

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

تاریخ: **۲۵/۰۵/۱۴۰۳**

ShahnamehMap: **پروژه**

تهیه کننده: **تیم فنی**

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

**خلاصه اجرایی و وضعیت کلی ۱. **##

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

معمولاً**خطر مستقیمی برای اجباری شدن انتشار سورس کد اختصاصی ما
**ایجاد نمی کنند.

Copyleft** با این حال، شناسایی و مدیریت چند وابستگی با**مجوزهای
حیاتی است. در حال حاضر،**هیچ یک از این (AGPL و GPL مانند)
به گونه ای استفاده نمی شوند که کل سورس کد Copyleft وابستگی های
کند**اکثر آنها در فرآیندهای توسعه Copyleft پروژه را مشمول شرایط
یا ابزارهای داخلی استفاده شده اند

در بخش AGPL ریسک اصلی:**استفاده ناخواسته از یک کتابخانه تحت**
که می تواند منجر به الزام انتشار سورس کد سمت (Backend) 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

****۲. روش‌شناسی و ابزارهای اسکن ##**

برای تهیه این گزارش از روش‌های زیر استفاده شده است:

برای (``npm audit``) اسکن خودکار: ****استفاده از ابزار ***
``license-checker`` (برای پایتون)، و ``pip-licenses``، ``Node.js`` / جاوااسکریپت ``checker``.

، ``package.json`` بررسی دستی: ****بررسی ***
در مخزن هر (``LICENSE``) و فایل‌های مجوز ``requirements.txt``
وابستگی مهم.

یا ****FOSSA**** ابزار تجاری/متن‌باز: ****استفاده از ابزارهایی مانند ***
اگر در آینده بודجه داشته باشیم) برای اسکن جامع‌تر ****Black Duck****.

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

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

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

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

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

نام وابستگی | نسخه | مجوز | نوع | ریسک و توضیح |

| :--- | :--- | :--- | :--- | :--- |

| `Django` | ۴,۱,۷ | ****BSD-3-Clause**** | Permissive |

| بی‌ریسک

| `django-rest-framework` | ۳,۱۴,۰ | ****BSD-2-Clause**** |

| Permissive | بی‌ریسک |

| `psycopg2-binary` (PostgreSQL adapter) | ۲,۹,۵ |

****GPL-3.0**** | ****Weak Copyleft**** | ****مهم: LGPL یک**

ضعیف" است. این کتابخانه یک ****فایل کتابخانه‌ای مشترک Copyleft**

(dynamic است. ما آن را ****لینک پویا (shared library)**

می‌کنیم. این به ما اجازه می‌دهد بدون انتشار کد اختصاصی ****linking)**

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

*** (DevOps) وابستگی‌های ابزارهای توسعه و عملیاتی ۳.۳ ***

| نام وابستگی | نسخه | مجوز | نوع | ریسک و توضیح |

| :--- | :--- | :--- | :--- |

| `Docker` (۲۰,۱۰ | +سکو) | **Apache 2.0** | Permissive |

| بی‌ریسک |

| `PostgreSQL` (۱۵ | دیتابیس) | **PostgreSQL License** |

| بی‌ریسک | (MIT/BSD شبیه) Permissive |

| `webpack` | ۵,۷۵,۰ | **MIT** | Permissive |

| **Strong** | **GPL-3.0** | یک ابزار داخلی قدیمی | **۱,۰,۰** |

ریسک متوسط: این یک ابزار داخلی برای پردازش ** Copyleft** |

اولیه دیتاست بود که در مرحله توسعه اولیه استفاده شد. **هرگز در

استفاده نشده است. ** از این رو، (Production) محصول نهایی runtime

نمی‌کند. ** با این حال، کد آن ابزار GPL ** کد محصول ما را مشمول

| .باقی بماند اگر منتشر شود GPL داخلی باید تحت

*** Copyleft (GPL/AGPL) تحلیل ریسک‌های خاص ۴.۴ ***

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

* **AGPL (GNU Affero General Public License)** ماهیت ریسک: **مجوز**
را به **کاربران شبکه** گسترش Copyleft شرط ** (Backend) در بخش سرور AGPL 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.
پس از اسکن عمیق، **هیچ ShahnamehMap: وضعیت در**
که در Frontend یا Backend در بخش‌های اصلی AGPL وابستگی
(dev اجرا می‌شوند، یافت نشد). یک وابستگی آزمایشی Production
شناسایی و حذف شد AGPL تحت (dependency)

✓ **فعلاً منتفی است AGPL نتیجه: ** ریسک** *

*** **۴. ۲ ریسک GPL)**

* **Copyleft شرط GPL** ماهیت ریسک: **مجوز**
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 ****** *
است که یک استثنا ****LGPL**** تحت ``psycopg2-binary`` Copyleft،
در هسته محصول GPL محسوب می شود (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 ۳. ۴ ****** ####
****** می شود؟

خیر: ****** بر اساس تحلیل فعلی ******

هسته اصلی پلتفرم (کد فرانت اند، بک اند و منطق کسب و کار) از 1.
(MIT, Apache, فریمورک ها و کتابخانه های تحت ****مجوزهای مجاز
استفاده می کند** ****BSD**

است که ****LGPL**** تحت ``psycopg2`` Copyleft تنها وابستگی 2.
با روش لینک پویا (استفاده به عنوان یک ماژول خارجی)، کد ما را مشمول
Copyleft نمی کند.

3. در معماری سرویس دهی وجود ندارد AGPL 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
مجازی، برنامه زیر اجرا خواهد شد

** فاز ۱: پاکسازی فوری (۱ ماهه) ** ###

تحت (devDependencies) حذف تمام وابستگی‌های توسعه ** [] -
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 ** [] -
AGPL ، GPL ، Apache ، MIT توسعه‌دهندگان در مورد تفاوت مجوزهای
Copyleft و خطرات استفاده ناخواسته از

** فاز ۲: ایجاد فرآیندهای کنترل (مستمر) ** ###

استقرار ابزار اسکن خودکار: ** یکپارچه‌سازی ابزار ساده‌ای مانند ** [] -
تا (GitHub Actions مثلاً در) CI/CD در خط لوله `license-checker`
، لیست مجوزهای وابستگی‌های جدید به طور ** Pull Request ** در هر
خودکار بررسی شود.

** (Approval Policy) تعیین خط‌مشی تأیید وابستگی ** [] -

تأیید خودکار MIT/Apache/BSD: ** مجوزهای *

نیاز به بررسی توسط مدیر فنی ارشد برای LGPL: ** مجوزهای *

اطمینان از عدم لینک استاتیک و رعایت شرایط

ممنوعیت استفاده در کد ** GPL/AGPL: ** مجوزهای *

مگر در موارد استثنایی و با تأیید صریح مدیرعامل و مشورت Production
حقوقی. ** استفاده تنها در ابزارهای کاملاً مستقل و خارج از معماری اصلی
مجاز است.

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

** فاز ۳: ممیزی دوره ای ** ###

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

** مستندات استفاده از مدل ها/داده های محدود. ** ##

از منابع داده و مدل های زیر که ممکن است ShahnamehMap در پروژه
محدودیت های استفاده داشته باشند، بهره می بریم

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

| :--- | :--- | :--- | :--- |

متن شاهنامه** (چاپ مسکو/خالقی مطلق) | داده متنی | اثر فردوسی ** |
مالکیت عمومی)** از نظر (Public Domain ** | (در گذشته ۴۱۱ ه. ق)
حقوق مؤلف. اما** نسخه‌های تصحیح‌شده 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
| می‌شود.

داده جغرافیایی | | **OpenStreetMap (OSM) نقشه‌های پایه** |
Open Database License مجوز** | OpenStreetMap جامعه
(Share-Alike) این مجوز شرط اشتراک‌گذاری-همانند **1.0 (ODbL)
به عنوان** لایه پایه** در نقشه تعاملی خود استفاده OSM دارد. | ما از
OSM (مجاز است، به شرطی که: ۱ ODbL می‌کنیم. این استفاده تحت مجوز
کنیم، و ۲) اگر لایه جغرافیایی attribution را به‌درستی
ایجاد کنیم (مثلاً یک نقشه تخصصی)، آن را OSM** مشتق‌شده** ای از
منتشر کنیم. لایه اساطیری ما یک لایه** جداگانه و ODbL نیز تحت
محسوب OSM اضافه‌شده** است و یک اثر مشتق جغرافیایی از
| ✓.*** نمی‌شود

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 نهایی: ** این گزارش منعکس‌کننده 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]****