New issue

Jump to bottom

Strict SQL filtering leads to xss injection vulnerability #17

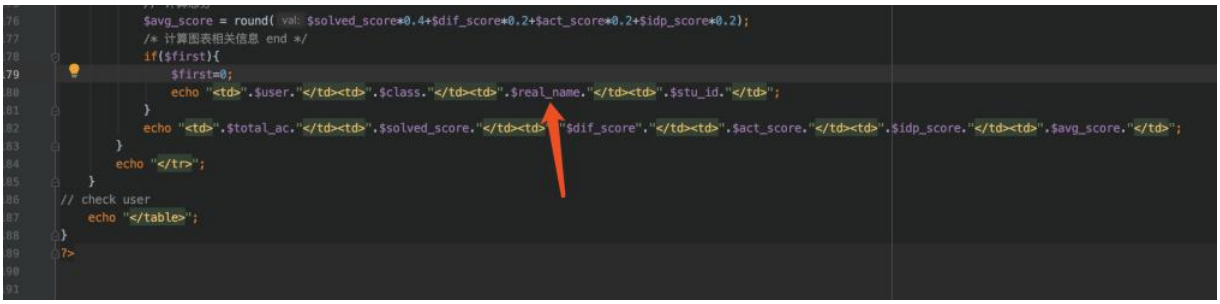
Closed plr47 opened this issue on Feb 25, 2020 · 1 comment

Labels bug

plr47 commented on Feb 25, 2020

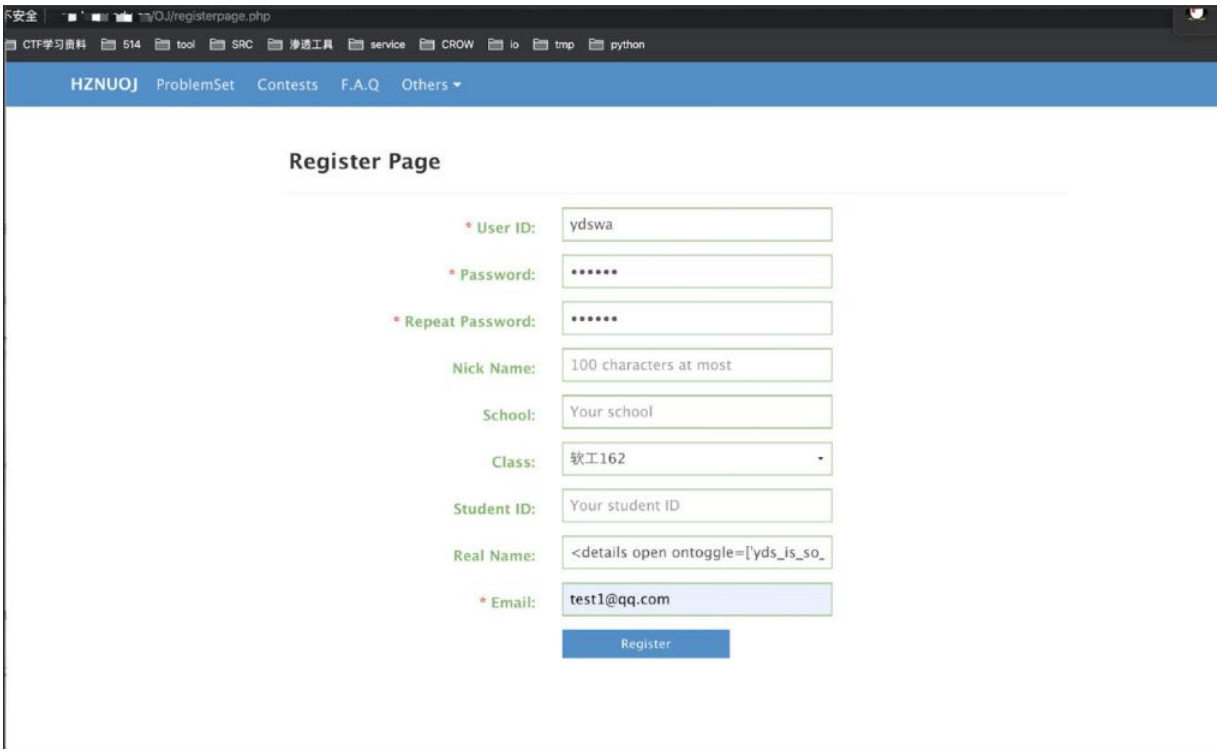
description

The code problem occurred in `OJ / 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

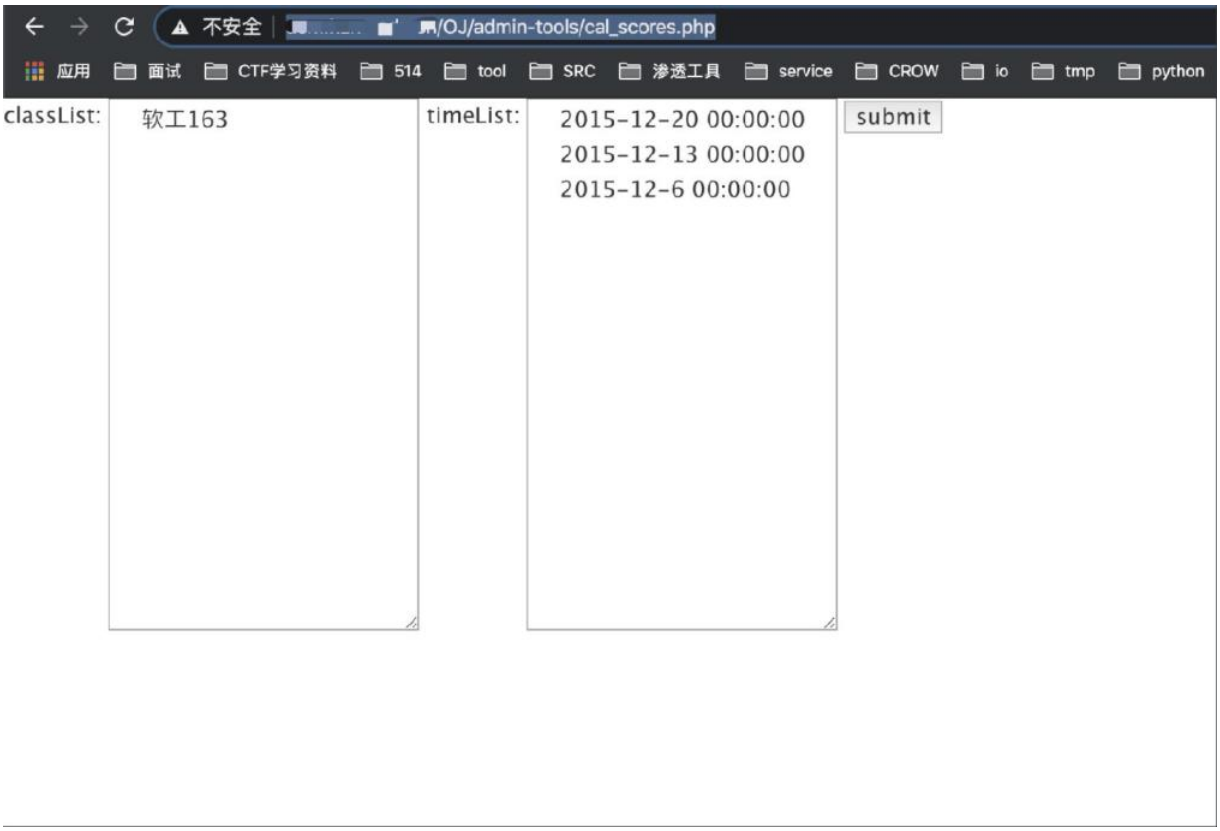


Attack process

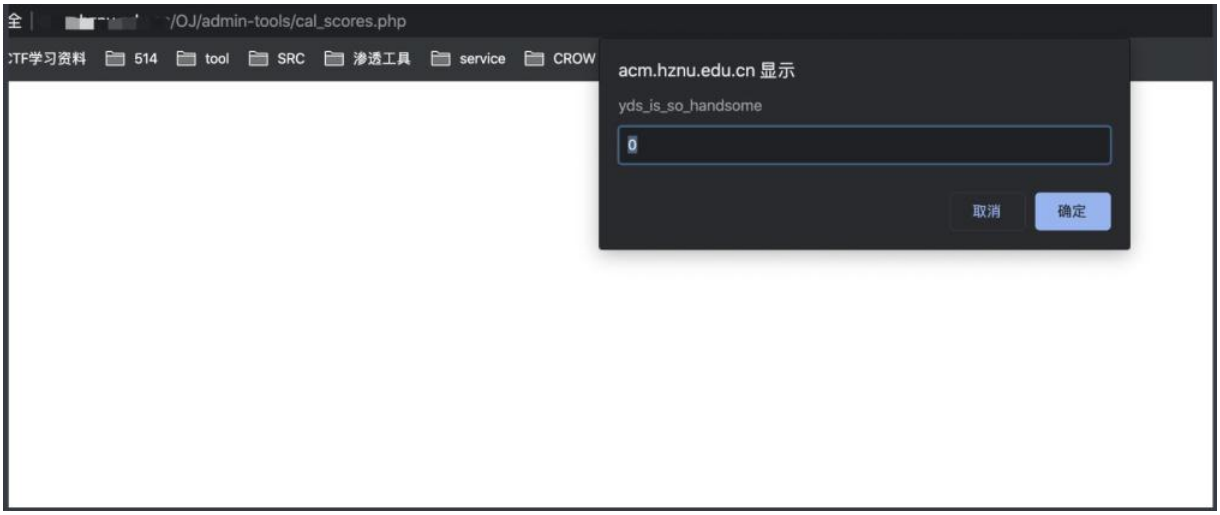
First register an account on the /OJ/modifypage.php page,Class is "软工163", Real Name is
<details open ontoggle=['yds_is_so_handsome'].find(\u0070rompt)>



Then visit `/ OJ / admin-tools / cal_scores.php` , set the classList to soft 软工163, and click 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