链滴

老树开花一个js函数引发的命案

作者：huomingfei
原文链接：https://ld246.com/article/1471042546727
来源网站：链滴

很多网站系统把一些功能放在客服端执行（javascript）,而服务端没有相应的验证,从而被非法利。本文就是一个 js 函数使用不当,导致网站以及整个服务器沦陷的案例。
前端漏洞挖掘
最新安全测试一个站旁注扫出一个 <a href="https://ld246.com/forward?goto=http%3A%2F2Fwww.xxx.com%2FUtility%2FUploadFile%2FFileList.asp" target="_blank" rel="nofollow ugc" www.xxx.com/Utility/UploadFile/FileList.asp
图一
<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile com/e/f2da91725a364ddb92ee1df2812259fe.png?imageView2/2/interlace/1/format/jpg"></
>
这个编辑器功能很强大,看能不能找到点其他可以利用的地方,习惯性的查看源码。看到一段 Javasc ipt,目测有猫腻。

="menumouseover(this)"onMouseOut="menumouseout(this)">
="selFolder"type="checkbox"id="selFolder"
value="D:\website9\www.xxx.com\UpFile\1"">
="javascript:transferFolder('/UpFile/1');">
="dir.gif"width="17"height="14"border="0"
align="absmiddle">1

这个是点击图一中的文件夹的 js 源码，爆出绝对路径,可能有用,然后又看到一个强大的 j 函数 tra sferFolder()，经过测试这个函数是点击击编辑器中的文件夹 js 是向服务端发送需要浏览文件夹,然后 a p 服务器返回传回文件夹的文件列表，以浏览文件。

//改变当前文件夹
functiontransferFolder(f)
{
document.formList.fder.value=f
document.formList.submit();
}

看 transferFolder 函数源码,每个载入浏览器的 HTML 文档都会成为 Document 对象,使我们可从脚本中对 HTML 页面中的所有元素进行访问。把传入的文件夹赋值给 Document.formList 用来操 formList 表单,formList 和 fder 为何物？

;overflow:auto;"name="formList"method="post"action="">
="rootFder"type="hidden"id="rootFder"value="/UpFile">
="fder"type="hidden"id="fder"value="/UpFile">

还是目测 fromList 是浏览文件的表单 fder 则是需要浏览的文件夹,由 transferFolder 函数赋值,试下这个函数是否可以传入任意浏览服务端文件夹,由于需要经常改代码,换了个 opera 浏览器,原来的 t ansferFolder 参数如下。

transferFolder('/UpFile/1');

传入 transferFolder(‘/Utility/UploadFile’);(这个目录绝对存在)，猛烈的点击.....悲剧了！！ 么都没有,欲罢而不能,继续目测之.rootFder 是根目录,而 fder 是当前目录,这里需要人工修改,遂把/UpFi e 改为/Utility
<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile com/e/995dbebdfc984d26b1b617f886a9cb41.png?imageView2/2/interlace/1/format/jpg"><
p>
改写
<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile com/e/39587c3bd062473d944bffc662637277.png?imageView2/2/interlace/1/format/jpg"><

p>
再次猛烈点击,奇迹般的出现了
<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile
com/e/ad2582be6c8540e58f44bf6209571a61.png?imageView2/2/interlace/1/format/jpg"></
>
如图四 ￥#*&￥#@！*无比鸡动！！！,这个函数果然有鬼,接下来就是扩大战果。
JS 函数利用
<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile
com/e/f38fd13f72f049718f7719c60060ed57.png?imageView2/2/interlace/1/format/jpg"></
>
整理一下思路先,如图五所示,编辑器可以重命名,通过 transferFolder 函数可以遍历整个网站目录
件,如果有权限还可以下载服务端的文件（有权限重命名），搞清此套程序的目录结构,如果是数据库 ac
ess 直接下载数据文件,进后台再说,是 sqlserver 看 1433 能不能利用,干！！！！
为了搞清此套系统的目录结构,不久拿下一个和这个系统的其他网站的 webshell,如图七。
<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile
com/e/1427519c9f0d4fbfb6fb84e343e18278.png?imageView2/2/interlace/1/format/jpg"></
>
在 System\Config.asp 找到其配置
<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile
com/e/be7635f7589b43a68e41a433dcb9ce04.png?imageView2/2/interlace/1/format/jpg"><
p>
看到图七,我很欣慰,回到安全监测的那个站,通过 transferFolder()这淫荡的函数,找到 Config.asp<
p>
<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile
com/e/9003a09256d64fe9886d5168fe1cf71f.png?imageView2/2/interlace/1/format/jpg"></
>
如图八果断改为 txt 直接访问.....
<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="https://b3logfile
com/e/8b3bb6f9df614de895969aa9250f232e.png?imageView2/2/interlace/1/format/jpg"></
>
总结
这个程序有多处致命漏洞,包括 fck 编辑器和以前的老漏洞,还有本文的 js 函数服务端缺乏验证导
任意文件可下载,查看(有的无权限),网上使用的众多,我们程序猿除了需要注 sql，编辑器等服务端的代
安全,也需要关注像 javascript 这样的前端语言,因为用户随意查看和修改前端的源码,这个更加危险！
！
笔者能力有限,文中难免有纰漏,恐贻笑于大方之家,万望海涵...