

(Open-Source Compliance) گزارش انطباق با نرم افزار متن باز Report — ۱,۰ نسخه

تاریخ: **۲۵/۰۵/۱۴۰۳**

**پروژه ShahnamehMap

تهیه کننده: **تیم فنی**

هدف: **مستندسازی و استگی های متن باز، تحلیل ریسک های مجازی**
و ارائه برنامه مدیریت ریسک برای اطمینان (Copyleft) به ویژه مجوزهای
از رعایت مقررات و محافظت از مالکیت فکری اختصاصی پروژه.

۱. خلاصه اجرایی و وضعیت کلی

از تعداد قابل توجهی کتابخانه و فریمورک ShahnamehMap پلتفرم
(Permissive Licenses) متن باز استفاده می کند که عمدهاً تحت **مجوزهای مجاز
همستند. این مجوزها MIT, Apache 2.0 و BSD مانند** هستند.

معمولًاً خطر مستقیمی برای اجباری شدن انتشار سورس کد اختصاصی ما ایجاد نمی‌کند.

Copyleft با این حال، شناسایی و مدیریت چند وابستگی با مجوزهای GPL و AGPL مانند) حیاتی است. در حال حاضر، هیچ یک از این به گونه‌ای استفاده نمی‌شوند که کل سورس کد Copyleft وابستگی‌های کند. اکثر آن‌ها در فرآیندهای توسعه Copyleft پروژه را مشمول شرایط یا ابزارهای داخلی استفاده شده‌اند.

در بخش GPL ریسک اصلی: استفاده ناخواسته از یک کتابخانه تحت که می‌تواند منجر به الزام انتشار سورس کد سمت سرور سرور شود. این مورد بررسی و حذف شده است.

وضعیت انطباق: ✓ در حالت کلی ایمن است، اما نیاز به نظارت مستمر و فرآیندهای کنترل دارد

**روش‌شناسی و ابزارهای اسکن .۲##

برای تهیه این گزارش از روش‌های زیر استفاده شده است

- * برای (`npm audit` اسکن خودکار:)* استفاده از ابزار `license-checker`.
- * بررسی دستی:*

 - ، `package.json` در مخزن هر (`LICENSE`) و فایل‌های مجوز وابستگی مهم.

- * استفاده از ابزارهایی مانند **FOSSA**** ابزار تجاری/متن‌باز:*
- * **Black Duck**** برای اسکن جامع‌تر).

**لیست کامل وابستگی‌های حیاتی و تحلیل مجوزها .۳##

این لیست شامل مهم‌ترین وابستگی‌ها از نظر عملکرد و ریسک مجوز است.

۳. ۱. (Frontend - React) وابستگی‌های سمت کلاینت

نام وابستگی	نسخه	مجوز	نوع	ریسک	توضیح
`react`	۱۸,۲,۰	**MIT**	Permissive	بی‌ریسک	
`react-dom`	۱۸,۲,۰	**MIT**	Permissive	بی‌ریسک	
`leaflet`	۱,۹,۴	**BSD-2-Clause**	Permissive		بی‌ریسک. کتابخانه اصلی نقشه
`react-leaflet`	۴,۲,۱	**Hippocratic-2.1**	Ethical		
یک مجوز جدید "اخلاقی"	که استفاده توسط نهادهای				
نقض‌کننده حقوق بشر را ممنوع می‌کند.	برای ما ریسکی ندارد، اما باید در				
					مستندات ثبت شود
`axios`	۱,۳,۰	**MIT**	Permissive	بی‌ریسک	
`@mui/material` (MUI)	۵,۱۱,۰	**MIT**	Permissive		
					بی‌ریسک

۳. ۲. (Backend - Django/Python) وابستگی‌های سمت سرور

نام وابستگی	نسخه	مجوز	نوع	ریسک	توضیح
-------------	------	------	-----	------	-------

`Django` ۴,۱,۷ **BSD-3-Clause** Permissive				
				بی‌ریسک
`django-rest-framework` ۳,۱۴,۰ **BSD-2-Clause**				
				بی‌ریسک
				`psycopg2-binary` (PostgreSQL adapter) ۲,۹,۵
یک **LGPL-3.0** **Weak Copyleft** **Mهم**:				
"Copyleft" است. این کتابخانه یک *فایل کتابخانه‌ای مشترک (shared library)* است. ما آن را *لینک پویا (dynamic linking)* می‌کنیم. این به ما اجازه می‌دهد بدون انتشار کد اختصاصی خود از آن استفاده کنیم، به شرطی که: ۱) تغییراتی در خود کتابخانه ایجاد نکنیم، و ۲) به کاربران اجازه دهیم نسخه تغییر یافته‌ای `psycopg2` از این کتابخانه را با برنامه ما لینک کنند. این شرایط در حال حاضر رعایت شده است ✓				
`Pillow` (۹,۴,۰ پردازش تصویر) **HPND** (Historical Permission Notice) Permissive				
				بی‌ریسک
`celery` ۵,۲,۷ **BSD-3-Clause** Permissive				
				بی‌ریسک

۳. (DevOps) وابستگی‌های ابزارهای توسعه و عملیاتی

نام وابستگی	نسخه	مجوز	نوع	ریسک	توضیح
Apache 2.0**	۲۰,۱۰	+ سکو)	Docker`	`	--- --- --- --- --- ---
PostgreSQL License**	۱۵	دیتابیس)	PostgreSQL`	`	بی‌ریسک
MIT/BSD)	۱۵	شبهیه	Permissive		بی‌ریسک
MIT**	۵,۷۵,۰		webpack`		بی‌ریسک
GPL-3.0**	۱,۰,۰		یک ابزار داخلی قدیمی		**Strong
Copyleft**			این یک ابزار داخلی برای پردازش		ریسک متوسط:*
			اولیه دیتابست بود که در مرحله توسعه اولیه استفاده شد.		هرگز در
runtime (Production)			استفاده نشده است.*		این رو،
محصول نهایی			نمی‌کند*.. با این حال، کد آن ابزار GPL		کد محصول ما را مشمول
					باقی بماند اگر منتشر شود GPL
					داخلی باید تحت

۴. Copyleft (GPL/AGPL) تحلیل ریسک‌های خاص

**۴. ۱ Copyleft) سخت‌ترین مجوز (AGPL ریسک

* **AGPL (GNU Affero General Public License)** را به **کاربران شبکه** گسترش شرط Copyleft تحت (Backend) در **بخش سرور GPL** می‌دهد. اگر از کتابخانه تحت پروژه خود استفاده کنید، ممکن است ملزم به انتشار **سورس کد کامل برنامه سرور** برای هر کاربری که از سرویس شما استفاده می‌کند، شوید.

* **هیچ وضعیت در ShahnamehMap:** پس از اسکن عمیق، **هیچ** که در بخش‌های اصلی Backend یا Frontend وابستگی Production) اجرا می‌شوند، یافت نشد**. یک وابستگی آزمایشی (dev dependency) و حذف شد GPL تحت

* **. فعلاً منتفی است GPL نتیجه:** ریسک

**۴. ۲ GPL ریسک

* **GPL** ماهیت ریسک: **مجوز** را برای Copyleft شرط GPL تحت ترکیب شده و یک اثر واحد را GPL برنامه‌ای اعمال می‌کند که با کد تحت تشکیل دهد**. اگر کد اختصاصی ما به صورت **استاتیک** با یک شود GPL لینک شود، ممکن است کل کد مشمول GPL کتابخانه تحت

* ** تنها وابستگی مهم تحت مجوز ShahnamehMap:** وضعیت در Copyleft ، `psycopg2-binary` تحت `LGPL** است که یک استثنا هیچ وابستگی در هسته محصول GPL محسوب می‌شود (بخش ۳.۲). هیچ وابستگی شناسایی نشد.

* مستقیم برای محصول نهایی بسیار پایین GPL نتیجه: *** ریسک * است ✓

سوال کلیدی: آیا محصول ما مجبور به متن باز شدن ۴.۳ *** می‌شود؟

: خیر. بر اساس تحلیل فعلی *

هسته اصلی پلتفرم (کد فرانت‌اند، بک‌اند و منطق کسب‌وکار) از 1. (فريمورک‌ها و کتابخانه‌های تحت *مجوزهای مجاز MIT, Apache, BSD) استفاده می‌کند

2. است که Copyleft (`psycopg2` تحت `LGPL** تنها وابستگی با روش لينك پويا (استفاده به عنوان يك ماژول خارجي)، کد ما را مشمول Copyleft نمی‌کند.

3. در معماری سرويس‌دهی وجود ندارد GPL هیچ وابستگی .

*پاسخ نهایی: محصول ما در حال حاضر تحت هیچ الزام قانونی برای متن باز **
**.شدن کامل قرار ندارد

** برنامه پاکسازی و مدیریت ریسک مستمر # # * * ۵.

برای حفظ این وضعیت ایمن و جلوگیری از ورود ناخواسته ریسک‌های
مجوزی، برنامه زیر اجرا خواهد شد

** فاز ۱: پاکسازی فوری (۱ ماهه) ***

تحت تمام وابستگی‌های توسعه [] (devDependencies) حذف
و جایگزینی با ابزارهای تحت مجوز مجاز (در GPL/AGPL** مجوزهای
صورت نیاز).

- در ریشه پروژه `NOTICE` تکمیل مستندات مجوزها: * ایجاد فایل [] **
که مجوزهای همه وابستگی‌های مهم و متن مربوط به مجوزهای آن‌ها را
فهرست کند.

- [] ** آموزش تیم فنی: برگزاری جلسه آموزشی کوتاه برای تمام []
توسعه‌دهندگان در مورد تفاوت مجوزهای MIT، Apache، GPL و AGPL
و خطرات استفاده ناخواسته از Copyleft.

- ** فاز ۲: ایجاد فرآیندهای کنترل (مستمر) ***
- [] ** استقرار ابزار اسکن خودکار: یک پارچه‌سازی ابزار ساده‌ای مانند []
`license-checker` در خط لوله CI/CD (مثلًا در GitHub Actions)،
لیست مجوزهای وابستگی‌های جدید به طور **Pull Request** در هر
خودکار بررسی شود.
- [] ** تعیین خط مشی تأیید وابستگی (Approval Policy): **
* * تأیید خودکار MIT/Apache/BSD:
* * نیاز به بررسی توسط مدیر فنی ارشد برای LGPL:
* * اطمینان از عدم لینک استاتیک و رعایت شرایط
* * ممنوعیت استفاده در کد GPL/AGPL:
* * مگر در موارد استثنایی و با تأیید صریح مدیر عامل و مشورت
حقوقی. استفاده تنها در ابزارهای کاملاً مستقل و خارج از معماری اصلی
مجاز است.

- [] ** حفظ و نگهداری Software Bill of Materials (SBOM):**
که تمام (SPDX مثلاً در قالب) به روزرسانی مستمر یک فایل ماشین خوان
وابستگی‌ها و مجوزهای آن‌ها را فهرست می‌کند.

* فاز ۳: ممیزی دوره‌ای ***

- [] ** بررسی سه‌ماهه: هر سه ماه یکبار، یک اسکن کامل مجدد انجام شده و گزارش مختصری برای مدیرعامل تهیه می‌شود.
- [] ** مشاوره حقوقی سالانه: ارائه گزارش انطباق به وکیل متخصص برای بررسی نهایی و اطمینان از رعایت تمام تعهدات

* مستندات استفاده از مدل‌ها/داده‌های محدود .۶**

از منابع داده و مدل‌های زیر که ممکن است ShahnamehMap در پروژه محدودیت‌های استفاده داشته باشند، بهره می‌بریم:

| نام منبع/داده | منبع | نوع | مجوز/شرایط استفاده | اقدامات انطباق ما |

— — | : — — |

متن شاهنامه** (چاپ مسکو/حالقی)

مالکیت عمومی)*** از نظر (Public Domain | (در گذشته ۴۱۱ ه. ق)

حقوق مؤلف. اما نسخه های تصحیح شده خاص ممکن است حق تکثیر

مصحح را داشته باشند. | ما از نسخه‌های مشهور و قدیمی که در مالکیت

عمومی هستند** (مانند نسخه‌ی اساس چاپ مسکو) برای استخراج داده‌های

خام استفاده می‌کنیم. تفسیر و بازنویسی مدرن، اثر خلاقانه تیم ما محسوب

می شود |

| داده جغرافیایی OpenStreetMap (OSM)** | نقشه‌های پایه** |

جامعه OpenStreetMap | ** مجوز Open Database License

(ODbL) 1.0.*^{**} (Share-Alike) همانند گذاری-اشتراک شرط مجوز این (ODbL)

به عنوان ***لایه پایه*** در نقشه تعاملی خود استفاده OSM دارد. | ما از

(مجاز است، به شرطی که: ۱ ODbL می‌کنیم. این استفاده تحت مجوز OSM

کنیم، و ۲) اگر لایه جغرافیایی attribution را به درستی

ایجاد کنیم (مثلاً یک نقشه تخصصی)، آن را OSM مشتق شده‌ای از

منتشر کنیم. لایه اساطیری ما یک لایه *** جداگانه و ODbL نیز تحت

محسوب OSM اضافه شده** است و یک اثر مشتق جغرافیایی از

نَمِي شُود . ✓ |

| احتمالاً | ML مدل زبانی (در صورت استفاده آینده)*** | مدل **|
، یا MIT مثلاً) یا مشابه | بسته به مدل متفاوت است Hugging Face
فعلاً استفاده نمی‌شود.*.* در **|. (**مشروط مانند** منع استفاده تجاری
صورت نیاز در آینده، مجوز مدل به دقت بررسی شده و تنها در صورت مجاز
| بودن استفاده تجاری، مورد استفاده قرار خواهد گرفت

| سرویس | شرکت | (**Mapbox مانند) **سرویس نقشه تجاری API
ارائه‌دهنده | *.*مجوز اختصاصی و پولی.*.* محدودیت‌های میزان درخواست و
استفاده می‌کنیم تا از این OSM** استفاده. | ما از *.*لایه پایه رایگان
محدودیت‌ها و هزینه‌ها اجتناب کنیم. در صورت نیاز به ویژگی‌های پیشرفته،
| قرارداد تجاری منعقد خواهد شد

* تأییدیه نهايی: * اين گزارش منعكس‌کننده وضعیت فعلی پروژه در تاریخ *
بالا است. تیم فنی متعهد به رعایت خط‌مشی‌های تعیین‌شده در بخش ۵ برای
ShahnamehMap حفظ انطباق و محافظت از دارایی‌های فکری اختصاصی
است.

[امضای مدیر فنی ارشد]

[امضای مدیرعامل]