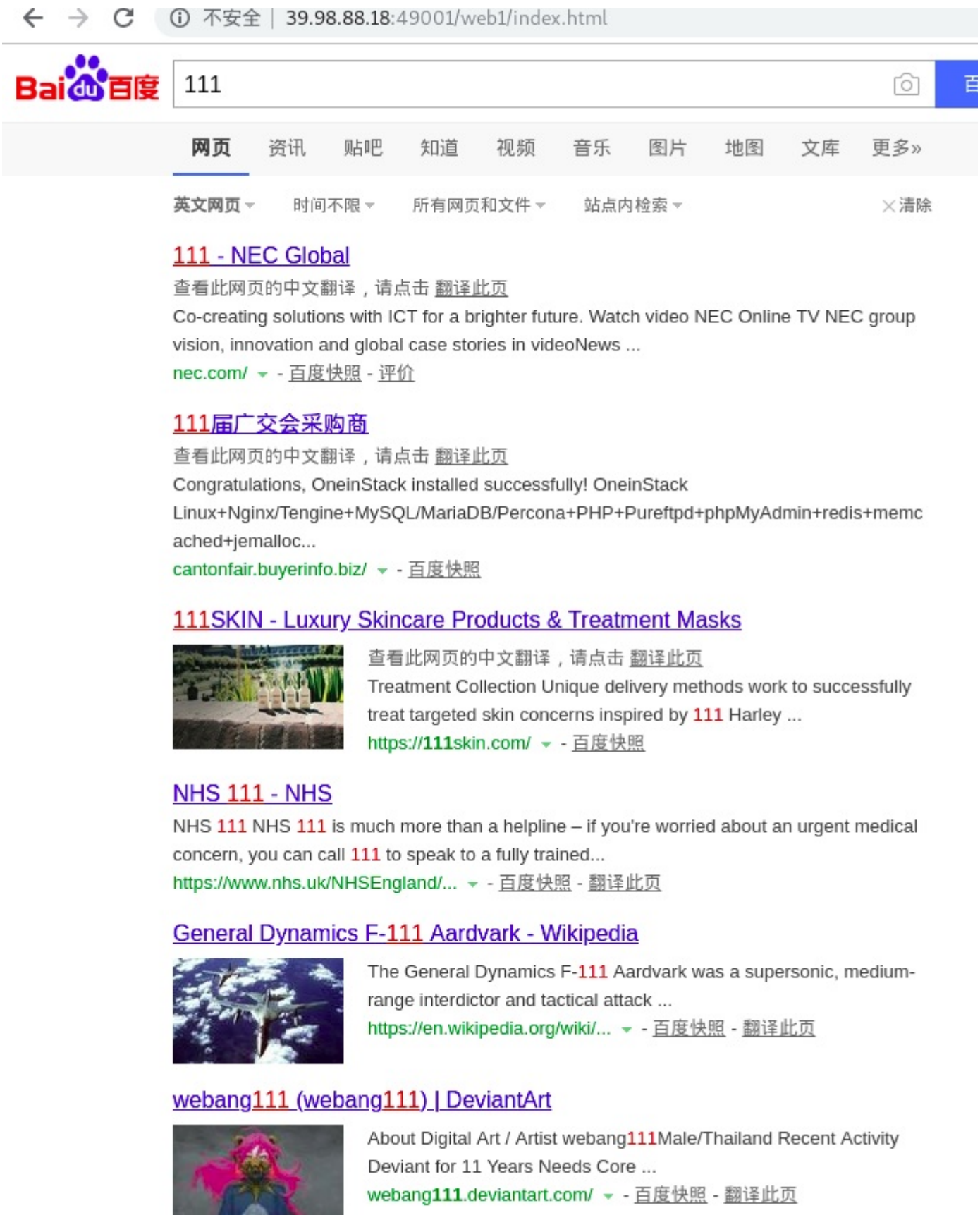
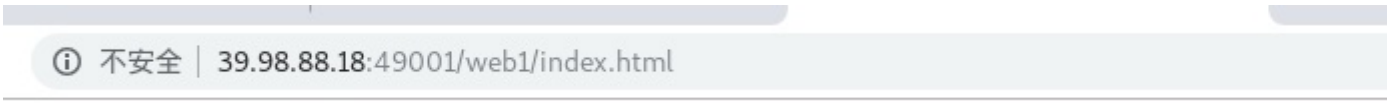
玄魂 - CTF(HTML基础WP)

HTML签到提

1 . 打开题目发现是一个百度的界面

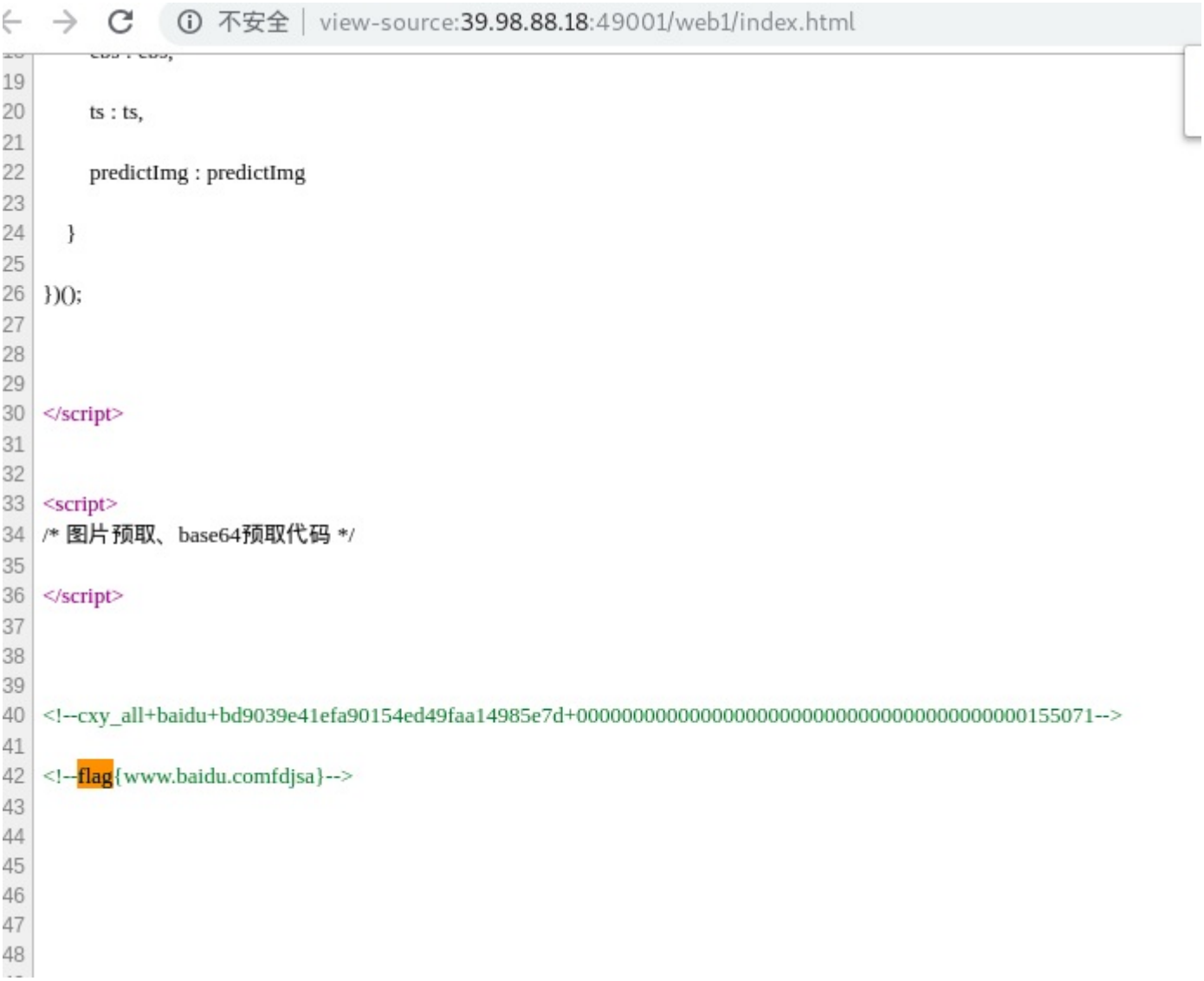


2 ．通过链接可以判断这是一个假的



3．查看源码

4．ctrl+f，然后输入flag进行搜索，成功发现flag.



html2

1．右键查看源码

2．发现在源码底部有一个js.flag

```
140     </div>
141 </div>
142 <div class="bg_b">
143     <div class="i_head"><a href="">关于我们</a><em> </em></div>
144     <dl class="i_mb clearfix">
145         <dt><a href=""><img src="Assets/upload/pic2.jpg" alt=""/></a></dt>
146         <dd>
147             <p>本公司成立于2011年，是一家OEM ODM类型企业，以出口为主，主要生产吉他功放机，吉他音箱，舞台
    备。出口产品销往世界各地。公司通过CEC UL UDE KCC CCC等认证。主要客户来自欧美 韩国.主要产品BLACK ST
148         </dd>
149     </dl>
150 </div>
151 <!--主体盒子-->
152 <!--底部-->
153 <div class="f_bg">
154     <div class="foot">
155         <div class="f_nav">
156             <a href="">法律申明</a>  |  
157             <a href="">隐私保护</a>  |  
158             <a href="">联系我们</a>
159         </div>
160     </div>
161 </div>
162 <!--底部-->
163 <script type="text/javascript" src="/js/ads/disou.js"></script>
164 <script type="text/javascript" src="/js/tongji.js"></script>
165 <script type="text/javascript" src="Assets/js/flag.js"></script>
166 </body>
```

39.98.88.18:49001/web2/Assets/js/flag.js

3.点击进去，成功发现flag

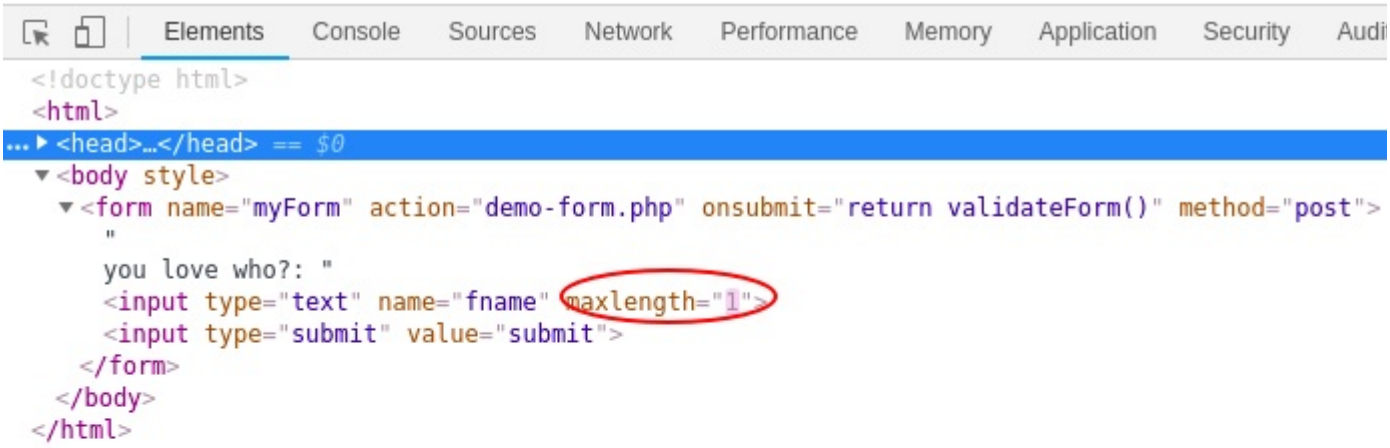
flag{wo_ai_xuan_huan_da}

jsjsjs

方法一

1.进入以后发现限制输入长度为 1 位

2 ．按F12，找到控制长度的maxlength



3.双击它，然后将其修改为100

```
<html>
▶ <head>…</head>
▼ <body style>
  ▼ <form name="myForm" action="demo-form.php" onsubmit="return validateForm()" method="post">
      "
      you love who?: "
      <input type="text" name="fname" maxlength="100"> == $0
      <input type="submit" value="submit">
    </form>
  </body>
</html>
```

4.然后题目问的是你爱谁，看到上方的xuanhun，输入。验证成功

方法二

1．题目为jsjs。故猜测此题与js有关。

2．因js文件也是传输到本地由浏览器执行。故右键，然后查看源码。

3．发现有一个js文件

```
id>
ta charset="utf-8">
e>xuanhun</title>
ad>
id>
ipt type="text/javascript" src="dsajldfafdas/1.js"></script>
ad>
ly>

m name="myForm" action="demo-form.php" onsubmit="return validateForm()" method="post">
love who?: <input type="text" name="fname" maxlength="1">
ut type="submit" value="submit">
rm>
```

4．点击查看，成功发现flag.

```
function validateForm(){
var x=document.forms["myForm"]["fname"].value;
if (x=="xuanhun"){
alert("flag{123qwewqeq}");
  }
}
```

小结

CTF（web和内网渗透系列教程）的清单请在“https://github.com/xuanhun/HackingResource”

查看，定时更新最新章节✓链接

答疑、辅导请加入玄魂工作室--安全圈，一起成长探讨更私密内容。微信扫码了解详情：

星主： 程序员－玄魂

星球： 玄魂工作室-安全圈

知识星球

长按扫码预览社群内容
和星主关系更近一步

及时获取更多消息，请关注微信订阅号