ALIBABA CLOUD

阿里云

安全众测
相关协议

文档版本：20220117

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.先知等保测评服务协议

本服务条款是阿里云计算有限公司 (以下简称“阿里云”)与您就先知等保测评服务相关事项所订立的有效合约。您通过盖章、网络页面点击确认或以其他方式选择接受本服务条款，包括但不限于未点击确认本服务条款而事实上使用了先知等保测评服务，即表示您与阿里云已达成协议并同意接受本服务条款的全部约定内容。如若双方盖章文本与网络页面点击确认或以其他方式选择接受之服务条款文本，存有不一致之处，以双方盖章文本为准。

关于本服务条款，提示您特别关注限制、免责条款，阿里云对您违规、违约行为的认定处理条款，以及管辖法院的选择条款等。限制、免责条款可能以加粗或加下划线形式提示您注意。在接受本服务条款之前，请您仔细阅读本服务条款的全部内容。如果您对本服务条款的条款有疑问的，请通过阿里云相关业务部门进行询问，阿里云将向您解释条款内容。如果您不同意本服务条款的任意内容，或者无法准确理解阿里云对条款的解释，请不要进行后续操作。

根据《中华人民共和国合同法》及其它相关法律法规的规定，就阿里云计算有限公司（以下简称“乙方”）向您（以下简称“甲方”）提供技术服务（以下简称“服务”）事宜，经甲乙双方共同协商，一致达成本如下各条款，以资共同遵照协议。

1 定义

1.1 “项目”是指乙方按照《等保合规咨询与测评服务说明书》中的约定，向甲方提供服务的具体项目。

1.2 “关联公司” 是指控制、受控于本协议一方或同本协议一方共同受某一公司控制的实体。

1.3 “本协议” 是指本《技术服务协议》及其所有附件。

1.4 “技术服务”或“服务”是指乙方技术服务人员按本协议及其所有附件的约定，为甲方所做的工作。

1.5 “可交付成果物”是指本协议实施过程中产出的工作成果。

1.6 “技术服务人员” 是指乙方雇用或指定的代理人、雇员或分包商。

1.7 “保密信息”是指双方在讨论、订立及履行本协议过程中向另一方提供的全部技术和商业信息，以及本协议及其所有附件的内容及可交付成果物（如有）。

1.8 “服务费用”是指依照本协议中约定的服务费用，已包括乙方应缴纳的税款。

1.9 “税款”是指根据中华人民共和国法律规定对可交付成果物和/或服务应征收的税款。

2 项目的实施

2.1 乙方应按本协议及《等保合规咨询与测评服务说明书》中的相关约定，向甲方提供相应的技术服务和/或可交付成果物。

2.2 项目的内容以《等保合规咨询与测评服务说明书》中的约定为准。

2.3 服务周期以《等保合规咨询与测评服务说明书》中的约定为准。

2.4 验收标准和验收方式以《等保合规咨询与测评服务说明书》中的约定为准。

3 双方权利义务

3.1 甲方权利义务

3.1.1 按照约定如期全额支付服务费用。

3.1.2 甲方应依照《等保合规咨询与测评服务说明书》中的约定，向乙方提供技术服务所必须的信息、数据、资料、系统/设备权限、系统/软件，并负责为乙方提供必要的设备、工作场地、后勤设施等。

3.1.3 甲方充分知晓并认可，甲方的支持与配合是乙方如期完成服务内容的必要条件。甲方承诺在制度上、人力上、系统环境上以及乙方人员的工作条件方面给予乙方充分的配合和支持，确保项目的顺利实施。

3.1.4 甲方应在项目小组指派一名甲方人员作为项目负责人，负责对乙方服务进行协调、监督，项目负责人应定期向甲方汇报，与乙方项目负责人沟通，并对服务和/或可交付成果物进行验收。

3.1.5 本协议及《等保合规咨询与测评服务说明书》中规定的其他义务。

3.2 乙方权利义务

3.2.1 乙方应尽勤勉义务，严格执行项目服务计划，依照《等保合规咨询与测评服务说明书》的约定交付服务和/或可交付成果。

3.2.2 未经双方项目负责人书面确认或者甲方书面同意，乙方不得延迟或进行内容上的变更。如果乙方在提供技术服务的过程中发现影响计划执行的不利因素的，乙方应及时通报给甲方。

3.2.3 鉴于该项服务的特殊性，甲方同意并认可乙方可将本项目的全部或部分服务内容委托给其合作伙伴完成。

3.2.4 乙方负责对其合作伙伴的能力和资质进行把控，确保合作伙伴提供的服务符合监管部门的要求。

3.2.5 本协议及《等保合规咨询与测评服务说明书》中规定的其他义务。

4 服务费用的支付

4.1 乙方将向甲方提供本协议及《等保合规咨询与测评服务说明书》约定的专业服务费用。该服务费用不含阿里云云服务产品的费用，就项目所需的云服务产品，甲乙双方另行签署协议确定。

4.2 本合同签订7日后，甲方应向乙方支付全部服务费用，乙方在收到款项后10日内向甲方开具等额发票。

4.3 甲方将上述服务费通过在阿里云官网线上购买的方式支付至乙方账户。

5 保密信息

5.1 未经披露方允许，接收方不得将属于披露方的任何资料用于本协议之外的目的。

5.2 接收方应妥善保管披露方提供的各种资料、信息和数据。

5.3 接收方对披露方所提供的技术资料承担保密义务。本协议履行完毕后，除双方另有约定外，接收方应按披露方要求退还披露方所提供的技术资料。

5.4 除为履行本协议需要，乙方有权将提供服务所必要的保密信息提供给其合作伙伴外，一方必须对所接触到的对方的保密信息进行严格保密，未经对方书面许可不得向任何第三方以任何形式进行披露。乙方应确保合作伙伴按照本协议规定条款承担保密责任。但是，如下信息不受此限：

a) 已成为公知信息，而接收方对此并无过错；

b) 披露时接收方已经知晓的信息；

c) 接收方从第三方合法获得的信息，且未附加保密的义务；

d) 接收方并未使用保密信息，而自行研发获得的信息；

e) 披露方事先书面同意披露或使用的信息；

5.5 一方发现“保密信息”发生泄露等事故时，应立即告知对方，经双方协商后采取合理的对策。另外，由于一方的故意或过失造成“保密信息”泄露时，该方须承担由此给另一方造成的直接经济损失，且须及时采取必要的措施将对方损失控制在最小限度内，并自行承担因此发生的费用和责任。如果一方未及时采取必要措施而使损失扩大，则该方对对方扩大的损失亦承担赔偿责任。

5.6 本条规定于本协议有效期内及终止后两（2）年内有效。

6 违约责任与免责条款

6.1 除非双方一致同意或本协议另有约定或法律规定，任何一方不得提前终止本协议。

6.2 因甲方未向乙方提供项目服务所需的信息、数据、资料、系统/设备权限、设备、工作场地、后勤设施等，致使乙方提供服务迟延或不符合约定的，乙方应予免责。

6.3 甲方未按约定支付服务费用的，乙方有权随时解除协议，并要求甲方支付服务费用20%的违约金。

6.4 甲方充分知晓并认可，乙方尽勤勉义务向甲方提供服务，但是乙方所提供的技术服务受项目实施当时的技术条件、网络状态、甲方的系统状况、服务周期等因素的影响和约束，乙方所提供的技术服务和/或可交付成果物仅仅是当时情况下给出的技术建议，乙方不对技术服务和/或可交付成果物的准确性、有效性、可持续性承担任何的保证责任。

6.5 如因乙方主观原因造成乙方未能够按《等保合规咨询与测评服务说明书》的约定交付服务成果的，乙方应向甲方出具电子邮件说明延误原因，并承诺加大投入以追赶项目进度。如乙方延误两周以上未能够按《等保合规咨询与测评服务说明书》的约定交付服务成果的，乙方应向甲方出具追赶进度计划，并加大投入以追赶项目进度。如乙方延误一个月以上未能够按《等保合规咨询与测评服务说明书》的约定交付服务成果的，甲方有权解除协议，并要求乙方返还所有已经支付的款项。

6.6 任何一方就本协议承担的违约金总额均不超过本协议总金额的20%。

7 协议的生效、变更和终止

7.1 本协议自双方加盖公章或合同专用章之日起生效。

7.2 甲、乙双方任何一方有正当理由要求变更本协议的，须提前15天以书面形式通知对方并协商解决，双方应签署变更协议。

7.3 如果发生以下情况，可以视为合同解除或终止，有关责任方承担相应的责任：

7.3.1 一方进入解散或清算阶段；

7.3.2 一方被判为破产或其它原因致使资不抵债；

7.3.3 本协议已有效、适当、全面得到履行；

7.3.4 双方共同同意以书面文件提前解除协议；

7.3.5 根据仲裁机构的生效裁决或司法机关的生效判决，本协议解除。

8 争议与解决

8.1 因执行本协议所发生的和本协议有关的一切争议，双方应首先友好协商解决。如果经协商不能达成协议，任一方均可向杭州市西湖区人民法院提起诉讼。

9 不可抗力

9.1 不可抗力必须是指一方不可控制的、不可预见的、不可克服的事件，包括但不限于：自然灾害：地震、洪水、火灾等；战争或准战争状态、恐怖活动、戒严、骚乱、大规模爆发的流行性传染病等。

9.2 协议生效后，由上述不可抗力因素造成的乙方服务期延误，则此类延误将被视为不可抗力，乙方不承担违约责任，但必须及时通知甲方。

9.3 不可抗力因素致使甲方无法继续履行本协议或不能及时提供相应支援而致使项目延误，甲方不承担违约责任，但必须及时通知乙方。

9.4 在不可抗力事件结束后十个工作日内，受不可抗力影响一方应以挂号或传真的方式将有关部门出具的证明送达至对方，否则对方可不予承认其遭受不可抗力影响，并要求其承担违约责任。

9.5 如不可抗力事故连续60天以上时，双方应通过友好协商解决本协议履行的问题。

10 附则

10.1 本协议所载任何内容不应被解释为在甲乙双方间创设合资、合伙、代理或任何其它本协议目的以外的关系。

10.2 本协议的所有附件均构成本协议的有效组成部分。本协议反映了双方对本协议所述主题的全部协定，并代替所有之前关于本协议所述主题的任何协议及以往惯例。

10.3 任何一方未能或延迟行使其在本项下的权利，不能解释为对该权利的放弃。

10.4 如有未尽事宜，甲乙双方可以签订补充协议进行说明。

10.5 若本协议中任何条款因任何原因而被认定无效，此种无效条款并不影响其他条款的有效性，且此种无效条款应自始视为不存在。

10.6 本协议及附件壹式贰份，甲乙双方各执壹份，每份具有同等的法律效力。

10.7 本协议附件为本协议不可分割之部分，具有同等法律效力。

附件一：《等保合规咨询与测评服务说明书》

1 技术服务的内容和范围

乙方根据甲方需求，委托具有等保测评资质的合作伙伴测评机构，按本说明书第四条所列明的信息系统安全等级保护测评项目清单的范围，提供以下内容的技术服务：

1、基于国家标准《GB/T22239-2008信息系统安全等级保护基本要求》，完成XX系统的Y级保护测评服务，包括物理安全、网络安全、主机系统安全、应用安全和数据安全、安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等十个方面的安全测评，并按照等级保护主管部门指定的报告模版要求，为每个测评系统编制信息系统安全等级保护测评报告。

2、为满足等级保护相关技术和管理要求，提供系统安全加固咨询、安全管理体系咨询、Web安全扫描和网站恶意代码检测等技术咨询服务。

2 技术服务标准和原则

1、测评机构依据国家等级保护相关标准和制度规范开展测评等工作，遵循的标准和规范包括但不限于如下所列：

 GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》

 GB/T 22240-2008《信息安全技术 信息系统安全等级保护定级指南》

 GB/T 25058-2010《信息安全技术 信息系统安全等级保护实施指南》

 GB/T 28448-2012《信息安全技术 信息系统安全等级保护测评要求》

 GB/T 28449-2012《信息安全技术 信息系统安全等级保护测评过程指南》

 行业标准。

2、本次信息系统等级保护测评服务的实施应遵循以下原则：

1) 保密性原则：乙方及合作测评机构对测评服务中的过程数据和结果数据严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据进行任何侵害被测评单位和被测评系统的行为，否则甲方有权追究乙方的责任。

2) 标准性原则：合作测评机构实施的第三方测评应依据国家等级保护制度公布的相关标准及行业规范进行，不得采用未经正式公布的私有规定。

3) 规范性原则：工作过程和相关文档应具有良好的规范性和一致性，可以便于项目的跟踪和控制管理。

4) 整体性原则：每个系统测评的范围和内容应当整体全面，包括国家等级保护相关要求涉及的各个层面，不能因疏漏而导致结果的不可用。

5) 最小影响原则：采取的测评方法应尽可能小的影响被测系统和网络的正常运行，控制且减少风险，避免对现有网络和业务的正常运行产生显著影响或导致不可恢复的损失。

3 服务质量保证

1、为了保证本次项目的服务质量，乙方承诺并保证：

1) 乙方要求合作测评机构指派经国家认可的测评工程师参与项目的全过程，以保证工作质量达到预期要求；

2) 乙方和合作测评机构以职业审慎的态度处理可能存在的风险性，特别是在关键测评内容实施前（如扫描或工具测试），应和被测评单位充分沟通和协商，使得双方都清楚地认识到风险的可能性和可控性，并制定慎密的实施方案，采取必要的防范措施，确保在项目实施过程中对被测评信息系统正常运行不造成危害性影响。

2、 甲方应为乙方和合作测评机构履行协议的要求提供所需要的便利条件：

1) 予以项目便利的配合，包括及时提供准确完整的相关资料、协调相关配合人员、提供必要的现场实施办公工作环境等。

2) 甲方应按照双方商定的工作要求（包括进度、人员、质量等）完成本协议服务内容所要求甲方配合的工作。

4 服务清单和价格

本协议列明所有的信息系统安全等级保护测评项目清单和价格如下：

服务属性	服务名称	服务说明	价格
测评服务	信息系统安全等级保护测评	根据国家和相关行业等级保护相关标准，选取测评指标开展等级测评，出具等级测评报告	根据各省测评指导价计算
测评服务	信息系统等级保护定级和备案辅导	协助开展信息系统定级和备案辅导，包括定级报告、备案表的填写指导	根据各省测评指导价计算

5 服务交付物

本服务的交付物为以下形式的技术资料输出或成果：

1) 信息系统等级保护测评方案

2) 信息系统等级保护测评报告（每系统一份）

3) 信息系统等级保护测评过程文档（甲方保存归档）

2.供应链漏洞验收及奖励标准

通用软件漏洞情报收集及奖励标准

为了更好地保障云上用户的安全，提升安全防御能力，阿里云盾（先知）专门制定了《供应链软件漏洞情报奖励计划》，以提供奖励的方式鼓励白帽子遵循负责任的漏洞披露机制，向我们提供供应链软件的安全漏洞情报信息。

云盾先知确认漏洞后，将按照流程向您提供现金奖励和荣誉奖励，同时在遵守国内相关法律的情况下将漏洞反馈给软件开发者公司，并向受到影响的合作伙伴共享漏洞情报信息。如果您发现供应链软件的漏洞，欢迎您向我们提交，我们会第一时间响应处理。

漏洞定义

攻击者通过操纵某些数据，使得程序偏离设计者的逻辑，进而引发的安全问题。先知计划漏洞平台主要收集应用软件和建站系统程序漏洞。

漏洞名称

白帽子自定义漏洞名称，尽量包含漏洞关键字等信息。

如：PHPTEST v1.0.0前台无限制Getshell。

收集的漏洞类型

我们关注的漏洞类型，包括： XSS跨站、SQL注入、XXE、命令执行、文件包含、任意文件操作、权限绕过、存在后门、文件上传、逻辑漏洞、栈溢出、堆溢出、内存破坏、整数溢出、释放后重用、类型混淆、沙盒绕过、本地提权、拒绝服务、CRLF注入、SSRF、点击劫持、时间竞争漏洞、敏感信息泄露等。

漏洞收集范围

我们关注当前应用广泛的互联网应用软件类及第三方建站系统程序，具体如下：

厂商类型	应用名	官网地址
A类厂商	phpMyAdmin	https://www.phpmyadmin.net/
A类厂商	DedeCMS	http://www.dedecms.com
A类厂商	Discuz!	http://www.discuz.net
A类厂商	ECShop	http://yunqi.shopex.cn/products/ecshop
A类厂商	CKEditor（FCKEditor）	https://ckeditor.com/
A类厂商	Wordpress	https://zh-cn.wordpress.com/

厂商类型	应用名	官网地址
A类厂商	Django	https://www.djangoproject.com/
A类厂商	WebX	http://www.openwebx.org/
A类厂商	Fastjson	https://github.com/alibaba/fastjson
A类厂商	Struts2	https://struts.apache.org/
A类厂商	Spring Framework	https://projects.spring.io/spring-framework/
A类厂商	Spring Boot	https://projects.spring.io/spring-boot/
B类厂商	ThinkPHP	http://www.thinkphp.cn/
B类厂商	phpCMS	http://www.phpcms.cn/
B类厂商	PHPWind	https://www.phpwind.com/
B类厂商	Flask	https://github.com/pallets/flask
B类厂商	Drupal	https://www.drupal.org/
B类厂商	Joomla	https://www.joomla.org/
B类厂商	Yii	https://www.yiiframework.com/
B类厂商	CodeIgniter	https://codeigniter.com/
B类厂商	ZenTaoPMS（禅道项目管理）	http://www.zentao.net/
B类厂商	Empire CMS（帝国CMS）	http://www.phome.net/

厂商类型	应用名	官网地址
B类厂商	Tornado	http://www.tornadoweb.org/
B类厂商	GitLab	https://gitlab.com
B类厂商	Jenkins	https://jenkins.io/
B类厂商	Redmine	https://www.redmine.org/
B类厂商	ElasticSearch	https://www.elastic.co/cn/
B类厂商	Openfire	https://www.igniterealtime.org/projects/openfire/
B类厂商	Atlassian Jira	https://www.atlassian.com/software/jira
B类厂商	Solr	http://lucene.apache.org/solr/
B类厂商	Zabbix	https://www.zabbix.com/
B类厂商	WildFly	http://wildfly.org/
B类厂商	Magento	https://magento.com/
B类厂商	Atlassian Confluence	https://www.atlassian.com/software/confluence
B类厂商	Kibana	https://www.elastic.co/products/kibana
B类厂商	DokuWiki	https://www.dokuwiki.org/dokuwiki
B类厂商	MediaWiki	https://www.mediawiki.org/

厂商类型	应用名	官网地址
B类厂商	cPanel	https://cpanel.com/
B类厂商	httpFileServer（HFS）	http://www.rejetto.com/hfs/
B类厂商	CoreMail	http://www.coremail.cn/
B类厂商	Apache Hadoop	http://hadoop.apache.org/
C类厂商	Laravel	https://laravel.com/
C类厂商	XAMPP	https://www.apachefriends.org/zh_cn/index.html
C类厂商	ownCloud	https://owncloud.org/
C类厂商	ShopEx	http://www.shopex.cn/
C类厂商	OpenCart	https://github.com/opencart/opencart
C类厂商	ThinkSNS	http://thinksns.com/
C类厂商	Typecho	http://typecho.org/
C类厂商	拓尔思（TRS WCM）	http://www.trs.com.cn/
C类厂商	万户ezOFFICE	http://www.whir.net/cn/cpzx/index_2.html
C类厂商	深信服-VPN	http://www.sangfor.com.cn/product/net-safe-ssl.html
C类厂商	金蝶OA	http://www.kingdee.com/solutions/field/oa

厂商类型	应用名	官网地址
C类厂商	致远OA	http://www.seeyon.com/
C类厂商	泛微OA Office	http://www.weaver.com.cn/
C类厂商	Sentry	https://sentry.io/
C类厂商	phpBB	https://www.phpbb.com/
C类厂商	CMSTOP	http://www.cmstop.com/
C类厂商	Piwik	https://matomo.org
C类厂商	F5-BIGipServer	https://f5.com/products/big-ip
C类厂商	RoundCube	https://roundcube.net/
C类厂商	Cacti	https://www.cacti.net/
C类厂商	WDCP 主机管理系统	http://www.wdlinux.cn/
C类厂商	Hudson	http://jenkins-ci.org/
C类厂商	TurboMail	http://www.turbomail.org/
C类厂商	亿邮	http://www.eyou.net/
C类厂商	Zimbra	https://www.zimbra.com/
C类厂商	live800	https://www.live800.com/
C类厂商	HDwiki	http://kaiyuan.hudong.com/
C类厂商	Webmin	http://www.webmin.com/

厂商类型	应用名	官网地址
C类厂商	vBulletin	https://www.vbulletin.com/
C类厂商	MyBB	https://github.com/mybb
C类厂商	SquirrelMail	https://squirrelmail.org/
C类厂商	AMH 云主机面板	http://amh.sh/
C类厂商	ActiveMQ	http://activemq.apache.org/
D类厂商	74cms	http://www.74cms.com/
D类厂商	齐博CMS	http://www.qibosoft.com/
D类厂商	HiShop	http://www.hishop.com.cn/
D类厂商	SiteServer CMS	http://www.siteserver.cn/
D类厂商	Odoo	https://www.odoo.com/zh_CN/
D类厂商	PHP168	http://www.php168.net/
D类厂商	B2Bbuilder	http://www.b2b-builder.com/
D类厂商	Gogs	https://gogs.io/
F类厂商	通达OA	https://www.tongda2000.com/
F类厂商	PbootCMS	http://www.asp4cms.com/
F类厂商	Destoon	https://www.destoon.com/
F类厂商	MetInfo	https://www.metinfo.cn/

厂商类型	应用名	官网地址
F类厂商	Z-Blog	https://www.zblogcn.com/
F类厂商	KesionCMS	http://www.kesion.com/aspb/
F类厂商	微擎	https://www.we7.cc/
F类厂商	emlog	http://www.emlog.net/
F类厂商	主机宝	http://z.admin5.com

> **说明**
>
> 如无特殊标注，漏洞收集的范围是上表中应用程序的最新版本。最新版本信息，可在应用程序的官网查看。

评分规则

为解决漏洞评级混乱问题，美国基础设施顾问委员会（NIAC）提出了CVSS公开标准，由FIRST组织进行维护，它被用来评价漏洞的严重与紧急程度。

CVSS漏洞评级标准计算器

基础分类型	基础分值名	基础分值数
攻击方式（AV）	• 远程网络（N） • 相邻网络（A） • 本地攻击（L） • 物理方式（P）	• 0.85 • 0.62 • 0.55 • 0.2
攻击复杂度（AC）	• 低（L） • 高（H）	• 0.77 • 0.44
权限要求（PR）	• 无（N） • 低（L） • 高（H）	• 0.85 • 0.62（如果影响范围有变化为0.68） • 0.27（如果影响范围有变化为0.50）

基础分类型	基础分值名	基础分值数
用户交互（UI）	• 不需要（N） • 需要（P）	• 0.85 • 0.62
• C（机密性） • I（完整性） • A（可用性）	• 高（H） • 低（L） • 无（N）	• 0.56 • 0.220
影响范围（S）	• 未改变（U） • 改变（C）	互联网中受影响实例的个数。

> **说明**
>
> 影响范围权重最高，能够客观检验一个漏洞在互联网上的影响程度。

得分算法

根据以上得分，漏洞得分划分为：

- 严重（9.6~10.0）
- 高危（7.0~9.5）
- 中危（4.0~6.9）
- 低危（0.1~3.9）
- 无效（0.0）

对应的奖励范围

厂商类型	严重漏洞奖励范围	高危漏洞奖励范围	中危漏洞奖励范围	低危漏洞奖励范围
A类厂商	奖金：50000~500000元 积分：150	奖金：20000~50000元 积分：120	奖金：4000~15000元 积分：60	奖金：500~1000元 积分：30
B类厂商	奖金：20000~50000元 积分：120	奖金：6000~15000元 积分：100	奖金：1500~3000元 积分：50	奖金：300~500元 积分：20
C类厂商	奖金：10000~15000元 积分：120	奖金：3000~6000元 积分：60	奖金：800~1500元 积分：30	奖金：200~300元 积分：15
D类厂商	奖金：2000~3000元 积分：120	奖金：1000~2000元 积分：40	奖金：500~800元 积分：20	奖金：100~200元 积分：10
F类厂商	奖金：1000~2000元 积分：120	奖金：600~1000元 积分：40	奖金：400~600元 积分：20	奖金：50~150元 积分：10

暂不在漏洞收集范畴的类型

- A、B类厂商以外的XSS漏洞一概不在收取范围。
- A、B类厂商不收取反射XSS漏洞，SELF-XSS漏洞。
- 事件型漏洞（如xx厂商的某cms，存在官方接口安全问题，接口在官方服务器上）。
- 其他影响十分有限的漏洞。

漏洞降级

- 漏洞利用过程中需要涉及非普通用户权限，或在满足一定条件下才能触发的漏洞，将会酌情降级或降低奖励。
- 后台漏洞目前只收取getshell（OA类、协作类产品的普通用户控制台算作后台），漏洞会降级低危处理。

厂商降级

当针对某个厂商收取的高危漏洞数大于30个（未修复状态池），且厂商官方再无能力修复漏洞时，将对厂商进行降级或下线处理，同时暂停收取漏洞。

付款条件和限制

- 奖励标准仅适用于列表中的厂商，列表外的厂商，我们将根据厂商应用流行程度和漏洞影响范围，酌情给予奖励；

- 同一漏洞多位白帽子在先知平台提交，以时间先后顺序只奖励首位提交者；
- 官方无开源代码并且无测试Demo的漏洞，需要提供至少5个互联网以实例证明危害；
- 同一个漏洞源产生的多个漏洞计漏洞数量为一。例如：同一功能模块下的不同接口，同一文件的不同参数、同一参数出现在不同文件、同一文件在不同目录、同一漏洞的不同利用方式、不同版本的同一漏洞、同一函数导致漏洞等；
- 可以通过修复一个点使得后续利用均不可行的情况，后续漏洞提交均视为重复漏洞。

> **说明**
>
> 如多个接口程序中都用到了同一个全局函数进行数据处理，这个全局数据处理函数被利用导致了漏洞形成，则所有此类漏洞均视为同一漏洞。

- 在先知平台通知第三方厂商修复漏洞之前，漏洞在互联网上被公开不给予奖励；
- 报告网上已公开的漏洞不给予奖励；
- 同一漏洞重复提交至其他第三方漏洞平台，先知平台有权不给予奖励；
- 在漏洞处理的任何阶段发现漏洞重复或被公开，先知平台都有权驳回漏洞并取消奖励；对于恶意提交重复漏洞骗取奖励的行为，会给予警告乃至封号处理。

漏洞提交报告要求

为了能够对每个漏洞进行客观评估，兼顾厂商对漏洞的实际影响判断，建议白帽子依据CVSS 3.0标准，补充如下关键信息，从而避免审核过程中造成的偏颇。

- 利用方式：远程/本地/物理
- 用户交互：不需要登录/需登录/需登录（开放注册）
- 权限要求：普通用户/功能管理员/系统管理员
- 利用接口：`http://example.com/XXXXXid=100&xxxxx`
- 漏洞利用点参数：利用接口URL中的id
- 漏洞证明：
  - SQL注入漏洞：请补充注入利用证明，包括数据库的 `user()` 或 `version()` 或 `database()` 的输出结果，建议提供截图。
  - 命令执行漏洞：请补充命令执行利用证明，运行命令 `whoami` 输出的结果，建议提供截图。

注意事项

- 恶意报告者将作封号处理。
- 报告无关问题的将不予答复。
- 阿里巴巴集团员工不得参与或通过朋友参与漏洞奖励计划。
- 奖励计划仅适用于通过先知平台报告漏洞的用户。

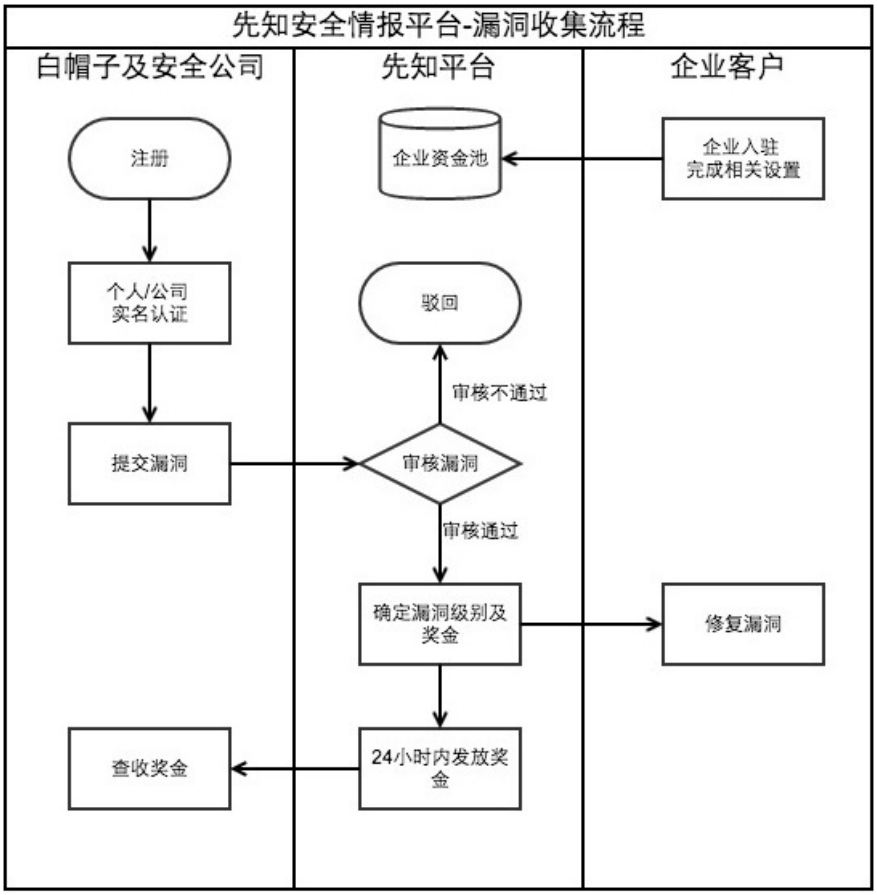
3.附件一：漏洞收集流程（先知安全情报）

云盾先知计划漏洞平台（以下简称先知平台）致力于构建和谐的互联网安全生态圈，为企业提供优质的SRC服务。同时，我们继续为白帽子提供全球通用软件0day漏洞收录平台。如果您发现入驻企业或第三方通用软件的漏洞，欢迎您向我们提交，我们会第一时间响应处理。为了表达您对互联网安全生态圈建设做出的贡献，我们将向您提供现金奖励和荣誉奖励，详见通用漏洞验收及奖励标准及各入驻企业奖励标准。

白帽子定义

白帽子指通过先知平台参与漏洞提交过程的安全专家，能够识别计算机系统或网络系统中的安全漏洞，但并不会恶意利用，而是报告漏洞，帮助企业在被其他人恶意利用之前修补漏洞，维护计算机和互联网安全。

漏洞收集流程



操作步骤

1. 登录并完善资料。
   - 白帽子使用淘宝网账号登录先知平台并完善资料和实名认证，请确保资料真实有效，并及时更新。
   - 企业入驻请访问：http://www.aliyun.com/product/xianzhi。
2. 提交漏洞。

   白帽子根据漏洞提交页面指引，提交安全漏洞信息。请务必详尽，漏洞描述越具体，越便于我们准确反馈给出合理的价格。

提交漏洞完成后，状态为**审核中**。

3. 审核漏洞。

   漏洞提交后48小时内（法定节假日顺延），我们会对收到的漏洞报告进行内部评估。

   - 漏洞不存在或者重复上报，我们将驳回漏洞，并告知驳回理由。状态：**已驳回**。
   - 漏洞描述不清，请白帽子在72小时内补充漏洞信息便于评估，超过72小时未补充系统将驳回漏洞。状态：**待补充**。
   - 漏洞经过验证确认存在，我们将在平台上确认漏洞。状态：**已审核**。

4. 确认奖励。

   我们将在漏洞确认存在后72小时内（法定节假日顺延），通用软件漏洞将按照《漏洞验收标准》中漏洞奖励标准确定奖励金额；第三方企业漏洞将根据企业自定义奖励标准奖励。状态：**已奖励**。

5. 发放奖励。

   漏洞奖励给出后，会直接发放到白帽子支付宝账户。状态：**已奖励**。

   若白帽子不接受奖励金额，可进行人工申述，我们将尽快与白帽子联系，共同协商奖励金额。状态：**已奖励**。

6. 企业修复漏洞。

   企业将在漏洞被确认后根据漏洞的修复情况，更新漏洞的状态到已修复。

通知企业流程（针对通用软件漏洞）

1. 漏洞经过验证确认存在，我们将及时通知企业确认漏洞。
2. 企业响应漏洞，并及时确认漏洞，告知漏洞处理进展。
3. 企业修复漏洞，告知漏洞已修复。

4.附件二：众测漏洞定级标准（先知安全情报）

通用奖励计划

企业可设置严重、高危、中危、低危漏洞的奖励金额，以吸引更多的白帽子发现漏洞，以下标准都是参考标准。平台奖励积分是白帽子虚拟荣誉值，积分越高的白帽子代表对平台贡献越大。

漏洞等级	建议奖励金额/单个漏洞（税前）	平台奖励积分
严重	8000~10000元	120分
高危	2500~5000元	60分
中危	500~1500元	20分
低危	50~200元	10分

漏洞等级

根据漏洞的危害程度将漏洞等级分为**严重**、**高危**、**中危**、**低危**。由先知平台结合利用场景中漏洞的严重程度、利用难度等综合因素给予相应分值的贡献值和漏洞级别。以下是每种等级包含的评分标准及漏洞类型。

- **严重漏洞**

  严重漏洞是指，发生在核心系统业务系统（核心控制系统、域控、业务分发系统、堡垒机等可管理大量系统的管控系统），可造成大面积影响的，获取大量（依据实际情况酌情限定）业务系统控制权限，获取核心系统管理人员权限并且可控制核心系统。

  包括但不限于：

  - 控制内网多台机器。
  - 核心后台超级管理员权限获取且造成大范围企业核心数据泄露，可造成巨大影响。

- **高危漏洞**
  - 获得系统的权限（getshell、命令执行等）。
  - 系统的SQL注入（后台漏洞降级，打包提交酌情提升）。
  - 敏感信息越权访问。包括但不限于绕过认证直接访问管理后台进行敏感操作、重要后台弱密码、获取大量内网敏感信息的SSRF等。
  - 读取任意文件。
  - 涉及金钱的交易、绕过支付逻辑（需最终利用成功，优惠券相关问题除外）。
  - 严重的逻辑设计缺陷和流程缺陷。包括但不限于任意用户登录漏洞、批量修改任意账号密码漏洞、涉及企业核心业务的逻辑漏洞等。**验证码爆破除外**。
  - 大范围影响用户的其他漏洞。包括但不仅限于重要页面可自动传播的存储型XSS、可获取管理员认证信息且成功利用的存储型XSS等。
  - 大量源代码泄露。

- **中危漏洞**
  - 需交互方可影响用户的漏洞。包括但不仅限于存储型XSS、涉及核心业务的CSRF等。
  - 平行越权操作。包括但不限于绕过限制修改用户资料、执行用户操作等。

- 由验证码逻辑导致任意账户登录、任意密码找回等系统敏感操作可被爆破成功造成的漏洞。
- 本地保存的敏感认证密钥信息泄露，需能做出有效利用。
- 四位验证码爆破重置密码或者登录账号。
- 心脏滴血漏洞。
- XML注入。
- 普通的后台或者边缘系统的后台。
- 任意文件上传（例如上传html导致存储XSS，其他情况除外）。

- **低危漏洞**
  - 普通信息泄露（纯静态文件泄露不收取，例如JS、CSS等）。
  - 反射型XSS（包括DOM XSS、Flash XSS）。
  - 普通的垂直越权。
  - 普通CSRF。
  - URL跳转漏洞。
  - 一些影响有限的越权（不涉及敏感信息，例如修改个人描述等）。
  - 短信炸弹。
  - 无回显的且没有深入利用成功的SSRF。
  - 无法利用的GIT HUB信息泄露（无敏感信息的泄露可能会不收取）。

- **暂不收取的漏洞类型**
  - SPF邮件伪造漏洞。
  - 接口穷举爆破已注册用户名类漏洞。
  - self-xss或post型反射XSS。
  - 邮件炸弹。
  - 非敏感操作的CSRF问题。
  - 单独的安卓APP android:allowBackup=”true” 问题，本地拒绝服务问题等（深入利用的除外）。
  - 修改图片size造成的请求缓慢等问题。
  - Nginx、Tomcat等版本泄露的问题。
  - 一些功能BUG，无法造成安全风险的问题。
  - 其他危害较低、不能证明危害的漏洞（如无法获取到敏感信息的CORS漏洞）。

重点金融行业企业奖励计划

企业可设置高危、中危、低危漏洞的奖励金额，以吸引更多的白帽子发现漏洞，以下标准都是参考标准。平台奖励积分是白帽子虚拟荣誉值，积分越高的白帽子代表对平台贡献越大。

漏洞等级	建议奖励金额/单个漏洞（税前）	平台奖励积分
高危	10000~50000	120分
中危	500~5000	60分
低危	50~200	10分

漏洞等级

根据漏洞的危害程度将漏洞等级分为**高危**、**中危**、**低危**。由先知平台结合使用场景中漏洞的严重程度、利用难度等综合因素给予相应分值的贡献值和漏洞级别，以下是每种等级包含的评分标准及漏洞类型。

- **高危漏洞**

  高危漏洞是指，发生在核心系统业务系统（核心控制系统、域控、业务分发系统、堡垒机等可管理大量系统的管控系统），可造成大面积影响的，获取大量（依据实际情况酌情限定）业务系统控制权限，获取核心系统管理人员权限并且可控制核心系统。

  包括但不限于：

  - 控制内网多台机器。
  - 核心后台超级管理员权限获取且造成大范围企业核心数据泄露，可造成巨大影响。
  - 获得系统的权限（getshell、命令执行等）。
  - 系统的SQL注入（后台漏洞降级，打包提交酌情提升）。
  - 敏感信息越权访问。包括但不限于绕过认证直接访问管理后台进行敏感操作、重要后台弱密码、获取大量内网敏感信息的SSRF等。
  - 读取任意文件。
  - 涉及金钱的交易、绕过支付逻辑（需最终利用成功，优惠券相关问题除外）。
  - 严重的逻辑设计缺陷和流程缺陷。包括但不限于任意用户登录漏洞、批量修改任意账号密码漏洞、涉及企业核心业务的逻辑漏洞等。**验证码爆破除外**。
  - 大范围影响用户的其他漏洞。包括但不仅限于重要页面可自动传播的存储型XSS、可获取管理员认证信息且成功利用的存储型XSS等。
  - 大量源代码泄露。

- **中危漏洞**
  - 需交互方可影响用户的漏洞。包括但不仅限于存储型XSS、涉及核心业务的CSRF等。
  - 平行越权操作。包括但不限于绕过限制修改用户资料、执行用户操作等。
  - 由验证码逻辑导致任意账户登录、任意密码找回等系统敏感操作可被爆破成功造成的漏洞。
  - 本地保存的敏感认证密钥信息泄露，需能做出有效利用。
  - 四位验证码爆破重置密码或者登录账号。
  - APP脱壳并成功反编译获取源码。
  - 心脏滴血漏洞。
  - XML注入。
  - 普通的后台或者边缘系统的后台。
  - 任意文件上传（例如上传html导致存储XSS，其他情况除外）。

- **低危漏洞**
  - 普通信息泄露（纯静态文件泄露不收取，例如JS、CSS等）。
  - 反射型XSS（包括DOM XSS或Flash XSS）。
  - 普通的垂直越权。
  - 普通CSRF。
  - URL跳转漏洞。
  - 一些影响有限的越权（不涉及敏感信息，例如修改个人描述等）。
  - 短信炸弹。
  - 无回显的且没有深入利用成功的SSRF。

- 无法利用的GITHUB信息泄露（无敏感信息的泄露可能会不收取）。

- **暂不收取的漏洞类型**
  - SPF邮件伪造漏洞。
  - 接口穷举爆破已注册用户名类漏洞。
  - self-xss、post型反射XSS。
  - 邮件炸弹。
  - 非敏感操作的CSRF问题。
  - 单独的安卓APP android:allowBackup=”true” 问题，本地拒绝服务问题等（深入利用的除外）。
  - 修改图片size造成的请求缓慢等问题。
  - Nginx、Tomcat等版本泄露的问题。
  - 一些功能BUG，无法造成安全风险的问题。
  - 其他危害较低、不能证明危害的漏洞。（例如：无法获取到敏感信息的CORS漏洞）。

漏洞提交规范

- 漏洞请求包或url（文字，非截图）或操作步骤（例如：设置->个人信息设置->图像上传处存在问题）。
- 漏洞payload。
- 漏洞危害证明（根据危害进行评级）。
- APP需要备注测试的版本信息。

评分标准通用原则

- 该标准仅适用于入驻先知平台的企业，并且只针对企业已明确说明接收漏洞的产品及业务。企业已明确说明不接收的漏洞将做驳回处理。企业已明确说明的漏洞等级调整将以企业为准。企业边缘业务将根据其重要程度适当调低漏洞等级。
- 各等级漏洞的最终贡献值数量由漏洞利用难度及影响范围等综合因素决定，若漏洞触发条件非常苛刻，包括但不限于特定浏览器才可触发的XSS漏洞，则可跨等级调整贡献值数量。
- 同一个漏洞源产生的多个漏洞计漏洞数量为一。例如同一个接口引起的多个安全漏洞、同一个发布系统引起的多个页面的安全漏洞、框架导致的整站的安全漏洞、泛域名解析产生的多个安全漏洞；因为厂商未做身份校验导致的同一系统多个接口越权或者是未做token校验导致的多个CSRF漏洞；同一文件的不同参数、同一参数出现在不同文件、同一文件在不同目录等。
- 第三方产品的漏洞只给第一个提交者计贡献值，等级不高于**中**，包括但不限于企业所使用的WordPress、Flash插件以及Apache等服务端相关组件、OpenSSL、第三方SDK等；不同版本的同一处漏洞视为相同漏洞。
- 通常，同一漏洞，首位报告者给予奖励，其他报告者均不计；同一漏洞，后提交的利用方式比第一个提交的利用造成的影响差距过大时，两个漏洞都通过，从第二个漏洞中分一部分奖金费第一个提交的同学。
- 不可公开已提交的漏洞细节，违者取消测试资格或封停账号。
- 报告网上已公开的漏洞不给予奖励。
- 漏洞打包。
  - 存在前后关系的漏洞，比如同一人提交的弱口令进入后台，后台SQL注入或者越权的漏洞合并处理，审核可以酌情提高漏洞等级。若已提交，后面又发现，则补充到该漏洞下面，可以提高奖金金额。
  - 对于漏洞拆分提交者，由管理员对漏洞进行打包，漏洞等级按打包漏洞中危害最高的计算，奖金按标准的最低额度发放，后期项目分配率会减低。对于严重拆分漏洞，刷漏洞等恶意行为进行冻结账户、甚至封号处理。

- 若存在以下情况者，小黑屋1个月。

  存在前后关系，先提交后者的。例如：发现邮箱弱口令，从邮箱中获知后台管理员密码，提交漏洞时先提交后台弱口令，再提交邮箱弱口令者。

- 以测试漏洞为借口，利用漏洞进行损害用户利益、影响业务运作、盗取用户数据等行为的，将不会计贡献值，同时先知平台将联合入驻企业保留采取进一步法律行动的权利。
- 对于提交描述不清的漏洞，将会直接驳回处理；每个漏洞需要明确产生漏洞的URL地址、文字细节、完整的截图、清晰的语言表达。
- SQL注入需要证明可以注入出一条数据，单纯报错提交会忽略。
- 弱口令问题（正常对外可注册的系统不算在弱口令范围内）：
  - 对于同一个人发现同一系统的不同的弱口令，将合并处理（如果厂商已经处理了之前的弱口令，后面再次提交的降级处理，第二次以后提交的都会合并处理）。
  - 对于默认的初始密码，只按照一个漏洞进行处理（比如邮箱的初始密码都是同一个密码，视为一个漏洞）。
  - 对于非重点系统，审核过程只正常确认该系统的第一个弱口令，后续提交的弱口令酌情忽略处理。
  - 对于重点系统或者核心业务，在评级过程中只正常确认前2个弱口令，后续的提交弱口令问题酌情降级或者忽略处理。
- 对于边缘或废弃业务系统，根据实际情况酌情降级。
- 存在前后关系的漏洞，比如同一人提交的弱口令进入后台，后台SQL注入的漏洞合并处理，可以提高漏洞等级，希望大家不要拆分漏洞，先知将根据实际情况对严重拆分漏洞，刷漏洞等恶意行为进行冻结账户、甚至封号的处理。
- 信息泄露类的漏洞如github信息泄露，memcache、redis等未授权访问等，根据存储的内容的有效、敏感程度进行确认评级，单独的危害较低的信息泄露如路径泄露，phpinfo信息泄露等将会忽略处理。
- 对于已经得到Webshell的情况，如果想打包源代码审计，请事先联系审核人员，审核人员将会与厂商沟通相关事宜，如果厂商同意审计，再进行后续操作，发现的漏洞可单独提交。否则，禁止下载源代码，将视为违规操作、一经发现行冻结账户、甚至封号的处理。
- 对于使用采用低版本的CMS导致的漏洞，每个漏洞类型只确认第一个提交的安全问题。
- 切勿进行可能引起业务异常运行的测试，例如：IIS的拒绝服务或者slow_http_dos等漏洞。
- 前台撞库、爆破类漏洞，需有成功案例证明；后台爆破，仅收取成功登录的案例，仅能爆破但没有进入后台的漏洞将驳回。
- 对于一些难以利用的安全漏洞，例如：HTTP.sys远程命令执行类漏洞，只确认一个提交的漏洞，评为低危漏洞，只是为了提示厂商做对应的升级。
- 对于PC端和APP端同一接口同一套代码的两个漏洞（即使域名可能不同），同一白帽子分开提交平台将会合并处理，主动合并会酌情提高奖励；不同的白帽子分别提交，在厂商未修复之前，评为重复漏洞。
- 对于信息泄露相关漏洞（包括GITHUB，提交的时候请说明，有哪些特征可以证明是某厂商的），可以深入利用造成很大危害的，一般为高危或者严重；对于是厂商线上对外核心应用服务配置、代码等信息泄露，一般为中危；如果不能做出有效利用且非核心业务的，一般为低危或者驳回处理。
- 严禁进行内网渗透，安全测试点到为止即可。

厂商保护机制

如果同一个系统中短时间发现了大量的同类型高危漏洞（如SQL注入、命令执行等），审核人员判定该系统几乎没有做任何防护，会与厂商沟通该系统的该类型漏洞是否要继续收取；若厂商表示该类漏洞已知不再收取，则平台方正常审核前三个该类型漏洞，发布通知前同系统其他同类型漏洞均降级处理，发布通知后同系统同类型漏洞均不再收取，直到厂商重新开放该漏洞类型收取。对于厂商漏洞修复被绕过或者代码回滚的原因导致漏洞还能被继续利用的，一年内再次提交降级收取。

注意事项

- 白帽子在测试SQL注入漏洞时，对于 `UPDATE` 、 `DELETE` 、 `INSERT` 等注入类型，使用手工测试，禁止直接使用工具测试。
- 测试过程中，社工企业员工，注意分寸，切勿对个人造成名誉影响。
- 禁止修改厂商的任何数据，包括数据库内容、账户密码、数据库连接密码等。
- 不允许使用扫描器对后台系统进行扫描。
- 对于不在客户测试范围内的系统的测试，**属于未授权测试，平台和厂商有权追究其责任**。
- 以上所有漏洞级别可视应用场景再具体定级，如SQL注入涉及到的数据为边缘系统或者测试数据则降低漏洞等级等。
- 以上所有漏洞级别为厂商参考的基础标准，可视应用业务场景再具体定级，具体定级主要是由厂商反馈而定。

奖金发放相关

- 请一定确认好，自己填写的收款账号和姓名一致（不要填写*）.
- 奖金发放周期，对于提交的漏洞，厂商复盘完成后，可以马上发放奖金，最快可做到当天，但是因为厂商结合业务评估或者内部推动需要时间周期，对于超过一个月仍未复盘完成的漏洞，平台会默认先发放奖金（即默认发放周期是一个月）。

争议解决办法

在漏洞报告处理过程中，如果报告者对流程处理、漏洞定级、漏洞评分等有异议的，可以通过漏洞详情页面的留言板或者通过即时通讯联系在线工作人员及时沟通。先知平台将按照漏洞报告者利益优先的原则与企业三方协调处理，必要时可引入外部安全人士共同裁定。

5.附件三：漏洞奖励发放规则（先知）

云盾先知计划漏洞平台（以下简称“先知平台”）致力于构建和谐的互联网安全生态圈，为白帽子提供供应链软件的0day漏洞收录。如果您发现供应链软件的相关漏洞，欢迎您向我们提交，我们会第一时间响应处理。为了表达您对互联网安全生态圈建设做出的贡献，我们会向您提供现金奖励和荣誉奖励。

现金奖励

对于入驻企业，我们将根据企业自定义的奖励标准发放奖励。

对于第三方供应链软件，我们将根据漏洞对应用的危害程度以及企业的流行程度给出相应的现金奖励。现金奖励金额请参考下表。详细信息请参见供应链漏洞验收及奖励标准。

企业类型	高危漏洞	中危漏洞	低危漏洞
流行厂商	10000~500000元	1000~10000元	500~1000元
一般厂商 I	3000~10000元	800~1000元	300~500元
一般厂商 II	1000~3000元	500~800元	200~300元
一般厂商III	500~1000元	200~500元	100~200元

荣誉奖励

对于成功上报的入驻企业漏洞，我们将统一按照高危12~20分、中危6~10分、低危2~4分的标准进行积分奖励。

对于成功上报的供应链软件漏洞，我们将根据漏洞对应用的危害程度给出相应的积分奖励。

漏洞积分由漏洞的危害程度以及企业的重要程度决定：积分=漏洞等级值×企业级别系数。

- 企业级别系数为1、5、10、20，分别对应一般厂商III、一般厂商 II 、一般厂商 I 和流行厂商。
- 漏洞等级值为1、2、4，分别对应低危、中危、高危。

例如：一个phpwind9的注入漏洞积分为80分，计算方法为：漏洞等级值（高危4）×厂商级别系数（流行厂商20）。

先知平台将根据白帽子的积分排行给予榜单公示。下表是不同积分对应的白帽等级和荣誉称号。

白帽等级	荣誉称号	积分
12	12级先知	>12800分
11	11级先知	6401分~12800分

白帽等级	荣誉称号	积分
10	级先知	3201分~6400分
9	9级先知	1601分~3200分
8	8级先知	801分~1600分
7	7级先知	401分~800分
6	6级先知	201分~400分
5	5级先知	101分~200分
4	4级先知	51分~100分
3	3级先知	25分~50分
2	2级先知	1分~24分
1	游民	0

注意事项

- 恶意报告者将作封号处理。
- 报告无关问题不予答复。
- 报告网上已公开的漏洞不计贡献值。
- 漏洞在先知平台上报后不得再上报到其他漏洞平台或自行公开（已得到企业及先知授权的除外），否则先知有权利取消该漏洞奖励，并追究法律责任。
- 阿里巴巴集团员工不得参与或通过朋友参与漏洞奖励计划。
- 奖励计划仅适用于通过先知平台报告漏洞的用户。

6.附件四：常见漏洞危害及定义（先知计划）

Web服务端漏洞

- **SQL注入攻击**
  - **名词解释：**

    SQL注入攻击（SQL Injection），简称注入攻击、SQL注入，被广泛用于非法获取网站控制权，是发生在应用程序的数据库层上的安全漏洞。由于在设计程序时，忽略了对输入字符串中夹带的SQL指令的检查，被数据库误认为是正常的SQL指令而运行，从而使数据库受到攻击，可能导致数据被窃取、更改、删除，甚至执行系统命令等，以及进一步导致网站被嵌入恶意代码、被植入后门程序等危害。
  - **常见发生位置**
    - URL参数提交，主要为GET请求参数。
    - 表单提交，主要是POST请求，也包括GET请求。
    - Cookie参数提交。
    - HTTP请求头部的一些可修改的值，例如Referer、User_Agent等。
    - 一些边缘的输入点，例如mp3、图片文件的一些文件信息等。
  - **防御措施**
    - 使用预编译语句。一般来说，防御SQL注入的最佳方式，就是使用预编译语句，绑定变量，但对现有代码的改动量较大。
    - 使用存储过程。使用安全的存储过程可在一定程度上对抗SQL注入，但要注意此种方法并不是100%安全。
    - 严格检查用户数据。对用户传入的数据类型及内容进行严格的检查。对数据类型检查，如利用ID查询时判断是否为整型，输入邮箱时判断邮箱格式，输入时间、日期等必须严格按照时间、时期格式等；对数据内容进行检查，如严格检测用户提交数据中是否包含敏感字符或字符串，是否匹配某种注入规则，严格转义特殊字符等。注意此种方法虽然便于实施，但容易产生误报和漏报，且容易被绕过。
    - 其他。使用安全的编码函数、统一各数据层编码格式（如统一使用UTF-8等）、严格限制数据库用户权限、定期进行代码黑盒白盒扫描、避免将错误信息显示到页面等。
- **文件上传**
  - **名词解释**

    文件上传漏洞是指由于程序代码未对用户提交的文件进行严格的分析和检查，导致攻击者可以上传可执行的代码文件，从而获取Web应用的控制权限（Getshell）。
  - **常见发生位置**
    - 所有使用到上传功能的位置。
    - 用户可自定义的头像、背景图片等。
    - 富文本编辑器中的文件上传功能。

- **防御措施**
  - 上传目录设置为不可执行。
  - 严格判断文件类型，使用白名单而不是黑名单（注意大小写问题）。需要注意的是一些与Web Server相关的漏洞所造成的问题，如Apache、IIS、Nginx等的文件解析漏洞。
  - 使用随机数改写上传后的文件名和文件路径。
  - 单独设置文件服务器及域名。

- **权限漏洞**
  - **名词解释**

    访问控制是指用户对系统所有访问的权限控制，通常包括水平权限和垂直权限。访问控制问题是所有业务系统都可能产生的逻辑类漏洞，很难通过日常的安全工具扫描或防护，通常会造成大量用户数据泄露事件。

    - 水平越权：同一权限（角色）级别的用户之间所产生的问题，如A用户可以未授权访问B用户的数据等。
    - 垂直越权：不同权限（角色）级别的用户之间所产生的问题，如普通用户可未授权进行管理操作，未登录用户可以访问需授权应用等。

  - **常见发生位置**
    - 所有涉及到与用户相关数据的位置，如用户资料、地址、订单等。
    - 所有涉及到登录及权限控制的位置，如后台登录、当前用户权限校验等。

  - **防御措施**
    - 对于所有涉及到用户数据的操作，严格判断当前用户的身份。
    - 对于所有需要权限控制的位置，严格校验用户权限级别。

- **暴力破解**
  - **名词解释**

    暴力破解是指攻击者通过遍历或字典的方式，向目标发起大量请求，通过判断返回数据包的特征来找出正确的验证信息，从而绕过验证机制。随着互联网众多网站的数据库被泄露，攻击者选择的样本可以更具针对性，暴力破解的成功率也在不断上升。

  - **常见发生位置**
    - 用户登录处的账号密码暴力破解。
    - 人机验证机制容易绕过，如使用较易识别的验证码。
    - 找回密码或二次身份验证等可能用到的手机短信验证码。

  - **防御措施**
    - 强制使用强密码，并定期修改。
    - 限制密码错误尝试次数。
    - 使用强人机验证机制。
    - 限制一定时间内的高频访问次数。

- **拒绝服务攻击**
  - **名词解释**

    拒绝服务攻击（DoS，Denial of Service）是利用合理的请求造成资源过载，从而导致服务不可用的一种攻击方式。分为针对Web应用层的攻击、客户端/APP的攻击。

- **常见发生位置**
  - Web层常见于会大量消耗资源的位置，如查找功能等。
  - 客户端/APP常见于异常输入数据造成的程序崩溃。
- **防御措施**
  - 针对Web层DoS：
    - 限制每个客户端的请求频率。
    - 使用验证码过滤自动攻击者。
    - 做好应用代码的性能优化，网络架构优化等。
  - 针对客户端/APP拒绝服务攻击：
    - 删除不必要的组件。
    - 对用户输入数据进行过滤和检查。

- **敏感信息泄露**
  - **名词解释**

    敏感信息泄露是指包括用户信息、企业员工信息、内部资料等不应当被外部访问到的数据通过网站、接口、外部存储等途径被未授权泄露到外部的漏洞。信息泄露漏洞会导致大量用户或企业信息被恶意利用，进行诈骗、账户窃取等，给用户和企业带来严重的不良影响。并且信息一旦信息被泄露，影响会很难消除。
  - **常见发生位置**
    - 获取用户、企业信息等数据的网站或客户端接口。
    - 企业可访问到的外部存储，如网盘、邮箱等。
    - 其他一切可能泄露数据的途径。
  - **防御措施**
    - 对数据接口进行严格的权限检查和访问限制。
    - 划分企业安全边界，限制内部数据外流，如禁止访问外部存储应用等。
    - 提高员工数据安全意识。

- **业务逻辑漏洞**
  - **名词解释**

    业务逻辑漏洞是指由于业务在设计时考虑不全所产生的流程或逻辑上的漏洞，如用户找回密码缺陷，攻击者可重置任意用户密码；如短信炸弹漏洞，攻击者可无限制利用接口发送短信，恶意消耗企业短信资费，骚扰用户等。由于业务逻辑漏洞跟业务问题贴合紧密，常规的安全设备无法有效检测出，多数需要人工根据业务场景及特点进行分析检测。
  - **常见发生位置**

    所有涉及到用户交互的位置。
  - **防御措施**

    针对业务场景进行全面的检测。

- **安全配置缺陷**

- 安全配置缺陷包括：文件遍历、源码泄露、配置文件泄露等。
  - 文件遍历：可以浏览服务器Web目录下的文件列表，可能会泄露重要文件。
  - 源码泄露：可以查到的Web程序的源代码。
  - 配置文件泄露：Web服务器及程度代码的配置文件泄露等。
- **防御措施**

  检查所有可能存在安全配置问题的点，在满足业务需求的情况下，最大化安全配置。

Web客户端安全

- **跨站脚本攻击（XSS）**
  - **名词解释**

    跨站脚本攻击（XSS, Cross Site Script）通常指黑客通过“HTML注入”篡改了网页，插入恶意脚本，从而在用户浏览网页时，控制用户浏览器的一种攻击。XSS漏洞可被用于用户身份窃取（特别是管理员）、行为劫持、挂马、蠕虫、钓鱼等。XSS是目前客户端Web安全中最重要的漏洞。

    XSS按效果的不同可以分为以下3种。
    - 反射型XSS攻击：页面仅把用户输入直接回显在页面或源码中，需要诱使用户点击才能成功。
    - 存储型XSS攻击：XSS攻击代码会被存储在服务器中，由于用户可能会主动浏览被攻击页面，此种方法危害较大。
    - DOM型XSS攻击：通过修改页面的DOM节点形成XSS，严格来讲也可划为反射型XSS。
  - **常见发生位置**

    所有涉及到用户可控的输入输出点，如个人信息、文章、留言等。
  - **防御措施**
    - 对重要的Cookie字段使用HTTPOnly参数。
    - 检查所有用户可控输入。对所有的输入点进行严格的检查，过滤或拦截所有不符合当前语境的输入。由于无法预期所有可能的输出点语境，此种方法效果较差。
    - 检查所有用户输入的输出点。因为XSS最终攻击是发生在输出点，因此需要分析出用户输入数据的所有输出点的环境，是输入在HTML标签中，还是HTML属性、<script>标签、事件、CSS位置中，针对不同的输出位置，制定不同的转义或过滤规则。
    - 处理富文本。在文章、论坛等需要用到富文本的地方，需要特别注意富文本与XSS的区分，严格禁止所有的危险标签及“事件”，原则上应当使用白名单过滤标签、事件及属性。
- **跨站点请求伪造（CSRF）**
  - **名词解释**

    跨站点请求伪造（CSRF, Cross Site Request Forgery）。由于重要操作的所有参数都是可以被攻击者猜到，攻击者即可伪造请求，利用用户身份完成攻击操作，如发布文章、购买商品、转账、修改资料甚至密码等。
  - **常见发生位置**

    所有由用户（包括管理员）发起的操作点。

- **防御措施**
  - 辅助验证方法：使用验证码。验证码是对抗CSRF攻击最简单有效的方法，但会影响用户的使用体验，并且不是所有的操作都可以添加验证码防护。因此，验证码只能作为辅助验证方法。
  - 通用防护方法：添加足够随机的csrf_token并每次更新，以防止参数被猜解。使用CSRF_token是目前通用的防护方法。
  - 其他防御措施：验证HTTP Referer，拒绝不安全的来源。但服务器并非在任何情况下都能获取到Referer值。

> **说明** 建议结合上述三种方法进行防御。