专注APT攻击与防御

https://micropoor.blogspot.com/

任务背景：

需要得知周某某的今年采购的其中一个项目具体信息，目前已知该成员是xxx电网。负责丰满大坝的采购人员。整体思路如下：

找到开发公司，得到源码，审计问题，得到shell，拿到服务器，得到域控（或者终端管理）。得到个人机。下载任务文件。

得知该电网公司电网相关网站是某公司出品，得到某公司对外宣传网站，并且得到该公司服

务器权限，下载源码模板。

源码审计：

全局共计2个主要文件，分别是Func on.asp，Startup.asp

后台验证项：Function.asp来源验证：

注入验证：

（目标服务器waf，遂放弃）

错误处理：

XSS字符处理：

直接输入admin/下文件名处理：

目录生成：针对iis6以及iis7 php版本

Startup.asp

配置文件：当不可以执行的时候，是否可以备份出数据库，以便下载。

关于新闻显示，全局incude head.asp

其中check\_si.asp 主要为防止注入Get注入

Post 注入 新版本中加入post注入

过程中遇到服务器卡顿现象，也就是不清楚列名数，本地二分法测试如下：

在admin 目录下有个database.asp文件

目标测试：

根据以上信息，构造referrer，构造参数，禁止js。产生出越权漏洞。

根据越权漏洞，继续看upload.asp文件，允许匿名上传图片文件。在根据越权漏洞备份出webshell文件

82：

得到webshell

对方没有开启远程桌面：

开启：REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG\_DWORD /d 00000000 /f

通过该服务器得到mssql 数据库。得到终端管理权限。

查看在线机器，查找目标人物。

推送payload 反弹。

确定是否为目标人物：采购员 桌面截图

按照任务 取得该人员的其中一个xls文件

任务完成。

Micropoor