## 外部API接口

### 1.1.1.概述

|  |  |
| --- | --- |
| 用途 | 用于对接观星台等外部应用 |
| 功能 | 发起漏洞验证任务、获取漏洞验证结果 |
| 操作步骤 | 1. 通过获取凭证接口获得access\_token；  2. 使用access\_token调用下发验证任务、获取验证结果、反馈验证结果意见等接口。 |

### 1.1.2.获取凭证

请求说明：

|  |  |
| --- | --- |
| URL | /accessToken |
| 请求方式 | POST |
| 请求正文 | {  "appId":"APPID", // API Key  "secretKey":"SECRET", // API 认证秘钥  } |
| 响应正文 | {  "status": 0,  "accessToken":"ACCESS\_TOKEN",  "expiresIn":7200  } |
| 用途 | 用于获取调用接口的凭证。 |

请求参数说明：

|  |  |  |
| --- | --- | --- |
| 参数 | 是否必填 | 说明 |
| appId | 是 | 客户唯一标识，以此识别是哪个客户发起的验证请求 |
| secretKey | 是 | 调用验证接口的认证秘钥，由平台开分配，可多个客户绑定一个秘钥，也可以一个客户一个秘钥 |

响应参数说明：

|  |  |
| --- | --- |
| 参数 | 说明 |
| status | API接口的响应状态，常见状态值如下：  0 - 成功  1 - 失败，此时响应中会出现错误代码（errcode）和错误消息（errmsg）两个参数，调用方啊可以记录错误值，展示错误消息 |
| accessToken | 接口调用凭证 |
| expiresIn | 凭证有效时长，单位为分钟 |

错误消息定义：

|  |  |
| --- | --- |
| 错误代码 | 错误消息 |
| 1001 | accessToken 已失效 |
| 1002 | 获取凭证失败 |
| 1003 | 参数错误 |
| 1004 | 新增任务失败 |
| 1005 | 获取任务详情失败 |
| 1006 | 没有操作此数据的权限 |
| 1007 | 数据状态错误 |
| 2003 | 添加任务：目标错误 |
| 2005 | 添加任务：HTTP头格式错误 |
| 2004 | 添加任务 ：无效 http方法 |
| 2006 | 添加任务 ： cookie 格式错误 |
| 2007 | 添加任务 ：弱口令错误 |
| 2008 | 添加任务：漏洞参数错误 |
| 3000 | 系统错误 |

### 1.1.3.发起验证任务

请求说明：

|  |  |
| --- | --- |
| URL | /addTask |
| 请求方式 | POST |
| 请求正文 | {  "accessToken":"ACCESS\_TOKEN",  "data":{  "dsoId": "DSO-00001",  "target":"http://192.168.1.1/test.jsp?id=5",  "method":"1",  "param":"type",  "header":"header1: value1\nheader2: value2",  "cookie":"cookie1=value1; cookie2=value2;",  "body":"type=aaa&count=0",  "weakPassword":"name:password"  }  } |
| 响应正文 | {  "status": 0,  "taskId":"1"  } |
| 用途 | 通过接口发起漏洞验证任务。 |

请求参数说明：

|  |  |  |
| --- | --- | --- |
| 参数 | 是否必填 | 说明 |
| data/dsoId | 是 | 指定要验证的漏洞的编号  数据库中存在 |
| data/target | 是 | 指定漏洞所在的URL或IP:PORT  不能为空 |
| data/method | 否 | HTTP请求的方法，非HTTP(S)漏洞可留空  GET(1),  HEAD(2),  POST(3),  PUT(4),  PATCH(5),  DELETE(6),  OPTIONS(7),  TRACE(8); |
| data/issueParam | 否 | 存在漏洞的参数，可以是HTTP请求的参数或target、headers、cookies、body中的占位符  校验规则：长度不能超过255 |
| data/header | 否 | 纯文本的HTTP请求的头信息，格式为：  header1: value1\nheader2: value2  校验规则：校验格式（同上格式），名称不能包含中文 |
| data/cookie | 否 | 纯文本的HTTP请求的Cookie信息，格式为：  cookie1=value1; cookie2=value2;  校验格式,名称不能为空 |
| data/body | 否 | 纯文本的请求体信息，请求体支持多种格式，例如：  application/x-www-form-urlencoded  multipart/form-data  application/json  application/xml  不做校验 |
| data/weakPassword | 否 | 弱口令漏洞时必填，格式为“用户名:密码”，  只校验格式，长度不能超过255 |

响应参数说明：

|  |  |
| --- | --- |
| 参数 | 说明 |
| status | 参见“获取凭证”接口相同参数的说明 |
| data/taskId | 任务编号,调用方根据这个编号获取任务的结果、状态 |

### 1.1.4.获取验证结果

请求说明：

|  |  |
| --- | --- |
| URL | /getTask |
| 请求方式 | POST |
| 请求正文 | {  "accessToken":"ACCESS\_TOKEN",  "taskId":"31afd-452s3-4avta-24rfa-af3fa"  } |
| 响应正文 | {  "status": 0,  "data":{  “isIssue”:1,  "status":1,  "payload":"\"><script>alert(123)</script>",  "outputs":[  "<html>... ...</html>"  ],  "snapshots":[  "iVBORw0KGgoAAAAN...=="  ],  "solution":{  "env":"应用场景名称",  "steps":[  {  "title":"存文本标题",  "content":"这里是Markdown文本",  "attachments":[  "http://x.x.x.x/upload/ssss.zip"  ]  },  ... ...  ]  },  "author":"花名"  }  } |
| 用途 | 获取漏洞验证结果 |

请求参数说明：

|  |  |  |
| --- | --- | --- |
| 参数 | 是否必填 | 说明 |
| taskid | 是 | 指定验证任务的标识 |

响应参数说明：

|  |  |
| --- | --- |
| 参数 | 说明 |
| status | 参见“获取凭证”接口相同参数的说明 |
| data/isIssue | 0待定 1有漏洞 2没有漏洞 |
| data/status | 1 :"未开始" , 2 : "进行中" , 3 : "待审核" ,  4:"已领取", 5 : "审核完成",6: "待补充修复方案"),  7:"取消",  8: "完成" ; |
| data/payload | 验证成功时的测试Payload，只有存在漏洞时才会有，否则为空字符串。 |
| data/outputs | 验证时收集的输出信息列表，通常为命令行工具的输入信息。 |
| data/snapshots | 验证收集的漏洞触发图形界面显示，通常为浏览器或系统桌面的输出信息。 |
| data/solution | 漏洞修复方案 |
| data/solution/env | 环境名 |
| data/solution/steps | 漏洞修复方案步骤列表 |
| data/solution/steps/title | 漏洞修复方案步骤标题 |
| data/solution/steps/content | 漏洞修复方案步骤详细描述，适用Markdown格式 |
| data/solution/steps/attachments | 漏洞修复方案步骤包含的附件列表 |
| data/author | 审核漏洞的运营用户花名 |

### 1.1.5.提交验证结果反馈

客户能够对平台提供的验证结果和修复方案给与评价，以帮助平台改善验证体验、完善修复方案。同时这些数据最终会反馈到任务、运营人员、修复方案、修复方案步骤上面，作为指导运营人员做出选择的依据，也可作为公司考核运营人员技术能力的依据。

请求说明：

|  |  |
| --- | --- |
| URL | /feebackTask |
| 请求方式 | POST |
| 请求正文 | {  "access\_token":"ACCESS\_TOKEN",  "data":{  "taskid":"31afd-452s3-4avta-24rfa-af3fa",  "verify":1,  "verify\_note": "",  "solution":1,  "solution\_note": ""  }  } |
| 响应正文 | {  "status": 0  } |

请求参数说明：

|  |  |  |
| --- | --- | --- |
| 参数 | 是否必填 | 说明 |
| data/verify | 是 | 指定漏洞验证的结果是否准确：  1 - 准确，2 - 不准确 |
| data/verify\_note | 否 | 客户/工程师反馈的验证结果不准确的说明 |
| data/solution | 是 | 指定平台提供的修复方案是否准确：  1 - 适用，2 - 不适用 |
| data/solution\_note | 否 | 客户/工程师反馈的修复建议不适用的说明 |

响应参数说明：

|  |  |
| --- | --- |
| 参数 | 说明 |
| status | 参见“获取凭证”接口相同参数的说明 |