

XSS injection vulnerability exists in name parameter of /admin/add-category.php file of Beauty Salon Management System

With XSS, cybercriminals can turn trusted websites into malicious ones, thus causing inordinate harm and damage not only to the victims but also to the reputation of the trusted website's owner.

Websites that are compromised by XSS can cause any number of threats to attack a user's system. This can involve anything from inappropriate content being displayed to malware being downloaded onto the system without the user knowing.

```
12 $name = mysqli_escape_string($con, $_POST['name']);
13
14
15 $sql = "INSERT INTO category (name) VALUES ('$name') ";
16 $run_sql = mysqli_query($con, $sql);
17
```

The image shows a web application interface with a list of categories. The 'Body Massage' category is highlighted. A red arrow points to the 'Body Massage' category in the list. Below the list, a red arrow points to the 'Body Massage' category in the list. The screenshot also shows a network traffic analysis tool (Burp Suite) displaying a request and response. The request is a POST to /Chic_Beauty_Salon_System/admin/add-category.php. The response is a 200 OK status. The payload is name=<ScRiPt%20>alert(9025)</ScRiPt><!--. The screenshot also shows a browser window displaying the alert(9025) message.

Chic Beauty Salon | Add Category

9025

Payload: name=<ScRiPt%20>alert(9025)</ScRiPt><!--

Source Download:

<https://www.campcodes.com/projects/beauty-salon-management-system-in-php-and-mysql/>