File upload

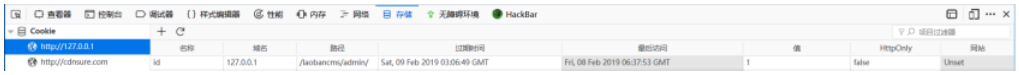
In `laobancms/admin/wenjian.php` line 103 to 112

```
103 if(isset($_POST['shangchuan'])){
104     $total = count($_FILES['sc']['name']);//上传数量
105     for($i=0; $i<$total; $i++){
106         if(strstr($_FILES['sc']['name'][$i],'.jpg') || strstr($_FILES['sc']['name'][$i],'.png') || strstr($_FILES['sc']['name
            ][$i],'.gif') || strstr($_FILES['sc']['name'][$i],'.jpeg') || strstr($_FILES['sc']['name'][$i],'.html') ||
            strstr($_FILES['sc']['name'][$i],'.js') || strstr($_FILES['sc']['name'][$i],'.css')){
107             move_uploaded_file($_FILES['sc']['tmp_name'][$i],"$wj/".$_FILES['sc']['name'][$i]);
108         }
109         else{echo "<script>alert('你上传的文件格式不正确，请重新选择上传文件');window.location='wenjian.php?wj=$wj';</script>";}
110     }
111     echo "<script>alert('上传成功');window.location='wenjian.php?wj=$wj';</script>";
112 }
```

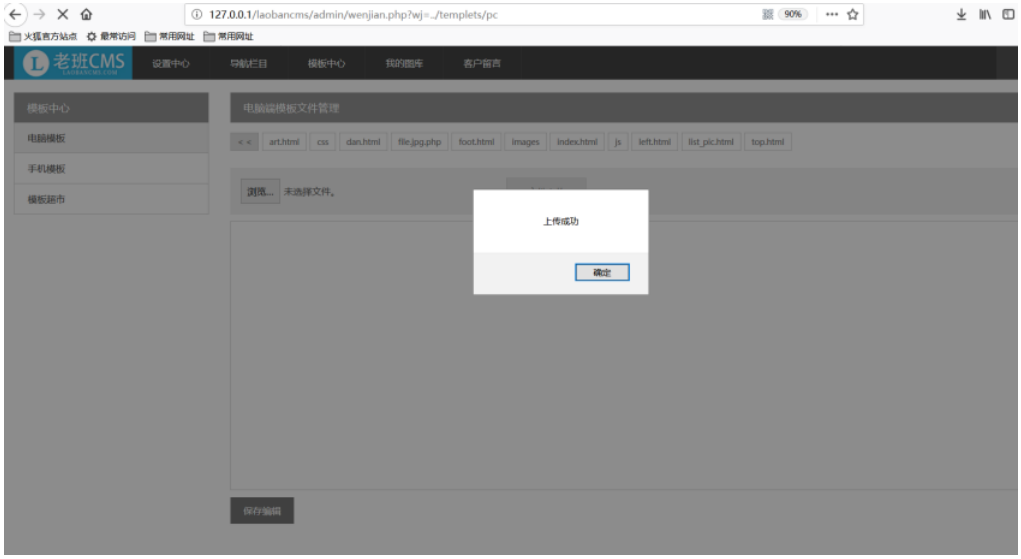
It simply validates the existence of '.jpg |.png |.gif |.jpeg |.html |.js |.css' in the file name by using the strstr() function.

So ,upload `test.jpg.php`

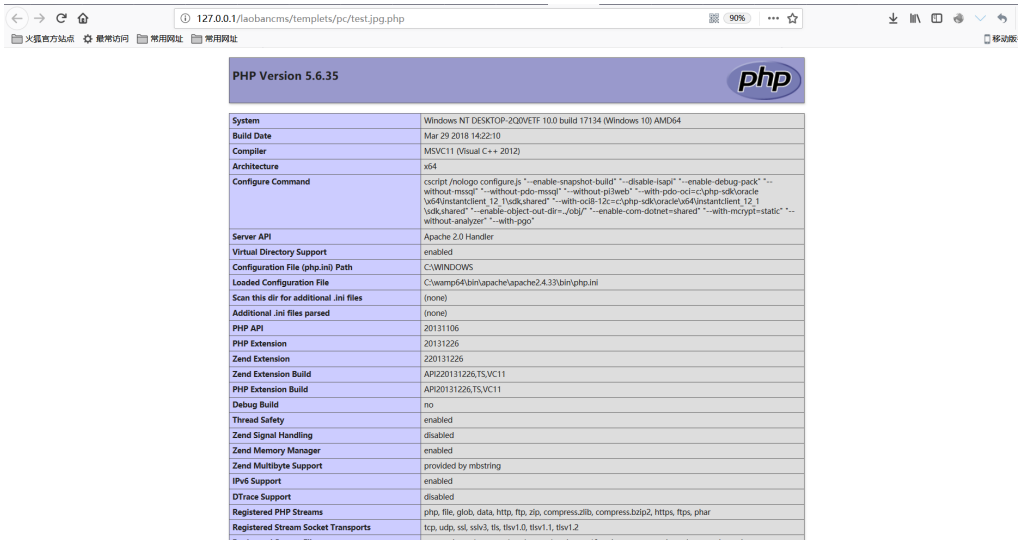
First,login the admin page by setting the cookie(id=1) (CVE-2018-19224)



Visit `admin/wenjian.php?wj=../templets/pc` , upload `test.jpg.php`



Vist: `templets/pc/test.jpg.php`



We can get shell !

XSS1

Login the admin page by setting the cookie(id=1) (CVE-2018-19224)

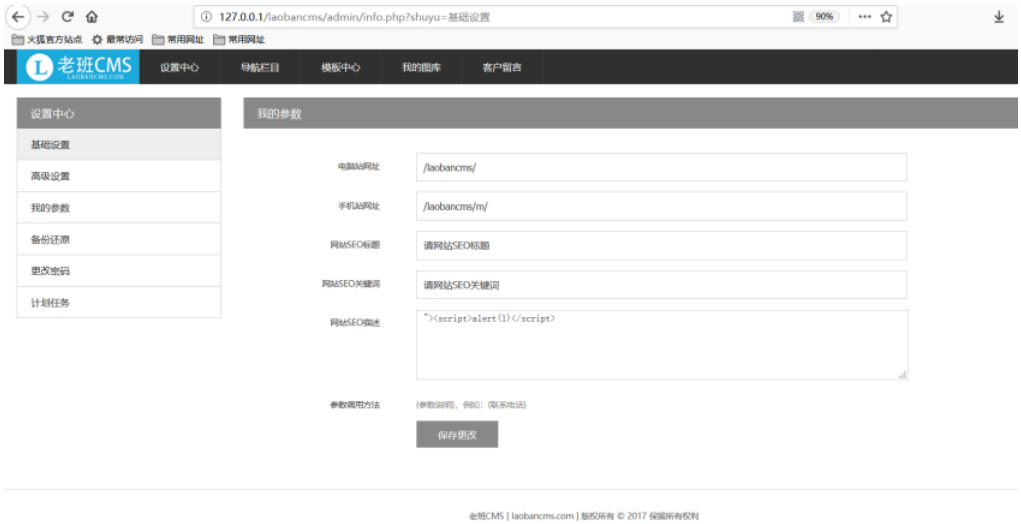
Visit: `admin/info.php?shuyu=基础设置`

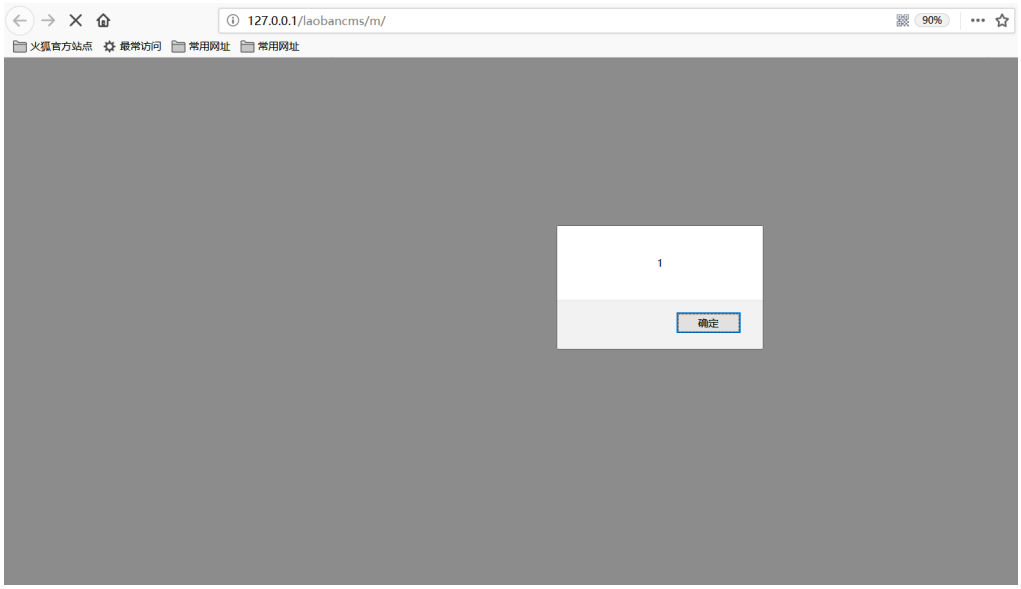
Fill `"><script>alert(1)</script>` in the "网站SEO关键词" form

Click the '保存更改' button to save the changes

Click the '生成'->'更新今日' button in the upper right corner to update

Then visit the index





XSS2

Login the admin page by setting the cookie(id=1) (CVE-2018-19224)

Visit: `admin/info.php?shuyu=我的参数`

Fill `<script>alert(1)</script>` in the "首页简介" form

Click the '保存更改' button to save the changes

Click the '生成'->'更新今日' button in the upper right corner to update

Then visit the index