计算指标

指标	选取理由	记号
CVSS	CVSS 是业界标准，对漏洞的“影响”和“可利用性”提供了统一量化	X1
EPSS	EPSS 基于对历年实测攻击数据、公开 PoC 频度等进行建模，更贴近“攻击者最可能利用的漏洞”,EPSS 会随时间、社区兴趣波动而调整	X2
CWE-ID	不同 CWE（如缓冲区溢出 vs. 信息泄露 vs. 权限绕过）在攻击路径、检测手段、补丁难度上存在本质区别，加入类别特征能帮助模型认识“哪类漏洞更危险”	X3
发布日期（Age）	古早漏洞通常已有成熟 PoC，与之对应的“真实风险”可能进一步提高，或者相反因补丁普及而降低	X4
环境适配度（ENV）	只有当漏洞特征与目标环境高度匹配时，才真正构成风险；没有 ENV，就无法区分“此漏洞对本次靶机是否致命”	X5
PoC质量得分	不仅关乎 PoC 是否存在，还要考量其成熟度、可移植性、所需权限等，直接决定攻击者落地的成本	X6
Trend得分	通过 GitHub 上相关仓库的 Star、Fork、Issue 数量衡量社区对该漏洞利用代码的关注度与活跃度	X7

通过这七类指标的互补融合，模型既兼顾了漏洞本身的**固有严重度**（CVSS、CWE、Age），也体现了**当前可利用性**（EPSS、PoC、Trend），更加入了**场景相关性**（ENV）

参考模型：Factorization Machines（FM）

评分模型

$$R(\mathbf{x}_c) = \sigma\Big(\underbrace{\mathcal{F}_{\text{core}}(\mathbf{x}_c)}_{\text{基础风险}} + \underbrace{\mathcal{F}_{\text{interaction}}(\mathbf{x}_c)}_{\text{语义交叉}} + \underbrace{\mathcal{F}_{\text{temporal}}(\mathbf{x}_c)}_{\text{时序调制}}\Big) \cdot \underbrace{G(x_5^c)}_{\text{上下文环境门控}}$$

核心风险映射 $Fcore$，定义为线性泛函组合：$Fcore(x) = i \in 1,2,6 \sum wixi$

其中x_1：$CVSS$，x_2：$EPSS$，x_6：PoC，表示“静态-动态-代码可用性”三位一体的风险强度

指标交叉结构 $Finteraction$，构造语义驱动的特征图谱 $Grisk = (V, E)$：

- 顶点集合 $V = xi$，边$(x_i, x_j) \in E$ 表示存在风险协同
- 权重矩阵 $\Gamma = [\gamma ij]$ 表示协同放大系数

其形式可定义为：$Finteraction(x) = (i,j) \in E \sum \gamma ij \cdot xixj$

可解释实例：

- $x1x2$：高危 CVE + 高利用率 → 高实际攻击概率；
- $x3x6$：某 CWE 类型易开发高质量 PoC；
- $x6x7$：社区高关注漏洞其 PoC 质量通常也更好。

时序趋势调制项 $Ftemporal$，由“时间衰减项+趋势增强项”构成：
$Ftemporal(x) = \lambda 1 \cdot e^{(} - \mu x4) + \lambda 2 \cdot x7^{\beta}$

其中：

- $x4$：年龄 → 年越久越不敏感（除非仍被关注）；
- $x7$：趋势指标 → 高 trend 放大热度漏洞的风险传播。

环境门控函数$G(x5)$

上下文控制器：$G(x5) = \eta \cdot x5$，其中$\eta \in [0.5, 2]$控制ENV的主导程度，它**调节整个评分公式的全局放大/抑制。**

Sigmoid 映射 最终评分归一化：$\sigma(z) = 1/1 + e^{-}z$

模型模块	推荐理论支撑机制	网络安全建模意义
$Fcore$	显式评分建模（Rating）	漏洞本身强度主导项
$Finteraction$	特征交叉建模（Feature Interaction）	捕捉联合影响：协同放大、非线性组合
$Ftemporal$	时间推荐（Temporal Models）	趋势性、生命周期映射
$G(x5)$	上下文推荐（Context-Aware）	融入环境敏感性，体现靶机对该 CVE 的“真实危险”
$\sigma(\cdot)$	函数映射（Bounded Preference）	将危险评分映射到 [0,1]，可用于排序与阈值分类

cve_id	risk_score
CVE-2021-43798	0.9132
CVE-2023-0507	0.8715
CVE-2022-31097	0.8621
CVE-2023-2183	0.8573
CVE-2023-0594	0.8556
CVE-2022-23552	0.837
CVE-2022-39324	0.8327
CVE-2022-21702	0.8303
CVE-2023-1410	0.8303
CVE-2022-39201	0.8244
CVE-2022-36062	0.8241
CVE-2022-31107	0.8203
CVE-2022-39307	0.8177
CVE-2022-35957	0.8171
CVE-2022-21703	0.8148
CVE-2022-31123	0.813
CVE-2022-39306	0.8126
CVE-2022-31130	0.81
CVE-2022-39229	0.8053
CVE-2022-21673	0.8046
CVE-2021-43813	0.803
CVE-2021-43815	0.7982
CVE-2022-21713	0.7981

cve_id	risk_score
CVE-2019-14234	0.9077
CVE-2020-7471	0.9047
CVE-2020-9402	0.9001
CVE-2019-19844	0.8933
CVE-2017-12794	0.8657
CVE-2018-14574	0.8473
CVE-2019-12308	0.8274
CVE-2019-6975	0.8263
CVE-2019-14233	0.8257
CVE-2019-14235	0.8256
CVE-2019-14232	0.8235
CVE-2019-3498	0.8163
CVE-2019-12781	0.807
CVE-2018-7537	0.8068
CVE-2018-7536	0.8063
CVE-2021-33203	0.8028