你的名字 -- 题目指北

看来你真的很想知道提问者的名字hh

好吧。。。为了知道ta是谁，你不一定需要打穿这台服务器。你可以借助XSS进行钓鱼（真的还有那么好心的出题人把考点直接告诉你吗）

可能同学们并不熟悉CTF中前端题的机制，我这里简单介绍一下。

既然要钓鱼，就必须有人去点击页面。但是你真的忍心让bridge 24小时在电脑前帮你点链接吗 = =

为了达到模拟受害者的目的，CTF中通常会设置一个xss bot来访问钓鱼界面。以这一题为例：

当你回答好问题后，点击`让TA看看我的回答！`按钮，题目中的BOT就会以此问题提问者的身份去访问`/myasks`界面（即`我的提问`）查看你的回答。如果该页面存在xss漏洞，就很有可能造成信息泄露。而此问题的提问者用户名就是flag。

至于怎么在该页面制造xss并泄露信息，这就需要同学们自行发挥咯！

好吧 xD 测题的时候还是被 diss 难度太大555。能造成xss的可控制输入点`username`和`answer`是有过滤的。过滤函数如下

```
function checkUserName(username){
  return username.length<=10
}
```

```
async function sanitizeAnswer(questions){
    for(q of questions){
        // 把 < 替换成html实体 &lt;
        q.answer=q.answer.replace(/</g,'&lt;')
        // 这是后端的逻辑，并不重要hhh
        const askee=await usersDB.findOne({'userId':q.askeeId})
        q.askeeName=askee.username
    }
}
```

想想看怎么绕过呢？

最后最后，同学们可能需要用到信息外带（即把flag发送到远程服务器）。这里推荐一个比较稳定的webhook网站。

https://requestbin.com/r

亲测在本题环境中，http协议（把网站给你提供的https链接中的s去掉即可）GET方法可以接收到请求。

另外如果有条件代理的同学可以使用这个网站，更加稳定

https://webhook.site/

实在不行，可以google搜索`xss平台`。如果用不了google，可以试试这几个xss平台网站

https://xss8.cc/

https://xssaq.com/

http://xss.hwact.org/index.php?do=login

如果你觉得题目还有任何问题（which几乎肯定会有XD），请务必私聊我 qq: 1244992934

你的名字是？