به منظور تحلیل ریسک، از متدولوژی رتبه بندی ریسک OWASP استفاده شده است.

جدول زیر، واژگان مرتبط با رتبه ریسک را مختصرا نشان می‌دهد.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **عوامل تهدید** | **قابلیت بهره برداری** | **میزان شیوع آسیب‌پذیری** | **قابلیت شناسایی آسیب‌پذیری** | **پیامد فنی** | **تاثیر بر کسب و کار** |
| **خاص API** | **آسان: 3** | **گسترده: 3** | **آسان: 3** | **شدید: 3** | **خاص کسب و کار** |
| **متوسط: 2** | **متداول: 2** | **متوسط: 2** | **متوسط: 2** |
| **سخت: 1** | **سخت: 1** | **سخت: 1** | **جزئی: 1** |

در این رویکرد، نوع فناوری مورد استفاده و احتمال وقوع آسیب‌پذیری در رتبه ریسک تاثیر ندارند؛ بعبارت دیگر در این روش رتبه بندی ریسک، راهکار مورد استفاده برای پیاده سازی API ، با رویکردی مستقل از جزئیات فناوری به ارزیابی ریسک می‌پردازد. هرکدام از عوامل یاد شده می‌تواند در پیداکردن و سواستفاده از یک آسیب‌پذیری به مهاجم کمک بسزایی کند. این رتبه بندی تاثیر واقعی بر کسب و کارها را نشان نداده و این سازمان‌ها هستند که با توجه به نوع کسب و کار و فرهنگ سازمانی خود، در میزان پذیرش خطر امنیتی استفاده از اپلیکیشن‌ها و APIها تصمیم گیرنده هستند. هدف از مستند ده آسیب‌پذیری بحرانی امنیت API، تحلیل ریسک نیست.

**مراجع**

**OWASP**

* [OWASP Risk Rating Methodology](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology)
* [Article on Threat/Risk Modeling](https://www.owasp.org/index.php/Threat_Risk_Modeling)

**خارجی**

* [ISO 31000: Risk Management Std](https://www.iso.org/iso-31000-risk-management.html)
* [ISO 27001: ISMS](https://www.iso.org/isoiec-27001-information-security.html)
* [NIST Cyber Framework (US)](https://www.nist.gov/cyberframework)
* [ASD Strategic Mitigations (AU)](https://www.asd.gov.au/infosec/mitigationstrategies.htm)
* [NIST CVSS 3.0](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator)
* [Microsoft Threat Modeling Tool](https://www.microsoft.com/en-us/download/details.aspx?id=49168)