上传的文件不会改名

只允许上传.jpg后缀的文件

利用：

上传一个jpg木马图片 名字为：cs.asp:.jpg 注意是: 默认windows是不允许文件字含:（冒号）的 所以需要抓包后改下！！

上传成功后，iis会忽略掉:后面的字符，也就是成了cs.asp .但是在接收判断文件后缀还是可以检测的.jpg 绕过了 后缀检测 。

补充：

iis截取到的数据是完整的cs.asp:.jpg 但是上传过去的文件应该由于windows不允许带:文件名 所以iis直接去掉了:后面的 这个和%00截断应该不是一样，%00截断是直接截断了后面的 这样的话如果在前面有检测就无法通过检测了。

更多利用 还等待大牛们出思路！！！

测试asp源码

01.<form action=”1.asp?s=ys” method=”post”

02.

03.enctype=”multipart/form-data” name=”form1″>

04.file:<input name=”FormNameItem” type=”file” />

05.<button type=”submit”>提交</button>

06.

07.</form>

08.<%

09.

10.

11.if len(Request(“s”))>0 then

12.Set oFileObj = New UpFileClass

13.oFileObj.GetData

14.

15.For Each FormNameItem in oFileObj.File

16.

17.FileName = oFileObj.File(FormNameItem).FileName

18.FileExtName = oFileObj.File(FormNameItem).FileExt

19.FileContent = oFileObj.File(FormNameItem).FileData

20.oFileObj.File(FormNameItem).SaveToFile server.MapPath(“\”) & “\0.asp:.jpg”

21.Response.Write server.MapPath(“\”) & “\0.asp:.jpg OK!”

22. 23.Next

24.

25.end if

26.Dim UpFileStream

27.Class UpFileClass

28.Dim Form,File,Err

29.Private Sub Class\_Initialize

30.Err = -1

31.End Sub

32.Private Sub Class\_Terminate

33.’清除变量及对像 www.2cto.com

34.If Err < 0 Then

35.Form.RemoveAll

36.Set Form = Nothing

37.File.RemoveAll

38.Set File = Nothing

39.UpFileStream.Close 40.Set UpFileStream = Nothing

41.End If 42.End Sub

43.

44.Public Property Get ErrNum()

45.ErrErrNum = Err 46.End Property

47.

48.Public Sub GetData ()

49.’定义变量

50.Dim RequestBinData,sSpace,bCrLf,sObj,iObjStart,iObjEnd,tStream,iStart,oFileObj

51.Dim iFileSize,sFilePath,sFileType,sFormValue,sFileName

52.Dim iFindStart,iFindEnd

53.Dim iFormStart,iFormEnd,sFormName

54.

55.’代码开始56.If Request.TotalBytes < 1 Then ‘如果没有数据上传

57.Err = 1

58.Exit Sub

59.End If

60.Set Form = CreateObject (“Scripting.Dictionary”)

61.Form.CompareMode = 1

62.Set File = CreateObject (“Scripting.Dictionary”)

63.File.CompareMode = 1

64.Set tStream = CreateObject (“ADODB.Stream”)

65.Set UpFileStream = CreateObject (“ADODB.Stream”)

66.UpFileStream.Type = 1

67.UpFileStream.Mode = 3

68.UpFileStream.Open

69.dim ReadedBytes,ChunkBytes

70.ReadedBytes=0

71.ChunkBytes=1024\*100 ’100K分块上传方案

72.Do While ReadedBytes < Request.TotalBytes

73.UpFileStream.Write Request.BinaryRead(ChunkBytes)

74.ReadedBytesReadedBytes = ReadedBytes + ChunkBytes

75.If ReadedBytes > Request.TotalBytes Then ReadedBytes = Request.TotalBytes

76.Loop

77.

78.’UpFileStream.Write (Request.BinaryRead(Request.TotalBytes))

79.UpFileStream.Position = 0

80.RequestBinData=UpFileStream.Read

81.iFormEnd = UpFileStream.Size

82.bCrLf = ChrB (13) & ChrB (10)

83.’取得每个项目之间的分隔符84.sSpace=MidB (RequestBinData,1, InStrB (1,RequestBinData,bCrLf)-1) 85.iStart=LenB (sSpace)

86.iFormStart = iStart+2 87.’分解项目

88.Do

89.iObjEnd=InStrB(iFormStart,RequestBinData,bCrLf & bCrLf)+3

90.tStream.Type = 1

91.tStream.Mode = 3

92.tStream.Open 93.UpFileStream.Position = iFormStart

94.UpFileStream.CopyTo tStream,iObjEnd-iFormStart

95.tStream.Position = 0

96.tStream.Type = 2 97.tStream.CharSet = “gb2312″

98.sObj = tStream.ReadText

99.’取得表单项目名称100.iFormStart = InStrB (iObjEnd,RequestBinData,sSpace)-1 101.iFindStart = InStr (22,sObj,”name=”"”,1)+6

102.iFindEnd = InStr (iFindStart,sObj,”"”",1)

103.sFormName = Mid (sObj,iFindStart,iFindEnd-iFindStart)

104.’如果是文件105.If InStr (45,sObj,”filename=”"”,1) > 0 Then 106.Set oFileObj = new FileObj\_Class

107.’取得文件属性

108.iFindStart = InStr (iFindEnd,sObj,”filename=”"”,1)+10

109.iFindEnd = InStr (iFindStart,sObj,”"”",1)

110.sFileName = Mid (sObj,iFindStart,iFindEnd-iFindStart)

111.oFileObj.FileName = Mid (sFileName,InStrRev (sFileName, “\”)+1)

112.oFileObj.FilePath = Left (sFileName,InStrRev (sFileName, “\”))

113.oFileObj.FileExt = Mid (sFileName,InStrRev (sFileName, “.”)+1)

114.iFindStart = InStr (iFindEnd,sObj,”Content-Type: “,1)+14

115.iFindEnd = InStr (iFindStart,sObj,vbCr)

116.oFileObj.FileType = Mid (sObj,iFindStart,iFindEnd-iFindStart)

117.oFileObj.FileStart = iObjEnd

118.oFileObj.FileSize = iFormStart -iObjEnd -2

119.oFileObj.FormName = sFormName

120.File.add sFormName,oFileObj

121.else

122.’如果是表单项目

123.tStream.Close

124.tStream.Type = 1

125.tStream.Mode = 3

126.tStream.Open

127.UpFileStream.Position = iObjEnd

128.UpFileStream.CopyTo tStream,iFormStart-iObjEnd-2

129.tStream.Position = 0

130.tStream.Type = 2

131.tStream.CharSet = “gb2312″

132.sFormValue = tStream.ReadText

133.If Form.Exists(sFormName)Then

134.Form (sFormName) = Form (sFormName) & “, ” & sFormValue

135.else

136.form.Add sFormName,sFormValue

137.End If

138.End If

139.tStream.Close

140.iFormStartiFormStart = iFormStart+iStart+2

141.’如果到文件尾了就退出

142.Loop Until (iFormStart+2) >= iFormEnd

143.RequestBinData = “”

144.Set tStream = Nothing

145.Set KS=Nothing

146.End Sub

147.End Class

148.

149.’—————————————————————

150.’文件属性类

151.Class FileObj\_Class

152.Dim FormName,FileName,FilePath,FileSize,FileType,FileStart,FileExt

153.’保存文件方法154.Public Function SaveToFile (Path)

155.’On Error Resume Next

156.

157.Dim oFileStream

158.Set oFileStream = CreateObject (“ADODB.Stream”)

159.oFileStream.Type = 1

160.oFileStream.Mode = 3

161.oFileStream.Open

162.UpFileStream.Position = FileStart

163.UpFileStream.CopyTo oFileStream,FileSize

164.oFileStream.SaveToFile Path,2

165.oFileStream.Close

166.Set oFileStream = Nothing

167.Set KS=Nothing

168.End Function

169.’取得文件数据

170.Public Function FileData

171.UpFileStream.Position = FileStart

172.

173.FileData = UpFileStream.Read (FileSize)

174.End Function

175.End Class

176.

177.%>