有条件限制 不一定所有验证Refere就可以绕过

## 1.Refere为空条件下

解决方案:

    利用[ftp://,http://,https://,file://,javascript:,data:](http://ftp/,http:/,https:/,file:/,javascript:,data:" \t "_blank)这个时候浏览器地址栏是file://开头的，如果这个HTML页面向任何http站点提交请求的话，这些请求的Referer都是空的。

    例:

    利用data:协议

<html>  
    <body>  
       <iframe src="data:text/html;base64,PGZvcm0gbWV0aG9kPXBvc3QgYWN0aW9uPWh0dHA6Ly9hLmIuY29tL2Q+PGlucHV0IHR5cGU9dGV4dCBuYW1lPSdpZCcgdmFsdWU9JzEyMycvPjwvZm9ybT48c2NyaXB0PmRvY3VtZW50LmZvcm1zWzBdLnN1Ym1pdCgpOzwvc2NyaXB0Pg==">  
    </body>   
</html>

    bese64编码 解码即可看到代码

  利用https协议

  https向http跳转的时候Referer为空

  拿一个https的webshell

  <iframe src="https://xxxxx.xxxxx/attack.php">

 attack.php写上CSRF攻击代码

## 2.判断Referer是某域情况下绕过

 比如你找的csrf是xxx.com  验证的referer是验证的\*.xx.com  可以找个二级域名 之后<img "csrf地址">  之后在把文章地址发出去 就可以伪造。

## 3.判断Referer是否存在某关键词

  referer判断存在不存在google.com这个关键词

  在网站新建一个google.com目录 把CSRF存放在google.com目录,即可绕过

## 4.判断referer是否有某域名

判断了Referer开头是否以126.com以及126子域名  不验证根域名为126.com 那么我这里可以构造子域名x.126.com.xxx.com作为蠕虫传播的载体服务器，即可绕过。