

XSS injection vulnerability exists in adminname parameter of /admin/admin-profile.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.

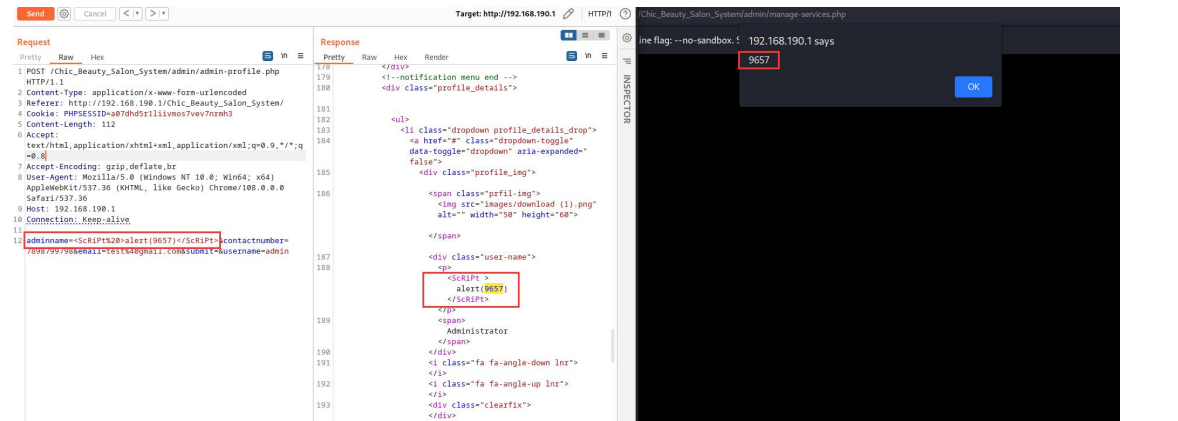
Websites that are compromised by XSS can cause any number of threats to attack a user's system. This can involve anything from inappropriate content being displayed to malware being downloaded onto the system without the user knowing.

When visit /admin/admin-profile.php, it will include /admin/includes/header.php, and can do XSS injection.

```
8         if(isset($_POST['submit']))
9         {
10            $adminid=$_SESSION['bpmsaid'];
11            $aname=$_POST['adminname'];
12            $mobno=$_POST['contactnumber'];
13
14            $query=mysqli_query($con, "update tbladmin set AdminName=' $aname', MobileNumber=' $mobno' where ID=' $adminid'");
```

```
63      <?php include_once('includes/header.php');?>
```

```
36 $name=$row['AdminName'];
37
38 <?>
39
40 <ul>
41 <li class="dropdown profile_details_drop">
42 <a href="#" class="dropdown-toggle" data-toggle="dropdown" aria-expanded="false">
43 <div class="profile_img">
44 <span class="profil-img"> </spa
45 <div class="user-name">
46 <p><?php echo $name; ?></p>
47 <span>Administrator</span>
</div>
```



Payload:adminname=<ScRiPt%20>alert(9657)</ScRiPt>

Source Download:

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