OWASP Risk Rating Methodology

OWASP 风险评级方法论

Contents

目录：

The OWASP Risk Rating Methodology

OWASP 风险评级方法论

Discovering vulnerabilities is important, but just as important is being able to estimate the associated risk to the business. Early in the lifecycle, you may identify security concerns in the architecture or design by using threat modeling. Later, you may find security issues using code review or penetration testing. Or you may not discover a problem until the application is in production and is actually compromised.

发现漏洞很重要，能够评估对业务相关的风险同样重要。在软件生命周期的早期，你可能在架构中定义或者用威胁模型设计安全的概念。随后，也许你会通过代码审查或渗透测试发现安全问题，也许直到发布后被真正攻破了才发现。

By following the approach here, you'll be able to estimate the severity of all of these risks to your business, and make an informed decision about what to do about them. Having a system in place for rating risks will save time and eliminate arguing about priorities. This system will help to ensure that you don't get distracted by minor risks while ignoring more serious risks that are less well understood.

通过这里提供的方法，你将能够评估所有与业务有关的风险的严重性，从而明智的决定如何应对。拥有一套风险评级系统，不但节约时间，而且能消除对优先次序的争论。这种系统可以确保不会因为一些小问题而忽略那些不易理解却更严重的大风险。

Ideally, there would be a universal risk rating system that would accurately estimate all risks for all organizations. But a vulnerability that is critical to one organization may not be very important to another.

理想的情况是有一个通用的风险评级系统，能够准确评估所有组织的所有风险。但同一个漏洞，对某些组织来说很关键，对其他单位可能就没那么重要。。

So a basic framework is presented here that you *should customize* for your organization. The authors have tried hard to make this model simple enough to use,

while keeping enough detail for accurate risk estimates to be made. Please reference the section below on customization for more information about tailoring the model for use in your organization.

所以我们提供一个基础的框架，以便使用者能够按需定制。在确保这个模型简单易用的同时，也尽力保留了与风险评估准确性相关的足够多的细节。请参阅以下章节以获取更多信息关于定制适合你组织使用的模型

Approach

方法

There are many different approaches to risk analysis. See the reference section below for some of the most common ones. The OWASP approach presented here is based on these standard methodologies and is customized for application security. Let's start with the standard risk model：

风险分析的方法有很多种，请参看一下参考章节来了解最常用的那些方法。本文介绍的 OWASP 方法是基于以下这些规范，为应用安全定制的。让我们从标准的模型开始

Risk = Likelihood * Impact 风险=可能性*影响

In the sections below, we break down the factors that make up "likelihood" and "impact" for application security and show how to combine them to determine the overall severity for the risk.

在本节中，我们分解这些构成应用程序安全“可能性”和“影响”因素，并且展示如何将它们结合起来，以决定风险的整体严重程度。

Step 1: Identifying a Risk

步骤一：确定风险类别

The first step is to identify a security risk that needs to be rated.You'll need to gather information about the threat agent involved, the attack they're using, the vulnerability involved, and the impact of a successful exploit on your business. There may be multiple possible groups of attackers, or even multiple possible business impacts. In general, it's best to err on the side of caution by using the worst-case option, as that will result in the highest overall risk.

第一步是确定评级对象的安全风险。需要收集涉及到的攻击者、攻击方法、利用漏洞和业务影响方面的信息。也许存在多组攻击，或许对业务有多种影响。总的来说，最好是慎之又慎地将攻击当成最坏的情况造成最高了风险而产生的影响来对待。

Step 2: Factors for Estimating Likelihood

步骤二：评估可能性的因素

Once you've identified a potential risk, and want to figure out how serious it is, the first step is to estimate the "likelihood". At the highest level, this is a rough measure of how likely this particular vulnerability is to be uncovered and exploited by an attacker. We do not need to be over-precise in this estimate. Generally, identifying whether the likelihood is low, medium, or high is sufficient.

一旦你确定了潜在风险，并想知道该风险有多严重，那么第一步是评估它发生的可能性。在最高级别中，“发生的可能性”是评估攻击者发现和利用特定漏洞的粗略计量。我们在此评估中无须过于小心。通常，确定可能性是否是低、中或者高就足够了。

There are a number of factors that can help us figure this out. The first set of factors are related to the threat agent involved. The goal is to estimate the likelihood of a successful attack from a group of possible attackers. Note that there may be multiple threat agents that can exploit a particular vulnerability, so it's usually best to use the worst-case scenario.

有很多因素可以帮助我们分析“发生的可能性”。第一类相关因素就是攻击者。这一步的目标是估计一个可能发起攻击的团体成功攻击的可能性。由于存在多个攻击者利用同一个特定漏洞的情况，所以通常设定为最坏的情形。

For example, an insider may be a much more likely attacker than an anonymous outsider - but it depends on a number of factors. Note that each factor has a set of options, and each option has a likelihood rating from 0 to 9 associated with it. We'll use these numbers later to estimate the overall likelihood.

举例来说，内部人员可能比外部某某某更可能成为攻击者——这取决于多种因素。每个因素都有一系列选项，每个选项都有“发生的可能性”。我们使用 0-9 的数字评估最后的可能性。

Threat Agent Factors

攻击者因素

The first set of factors are related to the threat agent involved. The goal here is to estimate the likelihood of a successful attack by this group of threat agents.

第一类相关的因素就是攻击者，本项目的目标就是评估攻击者成功攻击的可能性。

Use the worst-case threat agent.使用最坏结果法分析攻击者。

Skill level 技术水平

How technically skilled is this group of threat agents?
攻击者的技术水平如何？
No technical skills (1), 不具备能力（1），
some technical skills (3), 具备初级能力（3），
advanced computer user (4), 高级计算机使用者（4），
network and programming skills (6), 具备网络和编程能力（6），
security penetration skills (9) 具备渗透能力（9）

Motive 动机

How motivated is this group of threat agents to find and exploit this vulnerability?
攻击者发现和利用漏洞的动力是什么？
Low or no reward (1), 低或者零回报（1），
possible reward (4), 可能带来回报（4），
high reward (9), 很高的回报（9），

Opportunity 权限和成本

What resources and opportunity are required for this group of threat agents to find and exploit this vulnerability?
攻击者寻找和利用某个漏洞的成本有哪些？
full access or expensive resources required (0), 完全访问权限或高昂的成本（0），
special access or resources required (4), 特定访问权限或较高的成本（4），
some access or resources required (7), 部分访问权限或一般的成本（7），

no access or resources required (9) 无需访问权限或者没有成本（9）

Size 人员构成

How large is this group of threat agents?
攻击者的人员构成有哪些？
Developers (2), 开发者（2），
system administrators (2), 系统管理员（2），
intranet users (4), 内部用户（4），
partners (5), 合伙人
authenticated users (6), 认证用户
anonymous Internet users (9) 匿名互联网用户

Vulnerability Factors

漏洞因素

The next set of factors are related to the vulnerability involved. The goal here is to estimate the likelihood of the particular vulnerability involved being discovered and exploited. Assume the threat agent selected above.

第二类相关的因素就是漏洞本类项目的目标是评估特定的漏洞被发现和利用的可能性。假定攻击者危害性选择同上文。

Ease of discovery 发现难易程度

How easy is it for this group of threat agents to discover this vulnerability?
攻击者发现这个漏洞难易程度如何？
Practically impossible (1), 几乎不可能（1），
difficult (3), 困难（3），
easy (7), 容易（7），
automated tools available (9) 可以使用自动化工具（9）

Ease of exploit 利用难易程度

How easy is it for this group of threat agents to actually exploit this vulnerability?
攻击者实际利用这个漏洞的难易程度如何？
Theoretical (1), 几乎不可能（1），
difficult (3), 困难（3）
easy (5), 容易（7），
automated tools available (9) 可以使用自动化工具（9）

Awareness 知晓度

How well known is this vulnerability to this group of threat agents?
漏洞在攻击者中存在的知晓率
Unknown (1), 未知的（1），
hidden (4), 有隐蔽性的（4），
obvious (6), 比较显著的（6），

public knowledge (9) 众所周知的（9）

Intrusion detection 入侵检测

How likely is an exploit to be detected?

漏洞被利用后如何检测？

Active detection in application (1), 应用程序主动发现（1），

logged and reviewed (3), 日志记录和审核（3），

logged without review (8), 日志记录（8），

not logged (9) 没有日志（9）

Step 3: Factors for Estimating Impact

步骤三：评估影响的因素

When considering the impact of a successful attack, it's important to realize that there are two kinds of impacts. The first is the "technical impact" on the application, the data it uses, and the functions it provides. The other is the "business impact" on the business and company operating the application.

当考虑成功攻击的影响时，关键要意识到有两类影响。第一类对应用程序、应用程序所使用的数据以及它所提供的功能的“技术影响”。另一个是对该项业务本身和公司开展这项业务应用的“业务影响”。

Ultimately, the business impact is more important. However, you may not have access to all the information required to figure out the business consequences of a successful exploit. In this case, providing as much detail about the technical risk will enable the appropriate business representative to make a decision about the business risk. Again, each factor has a set of options, and each option has an impact rating from 0 to 9 associated with it. We'll use these numbers later to estimate the overall impact.

毋容置疑，业务性影响更为重要。然而，你可能无法得到所需信息去分析对业务的影响结果。在这种情况下，向恰当的业务代表提供足够详细的技术风险信息，由业务代表决定相关的业务风险。最后，每个因素有每个因素有一系列的选项，每个选项的可能性评级分布从 0 到 9。我们将使用这些数字评估总体的影响。

Technical Impact Factors

技术影响因素

Technical impact can be broken down into factors aligned with the traditional security areas of concern: confidentiality, integrity, availability, and accountability.

The goal is to estimate the magnitude of the impact on the system if the vulnerability were to be exploited.

技术影响由多个因素组成并和传统的安全考虑相一致，即保密性，完整性，可用性以及可追溯性。目标是评估漏洞被利用后对系统的影响的大小。

Loss of confidentiality 损失保密性

How much data could be disclosed and how sensitive is it?
有多少信息被泄露，敏感程度如何？
Minimal non-sensitive data disclosed (2),
少量不敏感信息被泄露（2），
minimal critical data disclosed (6),
少量关键数据被泄露（6），
extensive non-sensitive data disclosed (6),
大量不敏感信息被泄露（6）
extensive critical data disclosed (7),
大量敏感信息被泄露（7），
all data disclosed (9)
所有数据丢失（9）

Loss of integrity 损失完整性

How much data could be corrupted and how damaged is it?
有多少数据被破坏，破化的程度如何?
Minimal slightly corrupt data (1) ,
少量轻微的数据破坏（1），
minimal seriously corrupt data (3),
少量严重的数据破坏（3），
extensive slightly corrupt data (5),
大量轻微的数据破坏（5），
extensive seriously corrupt data (7),
大量严重的数据破坏（7），
all data totally corrupt (9)
所有数据完全彻底破坏（9）

Loss of availability 损失可用性

How much service could be lost and how vital is it?
多少服务会中断，重要程度如何？
Minimal secondary services interrupted (1),
少量二线服务中断（1），
minimal primary services interrupted (5),
少量主要服务中断（5），
extensive secondary services interrupted (5),
大量二线服务中断（5），
extensive primary services interrupted (7),
大量主要服务中断（7），
all services completely lost (9)

全部服务中断（9）

Loss of accountability 损失问责性

Are the threat agents' actions traceable to an individual?
攻击者的行动是否追溯到个人？
Fully traceable (1), 完全可追溯（1），
possibly traceable (7), 可能可追溯（7），
completely anonymous (9) 完全匿名（9）

Business Impact Factors

业务影响因素

The business impact stems from the technical impact, but requires a deep understanding of what is important to the company running the application. In general, you should be aiming to support your risks with business impact, particularly if your audience is executive level. The business risk is what justifies investment in fixing security problems.

业务影响源于技术影响，但是需要进一步理解对于公司应用来说什么重要。通常，你需要有业务影响分析支持你提出风险，尤其是你面对公司执行层的时候。业务风险将是投资解决安全问题的理由。

Many companies have an asset classification guide and/or a business impact reference to help formalize what is important to their business. These standards can help you focus on what's truly important for security. If these aren't available, then talk with people who understand the business to get their take on what's important. The factors below are common areas for many businesses, but this area is even more unique to a company than the factors related to threat agent, vulnerability, and technical impact.

许多公司有资产分类指引或者业务影响参考来帮助确定什么是公司是重要的。这些标准能够帮你将目光聚集到真正重要的安全事务上来。如果没有这些，那么和懂得业务的人去沟通，尤其去决定什么是重要的。以下因素是很多业务共有的，与攻击者、漏洞和技术影响方面相比，这个领域还是比较单一的。

Financial damage 财务损失

How much financial damage will result from an exploit?
在一次漏洞被利用的事件里，财务损失情况如何？
Less than the cost to fix the vulnerability (1),
少于修复漏洞（1），
minor effect on annual profit (3),
对于年收益影响很小（3），
significant effect on annual profit (7),

对年收益显著影响（7），
bankruptcy (9)
破产（9）

Reputation damage 声誉损失
Would an exploit result in reputation damage that would harm the business?
漏洞被利用是否会对业务造成声誉损失？
Minimal damage (1),
很小的损失（1），
Loss of major accounts (4),
损失主要客户（4），
loss of goodwill (5),
损失发展前景（5），
brand damage (9)
失去品牌（9）

Non-compliance 不合规
How much exposure does non-compliance introduce?
在多大程度上不遵守规范会导致泄露？
Minor violation (2), 很小的违反（2），
clear violation (5), 明显的违反（5），
high profile violation (7) 严重的违反（7）

Privacy violation 侵犯隐私
How much personally identifiable information could be disclosed?
多少个人身份信息被泄露？
One individual (3), 一个人（3），
hundreds of people (5), 百余人（5），
thousands of people (7), 千余人（7），
millions of people (9) 百万人（9）

Step 4: Determining the Severity of the Risk

步骤四：确定风险的严重程度

In this step we're going to put together the likelihood estimate and the impact estimate to calculate an overall severity for this risk. All you need to do here is figure out whether the likelihood is LOW, MEDIUM, or HIGH and then do the same for impact. We'll just split our 0 to 9 scale into three parts.

在这一步，我们将把可能性评估和影响评估放在一起，计算风险的总体严重程度。你需要做的是明确可能性的低、中或者高，影响度也这样做。我们仅把 0 到 9 的纬度分为三部分

Likelihood and Impact Levels

0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

可能性和影响程度	
0 to <3	低
3 to <6	中
6 to 9	高

Informal Method 非正式方法

In many environments, there is nothing wrong with "eyeballing" the factors and simply capturing the answers. You should think through the factors and identify the key "driving" factors that are controlling the result. You may discover that your initial impression was wrong by considering aspects of the risk that weren't obvious.

在很多情况下，目测各种因素，直接得到答案也没有什么错。你需要考虑各种因素并确定对于结果有影响的关键因素。但通过考虑不明显的风险，你可能发现第一印象是错的。

Repeatable Method 可重复使用的方法

If you need to defend your ratings or make them repeatable, then you may want to go through a more formal process of rating the factors and calculating the result. Remember that there is quite a lot of uncertainty in these estimates, and that these factors are intended to help you arrive at a sensible result. This process can be supported by automated tools to make the calculation easier.

如果需要让评级更可靠并且可以重复使用，那么你可能要通过一个更加正式的因素评级和结果计算流程。请牢记，在这些评估中，有很多不确定性，这些因素是为了帮助你达成一个合理的结果。这个流程可以被自动化工具所支持，使得计算更容易。

The first step is to select one of the options associated with each factor and enter the associated number in the table. Then you simply take the average of the scores to calculate the overall likelihood. For example:

第一步是选择与每个因素相关的选项，并在表中输入关联的编号。然后，只需采取的分数平均计算总体的可能性。例如：

Threat agent factors				Vulnerability factors			
Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1	3	6	9	2
Overall likelihood=4.375 (MEDIUM)							

攻击者因素				漏洞因素			
技术水平	动机	机会	规模	发现难易程度	利用难易程度	知晓度	入侵检测
5	2	7	1	3	6	9	2
总体的可能性=4.375 (中)							

Next, we need to figure out the overall impact. The process is similar here. In many cases the answer will be obvious, but you can make an estimate based on the factors, or you can average the scores for each of the factors. Again, less than 3 is LOW, 3 to less than 6 is MEDIUM, and 6 to 9 is HIGH. For example:

接下来，需要搞清整体影响，这里流程相似。在许多情况下，答案是显而易见的，但你可以根据的因素来估计，也可以平均每个因素的得分。同样，小于 3 为低，3 至不到 6 中等，及 6 至 9 为高。例如：

Technical Impact				Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability	Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8	1	2	1	5
Overall technical impact=7.25 (HIGH)				Overall business impact=2.25 (LOW)			

技术影响				业务影响			
损失保密性	损失完整性	损失可用性	损失问责性	财务损失	声誉损失	不合规	侵犯隐私
9	7	5	8	1	2	1	5
整体技术影响=7.25 (高)				整体业务影响=2.25 (低)			

Determining Severity

确定严重程度

However we arrived at the likelihood and impact estimates, we can now combine them to get a final severity rating for this risk. Note that if you have good business impact information, you should use that instead of the technical impact information. But if you have no information about the business, then technical impact is the next best thing.

无论如何我们已经走到了测算“发生的可能性”和造成的影响，现在能够结合这两者得出最终风险等级了。请注意，如果你有可靠的业务影响的信息，你应该使用业务影响的信息而不是技术影响的信息。但如果你没有业务影响的信息，那么技术影响则是用于下一步评估最好的信息。

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

整体风险的严重性				
影响	高	中	高	关键
	中	低	中	高
	低	注意	低	中
		低	中	高
	可能性			

In the example above, the likelihood is MEDIUM, and the technical impact is HIGH, so from a purely technical perspective, it appears that the overall severity is HIGH. However, note that the business impact is actually LOW, so the overall severity is best described as LOW as well. This is why understanding the business context of the vulnerabilities you are evaluating is so critical to making good risk decisions. Failure to understand this context can lead to the lack of trust between the business and security teams that is present in many organizations.

在上面的例子，可能性是中等的，技术影响是高，所以从纯技术的角度来看，似乎整体严重程度为高。但是，请注意业务的影响实际上是低的，所以整体的严重程度是最好的描述为低。这就是为什么在评估漏洞时了解其对业务环境对于良好的风险决策是如此重要。对于这个环境的不理解会导致业务部门和安全团队之间缺乏信任，这样的现状存在于很多组织中。

Step 5: Deciding What to Fix

步骤 5：决定修复内容

After you've classified the risks to your application, you'll have a prioritized list of what to fix. As a general rule, you should fix the most severe risks first. It simply doesn't help your overall risk profile to fix less important risks, even if they're easy or cheap to fix. Remember, not all risks are worth fixing, and some loss is not only expected, but justifiable based upon the cost of fixing the issue. For example, if it would cost $100,000 to implement controls to stem $2,000 of fraud per year, it would take 50 years return on investment to stamp out the loss. But remember there may be reputation damage from the fraud that could cost the organization much more.

当你完成了对你应用程序的风险分类，你将能得到一份以优先级排列的修复列表。作为一般规则，您应该首先修复的最严重的风险。即使解决那些简单、且低成本的不太重要的风险，也无助于改善整个的风险状况。请记住，并不是所有的风险都值得修复，有些损失不仅是预期的，而且是基于修复成本合理的考虑。例如，如果将耗资 10 万实行控制，以阻止美元的每年 2,000 欺诈，为了杜绝了损失将需要 50 年收回投资。但要记住欺诈有可能造成声誉损害，可能使花费组织更多的成本。

Step 6: Customizing Your Risk Rating Model

步骤 6：定制风险评级模型

Having a risk ranking framework that's customizable for a business is critical for adoption. A tailored model is much more likely to produce results that match people's perceptions about what is a serious risk. There are several ways to tailor this model for your organization. You can waste lots of time arguing about the risk ratings if they're not supported by a model like this.

拥有一个定制的风险评级框架对于业务是至关重要的。量身打造的模型可能产生更符合人们关于什么是严重风险看法的结果。如果风险评级模型没有订制，那么你可能花费大量的时间去证明一个风险的评级。有几个方法可以去为您的组织定制风险评级模型。

Adding factors 增加因素

You can choose different factors that better represent what's important for your organization. For example, a military application might add impact factors related to loss of human life or classified information. You might also add likelihood factors, such as the window of opportunity for an attacker or encryption algorithm strength.

您可以选择那些能更好地代表什么对你的组织是重要的不同的因素。例如，一个军事应用程序可能添加于人员丧生或机密信息的丢失的影响因素。您还可以添加可能性的因素，例如攻击者机会窗口，加密算法强度等。

Customizing options

自定义选项

There are some sample options associated with each factor, but the model will be much more effective if you customize these options to your business. For example, use the names of the different teams and your names for different classifications of information.

每一个因素都会有些标本的选项，但是如果你能够自定义这些选项的话，这个评级模型将对您的业务更加有效。例如，使用不同的团队名字以及不同的信息分类。

You can also change the scores associated with the options. The best way to identify the right scores is to compare the ratings produced by the model with ratings produced by a team of experts. You can tune the model by carefully adjusting the scores to match.

你还可以更改与这些选项相关的得分。通过比较由模型产生的评级及专家团评级是确定分数中确的最好方法。你可以通过仔细的调整使得评级能够相匹配。

Weighting factors

因素加权

The model above assumes that all the factors are equally important. You can weight the factors to emphasize the factors that are more significant for your business. This makes the model a bit more complex, as you'll need to use a weighted average. But

otherwise everything works the same. Again, you can tune the model by matching it against risk ratings you agree are accurate.

以上模型设想所有因素都同样重要。你可以对因素进行加权以强调某些因素对你的业务更加重要。这会让评级模型变得有点复杂，因为你将需要使用加权平均得到结果。但是其他的方法都是一样的。同样，你可以通过调整模型使它和你同意的风险评级准确度相一致。

References

参考

- NIST 800-30 Risk Management Guide for Information Technology Systems [1]
- AS/NZS 4360 Risk Management [2]
- Industry standard vulnerability severity and risk rankings (CVSS) [3]
- Security-enhancing process models (CLASP) [4]
- Microsoft Web Application Security Frame [5]
- Security In The Software Lifecycle from DHS [6]
- Threat Risk Modeling
- Pratical Threat Analysis [7]
- A Platform for Risk Analysis of Security Critical Systems [8]
- Model-driven Development and Analysis of Secure Information Systems [9]
- Value Driven Security Threat Modeling Based on Attack Path Analysis[10]