# Wazifa_IN_PHP has Cross Site Scripting vulnerability in search_results.php

## supplier

[https://download-media.code-projects.org/2020/04/Wazifa_IN_PHP_CSS_Js_AND_MYSQL__FREE_DOWNLOAD.zip](https://download-media.code-projects.org/2020/04/Wazifa_IN_PHP_CSS_Js_AND_MYSQL__FREE_DOWNLOAD.zip)

## Vulnerability file

search_results.php

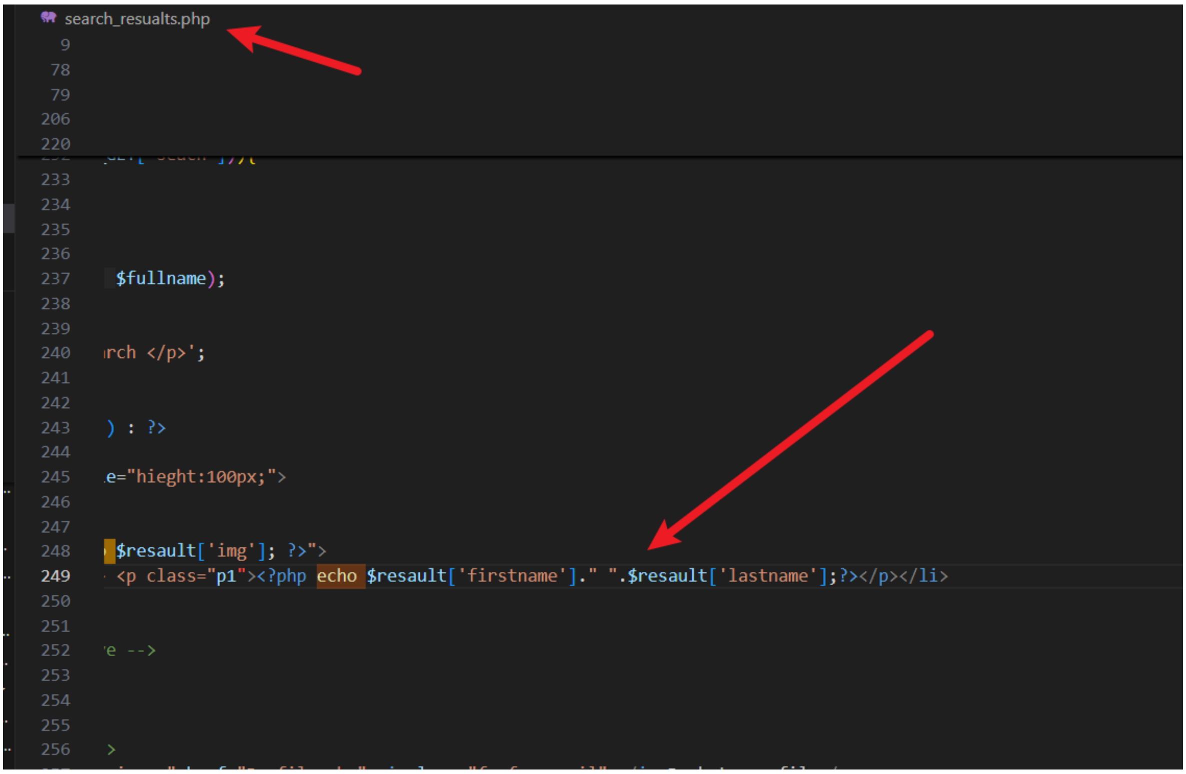
## describe

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

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

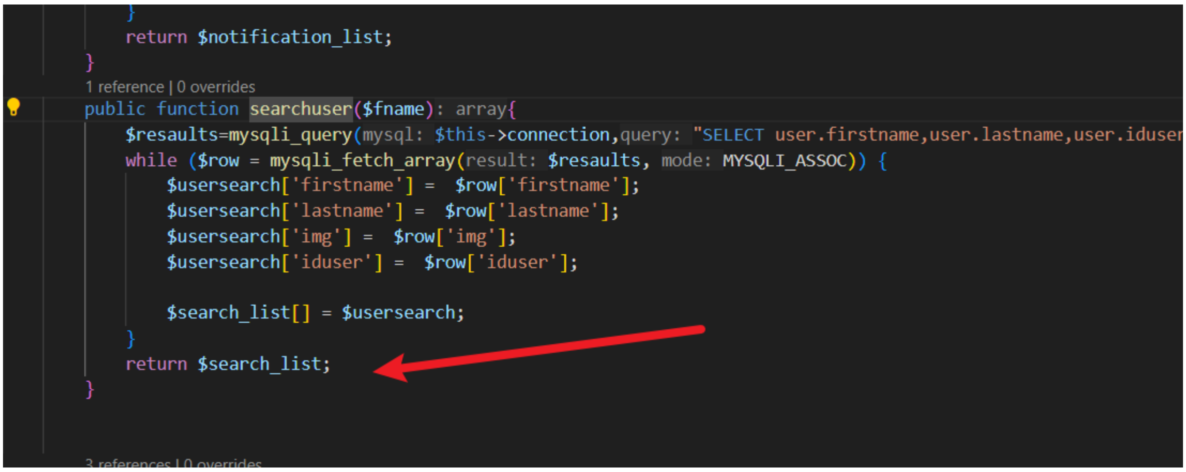
## code analysis

echo $result['lastname'] in no filer.



search_resualts.php

```
 $fullname);

rch </p>';

) : ?>

e="hieght:100px;">

 $resault['img']; ?>">
 <p class="p1"><?php echo $resault['firstname']." ".$resault['lastname'];?></p></li>

e -->

>
```

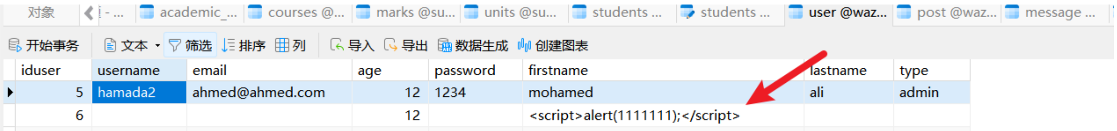


```
        }
        return $notification_list;
    }
    1 reference | 0 overrides
    public function searchuser($fname): array{
        $resaults=mysqli_query(mysql: $this->connection,query: "SELECT user.firstname,user.lastname,user.iduser
        while ($row = mysqli_fetch_array(result: $resaults, mode: MYSQLI_ASSOC)) {
            $usersearch['firstname'] =  $row['firstname'];
            $usersearch['lastname'] =  $row['lastname'];
            $usersearch['img'] =  $row['img'];
            $usersearch['iduser'] =  $row['iduser'];

            $search_list[] = $usersearch;
        }
        return $search_list;
    }

    3 references | 0 overrides
```

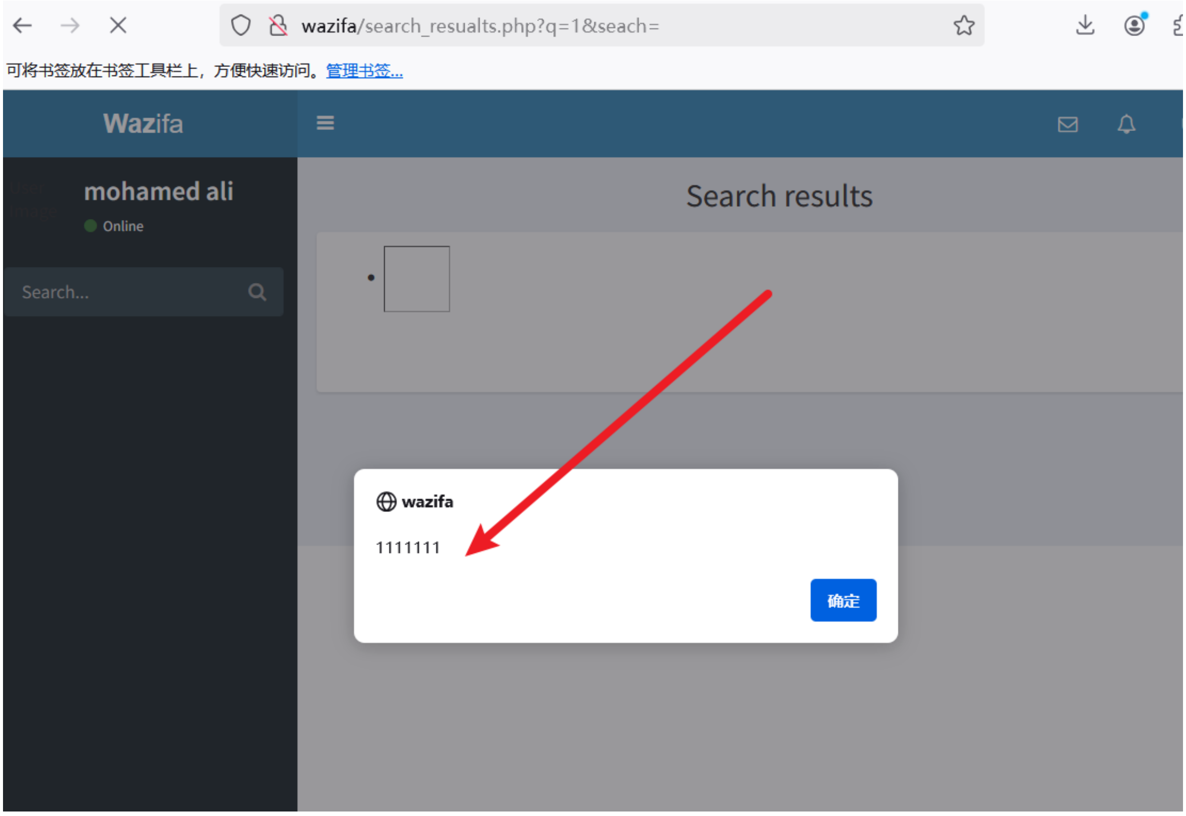
# POC

```
GET /search_resualts.php?q=1&seach= 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
Referer: http://wazifa/search_resualts.php?q=1&seach=
Cookie: PHPSESSID=vp9qmg441as10dtp4j4qfca9g7
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

### Result



| iduser | username | email | age | password | firstname | lastname | type |
|---|---|---|---|---|---|---|---|
| 5 | hamada2 | ahmed@ahmed.com | 12 | 1234 | mohamed | ali | admin |
| 6 | | | 12 | | <script>alert(1111111);</script> | | |



wazifa/search_resualts.php?q=1&seach=

可将书签放在书签工具栏上，方便快速访问。管理书签...

Search results

wazifa

1111111