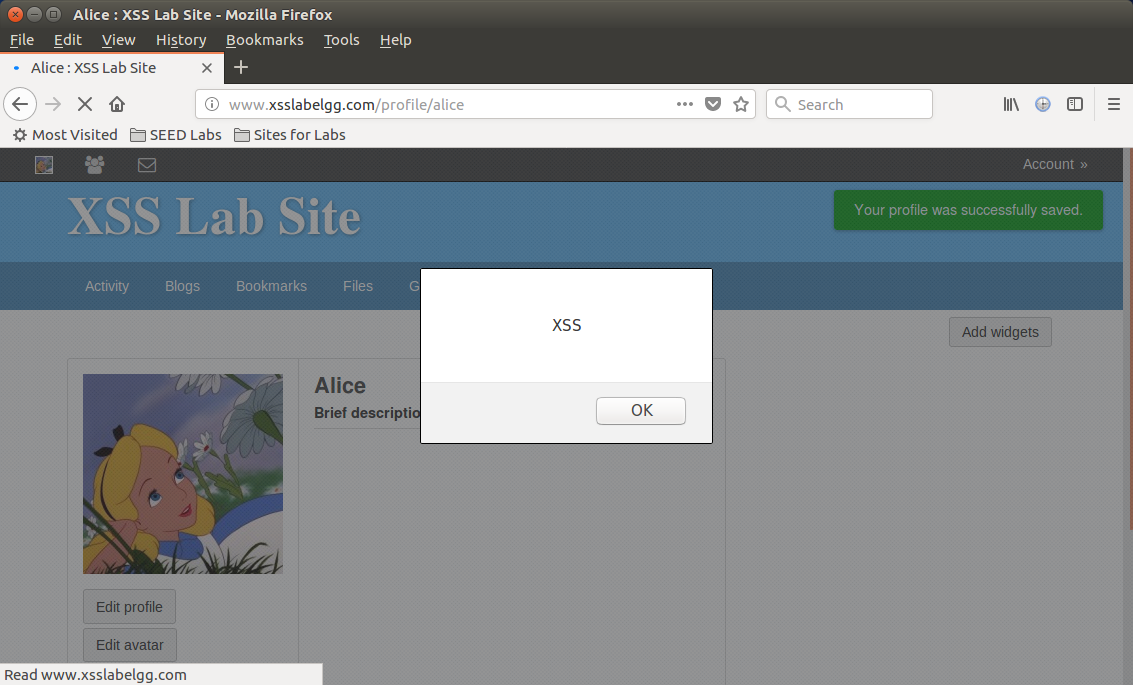
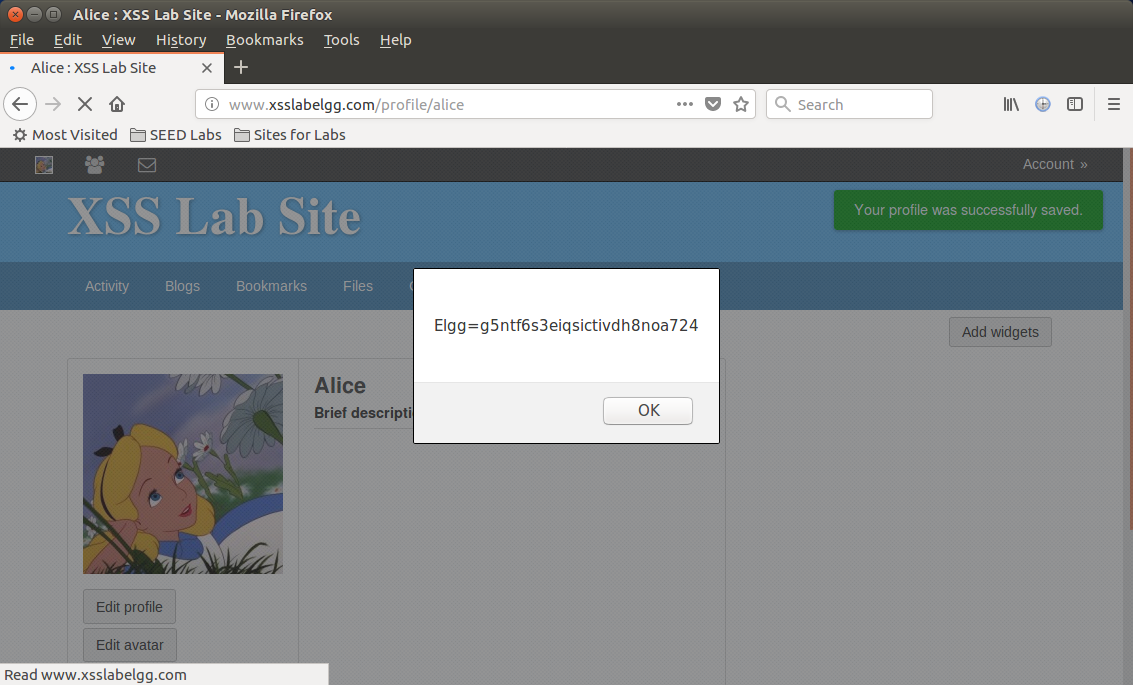
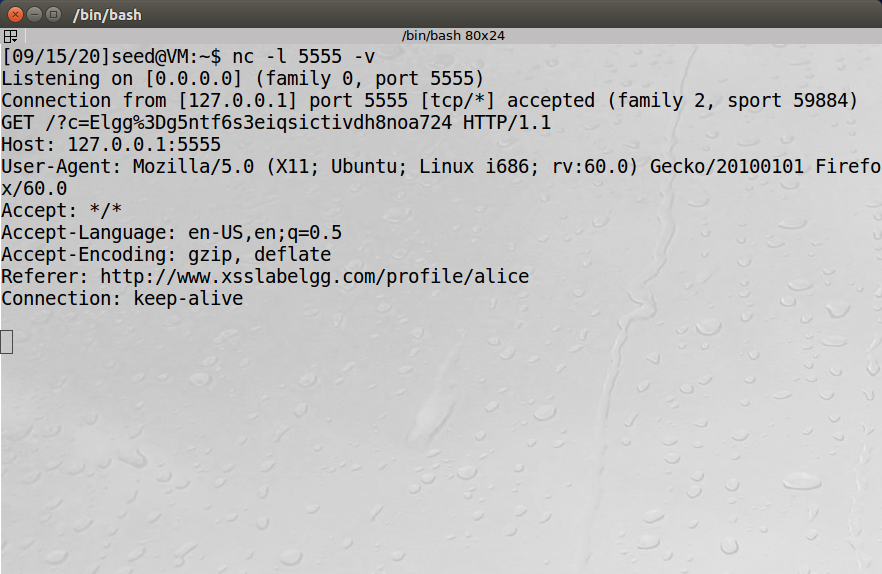
Task 1



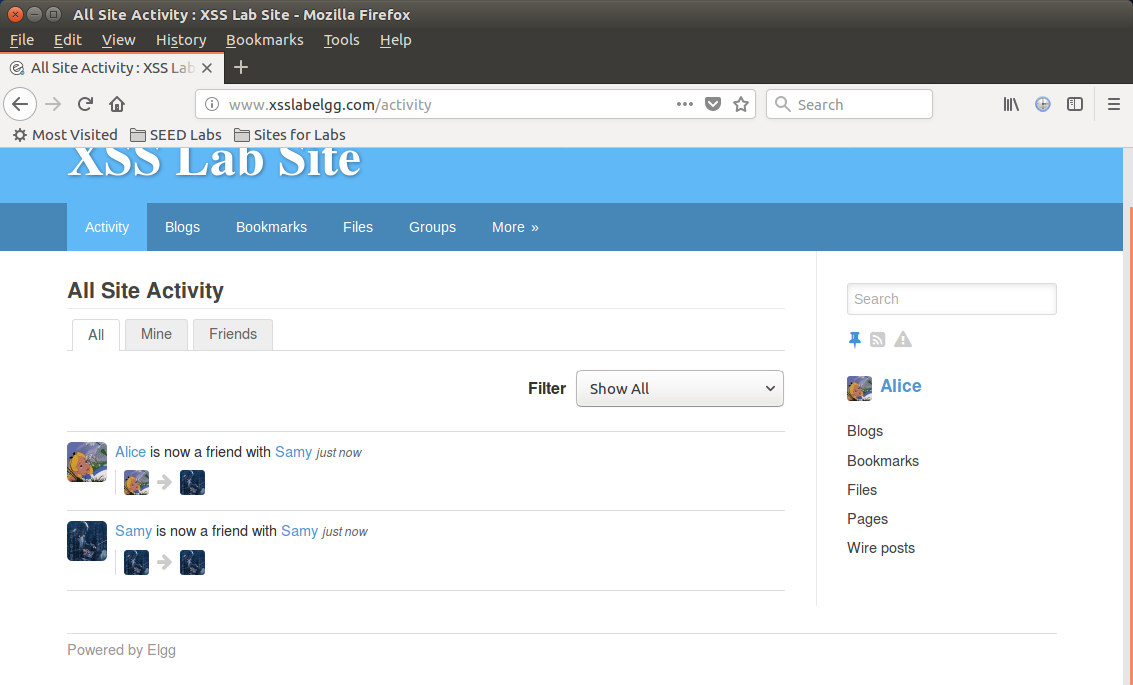
Task 2

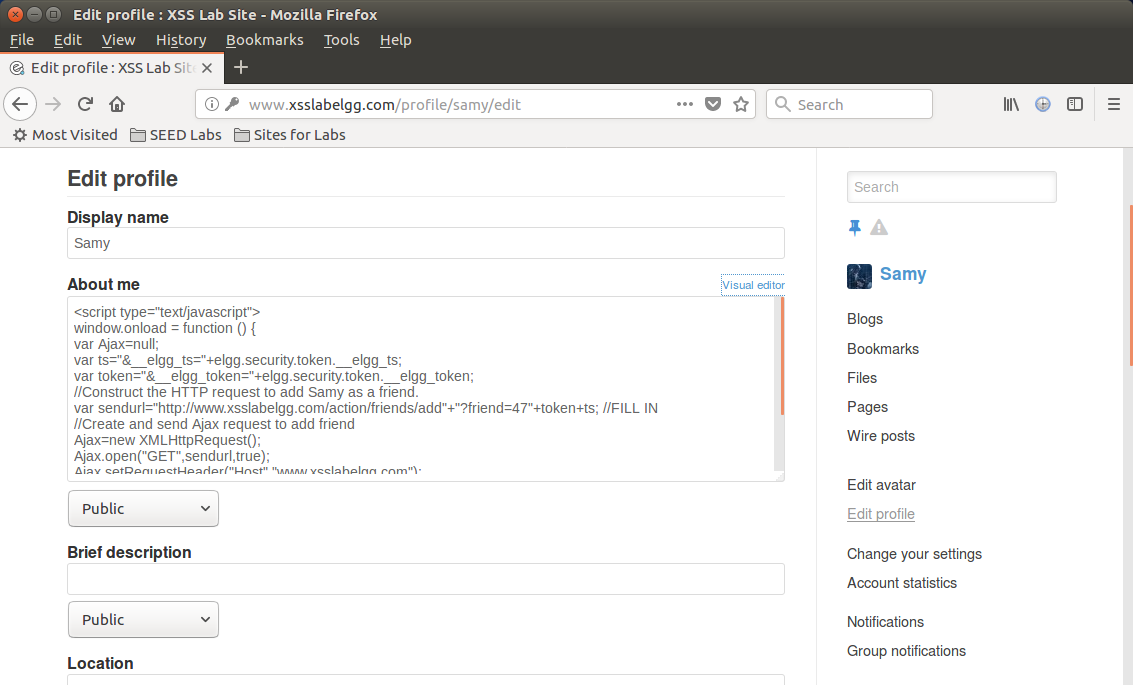


Task 3



Task 4

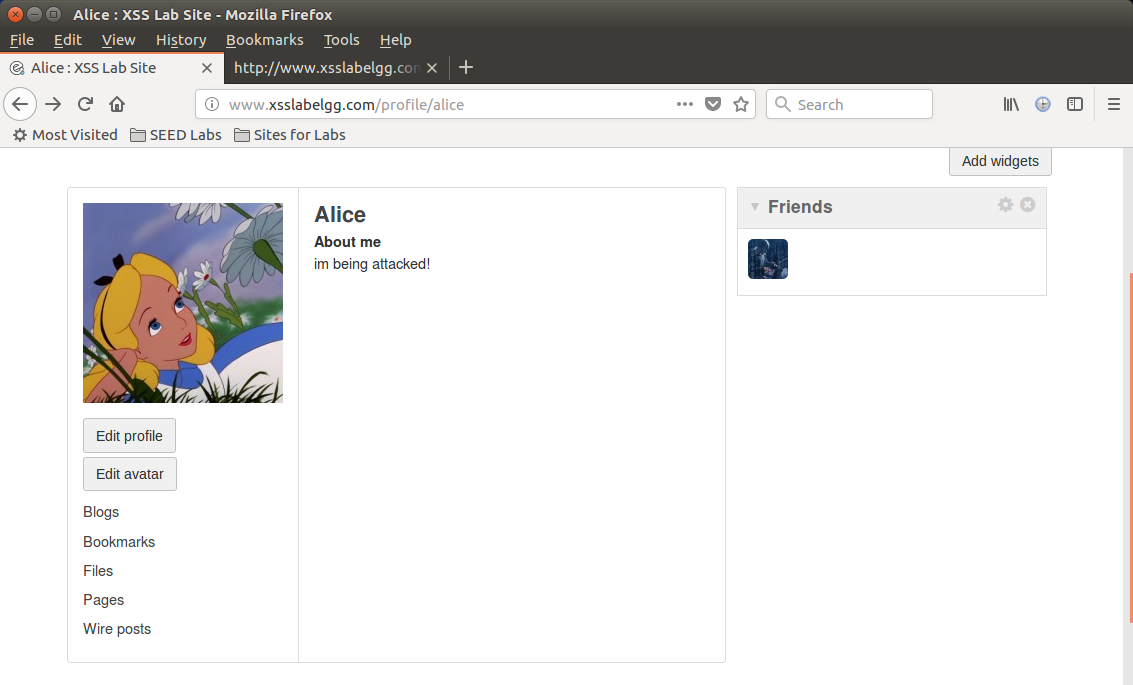


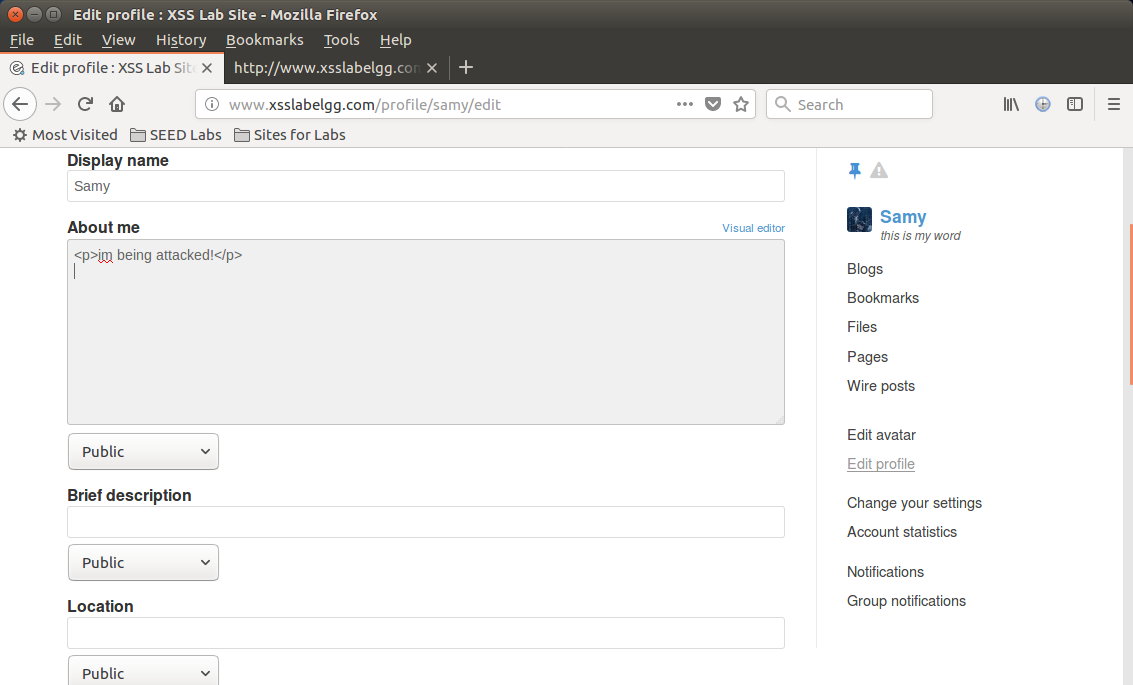


Ts和token是网站认证用户的手段，如果不加入http报文，网站将不会执行加好友操作。

不能，加入html的代码将会使得我们输入的代码变成文本在浏览器中显示而非执行。

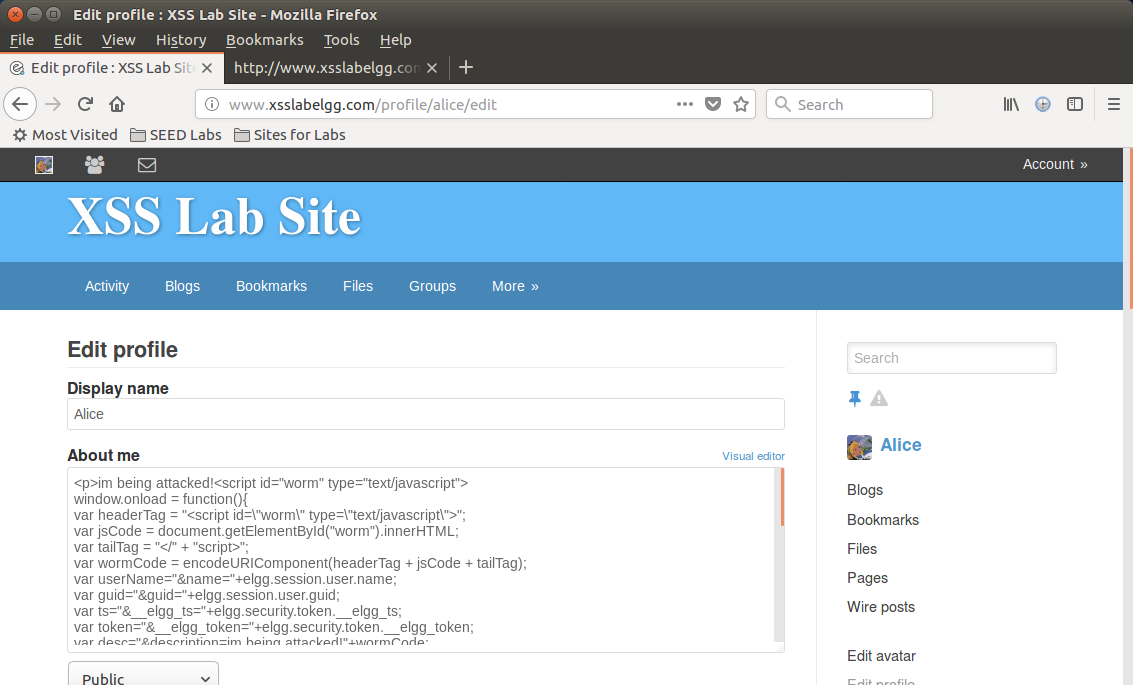
Task 5





攻击者访问自己的profile时也会被更改，导致无法再攻击他人

Task 6



增加了一个wormcode，就可以把自身复制到受害者的aboutme中

Task 7

