针对某 C/S 架构系统的渗透测试

这是 酒仙桥六号部队 的第 147 篇文章

1

前言

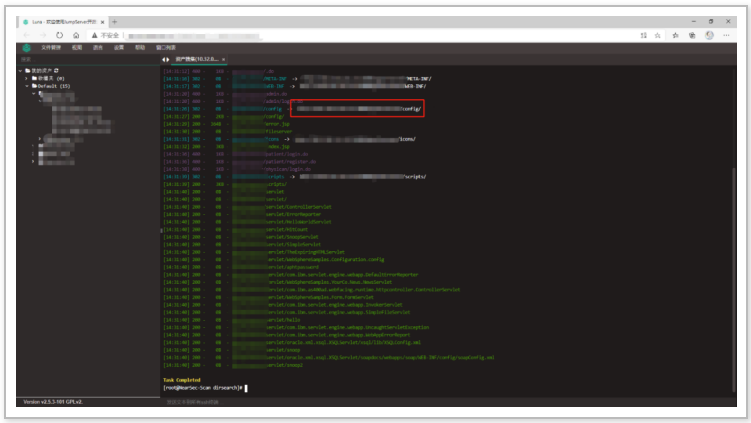
本文主要记录了某次金融类客户项目中遇到的一个 C/S 架构系统的渗透测试，多个漏洞组合最终导致的内网沦陷。

2

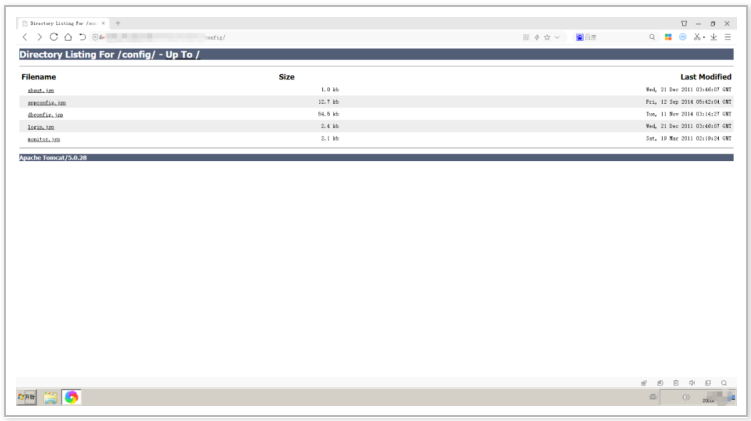
前期准备

首先打开目标站点

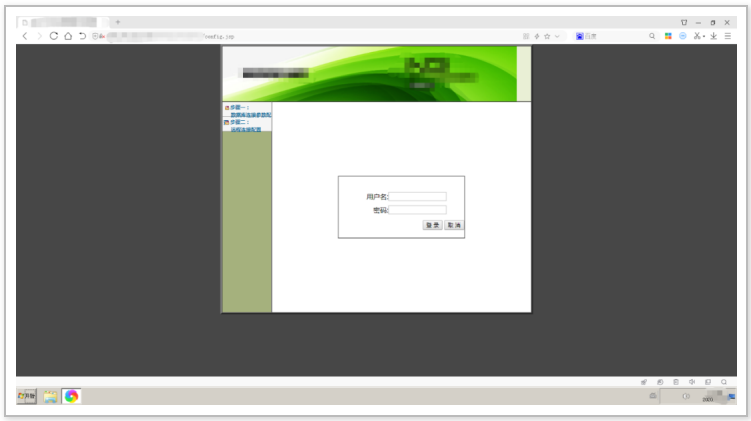
默认页面无任何交互点, 使用 dirsearch 进行简单扫描发现存在 / config 目录



访问后发现可直接列目录

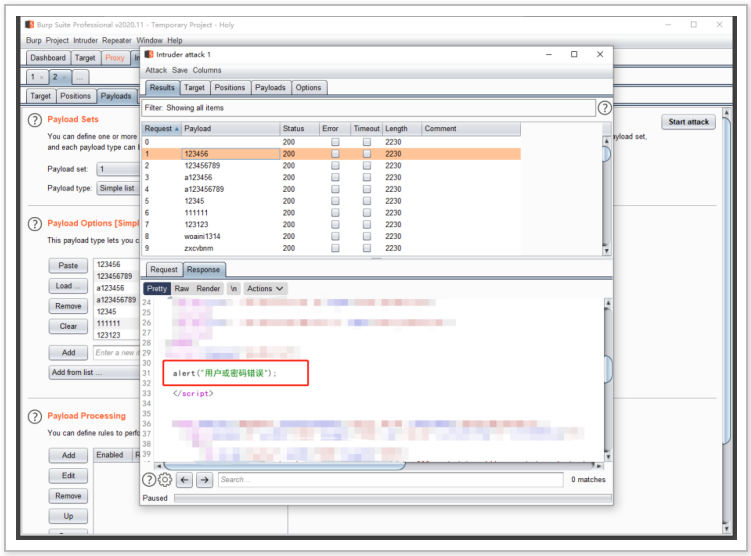


换用更强大的目录字典之后，扫描出了一个配置界面 config.jsp

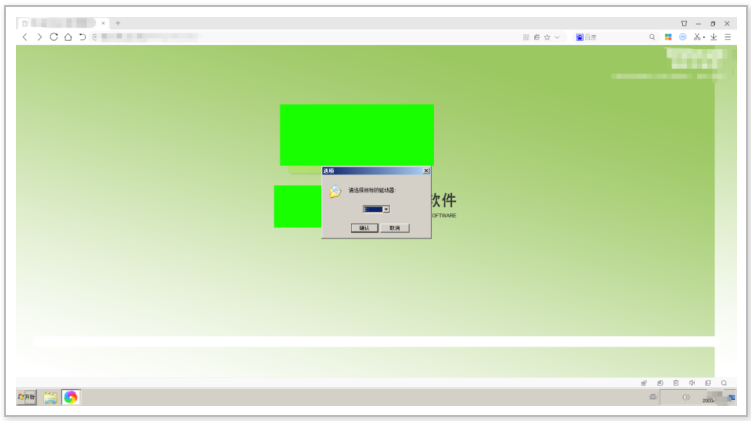


通过网上搜索这个系统的相关手册得知系统默认用户名为: 系统管理员 密码为: 12345

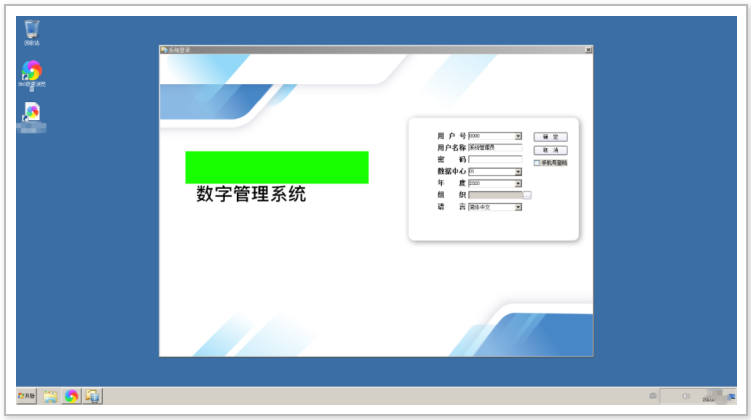
尝试登录发现默认密码已经修改, 通过 Burp 挂载 somd5top10w 字典爆破无果



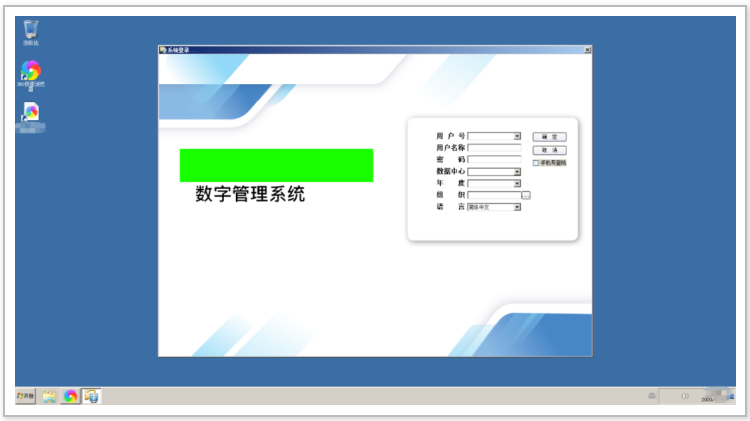
目前在 Web 端暂时没发现什么问题，把注意力回到他的 Index 页面上，页面下方写了需要运行 ActiveX 控件，将浏览器调整至兼容模式，安装控件后弹出了客户端安装界面



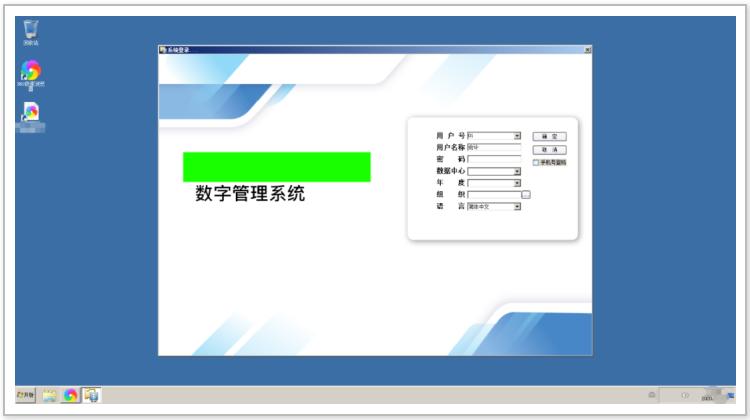
下载安装完成后，运行客户端以后发现系统默认已经显示了用户号和用户名称等信息

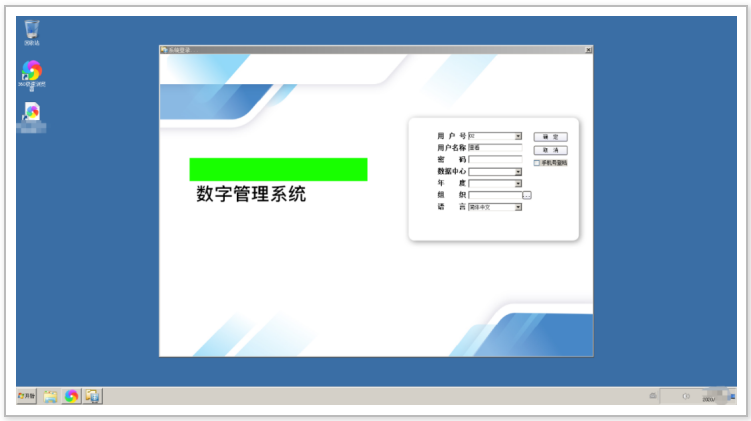


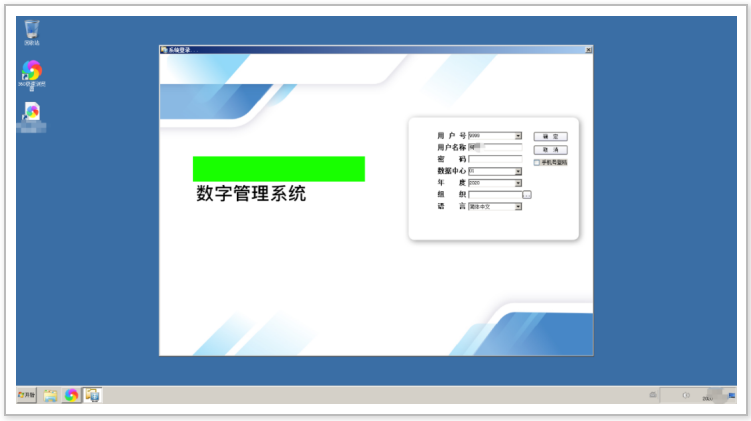
尝试了默认密码 12345 以及其他常见弱口令均无果，尝试修改用户号为 admin 发现系统会自动帮我删除掉，怀疑用户号只能为纯数字



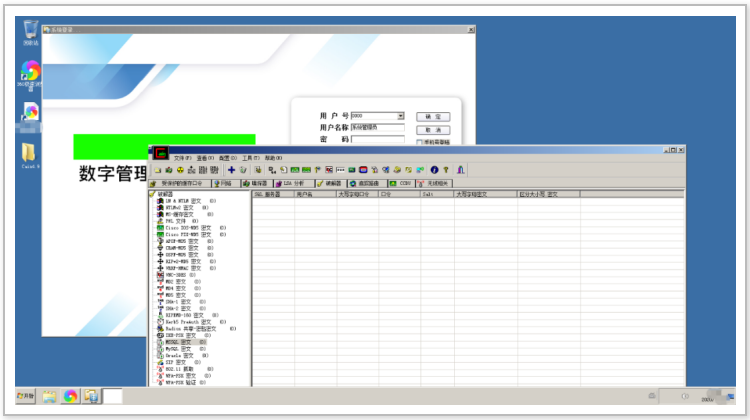
这个时候有意的事情就来了，当我尝试输入 123、12345 等用户号的时候，系统依旧会自动帮我删除输入的内容，但是在输入 01、02、9999 等用户号的时候，下面会有信息显示



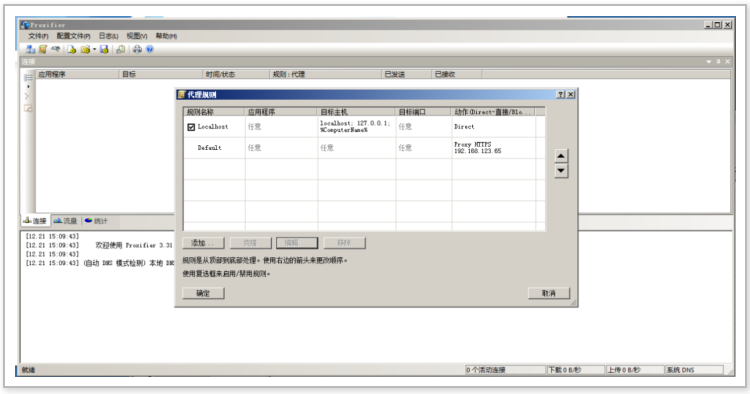




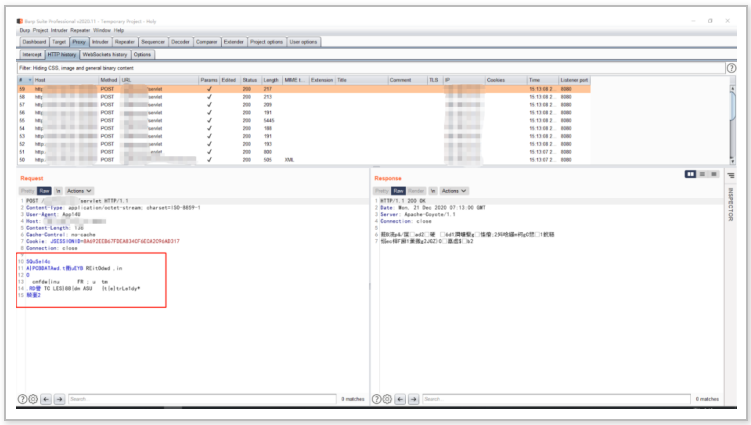
看到这个我的第一反应是想到了以前在学校期间研究过的 X 方教务管理系统，某些版本的 X 方系统是内置了数据库账号密码在程序里，程序直接与数据库交互的，想到这赶紧下载个 Cain 嗅探一下看看



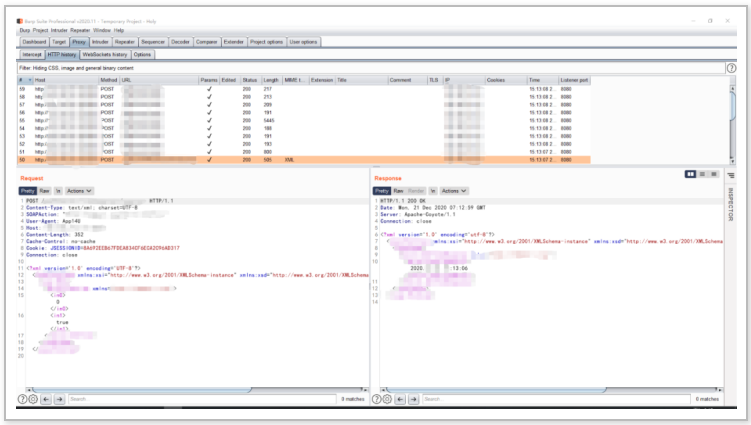
然而很遗憾，Cain 并没有嗅探到数据库信息，那么尝试安装 Proxifier，将客户端的流量代理到 Burp 康康



配置好 Proxifier，将流量全部转发出去，然后 Burp 查看抓到的包



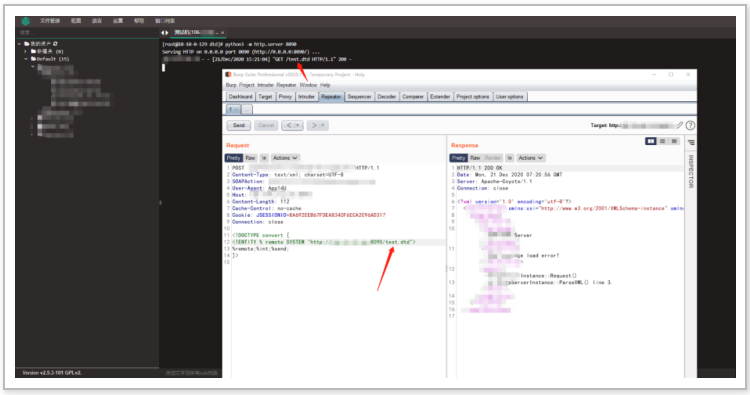
从 Burp 抓到的包来看，SQL 语句是加密传输的，但是翻了几个包以后，忽然发现有个 XML 的请求，直觉告诉我这里很有可能存在 XXE



3

SSRF

尝试将上面 Burp 抓到的 XML 请求的包内容进行修改，指向自己的服务器

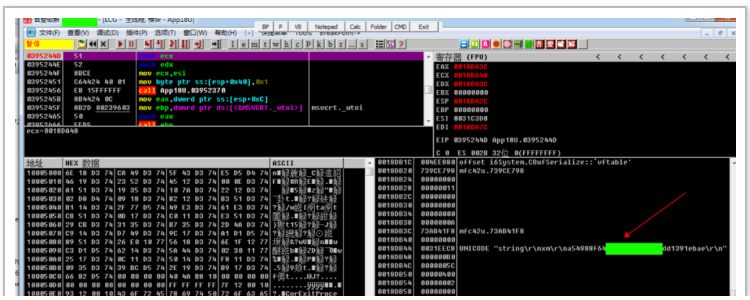


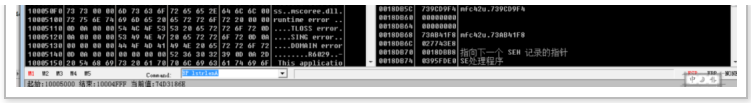
果然存在 XXE，但是测试了命令执行，文件读取等，均无法实现，只能当作 SSRF 进行简单的内容探测

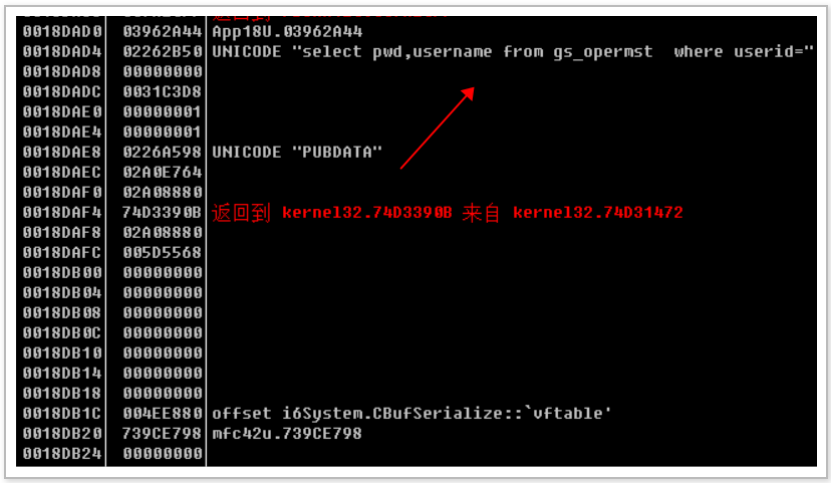
4

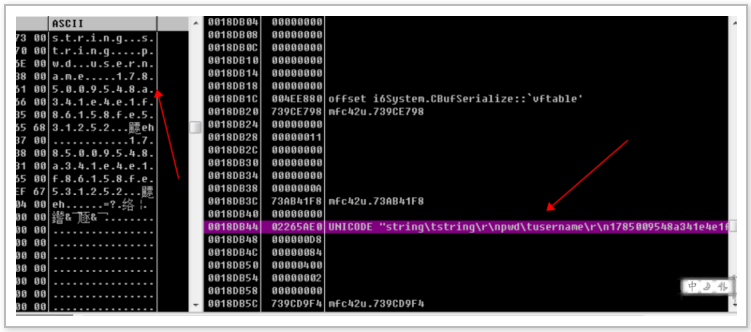
OD 调试

还是回到客户端上，客户端虽然加密传输了 SQL 语句，但是在程序运行的时候，内部肯定还是要解密成明文来校验的，那么可以尝试使用 ollydbg 来调试程序，从程序运行过程中读取到他解密后的内容

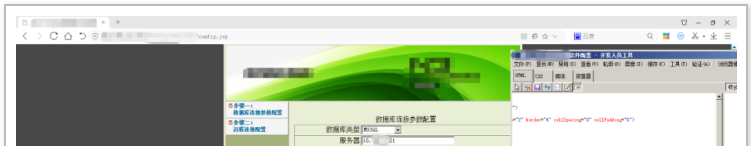


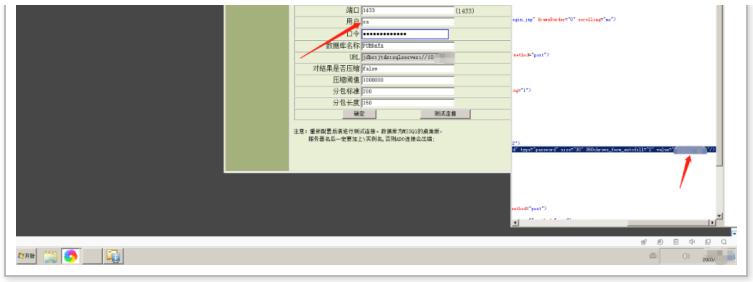






最终通过 OD 抓取到了系统管理员的密码，也成功登陆到了 Web 端的配置界面，在 Web 界面里可以看到使用的是 SQLServer 数据库，但是数据库是内网地址，密码可以通过 F12 直接查看到

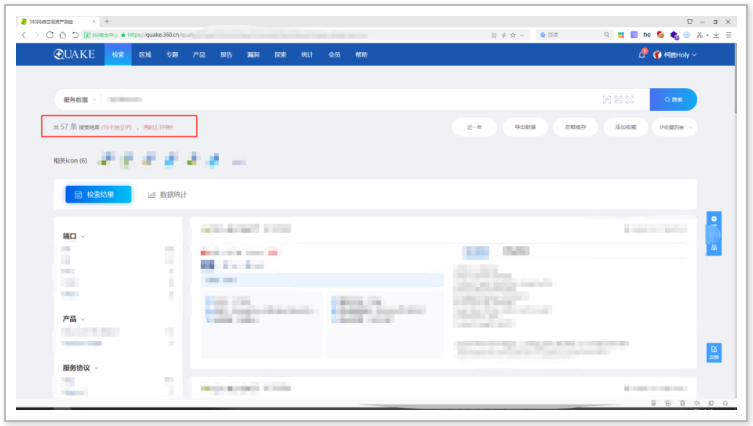




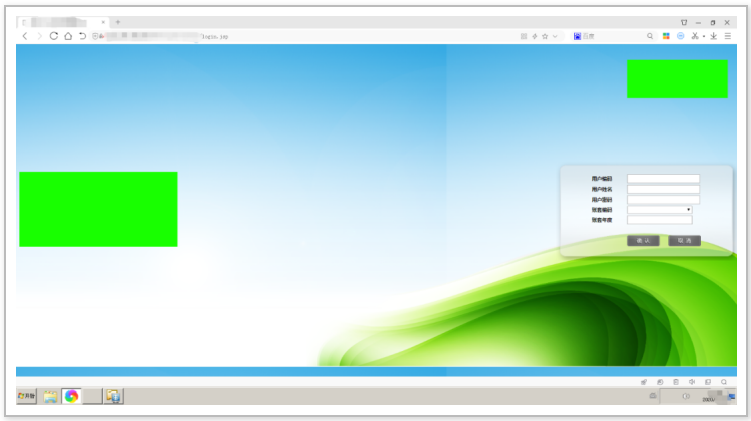
5

Quake 搜索

但是问题来了，数据库是内网，目前所拥有的洞并不足以链接到数据库，去反编译程序找加密算法又有点麻烦，回头看了眼 Dirsearch 的扫描结果，其中有 login 相关的接口，但是这个客户端明明只和 servlet 接口通讯，那么这套系统肯定还存在一个登陆接口，到 Index 页提取特征，使用 Quake 搜索互联网上的其他这台系统，还真找找不少

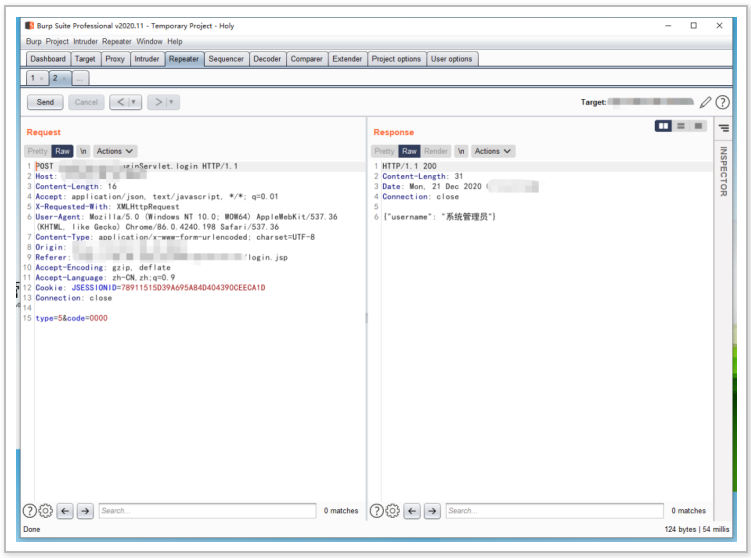


通过对互联网上其他这类系统的手工测试，果然发现存在一个 login.jsp 的登陆界面

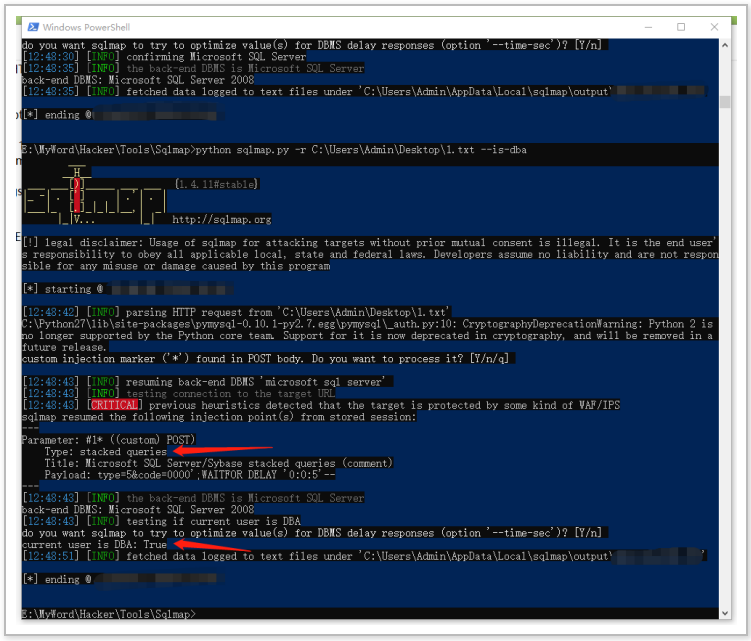


在 Web 登陆界面中，输入用户编码 0000，Web 页面也会直接返回用户姓名

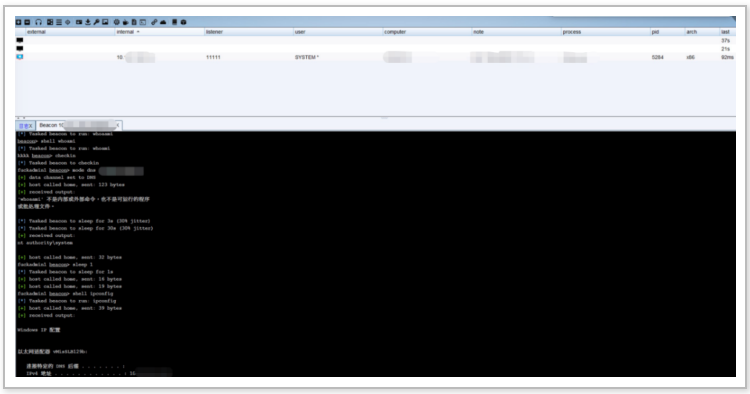
使用 Burp 抓包，将地址改为目标 IP，发现目标果然只是删除了登录页，但是接口还在



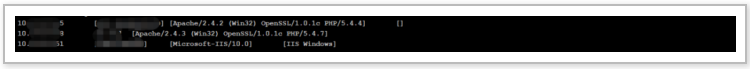
直接在 code 字段打上标识，SQLMAP 一把梭！



很舒服，SQLServer2008 的数据库，DBA 权限，堆叠查询，测试了下，目标只能 DNS 出网，CS 配置 DNS，直接上线！



内网简单的探测了下，因为客户没有授权，所以没有继续深入



6

总结

在这次渗透测试中，目标客户端虽然使用了加密传输，但是客户端本身未做反调试，可以通过 Od 直接附加进程。

客户服务器虽然限制了正常的出网，但是未对 DNS 协议进行限制，导致了 CS 使用 DNS 协议直接上线。

在 Quake 寻找互联网类似系统进行测试找 SQL 注入

纯粹是因为我对逆向还不是很熟。

如果是换成其他对逆向比较熟悉的师傅，完全可以做到逆向客户端找到加密算法，来实现 SQL 命令任意执行。

全文完

本文由 简悦 SimpRead 优化，用以提升阅读体验

使用了 全新的简悦词法分析引擎 beta，点击查看详细说明