

[New issue](#)[Jump to bottom](#)

## Strict SQL filtering leads to xss injection vulnerability #17

[Closed](#) plr47 opened this issue on Feb 25, 2020 · 1 comment

Labels

bug

plr47 commented on Feb 25, 2020

### description

The code problem occurred in 03 / admin-tools / cal\_scores.php . The \$ realname in the output form was obtained from the database. There was no filtering of angle brackets "<>" during registration, which caused the reorganization here. xss injection

```
76         $avg_score = round( $val: $solved_score*0.4+$dif_score*0.2+$act_score*0.2+$idp_score*0.2);
77         /* 计算图表相关信息 end */
78         if($first){
79             $first=0;
80             echo "<td>".$user."</td><td>".$class."</td><td>".$real_name."</td><td>".$stu_id."</td>";
81         }
82         echo "<td>".$total_ac."</td><td>".$solved_score."</td><td>".$dif_score."</td><td>".$act_score."</td><td>".$idp_score."</td><td>".$avg_score."</td>";
83     }
84     echo "</tr>";
85 }
86 // check user
87 echo "</table>";
88 }
89 <?>
```

### Attack process

First register an account on the /03/modifypage.php page,Class is "软工163", Real Name is  
<details open ontoggle=['yds\_is\_so\_'].find(\u0070rompt)>

The screenshot shows the HZNUOJ website's registration page. The form fields are filled as follows:

- User ID: ydswa
- Password: (masked with dots)
- Repeat Password: (masked with dots)
- Nick Name: 100 characters at most
- School: Your school
- Class: 软工162
- Student ID: Your student ID
- Real Name: <details open ontoggle=['yds\_is\_so\_'].find(\u0070rompt)>
- Email: test1@qq.com

The "Register" button is visible at the bottom of the form.

Then visit / 03 / admin-tools / cal\_scores.php , set the classList to soft 软工163, and click submit

← → ↻ ⚠ 不安全

应用 面试 CTF学习资料 514 tool SRC 渗透工具 service CROW io tmp python

classList:

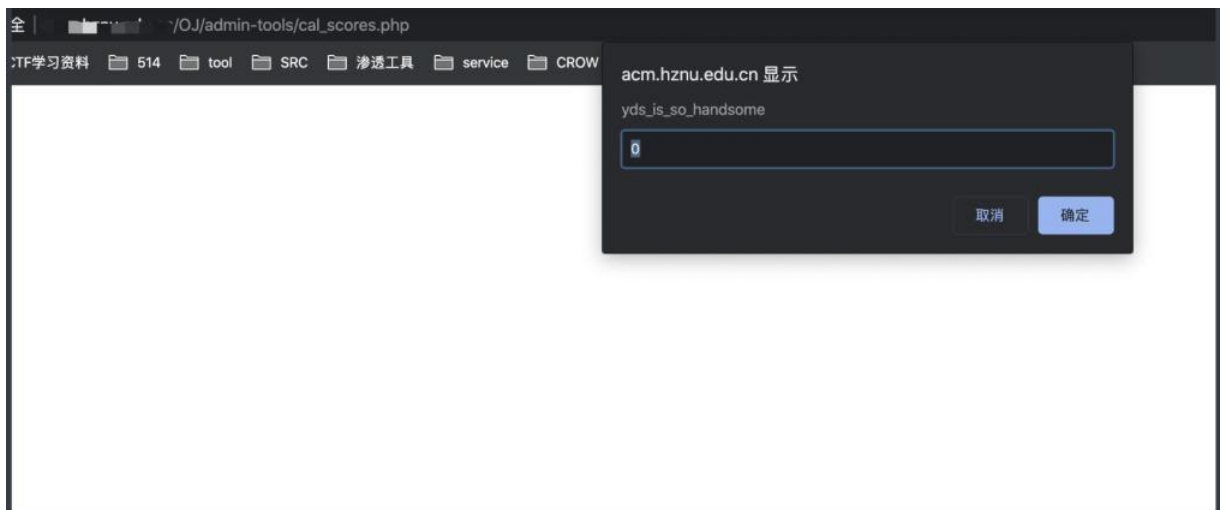
软工163

timeList:

2015-12-20 00:00:00  
2015-12-13 00:00:00  
2015-12-6 00:00:00

submit

the attack works



### poc

```
<details open ontoggle=['yds_is_so_handsome'].find(\u0070rompt)>
```

lixin-wei added the `bug` label on Feb 25, 2020

lixin-wei commented on Mar 15, 2020 • edited

Owner

hi @plr47 I've fixed it in commit [51a18c5](#)

thanks.

lixin-wei closed this as completed on Mar 15, 2020

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

