New issue

Jump to bottom

SQL injection vulnerability in Student Attendance Management System #2

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

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

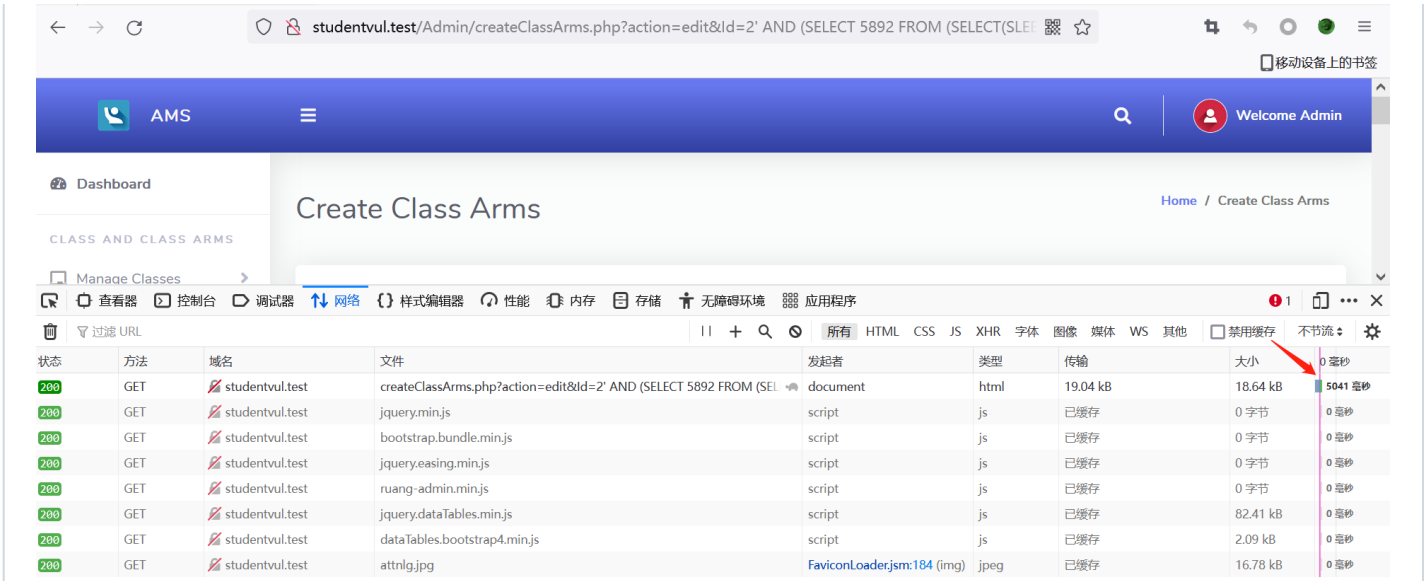
2.sql injectionPOC：

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

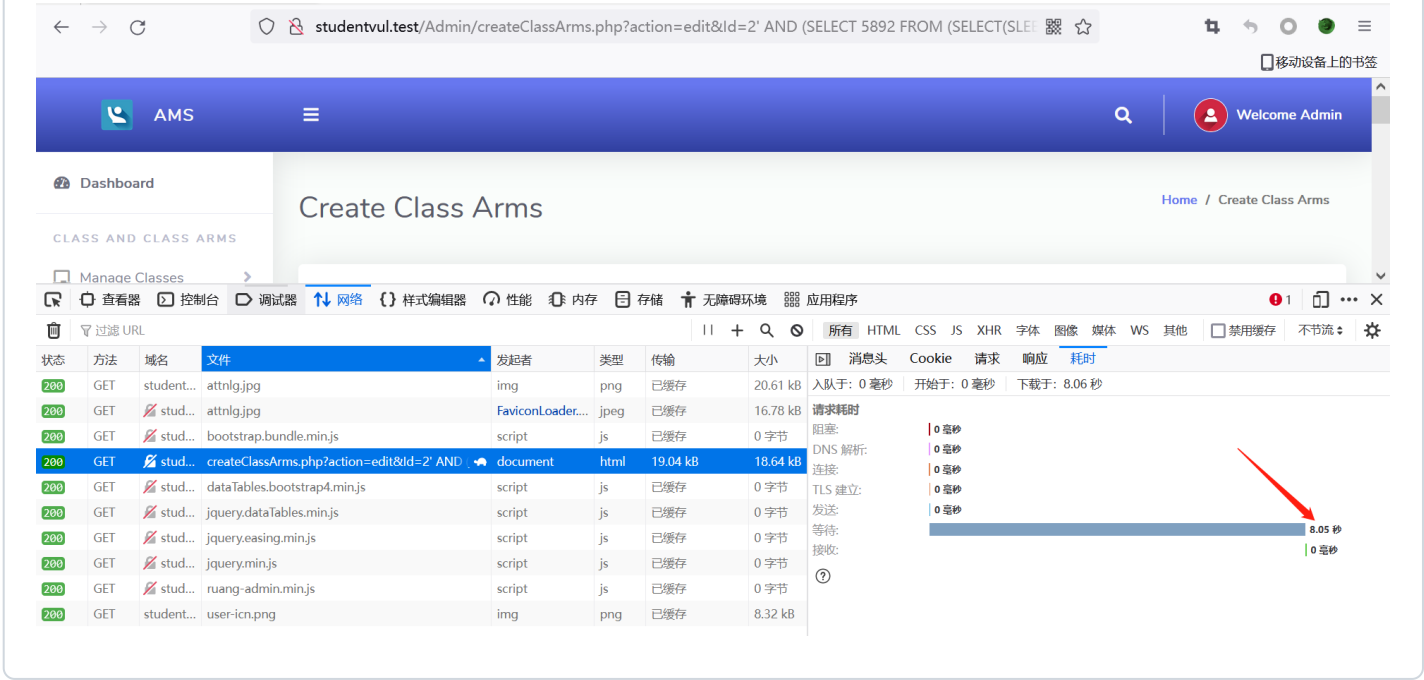
- Use sqlmap to verify

- Manual verification

1. SLEEP(5)



2. SLEEP(8)



huclilu closed this as completed 8 days ago

Assignees

No one assigned

Labels

None yet

Projects

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant