突破封闭Web系统的技巧之旁敲侧击

作者: LANDGREY ● 创建时间 2017年12月27日 22:50 ● 更新时间 2018年1月3日 00:50
浏览: 883 次. ● 标签: #分享, #渗透测试, #思考
您的IP地址: 140.207.23.83

前言：

在互联网安全服务公司乙方工作的人或者进行SRC众测等相关渗透测试时，经常碰到客户只给一个"xxx信息管理系统"、"xxx平台"之类的一个Web登录界面的系统的链接地址，其它全凭自己造化，去找漏洞吧!

我将上面讲的"需要认证后才能进入系统进行操作，但是当前没有认证凭证"的web系统统一称为"封闭的Web系统"，本文认为阅读人员有一定的渗透测试经验，并将就如何突破封闭的Web系统，进行探讨。分享自己的思路与常用技巧，欢迎同道中人一起交流思路。

注：本文有一定的攻击性操作，仅为安全从业人员渗透测试思路交流，请在法律条规允许的范围内进行安全测试。

一：文章脉络

《突破封闭Web系统的技巧》由两篇文章组成。这是第二篇文章"旁敲侧击"。下面是本文的脉络：

```
旁敲侧击
0x00：扫端口扩范围
0x01：寻找测试域名
0x02：微信公众号与APP
0x03：寻找蛛丝马迹
0x04：何方CMS
0x05：历史漏洞搜索
0x06：大杀四方
```

二：旁敲侧击

经过我们的一阵自杀式……哦不对，字典式冲锋，发现我们将自己意淫成管理员企图从心里战胜"封闭系统"的想法失败了。进不去就是进不去啊，一个低危洞都没有，看来是这系统比较安全了。但是回头一瞟，隔壁座位上的老王喜笑颜开，3个高危已经轻松提交上去，还有2个中危都不屑一看…… 自己心里想着"我真菜"，然后决定彻底放弃。直到某天，老王感觉亏欠你太多，向你娓娓道出他那天所施展的姿势……

0x00：扫端口扩范围

在正面冲锋失败后，我们应该暂时放弃"通过合法的凭证进入Web系统"这个想法，扩散思维，不再局限于Web系统，多关注操作系统、中间件的层面。

端口扫描做为一项常用技术，可用nmap、masscan、zmap等工具进行端口探测和服务识别，不再赘述。值得注意的是：不要着急就只扫描TCP协议的端口，UDP协议的端口也不要放过。

扫描到一些有趣的端口和服务，就可以尽情的去玩耍了。如果有较多有可能被拿下的服务端口开放，无形中我们直接拿下服务器的概率会大大增加。当别人还在"冲锋"时，我们可能早就通过某不知名端口部署的其它Web应用系统的中间件漏洞进入系统了~

0x01：寻找测试域名

有些厂商在开发其Web系统时，可能会先单独分配个测试域名来测试正在开发的系统，比如"testapi.land.com"。当系统开发完成后，厂商如愿以偿的将安全的系统部署在域名"api.land.com"上，但是确忘记关闭了"testapi.land.com"。然后，测试域名上仍然开放着N多端口，分别对应着不同版本的Web系统，俨然成为了一个天然的靶场。

0x02：微信公众号与APP

Web系统进不去？去看看厂家的微信公众号吧。为了迎合客户和流量，有点规模的企业都会建立自己的微信公众号，而且安全保护的受重视程度通常远低于Web系统。Web系统可能有复杂的图片验证码，而微信公众号可能为了用户体验，并没有设置任何图形验证码；Web系统难以发现的接口可能在浏览微信公众号时的数据包中找到；

同理，如果厂家的封闭Web系统是面向多业务员的，那么很可能存在某一或几款APP，存在同样的登录功能，而且也比Web系统要疏于保护。缺少验证码或可能找到一些请求接口和一些有意思的请求参数。除此之外，反编译APP获得其源码，梳理代码中所有敏感的请求接口、连接地址、关键认证逻辑，可能会有意外收获。另外，测试完安卓机上的APP后，如果APP有IOS版本，测下IOS版的APP，说不定有意外收获。

0x03：寻找蛛丝马迹

最好详细的记录下所有有关Web系统的相关信息。这些信息都有可能成为最后突破的方向，如服务器操作系统类型、使用的框架或组件、使用的容器、使用的CMS类型、服务器版本、开发语言、前端框架等信息。这部分的工具实在太多了，挑拣自己顺手的用就好，比如Firefox插件wapplayer、whatweb、云悉，其它不再赘述。搞不定的web系统，说不定一个Struts2 RCE、Weblogic RCE、Tomcat war包部署之类的漏洞，连服务器的权限都拿到了。

另外，对于信息量极少的封闭系统，右击查看源码基本成了必须要做的事，最好把能接触到网页，全部右击查看一遍网站源码。仔细浏览一遍，看看有没有特殊的网页注释、特殊链接之类的，也许一条测试后台的ip地址链接、放置在json文件中的明文配置密码信息，就能让你进入未受保护的测试系统。

最后，如果系统条件允许的话，最好用检测普通Web系统的手段对封闭的Web系统检测一遍。比如用主机漏洞扫描器Nessus、web漏洞扫描器 AWVS、Netsparker、Appscan等扫描下网站，防止遗漏重要的Web漏洞信息。

0x04：何方CMS

如果Web系统不是作为独苗被单独开发的话，那么很可能是由已知的CMS或框架写成的。知名的CMS在 0x03:寻找蛛丝马迹步骤就应该已经知道了。如果它是由没有开放源代码的商业化的CMS改造而成或者不知名的系统建成，我们还有以下几种方式得到它的名字或者源代码。

1. 观察页面的特殊css命名规则、js方法名等资源特征，用搜索引擎搜索；
2. 将有特点的页面比如登录页面，截图后利用在线试图，比对相似的系统，或者发到某群中，问下有经验的师傅；
3. 在搜索引擎、文库、Github、百度云盘和其它代码托管、云存储平台上，搜索目标的系统类型名，如"企业印鉴管理系统",同
4. 在页面底部或者扫描到的REAMDE等文件里如果有外包公司等名称或首页，可以借此得知是哪个外包公司开发的什么系统，寻找

0x05：历史漏洞搜索

经过我们上面的工作，我们很可能已经得知系统的名字和版本。这时候，就可以去搜索引擎、wooyun漏洞镜像站、安全客的漏洞搜索、cvel漏洞库去搜索下CMS的历史漏洞，或者厂商以前曾暴露出来的漏洞，可能会发现许多有用的信息！

有可能一个以前暴露出来的员工弱口令稍加变形或者xxxCMS 无条件getshell，封闭系统的大门就彻底向我们敞开了。

0x06：大杀四方

从上文所述，我们可以看出：所谓旁敲侧击的精华思想有两部分，一是规避安全措施做的很好的封闭Web系统，尝试从相关的弱点系统和人着手，间接突破封闭的Web系统；二是通过各种渠道，获得所使用系统的名字和源码，尝试使用历史漏洞或者审计源码，突破封闭的Web系统。

最后，老王也缓缓说出了他快速提交漏洞的秘密：原来在N月前，老王在某次渗透测试时，就通过其它网站的wwwroot.rar备份文件。获得了和这个Web系统一样的源码，审计一波已经得到几个0day，0day才是大杀四方的利器啊！

三：总结

当尝试突破封闭的Web系统并且正面强攻不奏效的情况下，旁敲侧击往往具有强大的杀伤力。

其中的技巧往往越猥琐、小众、另辟蹊径，效果越出彩，而且技巧也远远不止上面提到的一小部分。比如，针对性极强的邮件、网页钓鱼套出目标管理员的口令和密码；在所有思路全部中断时，去QQ群搜索下Web系统名或者机构名，编织个巧妙的不敢轻易拒绝的谎言，进去QQ群后，很可能系统源码、默认密码、测试帐号就全部都有了。

<