

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

[111 - NEC Global](#)

查看此网页的中文翻译, 请点击 [翻译此页](#)

Co-creating solutions with ICT for a brighter future. Watch video NEC Online TV NEC group vision, innovation and global case stories in videoNews ...

[nec.com/](#) ▾ - [百度快照](#) - [评价](#)

[111届广交会采购商](#)

查看此网页的中文翻译, 请点击 [翻译此页](#)

Congratulations, OneinStack installed successfully! OneinStack
Linux+Nginx/Tengine+MySQL/MariaDB/Percona+PHP+Pureftpd+phpMyAdmin+redis+memcached+jemalloc...

[cantonfair.buyerinfo.biz/](#) ▾ - [百度快照](#)

[111SKIN - Luxury Skincare Products & Treatment Masks](#)



查看此网页的中文翻译, 请点击 [翻译此页](#)

Treatment Collection Unique delivery methods work to successfully treat targeted skin concerns inspired by 111 Harley ...

<https://111skin.com/> ▾ - [百度快照](#)

[NHS 111 - NHS](#)

NHS 111 NHS 111 is much more than a helpline – if you're worried about an urgent medical concern, you can call 111 to speak to a fully trained...

<https://www.nhs.uk/NHSEngland/...> ▾ - [百度快照](#) - [翻译此页](#)

[General Dynamics F-111 Aardvark - Wikipedia](#)



The General Dynamics F-111 Aardvark was a supersonic, medium-range interdictor and tactical attack ...

<https://en.wikipedia.org/wiki/...> ▾ - [百度快照](#) - [翻译此页](#)

[webang111 \(webang111\) | DeviantArt](#)



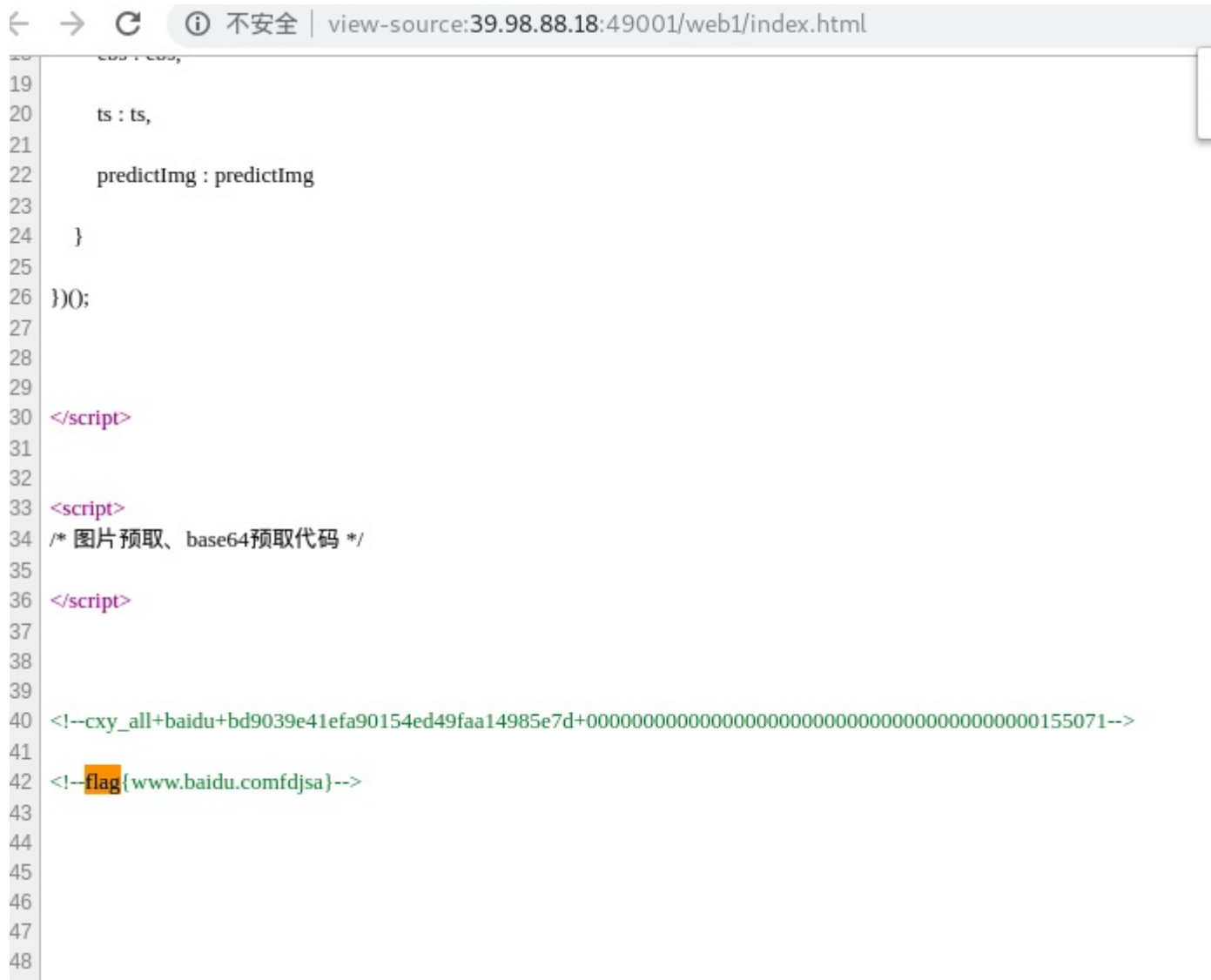
About Digital Art / Artist webang111Male/Thailand Recent Activity
Deviant for 11 Years Needs Core ...

<webang111.deviantart.com/> ▾ - [百度快照](#) - [翻译此页](#)

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

[illegible]

3.点击进去，成功发现flag

flag{wo ai xuan huan da}

jsjsjs

方法一

2. 按F12, 找到控制长度的maxlength

you love who?:

```
Elements Console Sources Network Performance Memory Application Security Audi
<!doctype html>
<html>
... ▶ <head>...</head> == $0
▼ <body style>
  ▼ <form name="myForm" action="demo-form.php" onsubmit="return validateForm()" method="post">
    "
    you love who?: "
    <input type="text" name="fname" maxlength="1">
    <input type="submit" value="submit">
  </form>
</body>
</html>
```

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

```

<html>
  <head>
    <meta charset="utf-8">
    <title>xuanhun</title>
  </head>
  <body>
    <script type="text/javascript" src="dsajldfadas/1.js"></script>
    <form name="myForm" action="demo-form.php" onsubmit="return validateForm()" method="post">
      you love who?: <input type="text" name="fname" maxlength="1">
      <input type="submit" value="submit">
    </form>
  </body>
</html>

```

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

