<code>customers.followups.view/manage</code>	<code>modules/customers/followups.php</code>
تاریخچه تخصیص بازاریاب به مشتری.	<code>customers.visitor.assignments.log.view</code>	<code>modules/customers/visitor_change_list.php</code>
JSON endpoint برای شهرها، ثبت مشتری و ویرایش مشتری.	<code>customers.modules</code> + جزئی	<code>modules/customers/process_customer.php</code>
JSON endpoint برای ساخت، انجام و لغو پیگیری.	<code>customers.modules</code> + <code>manage</code>	<code>modules/customers/followups_process.php</code>

۶.۳. فرم ثبت/ویرایش مشتری

اعتبارسنجی/رفتار	فیلدهای شاخص	بخش فرم
کد ملی الگوریتمی؛ تصویر فقط JPG/PNG/WEBP و حداکثر ۵MB.	accounting_id, category, shop_name, owner_name, national/economic code, birthday, shop_image	عمومی
mobile اصلی یکتا و الگوی ۰۹xxxxxxx.	mobile, alternative_mobile, phone, password	تماس
شهر با استان بررسی می‌شود؛ شهرها AJAX هستند.	province, city, address, postal_code, latitude, longitude	مکان
بازاریاب باید فعال و دارای role visitor باشد؛ بازاریاب عادی فقط خودش را می‌گیرد.	zone_id, visitor_id, visit_days, delivery_note	تخصیص
cash/credit/cheque/both و رتبه A/B/C.	payment_type, credit_limit, settlement_days, customer_grade	فروش
برای اطلاعات امانی و توضیحات توزیع.	has_company_equipment, equipment_note, notes	تجهیزات
lost بدون دلیل پذیرفته نمی‌شود؛ تغییر وضعیت log و history می‌سازد.	lifecycle_status_id, customer_status, lost_reason, status_reason	CRM

۶.۴. دسته‌بندی مشتریان

- دسته عمومی با id=۱ یا نام عمومی ثابت تلقی می‌شود و قابل ویرایش/حذف نیست.
- دسته‌بندی نام تکراری فعال/soft_deleted نشده نمی‌پذیرد.
- حذف دسته فقط وقتی مجاز است که مشتری وابسته نداشته باشد.
- status دسته ۱ فعال و ۰ غیرفعال است؛ در فرم ثبت، دسته غیرفعال برای مشتری جدید قابل انتخاب نیست.

۶.۵. کاربران

صفحه	رفتار
users/index.php	فهرست کاربران، نقش‌ها، وضعیت، آخرین ورود و عملیات.
users/add.php	ایجاد کاربر با username، رمز حداقل ۶ کاراکتر، status، email، mobile و نقش.
users/edit.php	ویرایش اطلاعات، رمز اختیاری و جایگزینی نقش.
users/profile.php	پروفایل، نقش‌ها، آخرین ورود، تاریخ ایجاد و تعداد مشتری ثبت‌شده.
users/process.php	اعتبارسنجی، یکتایی username/mobile، activate/deactivate و ثبت log.

۶.۶. نقش‌ها و دسترسی‌ها

- roles/index.php تعداد کاربران و permission‌های هر نقش را نمایش می‌دهد.
- roles/add.php و roles/edit.php امکان انتخاب permission‌ها را دارند.
- نقش superadmin قابل حذف نیست و slug آن نباید تغییر کند.
- حذف نقش دارای کاربر مجاز نیست.
- ذخیره permission‌های نقش ابتدا role_permissions را پاک و سپس انتخاب‌های جدید را درج می‌کند؛ این عملیات در تراکنش انجام می‌شود.

۶.۷. استان‌ها و شهرها

- استان‌ها با ordered نزولی و سپس نام مرتب می‌شوند.
- هر شهر به یک استان وابسته است؛ نام شهر در یک استان تکراری نیست.
- استان دارای شهر یا مشتری حذف نمی‌شود.
- شهر دارای مشتری حذف نمی‌شود.
- تغییر استان یک شهر باید در تست اثر آن بر مشتری‌های قبلی بررسی شود؛ process فعلی اجازه تغییر می‌دهد.

۶.۸. ماشین‌ها و زون‌ها

عملیات اصلی	صفحات	ماژول
تعریف ماشین، مالکیت، وضعیت، تخصیص راننده، پایان تخصیص و تاریخچه.	index/add/edit/profile/assignments/process	vehicles
تعریف زون، ناحیه، وضعیت، تخصیص ماشین، مشتریان زون و تاریخچه.	index/add/edit/profile/assignments/process	zones
برچسب وضعیت، مالکیت، ارقام فارسی و escape.	helper مشترک	fleet_helpers.php

۶.۹. لاگ سیستم

- modules/logs/index.php جدول خالی اولیه را می‌سازد و DataTables از AJAX تغذیه می‌شود.
- modules/logs/ajax/get_logs_list.php جست‌وجو، sort امن با whitelist ستون‌ها و pagination را پیاده می‌کند.
- کاربر حذف‌شده به صورت سیستم/مهمان نمایش داده می‌شود.
- رخدادهای authentication، مشتری، دسته، کاربر، نقش، zones، vehicles، location و followups در بخش‌های مختلف ثبت می‌شوند.

۶.۱۰. تغییر رمز و ابزار SQL

هشدار	رفتار	بخش
CSRF در این فرم مشاهده نشد؛ در تست امنیتی بررسی شود.	تغییر رمز با رمز فعلی، حداقل ۶ کاراکتر و جلوگیری از تکرار رمز.	adminsetting/adminpass.php
هیچ احراز هویت مدیریتی در فایل دیده نشد؛ انتشار عمومی آن بسیار خطرناک است.	اجرای فایل تکی/چند فایل SQL با CSRF و حذف تمام جدول‌های دیتابیس.	ADMIN/sql.php

۷. پنل بازاریاب

اصل مالکیت: پنل بازاریاب رابطی مستقل و موبایل‌محور است. این پنل از همان جدول customers استفاده می‌کند اما با شرط visitor_id فقط مالک فعلی مشتری را می‌بیند. تغییر مالک، تغییر CRM و ویرایش کامل مشتری در این پنل وجود ندارد.

۷.۱. مسیرها و مجوزها

قابلیت	مجوز	مسیر
ورود مستقل بازاریاب.	marketer.panel.login + role visitor	marketer/login.php/
شمارنده مشتری من، پیگیری باز و پیگیری امروز.	marketer.panel.access	marketer/index.php/
لیست مشتریان اختصاص یافته با جست‌وجوی نام/فروشگاه/موبایل.	marketer.customers.view	marketer/customers.php/
پروفایل مشتری خود، پیگیری‌ها و ۲۰ فعالیت آخر.	marketer.customers.view	...=marketer/customer.php?id/
ثبت مشتری پایه.	marketer.customers.create	marketer/customer_create.php/
ثبت مشتری و ساخت assignment/history/activity.	marketer.customers.create + CSRF	marketer/customer_process.php/
AJAX شهرهای استان.	marketer.customers.create + CSRF	marketer/cities.php/
لیست pendingهای اختصاص یافته.	marketer.followups.view	marketer/followups.php/
ثبت و انجام پیگیری؛ لغو عمدی ممنوع.	marketer.followups.manage + CSRF	marketer/followup_process.php/
تغییر رمز شخصی.	marketer.panel.access	marketer/password.php/
پاک‌سازی نشست بازاریاب.	session	marketer/logout.php/

۷.۲. داشبورد بازاریاب

توضیح	منبع داده	کارت/بخش
تعداد مشتریان مالک فعلی.	COUNT customers WHERE visitor_id	مشتری من
وظایف تعیین تکلیف نشده.	COUNT follow_ups WHERE assigned_to AND pending	پیگیری باز
با تاریخ ذخیره شده میلادی/زمان سرور.	(DATE(due_at)=CURDATE)	پیگیری امروز
لینک ثبت مشتری پایه.	permission marketer.customers.create	ثبت مشتری
دسترسی مستقیم به پروفایل مشتری.	۵ followup اول بر اساس due_at	پیگیری های پیش رو

۷.۳. ثبت مشتری جدید

رفتار سمت سرور	فیلدها	بخش فرم
owner_name/category/mobile معتبر الزامی؛ grade فقط A/B/C.	owner_name, shop_name, mobile, alternative_mobile, category, grade	اطلاعات اصلی
city باید متعلق به province باشد؛ zone باید فعال باشد.	province, city, zone, postal_code, address	موقعیت
در customers.notes ذخیره می شود.	notes	یادداشت
بازاریاب نمی تواند مالک دیگری انتخاب کند.	visitor_id = session user	تخصیص خودکار
یک زنجیره اولیه برای CRM ساخته می شود.	customer_assignments, status_history, customer_activities, logs	رخدادهای پس از ثبت

۷.۴. پروفایل مشتری

- اطلاعات هویتی، موبایل، دسته، استان/شهر و آدرس را نمایش می دهد.
- پیگیری های مشتری را به ترتیب pending, done, cancelled و due_at نشان می دهد.
- آخرین ۲۰ activity را نمایش می دهد.
- اگر permission مدیریت پیگیری وجود داشته باشد، فرم ثبت پیگیری فعال می شود.
- هیچ فرم ویرایش عمومی مشتری در پنل بازاریاب وجود ندارد.

۷.۵. پیگیری‌های بازاریاب

اثر	مجاز؟	عملیات
INSERT follow_ups با assigned_to خود بازاریاب.	بله، روی مشتری خودش	ثبت پیگیری
pending → done, activity جدید، last_activity_at و next_follow_up_at.	بله، فقط پیگیری اختصاص‌یافته به خودش	انجام پیگیری
endpoint عمدتاً خطا می‌دهد و تلاش را در logs ثبت می‌کند.	خیر	لغو پیگیری
query profile شرط c.visitor_id = session user دارد.	خیر	مشاهده مشتری دیگر
باید از پنل مدیریت انجام شود.	خیر	تغییر بازاریاب

۷.۶. طراحی رابط

- در موبایل bottom navigation ثابت و در نمایشگر بزرگتر درون صفحه قرار می‌گیرد.
- فرم‌ها با data-marketer-ajax-form بدون refresh ارسال می‌شوند.
- CSRF از data-csrf روی marketer-main تأمین می‌شود.
- رنگ‌بندی فعلی بین دو تعریف در marketer-panel.css تغییر کرده است؛ در انتهای فایل متغیرهای جدیدتر دوباره تعریف شده‌اند و باید در مرورگر نهایی بررسی شود.
- پنل از فونت IranSans FaNum و تاریخ شمسی استفاده می‌کند.

۸. جریان‌های کاری و قواعد کسب‌وکار

۸.۱. ثبت مشتری از پنل مدیریت

۱۳. کاربر مجاز فرم را باز می‌کند.
۱۴. دسته فعال و اطلاعات پایه انتخاب می‌شود.
۱۵. موبایل یکتا و سایر فیلدها اعتبارسنجی می‌شوند.
۱۶. بازاریاب فعال با role visitor باید انتخاب شود؛ اگر کاربر خودش visitor باشد، visitor_id به session او محدود می‌شود.
۱۷. تصویر با MIME واقعی بررسی و در uploads/shop_images ذخیره می‌شود.
۱۸. تراکنش customers، customer_assignments، status_history، activity و log را ثبت می‌کند.
۱۹. وضعیت اولیه lifecycle_status_id=۲ یعنی potential است.

۸.۲. ویرایش مشتری و کنترل permission جزئی

بخش قابل تغییر	permission
نام فروشگاه، مالک، اطلاعات هویتی و تصویر.	customers.edit.general
موبایل دوم، تلفن، رمز مشتری و اطلاعات تماس.	customers.edit.contact
استان، شهر، آدرس، کدپستی و مختصات.	customers.edit.location
شناسه حسابداری.	customers.accounting.edit
روش پرداخت، سقف اعتبار، مهلت تسویه و grade.	customers.sales.edit
زون، روزهای ویزیت، تجهیزات و راهنمای توزیع.	customers.distribution.edit
تغییر visitor و بستن/ایجاد assignment history.	customers.edit.assignment
status، lifecycle دسترسی، lost reason و status history.	customers.edit.crm

۸.۳. ثبت و انجام پیگیری

```

create:
  validate customer + owner + due_at + type
  INSERT follow_ups(status=pending)
  next_follow_up_at = MIN(pending.due_at)

complete:
  UPDATE follow_ups(status=done, completed_at, completed_by)
  INSERT customer_activities
  UPDATE customers.last_activity_at
  refresh next_follow_up_at

cancel (مدیریت):
  UPDATE follow_ups(status=cancelled)
  refresh next_follow_up_at
    
```

۸.۴. چرخه وضعیت مشتری

اثر داده‌ای	محرك فعلی	انتقال
customer_status_history اولیه.	ثبت مشتری	NULL → potential
first_purchase_at اگر خالی باشد پر می‌شود.	انتخاب دستی در ویرایش	potential → customer
lost_reason اجباری و lost_at ثبت می‌شود.	انتخاب lifecycle lost	lost → هر وضعیت
lost_at و lost_reason پاک می‌شوند.	ویرایش دستی	lost → وضعیت دیگر
اتوماسیون زمانی فعلی وجود ندارد.	ویرایش دستی	inactive → هر وضعیت

۸.۵. تخصیص راننده و ماشین

۲۰. ماشین باید active باشد.
۲۱. راننده باید کاربر active با role driver باشد.
۲۲. در تخصیص جدید، رکورد active قبلی ended می‌شود و رکورد جدید درج می‌گردد.
۲۳. ماشین فعال نمی‌تواند هم‌زمان در زون دیگری تخصیص فعال داشته باشد.
۲۴. تاریخچه در profile و assignments قابل مشاهده است.

۹. راهنمای راه‌اندازی و داده‌های تست

۹.۱. پیش‌نیازها

- Apache با فعال بودن mod_rewrite/AllowOverride مطابق vhost.txt.
- PHP با PDO MySQL و توابع فایل/تصویر مورد استفاده.
- MySQL یا MariaDB با پشتیبانی utf8mb4 و foreign key.
- تنظیم DocumentRoot روی F:/۱۳-Localhost/atashfaraz یا مسیر معادل.
- دامنه محلی atashfaraz.local در hosts ویندوز.
- دسترسی نوشتن به uploads/shop_images.

۹.۲. نصب دیتابیس با ابزار پروژه

۲۵. دیتابیس خالی syspakhshdb را بسازید.
۲۶. به ADMIN/sql.php/ بروید؛ فقط در محیط محلی و پس از حفاظت دسترسی.
۲۷. initial_schema.sql را اجرا کنید.
۲۸. required_data.sql را اجرا کنید.
۲۹. برای محیط تست test_data.sql را اجرا کنید.
۳۰. پس از نصب، login مدیریت و بازاریاب را با سناریوهای فصل ۱۰ بررسی کنید.

ترتیب صحیح:
 001_initial_schema.sql
 002_required_data.sql
 003_test_data.sql (اختیاری برای تست)

۹.۳. کاربران seed و رمز تست

کاربرد تست	رمز seed	نقش	username
تست کامل پنل مدیریت.	password	مدیر سیستم	admin
تست رفتار نقش بدون permissionهای تخصیص یافته پیش فرض.	password	کارشناس سیستم	expert_۱
تست کاربر دوم.	password	کارشناس سیستم	expert_۲
مالک مشتریان ۱ و ۲.	password	بازاریاب	visitor_۱
مالک مشتریان ۳ و ۴.	password	بازاریاب	visitor_۲
راننده ماشین ۱ و زون ۱.	password	راننده	driver_۱
راننده ماشین ۲ و زون ۲/۳.	password	راننده	driver_۲

امنیت: رمزهای seed فقط برای محیط توسعه هستند. در اولین نصب واقعی باید admin و تمام حسابهای نمونه حذف یا رمز آنها تغییر داده شود.

۹.۴. دادههای تست نمونه

نمونههای درج شده	حوزه
استان گیلان و مازندران و شهرهای پایه.	جغرافیا
عمومی، ویژه، تستی.	دسته مشتری
۴ مسیر نمونه تهران غرب/شرق/شمال/جنوب.	زون
ISUZU-۰۰۱ و VAN-۰۰۱.	ماشین
۴ مشتری با visitor، zone، grade و payment متفاوت.	مشتری
تخصیص بازاریاب مشتری و راننده/ماشین/زون.	assignment

نکته داده تست: در test_data.sql_۰۰۳ بعضی آدرسهای متنی با استان/شهر انتخاب شده همخوان نیستند؛ این موضوع برای تست constraint برنامه مفید است اما برای داده نمایشی واقعی باید اصلاح شود.

۱۰. برنامه تست جامع

روش ثبت نتیجه: هر تست را با شماره، نقش، URL، داده ورودی، نتیجه مورد انتظار و نتیجه واقعی ثبت کنید. تست مجوز را هم با پنهان شدن منو و هم با ورود مستقیم به URL انجام دهید.

۱۰.۱. تست دودویی راهاندازی

- دامنه atashfaraz.localhost باز می‌شود و خطای ۵۰۰/مسیر مطلق دیده نمی‌شود.
- اتصال PDO به syspakhshdb برقرار است.
- صفحه login مدیریت باز می‌شود.
- ورود admin با password موفق و last_login_at تغییر می‌کند.
- خروج مدیریت session را می‌بندد.
- ورود visitor_۱ به marketer/login.php/ موفق است.
- پنل بازاریاب در موبایل و دسکتاپ بدون overflow اساسی نمایش داده می‌شود.
- استان و شهر در فرم بازاریاب با AJAX کار می‌کند.
- تصویر فروشگاه در uploads/shop_images ذخیره می‌شود.
- لاگ‌های ایجاد مشتری و پیگیری در modules/logs نمایش داده می‌شوند.

۱۰.۲. تست ورود و نشست

نتیجه مورد انتظار	سناریو	کد
خطای اعتبارسنجی و عدم query مؤثر.	username/password خالی در مدیریت	AUTH-۰۱
عدم ورود و ثبت log شکست.	رمز اشتباه مدیریت	AUTH-۰۲
عدم ورود با پیام وضعیت مربوط.	کاربر pending/blocked/inactive	AUTH-۰۳
session regenerate، نقش و permission در session.	ورود موفق مدیریت	AUTH-۰۴
پاک شدن session و redirect به login.	خروج مدیریت	AUTH-۰۵
رد شدن در login بازاریاب.	بازاریاب بدون role visitor	AUTH-۰۶
رد شدن در login بازاریاب.	visitor بدون marketer.panel.login	AUTH-۰۷
ساخت session مستقل و CSRF.	ورود موفق بازاریاب	AUTH-۰۸
redirect به login متناظر.	باز کردن URL پنل بدون session	AUTH-۰۹
نباید مجوز پنل مدیریت تلقی شود.	باز کردن صفحه مدیریت با session بازاریاب	AUTH-۱۰

۱۰.۳. تست CRUD مشتری

بررسی	سناریو	کد
رکورد customers، assignment، history، activity و log ایجاد شود.	ثبت با owner/mobile/category معتبر	CUS-۰۱
خطا و عدم ایجاد رکورد دوم.	ثبت با موبایل تکراری	CUS-۰۲
در صورت ورودی پنهان مناسب، رفتار normalize بررسی شود.	موبایل با رقم فارسی	CUS-۰۳
خطا.	alternative_mobile نامعتبر	CUS-۰۴
خطا.	کد ملی نامعتبر/تکراری	CUS-۰۵
خطا.	کد اقتصادی غیر ۱۲ رقمی	CUS-۰۶
خطا.	کد پستی غیر ۱۰ رقمی	CUS-۰۷
خطا.	city متعلق به province دیگر	CUS-۰۸
خطا.	visitor غیرفعال یا بدون role	CUS-۰۹
خطا و فایل نباید در مقصد بماند.	آپلود فایل غیرتصویری/بیش از ۵MB	CUS-۱۰
رد دسترسی.	ویرایش توسط visitor روی مشتری دیگری	CUS-۱۱
فیلدهای خارج از permission نباید تغییر کنند.	ویرایش با permission جزئی	CUS-۱۲
assignment قبلی ended و جدید active.	تغییر visitor	CUS-۱۳
خطا.	تغییر lifecycle به lost بدون دلیل	CUS-۱۴
first_purchase_at پر شود.	تغییر lifecycle به customer	CUS-۱۵
فایل قبلی در صورت امکان حذف و فایل جدید ثبت شود.	حذف/تعویض تصویر	CUS-۱۶

۱۰.۴. تست پیگیری و فعالیت

نتیجه مورد انتظار	سناریو	کد
رکورد pending و next_follow_up_at.	ثبت pending توسط مدیر برای مشتری و کاربر فعال	FUP-۰۱
موفق.	ثبت توسط visitor برای مشتری خودش	FUP-۰۲
رد مالکیت.	ثبت visitor برای مشتری دیگری	FUP-۰۳
خطا.	تاریخ شمسی نامعتبر	FUP-۰۴
خطا.	نوع followup نامعتبر	FUP-۰۵
assigned_to، activity، last_activity_at و refresh موعده بعد.	complete توسط assigned_to	FUP-۰۶
رد.	complete توسط کاربر دیگر بدون others.manage	FUP-۰۷

نتیجه مورد انتظار	سناریو	کد
refresh و cancelled موعده بعد.	cancel توسط مدیر	FUP-۰۸
رد عمدی و log تلاش.	cancel توسط بازاریاب	FUP-۰۹
خطا و عدم activity تکراری.	تعیین تکلیف دوباره همان پیگیری	FUP-۱۰

۱۰.۵. تست پنل بازاریاب

نتیجه مورد انتظار	سناریو	کد
فقط visitor_id همان کاربر.	لیست مشتریان visitor_۱	MKT-۰۱
نتایج فقط در محدوده مالک.	جستجوی owner/shop/mobile	MKT-۰۲
۴۰۴/عدم نمایش.	پروفایل id مشتری دیگر	MKT-۰۳
مالکیت خودکار و سه رکورد CRM اولیه.	ثبت مشتری پایه	MKT-۰۴
پیام مشتری تکراری.	duplicate mobile مشتری خودش	MKT-۰۵
پیام شماره متعلق به مشتری دیگر.	duplicate mobile مشتری دیگری	MKT-۰۶
فقط شهرهای استان.	انتخاب استان و city	MKT-۰۷
۴۱۹ و عدم تغییر داده.	ارسال بدون یا با CSRF اشتباه	MKT-۰۸
تبدیل صحیح و نمایش شمسی.	ثبت followup با تاریخ شمسی	MKT-۰۹
redirect به لیست و ثبت activity.	انجام followup	MKT-۱۰
رد و log.	لغو followup	MKT-۱۱
خطا.	تغییر رمز با رمز فعلی اشتباه	MKT-۱۲
رمز جدید معتبر، قدیمی نامعتبر.	تغییر رمز موفق و ورود مجدد	MKT-۱۳

۱۰.۶. تست RBAC و پنل مدیریت

موارد	نقش/مجوز	کد
همه منوهای seed و عملیات مجاز.	superadmin	RBAC-۰۱
عدم مشاهده منوهای users/roles/fleet مگر permission دستی.	visitor	RBAC-۰۲
عدم نمایش لیست کامل و رد URL.	بدون customers.fulllist	RBAC-۰۳
عدم تغییر visitor حتی با POST دستکاری شده.	بدون customers.edit.assignment	RBAC-۰۴
فقط assigned خودش.	بدون customers.followups.others.manag	RBAC-۰۵

موارد	نقش/مجوز	کد
	e	
عدم نمایش/رد endpoint تخصیص.	بدون vehicles.driver.assign	RBAC-۰۶
دکمه حذف و endpoint هر دو مسدود.	بدون locations.delete	RBAC-۰۷
رفتار واقعی login و تصمیم اصلاحی ثبت شود.	کاربر فعال بدون permission panel.login	RBAC-۰۸

۱۰.۷. تست ناوگان و زون

- □ کد ماشین و پلاک تکراری رد شود.
- □ ماشین شخصی بدون owner_name رد شود.
- □ راننده غیر driver یا inactive رد شود.
- □ تخصیص راننده جدید، قبلی را ended کند.
- □ پایان تخصیص بدون رکورد active خطا دهد.
- □ ماشین در زون دوم همزمان قابل تخصیص نباشد.
- □ تخصیص ماشین غیرفعال به زون رد شود.
- □ تاریخچه راننده و زون در profile و assignments یکسان باشد.
- □ تعداد مشتری زون با customers.zone_id سازگار باشد.

۱۰.۸. تست لاگ و حسابرسی

- □ ورود موفق و ناموفق مدیریت و بازاریاب log داشته باشد.
- □ ثبت، ویرایش و تغییر visitor مشتری log داشته باشد.
- □ تغییر lifecycle با reason در history و log دیده شود.
- □ ثبت، انجام و لغو پیگیری log داشته باشد.
- □ تلاش لغو توسط بازاریاب log شود.
- □ IP در محیط واقعی مقدار معتبر داشته باشد.
- □ جستجوی لاگ با نام کاربر، نوع، شرح و IP نتیجه درست بدهد.
- □ مرتب سازی DataTables فقط روی ستون های whitelist انجام شود.

۱۱. بررسی‌های امنیتی و کیفیت

۱۱.۱. موارد مثبت موجود

- اتصال دیتابیس با PDO و emulate prepares=false است.
- رمزها با password_hash و password_verify مدیریت می‌شوند.
- session_regenerate_id در ورود استفاده شده است.
- پنل بازاریاب CSRF دارد و درخواست‌های تغییردهنده را بررسی می‌کند.
- خروجی‌های پنل بازاریاب با marketer_e escape می‌شوند.
- پارامترهای اصلی SQL با prepared statement ارسال می‌شوند.
- مرتب‌سازی لاگ با whitelist ستون‌ها کنترل شده است.
- فایل تصویر با extension و MIME واقعی بررسی می‌شود.

۱۱.۲. ریسک‌ها و آزمون‌های امنیتی اجباری

ریسک	شاهد کد	تست/اقدام اصلاحی
auth بدون ADMIN/sql.php بدون	فایل session و CSRF دارد اما requirePermission یا login ندارد.	در production مسدود/حذف؛ دسترسی فقط local یا admin.
CSRF ناقص در پنل مدیریت	فرم‌های users, roles, locations, vehicles, zones و adminpass توکن ندارند.	POST از سایت دیگر/توکن جعلی تست و CSRF سراسری اضافه شود.
رمز دیتابیس root خالی	ADMIN/sql.php و db_settings.php.	کاربر کم‌دسترسی و secret محیطی.
مسیرهای مطلق و DocumentRoot	layout و AJAX ها به / و SERVER['DOCUMENT_ROOT']\$_ متکی‌اند.	استقرار در root واقعی و تست subdirectory.
حذف سخت مشتری	FKهای وابسته CASCADE هستند.	محدود کردن DELETE و soft delete واقعی.
آپلود در web root	uploads/shop_images داخل ریشه عمومی.	هدر/پسوندد/دسترسی و جلوگیری از اجرای script.
نمایش خطای فنی	برخی JSONها e->getMessage () را برمی‌گردانند.	در production پیام عمومی و log داخلی.
عدم قید یکتایی فعال assignment	unique فقط در برخی جداول روی زوج اصلی نیست.	قفل منطقی/transaction و گزارش duplicate فعال.

۱۱.۳. کیفیت و نگهداری

- منطق مشابه در process های customers و marketer تکرار شده و تغییرات آینده ممکن است واگرا شوند.
- نامگذاری وضعیت‌ها و متن‌ها در بعضی فایل‌ها تکرار شده؛ enum/constant مرکزی مفید است.
- دو نسخه متغیرهای CSS در marketer-panel.css وجود دارد و آخرین تعریف برنده می‌شود.
- برخی لینک‌ها و asset به مسیرهایی اشاره می‌کنند که در مخزن فعلی موجود نیستند.
- وجود فایل‌های قدیمی و vendorهای متعدد نگهداری frontend را دشوار می‌کند.
- تست خودکار PHP و migration versioning در پروژه دیده نشد.

۱۲. نواقص، ریسک‌ها و موارد نیازمند تصمیم

اولویت	مورد	اثر	پیشنهاد
بحرانی	ADMIN/sql.php قابل دسترسی بدون احراز هویت	اجرای SQL یا حذف کل دیتابیس	حذف از web root یا افزودن auth قوی و محدودیت IP.
بالا	رمز دیتابیس root خالی	دسترسی کامل در صورت compromise	secret محیطی و کاربر محدود.
بالا	CSRF در اکثر فرم‌های مدیریت	تغییر داده با درخواست جعلی	helper مرکزی CSRF برای تمام POSTها.
بالا	ارجاع به modules/reports و modules/support بدون فایل	لینک ۴۰۴ در sidebar	ماژول بسازید یا لینک را حذف/غیرفعال کنید.
بالا	ارجاع به includes/search_۱.php وجود ندارد	جست‌وجوی modal کار نمی‌کند	endpoint را ایجاد یا modal را حذف کنید.
بالا	ارجاع به modules/forms/add.php وجود ندارد	دکمه سریع header خراب	ماژول forms را ایجاد یا لینک را حذف کنید.
متوسط	حذف مشتری به ajax/customer_delete_ajax.php اشاره می‌کند ولی فایل در tree دیده نشد	حذف مشتری احتمالاً ۴۰۴ است	endpoint امن با permission و soft delete.
متوسط	داشبورد هنوز خروجی print_r session/متن تست دارد	نشت اطلاعات و ظاهر غیرنهایی	پاک‌سازی قبل از production.
متوسط	initial_schema.sql idempotent_۰۰۱ کامل نیست	اجرای دوباره خطا می‌دهد	migrationهای نسخه‌دار یا IF NOT EXISTS برای ALTER.
متوسط	داده تست استان/آدرس ناسازگار	گزارش‌های غلط در تست نمایشی	داده seed را هماهنگ کنید.
کم	مرز PHP/HTML/SQL در فایل‌های بزرگ	تست و تغییر سخت‌تر	تفکیک service/repository/view در فاز refactor.

۱۲.۱. ارجاع‌های شکسته شناسایی شده

وضعیت در مخزن	محل ارجاع	ارجاع
پوشه modules/reports وجود ندارد.	templates/sidebar.php	modules/reports/
پوشه modules/support وجود ندارد.	templates/sidebar.php	modules/support/
پوشه includes و فایل endpoint وجود ندارد.	templates/footer_js.php	includes/search_۱.php/
پوشه modules/forms وجود ندارد.	templates/header_navbar.php	modules/forms/add.php/
در فهرست فایل‌های فعلی دیده نشد.	modules/customers/list.php	ajax/customer_delete_ajax.php

۱۲.۲. تصمیم‌های کسب‌وکاری باز

- چه رویدادی lifecycle_status را از potential به customer تغییر می‌دهد: ثبت سفارش، تأیید مدیر یا ورود دستی؟
- آیا بازاریاب دفتر باید بتواند پیگیری بازاریاب دیگر را انجام دهد؟
- آیا بازاریاب باید بتواند status CRM یا فقط followup را تغییر دهد؟
- آیا حذف مشتری باید ممنوع و به soft delete تبدیل شود؟
- تعریف دقیق استفاده از accounting_id و سرویس تست اتصال چیست؟
- منطق inactive شدن بعد از سه ماه بر اساس last_activity_at یا last_purchase چه باشد؟
- آیا یک ماشین می‌تواند در چند زون به‌صورت هم‌زمان باشد یا فقط انتقال تاریخی مجاز است؟

۱۳. نقشه مسیرها و فایل‌ها

۱۳.۱. مسیرهای عمومی

URL	فایل	احراز/خروجی
pages/login.php/	pages/login.php	ورود مدیریت؛ HTML.
pages/logout.php/	pages/logout.php	خروج مدیریت.
marketer/login.php/	marketer/login.php	ورود بازاریاب؛ HTML.
marketer/logout.php/	marketer/logout.php	خروج بازاریاب.
ADMIN/sql.php/	ADMIN/sql.php	اجرای SQL؛ خطرناک و باید حفاظت شود.

۱۳.۲. مسیرهای مشتری و CRM

مسیر	کارکرد
/modules/customers/	redirect به list.php.
modules/customers/list.php/	لیست مشتری.
modules/customers/add.php/	ثبت مشتری.
modules/customers/edit.php?id=N/	ویرایش مشتری.
modules/customers/profile.php?id=N/	پروفایل مشتری.
modules/customers/followups.php/	لیست و مدیریت پیگیری.
/modules/customers/visitor_change_list.php	تاریخچه بازاریاب.
/modules/customers/process_customer.php	POST/JSON ثبت، ویرایش و شهرها.
/modules/customers/followups_process.php.	POST/JSON پیگیری.
/modules/customerscat/	دسته‌بندی مشتری.

۱۳.۳. مسیرهای مدیریت سیستم و توزیع

صفحات	ماژول
index.php, add.php, edit.php, profile.php, process.php	users
index.php, add.php, edit.php, process.php	roles
index.php, province_add.php, province_edit.php, city_add.php, city_edit.php, process.php	locations
index.php, add.php, edit.php, profile.php, assignments.php, process.php	vehicles
index.php, add.php, edit.php, profile.php, assignments.php, process.php	zones
index.php, ajax/get_logs_list.php, js/logs_list.js	logs
adminpass.php, adminpass_process.php	adminsetting

۱۳.۴. مسیرهای پنل بازاریاب

شرح	نوع	فایل
session و helper.	shared	bootstrap.php_
داشبورد.	page	index.php
مشتریان من.	page	customers.php
پروفایل مشتری.	page	customer.php
فرم ثبت.	page	customer_create.php
ثبت مشتری.	endpoint	customer_process.php
شهرها.	endpoint	cities.php
پیگیری‌های من.	page	followups.php
ثبت/انجام پیگیری.	endpoint	followup_process.php
تغییر رمز.	page/endpoint	password.php / password_process.php

۱۴. جمع‌بندی عملیاتی

پروژه از نظر هسته CRM، مدل مشتری، مالکیت بازاریاب، پیگیری و تاریخچه، پایه قابل استفاده‌ای دارد. مسیر پیشنهادی برای بهره‌برداری ایمن این است که ابتدا موارد بحرانی فصل ۱۲ اصلاح شوند، سپس migration و داده seed پایدار شوند، بعد تست‌های فصل ۱۰ در یک محیط تمیز اجرا و مستند گردند.

۱۴.۱. ترتیب اولویت اصلاح

- ۳۱. بستن یا حفاظت کامل ADMIN/sql.php.
- ۳۲. حذف root بدون رمز و انتقال secrets به تنظیمات محیطی.
- ۳۳. افزودن CSRF به تمام POSTهای پنل مدیریت.
- ۳۴. رفع مسیرهای شکسته search، forms، support، reports و حذف مشتری.
- ۳۵. پاک‌سازی داشبورد و خروجی‌های debug.
- ۳۶. اصلاح idempotency فایل‌های SQL و ایجاد نسخه‌بندی migration.
- ۳۷. تعریف سیاست حذف مشتری و assignmentهای فعال در سطح دیتابیس.
- ۳۸. تکمیل تست‌های RBAC و قرارداد کسب‌وکاری lifecycle.
- ۳۹. سپس refactor تدریجی منطق تکراری مشتری/پیگیری به helper یا service مشترک.

۱۴.۲. چک‌لیست تحویل نسخه تست

- □ دیتابیس از صفر نصب شد.
- □ داده تست پاک و دوباره درج شد.
- □ visitor_۲، visitor_۱، admin و driverها تست شدند.
- □ تمام URLهای مجاز و غیرمجاز بررسی شدند.
- □ ثبت مشتری، ویرایش، تصویر، assignment و CRM تست شد.
- □ ثبت/انجام/لغو پیگیری و next_follow_up_at بررسی شد.
- □ لاگ‌های مهم قابل جست‌وجو و قابل تطبیق با عملیات هستند.
- □ ابزار SQL از دسترس عمومی خارج است.
- □ خطاهای PHP و ۴۰۴های منابع در مرورگر باقی نمانده‌اند.
- □ backup و rollback دیتابیس قبل از استقرار تهیه شده است.

نتیجه نهایی: این سند وضعیت کد موجود را توصیف می‌کند، نه الزاماً وضعیت مطلوب کسب‌وکار. هر جا رفتار فعلی با تصمیم سازمانی متفاوت است، تصمیم رسمی باید به permission، migration، تست و سپس کد تبدیل شود.