kishan0725 / Hospital-Management-System Public

Code Issues 23 Pull requests 5 Actions Projects Security ···

New issue

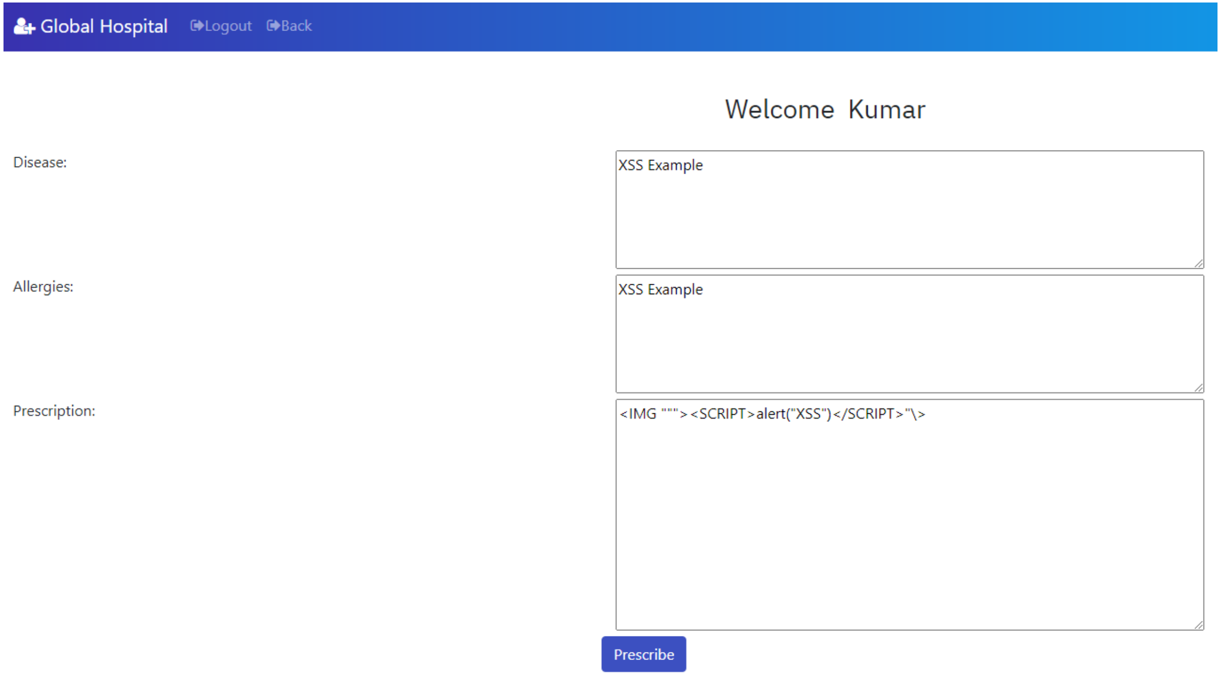
Jump to bottom

Persistent Cross Site Scripting (XSS) Vulnerability in Prescription #4

Open **dumpling-soup** opened this issue on Aug 10, 2021 · 0 comments

dumpling-soup commented on Aug 10, 2021

Add XSS in Prescription as DOCTOR



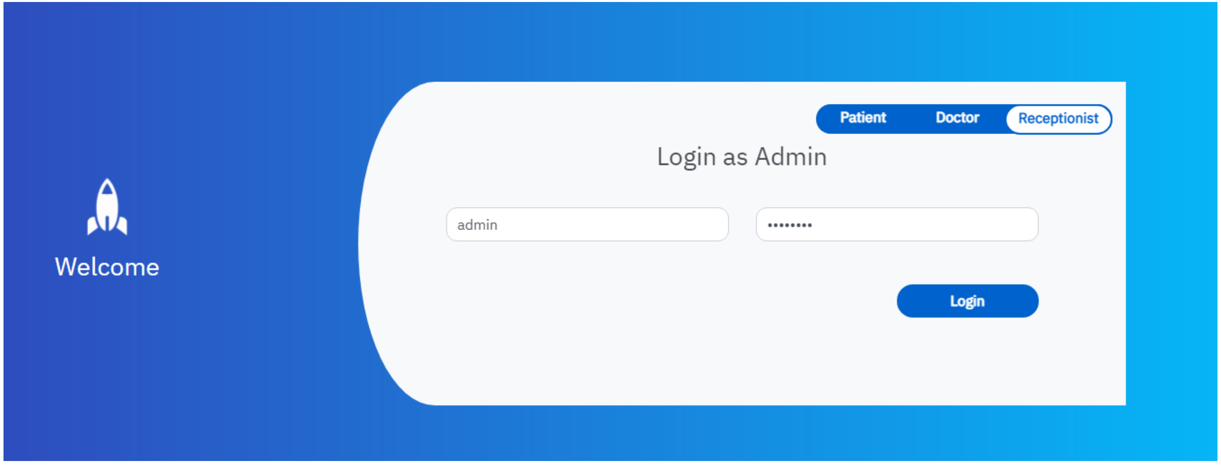
Welcome Kumar

Disease: XSS Example

Allergies: XSS Example

Prescription: <IMG """><SCRIPT>alert("XSS")</SCRIPT>"\>

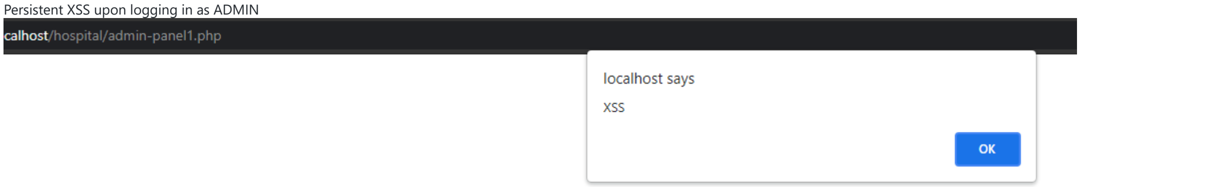
Login as ADMIN



admin

••••••••

Persistent XSS upon logging in as ADMIN

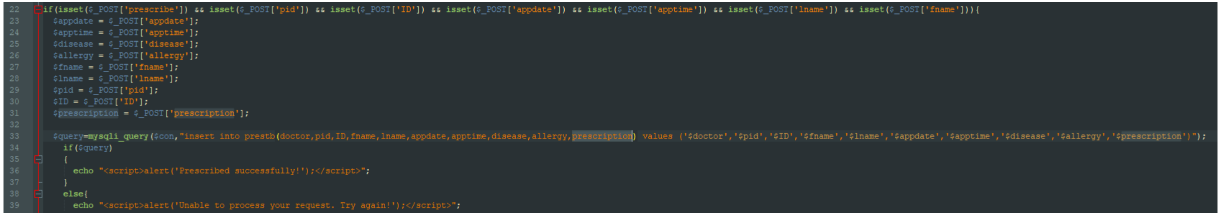


calhost/hospital/admin-panel1.php

localhost says

XSS

Issue in prescribe.php



```
if(isset($_POST['prescribe']) && isset($_POST['pid']) && isset($_POST['ID']) && isset($_POST['appdate']) && isset($_POST['apptime']) && isset($_POST['lname']) && isset($_POST['fname'])){
  $appdate = $_POST['appdate'];
  $apptime = $_POST['apptime'];
  $disease = $_POST['disease'];
  $allergy = $_POST['allergy'];
  $fname = $_POST['fname'];
  $lname = $_POST['lname'];
  $pid = $_POST['pid'];
  $ID = $_POST['ID'];
  $prescription = $_POST['prescription'];

  $query=mysqli_query($con,"insert into prestb(doctor,pid,ID,fname,lname,appdate,apptime,disease,allergy,prescription) values ('$doctor','$pid','$ID','$fname','$lname','$appdate','$apptime','$disease','$allergy','$prescription')");
    if($query)
    {
      echo "<script>alert('Prescribed successfully!');</script>";
    }
    else{
      echo "<script>alert('Unable to process your request. Try again!');</script>";
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant