先知计划

用户指南

用户指南

入驻条件

1、入驻企业必须为“企业实名认证”

2、公测期间需要通过审核才能开启,点击 **资格申请**

注：工单提交1个工作日内，有专人和您联系。

入驻流程

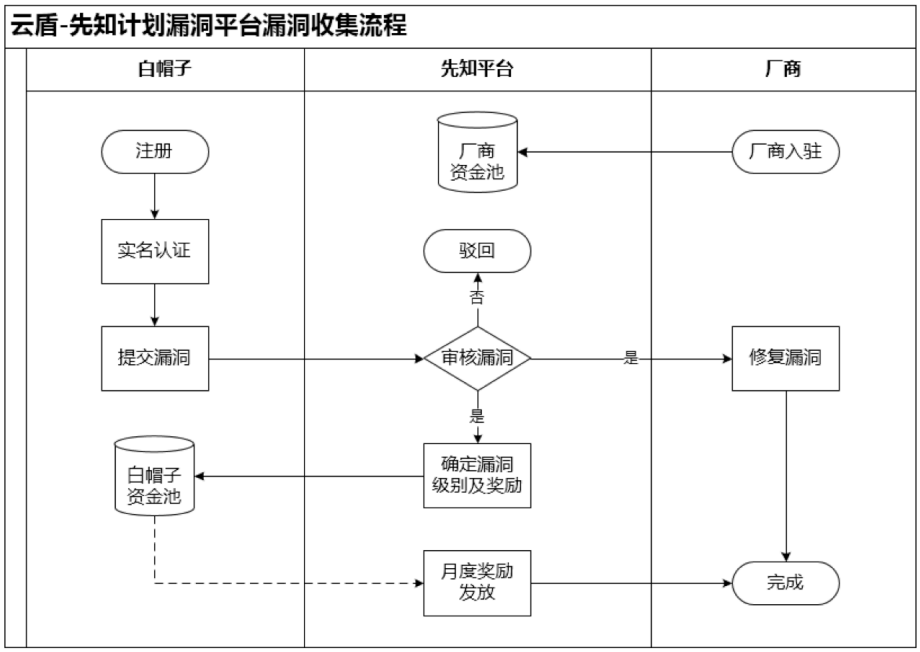
1、直接进入先知计划入驻页

2、缴纳1w-5w不等的奖励包，该奖励包将直接换算为奖励基金最终提供给白帽子。

3、付款成功后，进入云盾控制台-先知计划，填写对外展示企业资料（logo、名称等）、制定奖励计划（高、中、低危漏洞分别奖励的金额）。

4、入驻成功，等待白帽子提交漏洞。

漏洞收集流程图



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。【状态：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。

1) 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】

2) 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】

3) 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在平台上的账户内，白帽子可以直接申请提取现金或等待若干漏洞奖励一起申请提现。【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】

我们将在每月的固定时间统一处理上月度所有提现申请，详情可查看每月的奖励公告。

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。【状态：已修复】

1、提交需求

您完成付款后，可直接登录云盾控制台—专家服务-先知计划，提交企业名称和奖励计划

2、等待白帽子提交漏洞

设置奖励计划后，先知网站会同步更新企业状态，并开始对外收集漏洞。等待白帽子提交漏洞

3、查看漏洞并修复

白帽子提交漏洞后，客户在云盾控制台-先知计划处，可以同步看到白帽子提交的漏洞并去执行修复

等级保护测评是指测评机构依据国家信息安全等级保护制度规定，按照有关管理规范和技术标准对未涉及国家秘密的信息系统安全保护状况进行分等级测试评估的活动。

为规范等级保护测评项目收费，建立公平、公正、有序、竞争的测评市场环境，按照《信息安全测评联盟自律公约》要求，特制定本文件。

本文件所指信息系统是通用信息系统。

一、费用公式

F = A × B

费用（ F ）取自于收费基数（ A ）和调节因子（ B ），费用（ F ）四舍五入到千为单位。

二、收费基数

按照信息安全等级保护测评工作要求，充分体现渗透测试、风险评估、定量分析等工作的技术价值，同时考虑三级和四级系统的测评广度和深度的逐级增强，取值相应增加，制定信息系统等级测评的指导性收费基数（四舍五入到万）：

收费基数（A）=测评指标项数量*单项收费标准

各省收费基数（A）计算表各不一致，可以参考《各省市自治区等级测评项目收费基数（A）计算表》。

等级测评机构异地开展等级测评活动，原则上按被测评信息系统（非跨区域）所在地确定的收费基数进行收费计算。

三、调节因子

设定一个调节因子（B），调节内容主要考虑影响测评工作量较大的几个要素，包括系统规模（B1）、多系统测评（B2）、重复测评（B3）：

B=B1×B2×B3

1、系统规模（B1），以信息系统所包含的全部实际系统组件为依据，调节因子的选择主要体现在承载业务应用和数据的服务器主机设备数量上，对采用虚拟化服务器技术的，以虚拟主机台数为依据；对于承担安全运维管理等服务器（如防病毒服务器、审计服务器等）不作为B1的取值依据。

B1的取值，根据服务器主机台数按如下分段取值：

1) 5台以下：B1=0.8～0.9；

2) 6～19台：B1=0.9～1.0；

3) 20～49台：B1=1.0～1.2；

4) 50～100台：B1=1.2～1.5；

5) 100～200台：B1=1.5～2；

6) 200台以上：B1≥2。

主机服务器台数可以从信息系统定级报告和备案表获得，且要求在报价前获知，比如：可以要求在招标文件技术需求中明确。

针对纯网络系统B1取值：二级B1=0.8，三级B1=0.9，四级B1=1。

2、多系统测评(B2)，本调节因子适用于同一单位多个相同等级或不同等级信息系统同时测评的情况。

B2的取值，根据同时测评的信息系统数量按以下分段取值：

1) 2-5个系统同时测评的信息系统：B2≥0.9；

2) 6-10 个系统同时测评的信息系统：B2≥0.8；

3) 11-50个系统同时测评的信息系统：B2≥0.7；

4） 51-100个系统同时测评的信息系统：B2≥0.5；

5） 100个以上系统同时测评的信息系统：B2≥0.3。

3、重复测评（B3），由同一家测评机构对未做重大变更的同一信息系统进行再次测评时测评工作量相对减少，测评费用相应减少。

B3的取值：≥0.8。

重复测评以同一测评机构首次测评费用为基准。

各机构根据测评系统的实际情况综合考虑以上三个因素选取计算调节因子取值。 调节因子取值原则：系统规模（B1）、多系统测评（B2）、重复测评（B3）的取值不得低于各要素分段取值的下限值。

VPN接入教程

先知平台上部分项目要求必须通过VPN来进行测试，当厂商页面中出现如下提示框时：

表示厂商要求必须通过专用VPN来进行测试，否则无法通过审核。

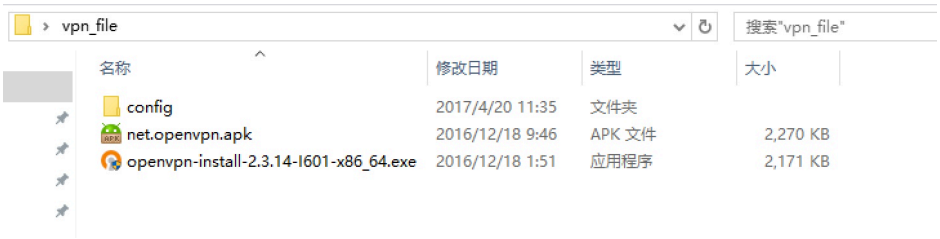
Mac下用OpenVPN可能会出现DNS问题，无法解析域名，如无法解决，建议：

1. 尝试对测试目标直接通过IP访问
2. 使用Windows虚拟机进行测试

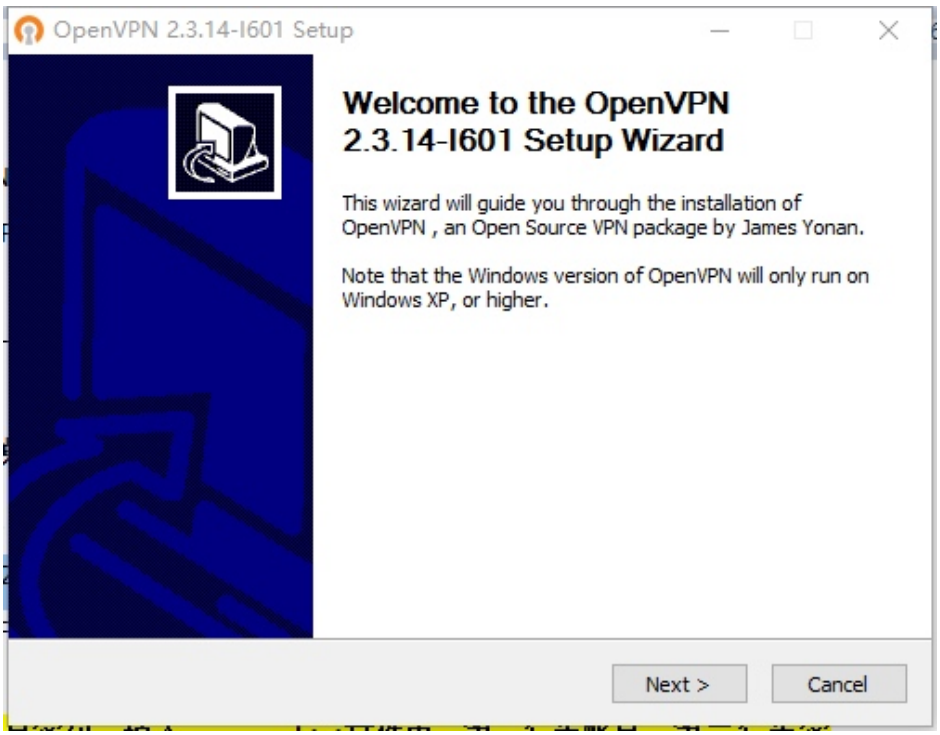
vpn_file.zip

Windows接入教程

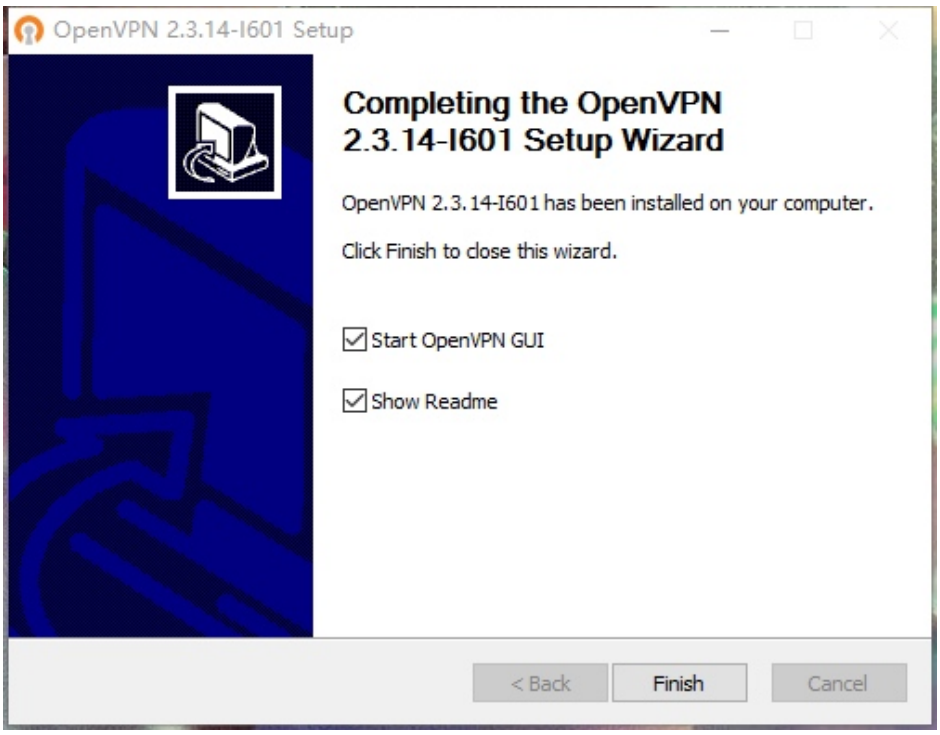
解压下载的vpn程序压缩包，得到如下文件：



运行 openvpn-install-2.3.14-I601-x86_64.exe，如图



安装完成后，直接打开



将分配的账号密码，填入password.txt文件中，第一行为帐号，第二行为密码

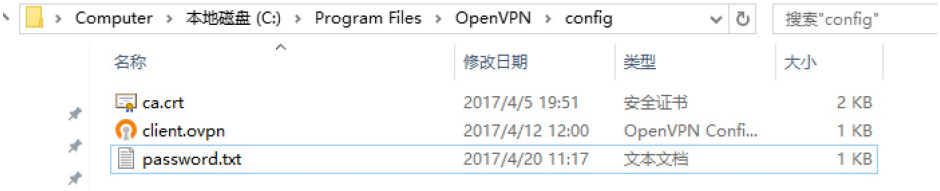
修改 client.ovpn 文件中，在 remote 后面添加VPN服务器的IP和端口，如 remote 1.1.1.1 1194：

```
client
dev tun
proto udp
##############################################
# The hostname/IP and port of the server.#
# You can have multiple remote entries   #
# to load balance between the servers.   #
##############################################
remote
##############################################
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
ns-cert-type server
comp-lzo
verb 3
auth-user-pass password.txt
```

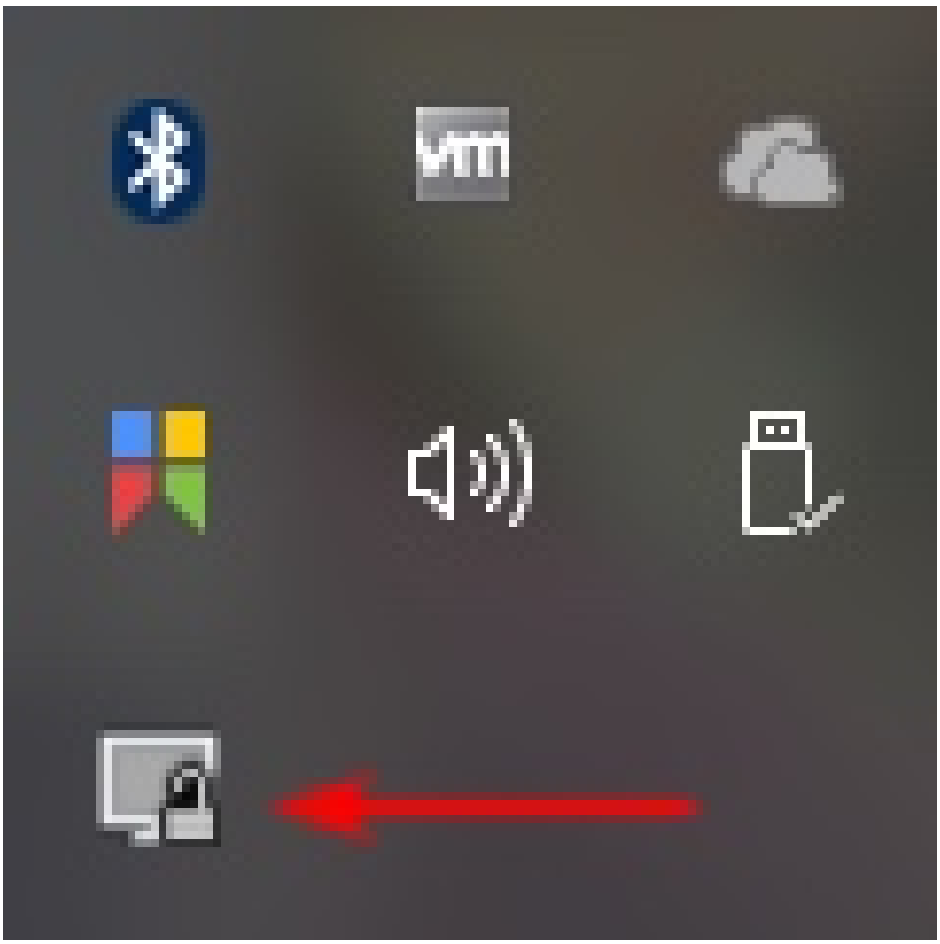
安装ca.crt，信任其为根证书，手机和电脑都需要手工导入此证书

之后顺利安装根证书。

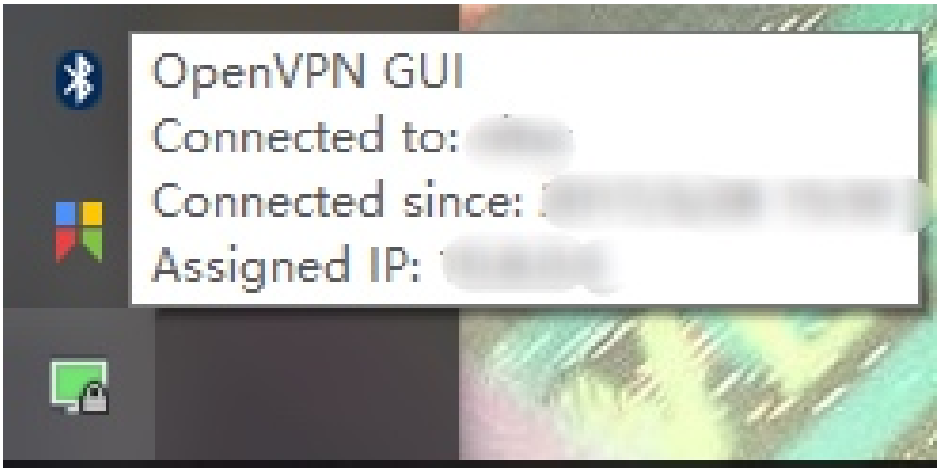
电脑上把配置ca.crt、client.ovpn、password.txt放在c:\Program Files\OpenVPN\config文件夹中



启动openvpn后，双击菜单栏右下角图标



之后连接成功：



漏洞说明

根据漏洞的危害程度将漏洞等级分为【高】、【中】、【低】三个等级。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，每种等级包含的评分标准及漏洞类型如下：

【高危】

基础分60-100，本等级包括：

1、直接获取系统权限的漏洞（服务器权限、PC客户端权限）。包括但不仅限于远程命令执行、任意代码执行、上传获取Webshell、SQL注入获取系统权限、缓冲区溢出（包括可利用的ActiveX缓冲区溢出）。

2、直接导致重要业务拒绝服务的漏洞。包括但不仅限于直接导致移动网关业务API业务拒绝服务、网站应用拒绝服务等造成严重影响的远程拒绝服务漏洞。

3、重要的敏感信息泄漏。包括但不仅限于重要业务DB 的 SQL 注入、可获取大量企业核心业务数据等接口问题引起的敏感信息泄露。

4、严重的逻辑设计缺陷和流程缺陷。包括但不仅限于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。

5、敏感信息越权访问。包括但不仅限于绕过认证直接访问管理后台、重要后台弱密码、获取大量内网敏感信息的SSRF等。

6、企业重要业务越权敏感操作。包括但不仅限于账号越权修改重要信息、重要业务配置修改等较为重要的越权行为。

7、大范围影响用户的其他漏洞。包括但不仅限于可造成自动传播的重要页面的存储型XSS（包括存储型DOM-XSS）。

【中危】

基础分30-50，本等级包括：

1、需交互方可影响用户的漏洞。包括但不仅限于一般页面的存储型XSS，涉及核心业务的CSRF等。

2、普通越权操作。包括但不仅限于包括但不限于绕过限制修改用户资料、执行用户操作等。

3、普通的逻辑设计缺陷和流程缺陷。包括但不仅限于不限次数短信发送、任意手机邮箱信息注册用户等。

【低危】

基础分10-20，奖励系数可为0，本等级包括：

1、本地拒绝服务漏洞。包括但不仅限于客户端本地拒绝服务（解析文件格式、网络协议产生的崩溃），由Android组件权限暴露、普通应用权限引起的问题等。

2、普通信息泄漏。包括但不仅限于客户端明文存储密码、以及web路径遍历、系统路径遍历等。

3、其他危害较低的漏洞。包括但不仅限于反射型 XSS（包括反射型 DOM-XSS）、普通CSRF、URL跳转漏洞

等。

1.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：

1）URL参数提交，主要为GET请求参数；

2）表单提交，主要是POST请求，也包括GET请求；

3）Cookie参数提交；

4）HTTP请求头部的一些可修改的值，比如Referer、User_Agent等；

5）一些边缘的输入点，比如.mp3、图片文件的一些文件信息等。

防御措施：

1）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；

2）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；

3）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；

4）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。

2.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：

1）所有使用到上传功能的位置；

2）用户可自定义的头像、背景图片等；

3）富文本编辑器中的文件上传功能。

防御措施：

1）上传目录设置为不可执行；

2）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；

3）使用随机数改写上传后的文件名和文件路径；

4）单独设置文件服务器及域名。

3.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：

1）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；

2）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：

1）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；

2）对于所有需要权限控制的位置，严格校验用户权限级别。

4.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： 1）用户登录处的账号密码暴力破解； 2）人机验证机制容易绕过，如使用较易识别的验证码； 3）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： 1）强制使用强密码，并定期修改； 2）限制密码错误尝试次数； 3）使用强人机验证机制； 4）限制一定时间内的高频访问次数。

5.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：

1) Web层常见于会大量消耗资源的位置，如查找功能等；

2) 客户端/APP常见于异常输入数据造成的程度崩溃。

防御措施：

针对Web层DoS：

1) 限制每个客户端的请求频率；

2) 使用验证码过滤自动攻击者；

3) 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：

1) 删除不必要的组件；

2) 对用户输入数据进行过滤和检查。

6.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：

1) 获取用户、企业信息等数据的网站或客户端接口；

2) 企业可访问到的外部存储，如网盘、邮箱等；

3) 其他一切可能泄露数据的途径。

防御措施： 1) 对数据接口进行严格的权限检查和访问限制；

2) 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；

3) 提高员工数据安全意识。

7.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。

8.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：

1）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

1.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3种：

a. 反射XSS：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；

b. 存储XSS：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；

c. DOM XSS：通过修改页面的DOM节点形成XSS，严格来讲也可划为反馈型XSS。

常见发生位置：

1）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：

1）对重要的Cookie字段使用HTTPOnly参数；

2）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；

3）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；

4）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。

2.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：

1）所有由用户（包括管理员）发起的操作处。

防御措施：

1）使用验证码。验证码是对抗CSRF攻击最简洁有效的方法，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；

2）添加足够随机的csrf_token并每次更新，以防止参数被猜解到。使用CSRF_token是目前通用的防护方法；

3）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；

4）建议配合使用上述方法。

1、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。

2、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。

3、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等。

4、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。

5、同一漏洞，首位报告者计贡献值，其他报告者均不计。

6、在漏洞未修复之前，被公开的漏洞不计分。

7、报告网上已公开的漏洞不计贡献值。

8、同一份报告中提交多个漏洞，只按危害级别最高的漏洞计贡献值。

9、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。

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。

欢迎加入先知公益计划！

先知和白帽子们的公益成就

2016年10月，先知正式开启了公益众测计划。先知公益的形式目前有以下两种：

- 一种是公益机构在先知平台发布安全测试需求，平台白帽子为他们输出安全能力，免费为其网站进行“安全体检”，保护这些公益机构背后保护的人。
- 另一种是在平台上开放公益众测项目，提供安全测试的企业和白帽子可以自愿捐出部分或全部漏洞奖金，奖金将累计到先知公益基金池里，用于助学和推动贫困地区的技术发展。

至今，已有近30名白帽子参与到先知公益计划当中，累计的先知公益基金超过100万。先知已于2017年3月份已将第一笔善款（45万人民币）捐赠给了中国扶贫基金会，通过“爱心包裹”项目资助山区孩子购买学习用品。

对于白帽子们的善举，先知也设计了完善的公益积分体系来进行奖励，首次公开如下：

公益等级	要求	福利
初出茅庐	公益积分达 500 及以上（根据漏洞等级进行积分，若参与公益捐献，30 元=1 公益积分）	先知官网展示称号
公益新秀	公益积分达 2000 及以上	先知官网展示称号
		提供陌陌安全工程师（后续会加更多公司）优先面试机会
		2000 元白帽技术学习基金
公益大侠	公益积分达 6000 及以上	公益机构颁发公益证书
		先知官网、阿里内网展示称号
		实地考查公益项目，和资助的孩子互动（自费）
		提供阿里云用人主管晚餐会、陌陌安全直通终面机会
		先知白帽大会、创新大会终身免票
		有机会参与白帽基金会日常运营和管理
		5000 元白帽技术学习基金
名震江湖	公益积分达 10000 及以上	先知、阿里公益、外部公益机构联合颁发公益证书（线上+线下）
		先知官网、阿里内网展示称号
		实地考查公益项目，和资助的孩子互动（活动费用由阿里或者白帽基金支出）
		提供阿里云用人主管晚餐会、陌陌安全直通终面机会
		先知白帽大会、创新大会终身免票
		有机会参与白帽基金会日常运营和管理
		全球顶尖安全会议（如 Blackhat、RSA）包来回机票及门票、住宿报销
		8000 元白帽技术学习基金

2017年3月24日，在先知白帽大会上，先知平台和中国扶贫基金会、阿里集团公益一起向公益积分排名前10名的爱心白帽子们颁发了公益证书，邀请了在公益众测中表现活跃的白帽子——木雁与千霄上台共同完成了阿里云先知公益基金的第一次捐款仪式。对自己利用业余时间完成的公益成就，两位白帽子激动而又自豪。

通过公益众测，先知平台希望借白帽子们的力量帮助到那些缺乏安全技术能力的公益机构和需要扶助的弱势群体。同时也帮助白帽子们在公益活动中提升技术、获得社会的认同感和荣誉背书。

我们需要您的共同参与

- 对于有安全测试需求的公共机构部门和公益机构，欢迎联系先知公益平台发布你们的安全测试项目需求。
- 欢迎那些愿意与先知一起，用技术力量去支持公益事业、温暖社会的白帽子们报名参与先知公益计划，你的一小步可能会改变很多人一生的命运。

参与形式

- 有安全测试需求的公共机构部门和公益机构，通过下面的链接，填写一份申请问卷，通过审核后，我们会联系您进行需求发布。「问卷链接」
- 愿意与我们一起做公益的白帽子们，可以发送邮件到 Aliyun_xianzhi@service.alibaba.com 申请，标题为《先知公益众测白帽子申请》，邮件中请包含先知登陆账号和昵称ID。