

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

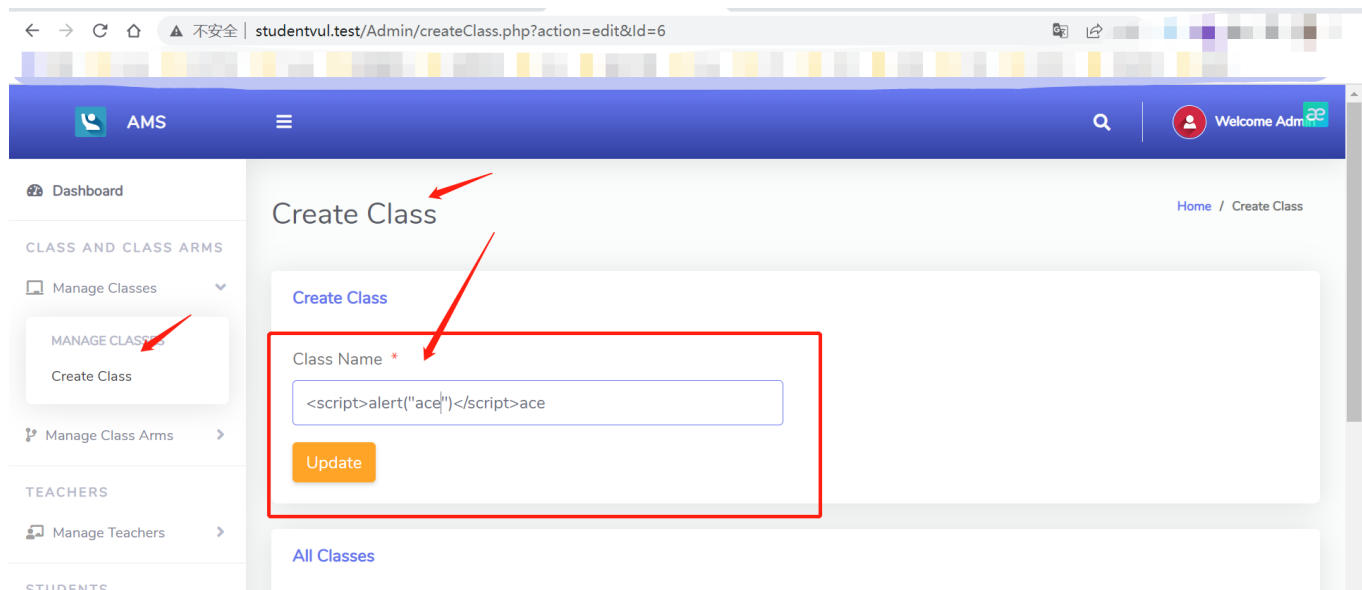
Student Attendance Management System has a storage XSS vulnerability #3

✓ Closed huclilu opened this issue 9 days ago · 0 comments

huclilu commented 9 days ago

Build environment: Aapche2.4.39; MySQL5.7.26; PHP7.3.4

input `admin@mail.com` / Password@123 Log in to the background. At manage classes, click create class, enter xsspayload: `<script>alert("ace")</script>`, and click save.

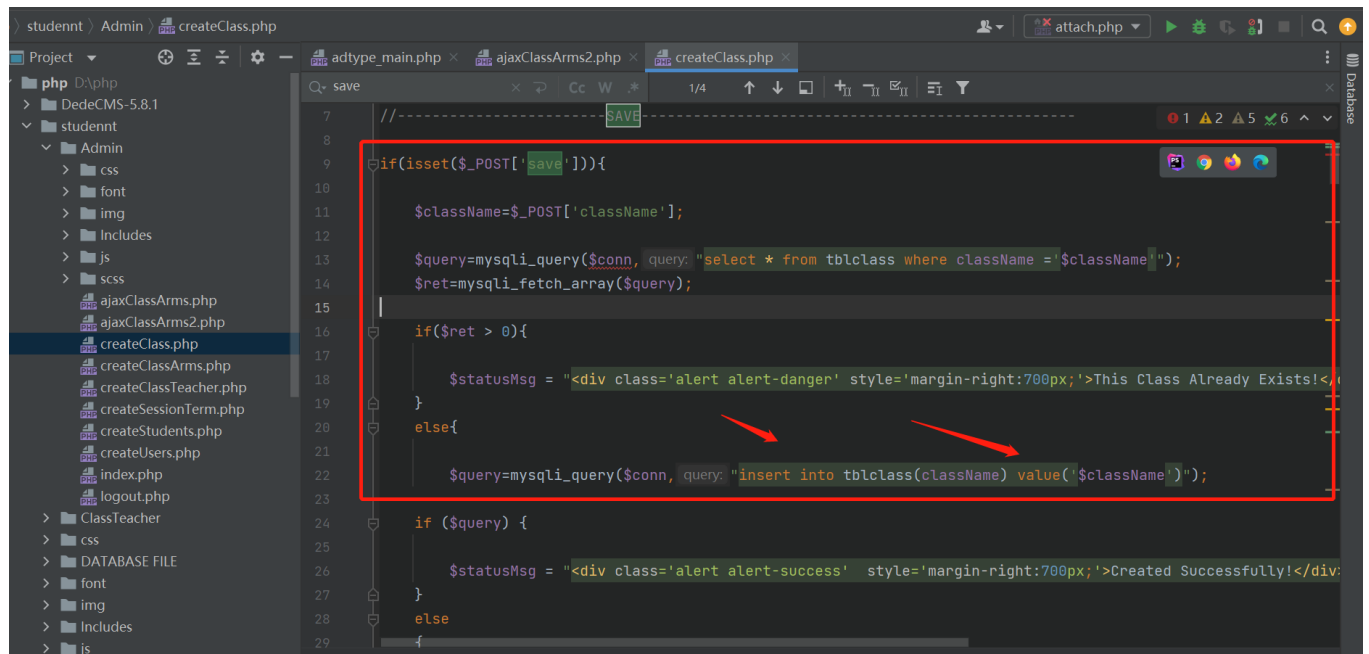


and then refresh the interface to pop up




createClass.php:


After clicking save, the className is substituted into the input for query. If it does not exist, the className will be reinserted into the database. Because the script is not escaped from html, the XSS vulnerability is caused



```
//-----SAVE-----
if(isset($_POST['save'])){
    $className=$_POST['className'];
    $query=mysqli_query($conn, query: "select * from tblclass where className = '$className'");
    $ret=mysqli_fetch_array($query);
    if($ret > 0){
        $statusMsg = "<div class='alert alert-danger' style='margin-right:700px;'>This Class Already Exists!</div>";
    }
    else{
        $query=mysqli_query($conn, query: "insert into tblclass(className) value('$className')");
    }
    if ($query) {
        $statusMsg = "<div class='alert alert-success' style='margin-right:700px;'>Created Successfully!</div>";
    }
    else
    {
    }
}
```

 hucililu closed this as completed 8 days ago

 hucililu reopened this 8 days ago

 hucililu closed this as completed 8 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

