

360POC++

POC 提交使用说明

应用信息字段说明

提交POC漏洞活动公告漏洞兑换排行榜推荐平台关于

欢迎你, 用户110+

提交漏洞

漏洞名称

漏洞类型

0day

匿名

专题

漏洞等级

搜索规则

搜索规则

CNVD编号

CNVD-0000-00000,CNVD-0000-00001

CVE编号

CVE-0000-00000,CVE-0000-0001

CNNVD编号

CNNVD-000000-00000,CNNVD-000000-0001

bugtraq编号

bugtraq编号

漏洞发现者

漏洞来源

发现时间

请选择日期

厂商

应用

版本

版本

去提交

漏洞简介

修复方案

B I U O M H H H E X X' E E T Normal A Sans Serif

漏洞详情

参考链接

POC脚本

```
#!/usr/bin/perl
# coding: utf-8
from pocsuite.api.request import req
from pocsuite.api.poc import reqinfo
from pocsuite.api.poc import Output, POCBase

class TestPOC(POCBase):
    valid = ''
    cveid = ''
    version = ''
    author = ''
    validdate = ''
    createdate = '2019-03-28'
    updatedate = '2019-03-28'

POC格式基于python 2.7的Pocsuite格式 (目前只支持Python脚本的POC, 不支持JSON脚本的POC), 详情请参考: https://github.com/knowsec/Pocsuite
```

测试URL

请输入上述上可测试的目标列表 (每行一个), 目标可以是地址、地址端口或URL, 例如:
192.168.10.100
192.168.10.100:22
http://www.192.168.10.100/test/

镜像路径

Docker上的镜像路径, 例如: thinkphp:5.6.29

应用类型

应用端口

测试说明

验证码

4k

未登录的漏洞不允许提交 去提交

漏洞名称 {必填项}

名称填写规则: 厂商简称 应用名 漏洞文件或路径 存在 XXX 漏洞
例如: 厂商简称 xxx 系统 x.php 存在 SQL 注入漏洞

漏洞分类 {必填项}

SQL 注入 命令执行 代码执行 远程文件包含 本地文件包含 目录遍历等

0day {选填项}

是否 0day, 是的话勾选即可

匿名 {选填项}

是否匿名提交漏洞, 是的话勾选即可

漏洞等级 {必填项}

低危 例如: 目录遍历, 信息泄露等

中危 例如: 默认账号密码漏洞, 敏感信息泄露, SSRF 等

高危 例如: 命令执行, 代码执行, SQL 注入等

严重 例如: 热门的应用存在命令执行, 代码执行可评级为严重.

暂不收录 例如: CSRF, XSS, 无重要信息的信息泄露等

搜索规则 {选填项}

填写应用的搜索规则, 可以通过这个规则搜索到这个资产

例如: fofa:title="xxx 系统"

CNVD 编号 CVE 编号 CNNVD 编号 bugtraq 编号 {选填项}

以上编号能找到的话, 填写到指定编号对应的位置

漏洞发现者 {必填项}

填写漏洞的发现者, 如果不知道漏洞的发现者, 留空即可

来源 {选填项}

填写漏洞的来源链接

发现时间 {选填项}

填写漏洞的发现时间, 如果不知道时间, 写当前时间即可

厂商 {必填项}

应用官网的全称

例如: 三六零数字安全科技集团有限公司

应用 {必填项}

应用名字就是该应用的指纹名字

例如: 360 云探安全监测系统

版本 {必填项}

该漏洞影响应用的版本, 如果影响所有版本的话填 all 即可

漏洞简介 {必填项}

填写漏洞的描述

修复方案 {必填项}

填写漏洞的修复方案

漏洞详情 {选填项}

填写漏洞的详细信息

参考链接 {选填项}

填写漏洞的参考链接

POC 脚本 {必填项}

填写基于 Python 2.7 的 Pocsuite 格式的 POC 脚本

测试 URL

填写线上可供测试的网站, 每行一个, 目标可以是地址、地址:端口或 URL

例如:

192.168.10.100

192.168.10.100:22

http://www.192.168.10.100/test/

镜像路径 应用类型 应用类型 {选填项}

暂时留空即可

测试说明 {选填项}

填写本地测试成功的截图, 或者想对审核人员说的注意事项等

查重按钮 提交按钮

填写完漏洞信息点击查重, 如果没重复的话, 可以继续填写其他信息并提交

完整的漏洞及 POC 填写信息样例如下

