

1.2 前端基础

1.2.0 前言

本次讲从实战的角度去讲解关于的html、css、以及javascript CTF实战题的做法。在我们浏览网页的过程中，html、css、javascript代码回直接发送到我们的客户端。故此类试题比较简单。

1.2.1 内容、展现和行为

前端代码的运行环境是浏览器，标准的前端语言只有Html、Css和Javascript。一般情况下，这些代码保存在服务端，通过http (https)传输到浏览器上。Html定义了要显示的内容，文档结构，可以理解为骨架。CSS定义了显示的样式，可以理解为衣服。想要执行动态更新样式，响应用户操作，和服务端交互，都需要JavaScript。



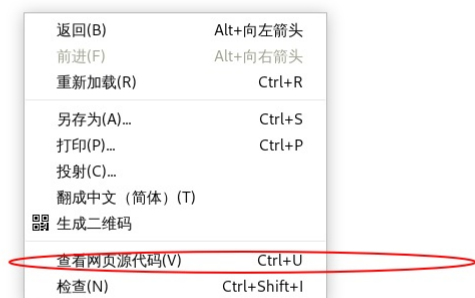
一篇文章不能讲述所有基层内容，希望大家去找相关的入门教程学习。

因为代码都是拉取到浏览来解析执行的，所以针对前端代码的任何加密和防护手段在浏览器端都是无效的。学会通过浏览器来完成渗透测试任务是必要的基本功。以Chrome为例，其开发者工具非常强大，可以动态修改内容，调试JavaScript，进行性能、安全性测试，配合代理可以完成任何前端任务。这里推荐一个官方教程的翻译版：

<https://www.css88.com/doc/chrome-devtools/>

△本行辦理C、D、E、F、G、H、I、J、K、L、M、N、O、P、Q、R、S、T、U、V、W、X、Y、Z、AA、AB、AC、AD、AE、AF、AG、AH、AI、AJ、AK、AL、AM、AN、AO、AP、AQ、AR、AS、AT、AU、AV、AW、AX、AY、AZ、BA、BB、BC、BD、BE、BF、BG、BH、BI、BJ、BK、BL、BM、BN、BO、BP、BQ、BR、BS、BT、BU、BV、BW、BX、BY、BZ、CA、CB、CC、CD、CE、CF、CG、CH、CI、CJ、CK、CL、CM、CN、CO、CP、CQ、CR、CS、CT、CU、CV、CW、CX、CY、CZ、DA、DB、DC、DD、DE、DF、DG、DH、DI、DJ、DK、DL、DM、DN、DO、DP、DQ、DR、DS、DT、DU、DV、DW、DX、DY、DZ、EA、EB、EC、ED、EE、EF、EG、EH、EI、EJ、EK、EL、EM、EN、EO、EP、EQ、ER、ES、ET、EU、EV、EW、EX、EY、EZ、FA、FB、FC、FD、FE、FF、FG、FH、FI、FJ、FK、FL、FM、FN、FO、FP、FQ、FR、FS、FT、FU、FV、FW、FX、FY、FZ、GA、GB、GC、GD、GE、GF、GG、GH、GI、GJ、GK、GL、GM、GN、GO、GP、GQ、GR、GS、GT、GU、GV、GW、GX、GY、GZ、HA、HB、HC、HD、HE、HF、HG、HH、HI、HJ、HK、HL、HM、HN、HO、HP、HQ、HR、HS、HT、HU、HV、HW、HX、HY、HZ、IA、IB、IC、ID、IE、IF、IG、IH、II、IJ、IK、IL、IM、IN、IO、IP、IQ、IR、IS、IT、IU、IV、IW、IX、IY、IZ、JA、JB、JC、JD、JE、JF、JG、JH、JI、JJ、JK、JL、JM、JN、JO、JP、JQ、JR、JS、JT、JU、JV、JW、JX、JY、JZ、KA、KB、KC、KD、KE、KF、KG、KH、KI、KJ、KK、KL、KM、KN、KO、KP、KQ、KR、KS、KT、KU、KV、KW、KX、KY、KZ、LA、LB、LC、LD、LE、LF、LG、LH、LI、LJ、LK、LL、LM、LN、LO、LP、LQ、LR、LS、LT、LU、LV、LW、LX、LY、LZ、MA、MB、MC、MD、ME、MF、MG、MH、MI、MJ、MK、ML、MM、MN、MO、MP、MQ、MR、MS、MT、MU、MV、MW、MX、MY、MZ、NA、NB、NC、ND、NE、NF、NG、NH、NI、NJ、NK、NL、NM、NN、NO、NP、NQ、NR、NS、NT、NU、NV、NW、NX、NY、NZ、OA、OB、OC、OD、OE、OF、OG、OH、OI、OJ、OK、OL、OM、ON、OO、OP、OQ、OR、OS、OT、OU、OV、OW、OX、OY、OZ、PA、PB、PC、PD、PE、PF、PG、PH、PI、PJ、PK、PL、PM、PN、PO、PP、PQ、PR、PS、PT、PU、PV、PW、PX、PY、PZ、QA、QB、QC、QD、QE、QF、QG、QH、QI、QJ、QK、QL、QM、QN、QO、QP、QQ、QR、QS、QT、QU、QV、QW、QX、QY、QZ、RA、RB、RC、RD、RE、RF、RG、RH、RI、RJ、RK、RL、RM、RN、RO、RP、RQ、RR、RS、RT、RU、RV、RW、RX、RY、RZ、SA、SB、SC、SD、SE、SF、SG、SH、SI、SJ、SK、SL、SM、SN、SO、SP、SQ、SR、SS、ST、SU、SV、SW、SX、SY、SZ、TA、TB、TC、TD、TE、TF、TG、TH、TI、TJ、TK、TL、TM、TN、TO、TP、TQ、TR、TS、TT、TU、TV、TW、TX、TY、TZ、UA、UB、UC、UD、UE、UF、UG、UH、UI、UJ、UK、UL、UM、UN、UO、UP、UQ、UR、US、UT、UU、UV、UW、UX、UY、UZ、VA、VB、VC、VD、VE、VF、VG、VH、VI、VJ、VK、VL、VM、VN、VO、VP、VQ、VR、VS、VT、VU、VV、VW、VX、VY、VZ、WA、WB、WC、WD、WE、WF、WG、WH、WI、WJ、WK、WL、WM、WN、WO、WP、WQ、WR、WS、WT、WU、WV、WW、WX、WY、WZ、XA、XB、XC、XD、XE、XF、XG、XH、XI、XJ、XK、XL、XM、XN、XO、XP、XQ、XR、XS、XT、XU、XV、XW、XX、XY、XZ、YA、YB、YC、YD、YE、YF、YG、YH、YI、YJ、YK、YL、YM、YN、YO、YP、YQ、YR、YS、YT、YU、YV、YW、YX、YY、YZ、ZA、ZB、ZC、ZD、ZE、ZF、ZG、ZH、ZI、ZJ、ZK、ZL、ZM、ZN、ZO、ZP、ZQ、ZR、ZS、ZT、ZU、ZV、ZW、ZX、ZY、ZZ

404.html ☆ ABP



```

1 <html>
2 <body>
3 <center><h1>404 Not Found</h1></center>
4 <p hidden>flag{qwjdsklafjdfadfa}</p>
5 </body>
6 </html>
7
```

2.查看引用文件 有时可能需要点击网站引用css文件或者其他引用文件才会发现提示信息或者flag。

```

<ol id="billBox" class="bill_box">
</ol>
</div>
<div id="moveInfo" class="move_info"> </div>
</div>
<script src="js/common.js"></script>
<script src="js/play.js"></script>
<script src="js/AI.js"></script>
<script src="js/bill.js"></script>
<script src="js/[abcmlvx1f2)ctff0-9]{3}.js"></script>
<script src="js/gambit.js"></script>
<div style="text-align:center;clear:both">
<p>适用浏览器：360、Firefox、Chrome、Safari、Opera、傲游、搜狗、世界之窗。不支持IE8及以下
```

1.2.3 操作js

直接查看

```

通过直接查看。即可获得到flag。
if ($('#input').val() != code && code != 9999) {
    alert("flag{CTF-bugku-0032}");
} else {
```

修改js

有些试题可能通过js来限制用户的某些输入，比如限制输入的长度。比如下面这道题。

56+74=?

验证

根据提示进行计算，却发现只可以输入一位。摁F12。

56+74=?2验证

来源:BugKu-ctf

```

<!doctype html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head></head>
<body style=
<span id="code" class="code" style="background: rgb(79, 236, 74); color: rgb(240, 213, 120);">56+74=?</span>
<input type="text" class="input" maxlength="1">
<button id="check">验证</button>
<div style="text-align:center;"></div>
<script src="js/jquery-1.12.3_min.js"></script>
<script type="text/javascript" src="js/code.js"></script>
</body>
</html>
```

发现其限制最大输入长度为一位。点击进行修改。

56+74=?

2

验证

来源:BugKu-ctf

body | 1424 x 64

Elements Console Sources Network Performance Memory Application Security Audits Adblock Plus

```
<!doctype html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>_</head>
  <body style=
    <span id="code" class="code" style="background: rgb(79, 236, 74); color: rgb(240, 213, 120);">56+74=?</span>
    <input type="text" class="input" maxlength="1" == $0
    <button id="check">验证</button>
    <div style="text-align:center;">_</div>
    <script src="js/jquery-1.12.3.min.js"></script>
    <script type="text/javascript" src="js/code.js"></script>
  </body>
</html>
```

修改为10，然后重新输入计算结果。验证成功。

Elements Console Sources Network Performance Memory Application Security Audits Adblock Plus

```
<!doctype html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"
il xmlns="http://www.w3.org/1999/xhtml">
ead>_</head>
ody style>
:span id="code" class="code" style="background: rgb(79, 236, 74); color: rgb(240, 213, 120);">56+74=?</span>
:input type="text" class="input" maxlength="10" == $0
:button id="check">验证</button>
:div style="text-align:center;">_</div>
:script src="js/jquery-1.12.3.min.js"></script>
:script type="text/javascript" src="js/code.js"></script>
body>
ml>
```

知 域渗透初探 (二) : 域 × 知 域渗透初探 (一) : 域 × 随机数字运算验证码 × view-source:123.206.87.240:8002 × 123.206.87.240:8002 × +

← → ↻ ⚠ 不安全 | 123.206.87.240:8002/yanzhengma/

56+74=?

130

验证

123.206.87.240:8002 显示
flag{CTF-bugku-0032}

确定

Elements Console Sources Network Performance Memory Application Security Audits Adblock Plus

```
<!doctype html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>_</head>
  <body style=
    <span id="code" class="code" style="background: rgb(79, 236, 74); color: rgb(240, 213, 120);">56+74=?</span>
    <input type="text" class="input" maxlength="10" == $0
    <button id="check">验证</button>
    <div style="text-align:center;">_</div>
    <script src="js/jquery-1.12.3.min.js"></script>
    <script type="text/javascript" src="js/code.js"></script>
  </body>
</html>
```

Styles Computed Event Listeners >> 1

Filter :hov .cls

element.style {
}

.input {
 width: 100px;
} (index)

input {
 padding: 1px 0px;
} user agent stylesh

input {
 -webkit-appearance: textfield;
 background-color: white;
 -webkit-rtl-ordering: logical;
 cursor: text;
 padding: 1px;
 border-width: 2px;
 border-style: inset;
 border-color: initial;
 border-image: initial;
} user agent stylesh

另外在调试阶段，我们可以通过在控制台直接修改变量值。详情查看上面推荐的chrome开发者的教程。

禁用js

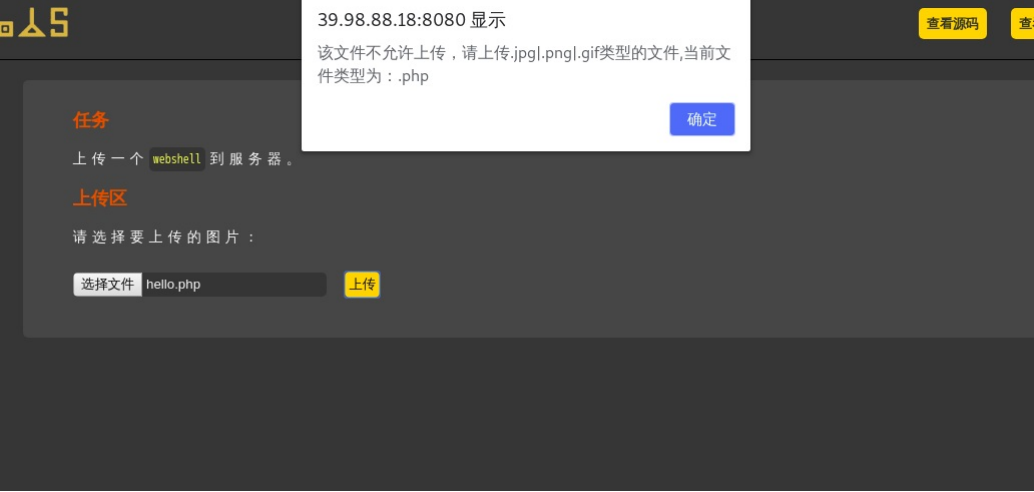
有写网站仅仅使用js做校验。比如文件上传时限制文件类型。此时我们可以直接禁用js来绕过。

比如靶场的第一关

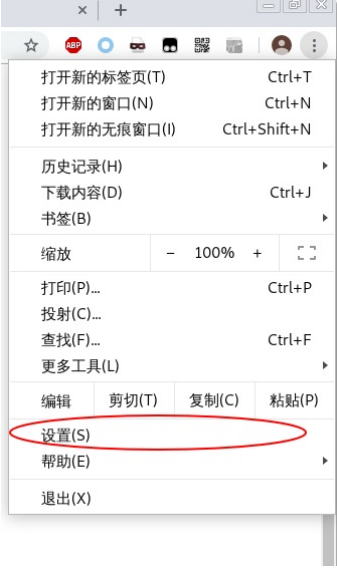
右键查看源码，发现它是通过js来做上传文件的校验。

```
<script type="text/javascript">
function checkFile() {
    var file = document.getElementsByName('upload_file')[0].value;
    if (file == null || file == "") {
        alert("请选择要上传的文件!");
        return false;
    }
    //定义允许上传的文件类型
    var allow_ext = ".jpg|.png|.gif";
    //提取上传文件的类型
    var ext_name = file.substring(file.lastIndexOf("."));
    //判断上传文件类型是否允许上传
    if (allow_ext.indexOf(ext_name) == -1) {
        var errMsg = "该文件不允许上传，请上传" + allow_ext + "类型的文件,当前文件类型为：" + ext_name;
        alert(errMsg);
        return false;
    }
}
}</script>
```

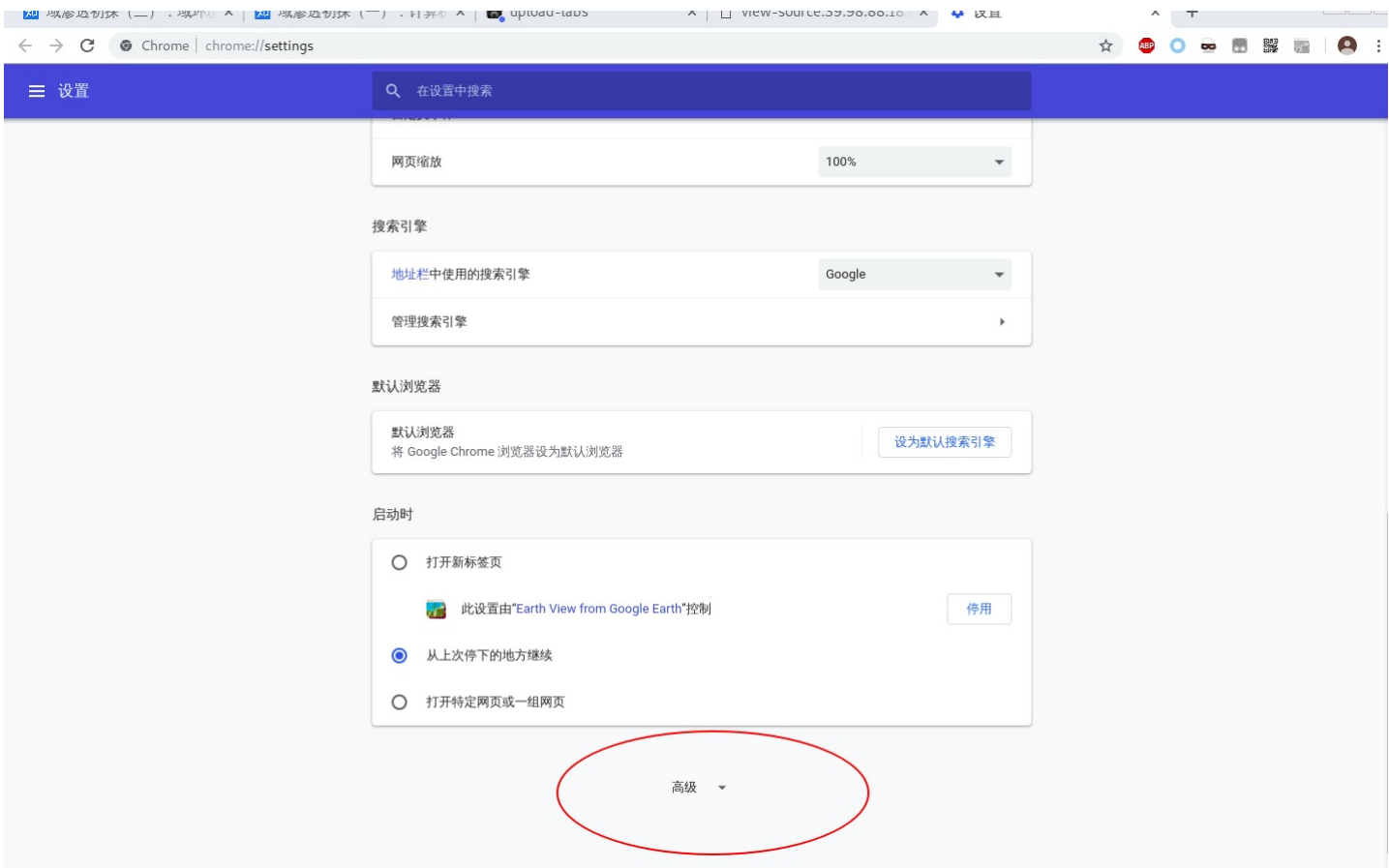
上传一个木马文件,发现禁止上传。仅允许上传图片文件。



浏览器禁止js运行。谷歌浏览器，点击右上角的三个点点。然后选择设置。



滑到底，然后选择高级。



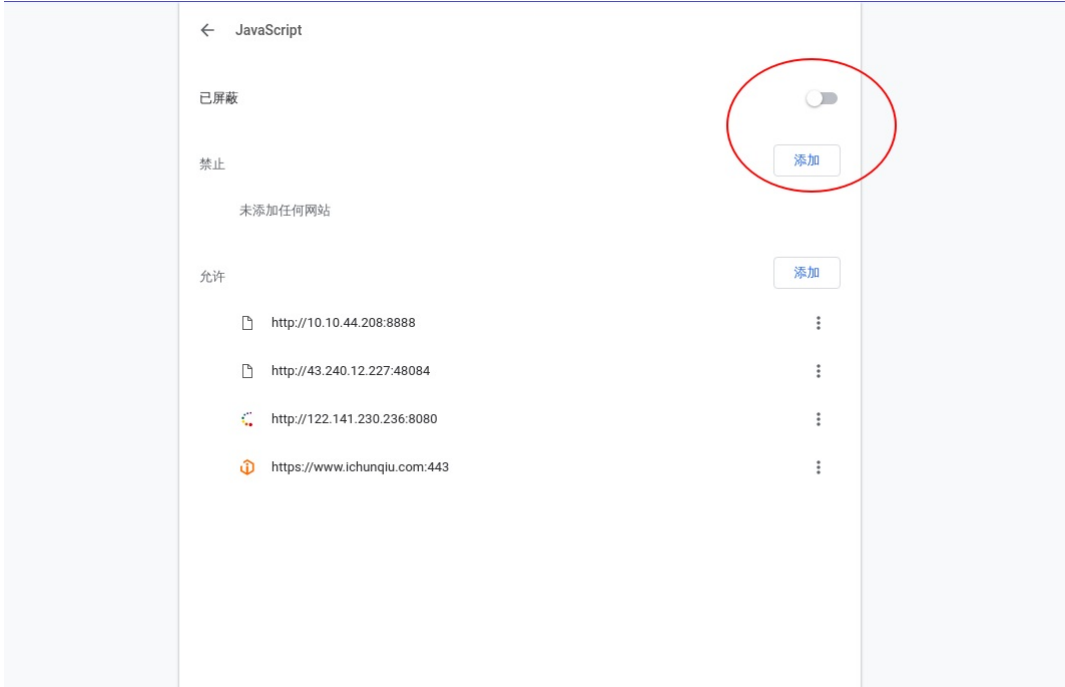
下滑，点击内容控制。



点击javascript.



点击右上方的开关。将其屏蔽掉。



然后我们再一次的上传木马，上传成功。



右键查看源码，发现文件路径


```
39 </div>
40 </div>
41
42 <div id="upload_panel">
43 <ol>
44 <li>
45 <h3>任务</h3>
46 <p>上传一个<code>webshell</code>到服务器。</p>
47 </li>
48 <li>
49 <h3>上传区</h3>
50 <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">
51 <p>请选择要上传的图片：<p>
52 <input class="input_file" type="file" name="upload_file"/>
53 <input class="button" type="submit" name="submit" value="上传"/>
54 </form>
55 <div id="msg">
56 </div>
57 <div id="img">
58  </div>
59 </li>
60 </ol>
61 </div>
62
63 </div>
64 <div id="footer">
```

1.2.3 课后习题

- 1.[html查看源码](#)
 - 2.[查看css文件](#)
 - 3.[修改查看js](#)
 - 4.[禁用js](#)
- 禁用js靶场地址：http://39.98.88.18:8080/upload/Pass-01/index.php

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
和星主关系更进一步

及时获取更多消息，请关注微信订阅号



玄魂工作室