

blood-bank-system-in-php has Cross Site Scripting vulnerability in o+.php

supplier

<https://code-projects.org/blood-bank-system-in-php-with-source-code/>

Vulnerability file

/BBfile/Blood/o+.php

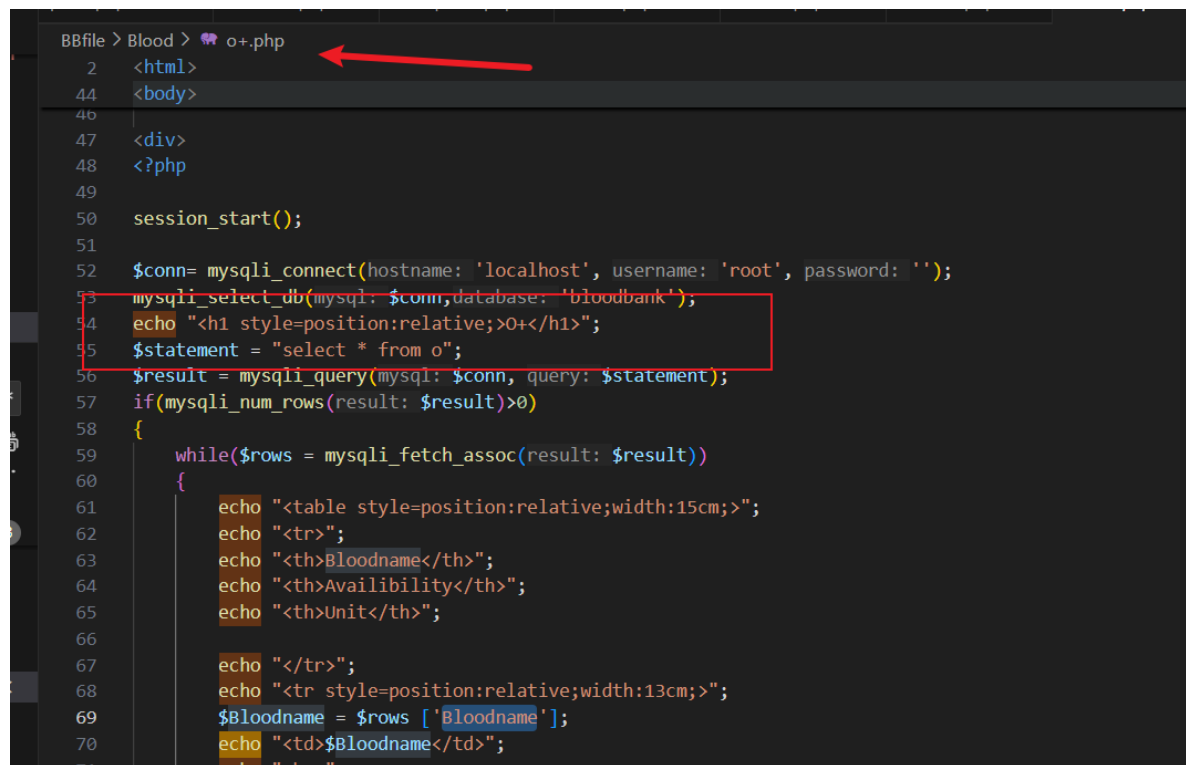
describe

There is an Cross Site Scripting vulnerability in blood-bank-system-in-php in /BBfile/Blood/o+.php. Control parameter: \$Bloodname

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

code analysis

In O+.php.php, get \$row['Bloodname'], and echo it in no filter.



```
BBfile > Blood > o+.php
 2  <html>
44  <body>
46
47  <div>
48  <?php
49
50  session_start();
51
52  $conn= mysqli_connect(hostname: 'localhost', username: 'root', password: '');
53  mysqli_select_db(mysqli: $conn,database: 'bloodbank');
54  echo "<h1 style=position:relative;>O+</h1>";
55  $statement = "select * from o";
56  $result = mysqli_query(mysqli: $conn, query: $statement);
57  if(mysqli_num_rows(result: $result)>0)
58  {
59      while($rows = mysqli_fetch_assoc(result: $result))
60      {
61          echo "<table style=position:relative;width:15cm;>";
62          echo "<tr>";
63          echo "<th>Bloodname</th>";
64          echo "<th>Availability</th>";
65          echo "<th>Unit</th>";
66
67          echo "</tr>";
68          echo "<tr style=position:relative;width:13cm;>";
69          $Bloodname = $rows ['Bloodname'];
70          echo "<td>$Bloodname</td>";
71          echo "<td>";
```

POC

```
GET /Blood/O+.php HTTP/1.1
Host: bloodbankmgmtsystem
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/122.0.6261.112 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

Result

The screenshot shows a web browser window with the address bar displaying "bloodbankmgmtsystem/blood/o+.php/". An alert box titled "bloodbankmgmtsystem 显示" contains the number "1". Below the alert, a table displays the following information:

Bloodname	Availability	Unit
O+	11	1 (in half liters)

At the bottom of the page, the copyright notice "© 2019 BBMS" is visible.

submiter

姓名：向宏力
单位：广州大学
导师：罗熙