سطح دسترسی ادمین‌ها در سیستم Greenshop

این سند به طور مفصل شرح می‌دهد که هر نقش مدیریتی تعریف شده در سیستم Greenshop دارای چه سطوح دسترسی (Permissions) و محدودیت‌هایی در بخش‌های مختلف سیستم است. هدف اصلی این سند، تضمین اصل "حداقل امتیاز" (Principle of Least Privilege) در مدیریت داخلی سیستم است.

---

1. ساختار نقش‌ها و تعاریف اولیه

سیستم Greenshop از چهار سطح اصلی کاربر تعریف می‌کند:

1. SuperAdmin (سوپرادمین): بالاترین سطح دسترسی، مسئول نگهداری و پیکربندی کل سیستم.
2. Manager (مدیر): سطح مدیریتی متوسط، مسئول عملیات روزمره فروش و مدیریت کاربران سطح پایین.
3. Seller (فروشنده): کاربر تجاری که مسئول مدیریت محصولات و موجودی خود است.
4. Customer (مشتری): کاربر نهایی سیستم.

این سند تمرکز اصلی خود را بر روی نقش‌های SuperAdmin و Manager قرار می‌دهد.

1.1. نقش سوپرادمین (super_admin)

نقش سوپرادمین به دلیل ماهیت حیاتی آن، دسترسی بی قید و شرط به تمامی بخش‌های مدیریتی و زیرساختی سیستم را دارد.

الف) مدیریت کاربران سیستم (User Management)

سوپرادمین می‌تواند تمامی عملیات CRUD (ایجاد، مشاهده، به‌روزرسانی، حذف) را بر روی هر چهار نوع کاربر اجرا کند: * ایجاد، ویرایش، حذف Admins (شامل نقش‌های Manager و دیگر SuperAdmins). * ایجاد، ویرایش، حذف Sellers (شامل تأیید هویت و تعلیق حساب‌های

فروشندگان). * ایجاد، ویرایش، حذف Customers (شامل بازنشانی رمز عبور و مسدودسازی حساب‌ها).

ب) مدیریت محصولات و موجودی (Inventory Management)

- مشاهده، ویرایش، و حذف محصولات متعلق به همه فروشندگان فعال در پلتفرم.
- تأیید یا رد محصولات جدید که نیاز به بازبینی دارند.

ج) مدیریت سفارشات و مالی (Order & Financial Management)

- مشاهده و مدیریت کامل تمامی سفارشات ثبت شده در سیستم، صرف نظر از وضعیت پرداخت یا ارسال.
- دسترسی به گزارش‌های مالی جامع و کل سیستم، شامل تمامی تراکنش‌ها و کمیسیون‌های دریافتی.

د) دسترسی به داده‌های حساس و تنظیمات هسته (Core System Access)

- دسترسی مستقیم به مسیرهای زیرساختی: مانند `api/admins/secure-data/` که شامل اطلاعات پیکربندی سرور، کلیدهای رمزنگاری و تنظیمات دیتابیس است.
- تنظیمات کل سیستم (Global Settings): شامل مدیریت توکن‌های امنیتی (JWT keys)، تنظیمات امنیتی (مانند Rate Limiting) و مدیریت نقش‌ها.
- دسترسی کامل به لاگ‌های عملیاتی (Audit Logs) و گزارش‌های خطای سیستم.

1.2. نقش مدیر معمولی (manager)

نقش مدیر معمولی برای اجرای عملیات تجاری و پشتیبانی روزانه طراحی شده است و دسترسی‌های زیرساختی را ندارد.

الف) مدیریت محتوا و محصولات

- مدیریت محصولات: توانایی کامل در افزودن، ویرایش، حذف محصولات (فقط محصولاتی که مالک آن‌ها (Seller) فعال است یا کاربر خودش آن را ایجاد کرده است).

- مدیریت فروشندگان: مشاهده لیست فروشندگان، تأیید وضعیت فعال/غیرفعال، و انجام عملیات نرم بر روی حساب‌های فروشنده (مانند تعلیق موقت).
- مدیوتریت مشتریان: مشاهده پروفایل مشتریان، پشتیبانی، و بازنشانی رمز عبور در صورت درخواست رسمی.

ب) گزارش‌دهی

- مشاهده گزارش‌های عملیاتی مانند حجم فروش روزانه/هفتگی، سطح موجودی انبار (Aggregate Inventory Levels)، و عملکرد کلی فروشندگان.
- محدودیت: گزارش‌های مالی حساس که مستقیماً به ساختار درآمدی و نرخ‌های کمیسیون مربوط می‌شوند، برای این نقش مسدود است.

ج) محدودیت‌های کلیدی (Constraints)

1. مدیریت ادمین‌ها: Manager توانایی CRUD بر روی SuperAdmin ها یا دیگر Manager ها را ندارد. او فقط می‌تواند نقش‌های Seller و Customer را مدیریت کند.
2. داده‌های حساس: دسترسی به مسیرهایی نظیر `api/admins/secure-data/` به شدت مسدود است. تلاش برای دسترسی منجر به خطای `Forbidden 403` خواهد شد.
3. تغییر نقش‌ها: Manager نمی‌تواند سطح دسترسی یا نقش‌های ادمین‌های دیگر را تغییر دهد.

---

2. بخش‌هایی که هر نوع Admin نمی‌تواند دسترسی داشته باشد

حتی سوپرادمین نیز در چارچوب امنیتی برخی از عملیات محدود می‌شود، به خصوص آن‌هایی که مربوط به هویت واقعی کاربران یا زیرساخت‌های بسیار حساس خارج از محیط اپلیکیشن است.

الف) داده‌های خصوصی سطح بالای ادمین‌ها

- رمز عبور هش نشده: هیچ نقشی (حتی SuperAdmin) نباید به نسخه plaintext رمز عبور سایر ادمین‌ها دسترسی داشته باشد. این داده‌ها باید تنها در زمان ورود (Login) با استفاده از مقایسه هش معتبر شوند.

- کلیدهای خصوصی: دسترسی به کلیدهای خصوصی JWT یا کلیدهای رمزنگاری SSL/TLS که در محیط‌های امن سخت‌افزاری (HSM) ذخیره شده‌اند، ممنوع است.

ب) عملیات نقش‌های دیگر (Role Hijacking Prevention)

- ثبت‌نام به عنوان فروشنده/مشتری: Admin ها نباید بتوانند از APIهای عمومی ثبت‌نام (Sign-up Endpoints) برای ایجاد اکانت جدید در نقش Seller یا Customer استفاده کنند. عملیات ایجاد Seller یا Customer باید از طریق پنل ادمین (Admin Panel) و با تعیین صریح نقش انجام شود.
- مدیریت سبد خرید شخصی: Admin ها نمی‌توانند به سبد خرید یا تاریخچه سفارشات شخصی یک مشتری خاص دسترسی پیدا کنند مگر از طریق مسیرهای پشتیبانی مجاز (مانند `api/admin/customer/{id}/cart/`).

ج) مالکیت (Ownership Checks)

در مواردی که یک عملیات بر اساس مالکیت انجام می‌شود (مثلاً حذف یک محصول): * اگر یک Manager سعی کند محصولی را که متعلق به یک Seller دیگر است، حذف کند، عملیات باید توسط سیستم رد شود، مگر آنکه مدیر سیستم (SuperAdmin) باشد. * APIهای عمومی محصول باید اطمینان حاصل کنند که درخواست از طرف مالک واقعی محصول یا یک ادمین مجاز (SuperAdmin/Manager) انجام شده است.

د) عملیات مالی تایید شده (Escrow & Treasury Operations)

- عملیات برداشت وجوه بزرگ از حساب‌های تجاری یا تغییر نرخ کمیسیون سیستمی معمولاً نیاز به یک نقش مجزا (مانند Finance Auditor) یا تأییدیه چند مرحله‌ای (Multi-Factor Approval) دارند که خارج از اختیارات SuperAdmin یا Manager استاندارد است.

---

3. جدول خلاصه دسترسی‌ها بر اساس نقش

این جدول نمای کلی دسترسی به مسیرهای کلیدی (API Endpoints) را نشان می‌دهد. (CRUD: Create, Read, Update, Delete)

مسیر / عملیات	customer	seller	manager	super_admin	توضیحات
`/api/admins/secure-data` (داده‌های حساس سیستمی)					تنظیمات زیرساختی و کلیدهای رمزنگاری.
CRUD Admin (تغییر نقش‌های ادمین)					فقط سوپرادمین مجاز به مدیریت ادمین‌ها است.
CRUD Sellers (ایجاد/ حذف فروشندگان)					مدیر می‌تواند فروشندگان را فعال/غیرفعال کند.
CRUD Customers (مدیریت حساب مشتریان)					پشتیبانی و مسدودسازی حساب‌ها.
CRUD Products (همه فروشندگان)					قابلیت نظارت بر موجودی کل.
CRUD Products (فقط محصولاتی که مالک خودش است)					فروشنده فقط محصولات خود را مدیریت می‌کند.
گزارش‌های مالی حساس (نرخ کمیسیون، سود خالص)					گزارشات سطح بالا برای تحلیل کسب و کار.
مدیریت سفارشات کل سیستم (مشاهده و تغییر وضعیت)					برای حل مشکلات ارسال و بازپرداخت.
دسترسی به گزارش‌های عملکرد (Performance Metrics)					داشبوردهای عملیاتی روزانه.
عملیات ورود به سیستم (Authentication)					همه نقش‌ها باید بتوانند وارد شوند.

---

4. توصیه و گام‌های بعدی برای افزایش امنیت

برای تضمین یک سیستم چندسطحی قوی، اقدامات زیر باید در فاز بعدی پیاده‌سازی شوند:

الف) پیاده‌سازی سیاست‌های دقیق در سطح API Gateway

تمام درخواست‌های ورودی به بک‌اند باید در سطح Gateway توسط یک middleware بررسی شوند تا نقش (Role) استخراج شده از JWT با مسیر درخواستی (Endpoint Path) مطابقت داشته باشد. در صورت عدم تطابق، پاسخ باید `HTTP 403 Forbidden` باشد، نه فقط `Unauthorized 401` .

ب) افزایش تست‌های منفی (Negative Testing)

توسعه دهندگان باید سناریوهای زیر را به طور مستمر تست کنند: 1. عدم وجود توکن: کاربر بدون توکن سعی می‌کند به یک مسیر ادمین دسترسی یابد (انتظار: 401). 2. توکن منقضی شده: کاربر با توکن منقضی سعی می‌کند دسترسی بگیرد (انتظار: 401 و الزام به بازنگری). 3. نقش غیرمجاز: یک `Manager` سعی می‌کند به مسیر سوپرادمین دسترسی یابد (انتظار: 403). 4. تلاش برای Role Escalation: کاربر با نقش پایین‌تر سعی می‌کند پارامترهای نقش خود را در درخواست‌های API دستکاری کند.

ج) استفاده از Authorization Claims در JWT

به جای بررسی نقش در هر درخواست، اطلاعات نقش (Role) و ID کاربر باید مستقیماً در Claims توکن JWT تعبیه شود. این امر باعث می‌شود که فرآیند اعتبارسنجی سریع‌تر شده و وابستگی به دیتابیس در هر درخواست کاهش یابد.

مثال ساختار JWT Claim (برای Manager):

```
                                        }
                                  ,"sub": "user_123"
                               ,roles": ["manager"]"
,permissions": ["product_crud_all", "customer_support"]"
                                  exp": 1678886400"
                                        {
```

د) ممیزی منظم (Regular Auditing)

باید یک سیستم خودکار برای بررسی دسترسی‌های غیرمعمول ادمین‌ها تنظیم شود. هر تلاشی که منجر به خطای 403 در مسیرهای حیاتی شود، باید به عنوان یک رویداد امنیتی به لاگ‌های سوپرادمین ارسال گردد.