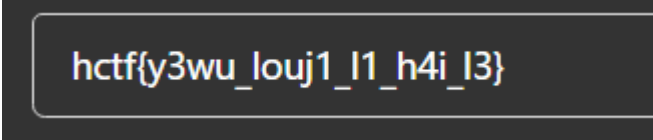


## LoRexxar 的渗透之战之二

根据 hint 业务逻辑漏洞，首先想到提交的 value 值存在漏洞

```
<input class="form-control" disabled="true" name="user" value="LoRexxar" type="text">  
<input class="form-control" style="display: none" name="user" value="LoRexxar" type="text">
```

在重置密码里，抓包，把 value 值改成 LoRexxar，改密码后就可以登上了,然后就看到 flag 了



hctf{y3wu\_louj1\_l1\_h4i\_l3}