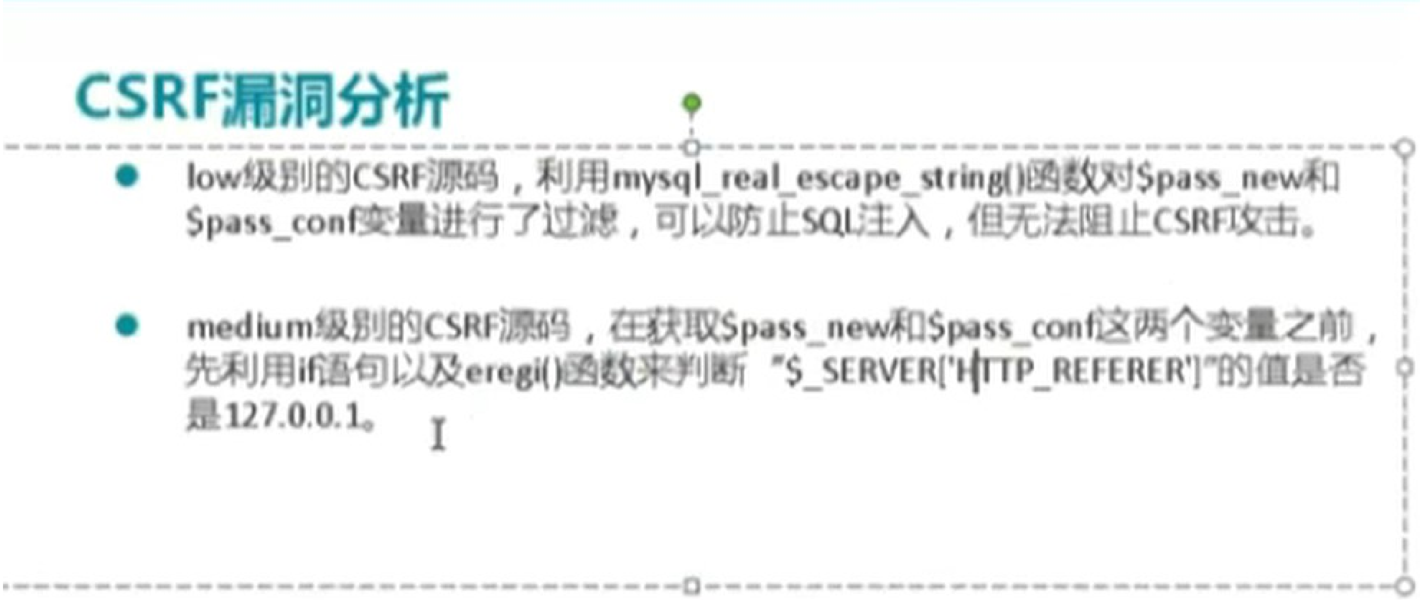
源码

低级

```
 <?php

    if (isset($_GET['Change'])) {

        // Turn requests into variables
        $pass_new = $_GET['password_new'];
        $pass_conf = $_GET['password_conf'];


        if (($pass_new == $pass_conf)){
            $pass_new = mysql_real_escape_string($pass_new);//防止sql注入的，这是！！
            $pass_new = md5($pass_new);//用MD5加密

            $insert="UPDATE `users` SET password = '$pass_new' WHERE user = 'admin';"
            $result=mysql_query($insert) or die('<pre>' . mysql_error() . '</pre>' );

            echo "<pre> Password Changed </pre>";
            mysql_close();
        }

        else{
            echo "<pre> Passwords did not match. </pre>";
        }

    }
?>
```

中级

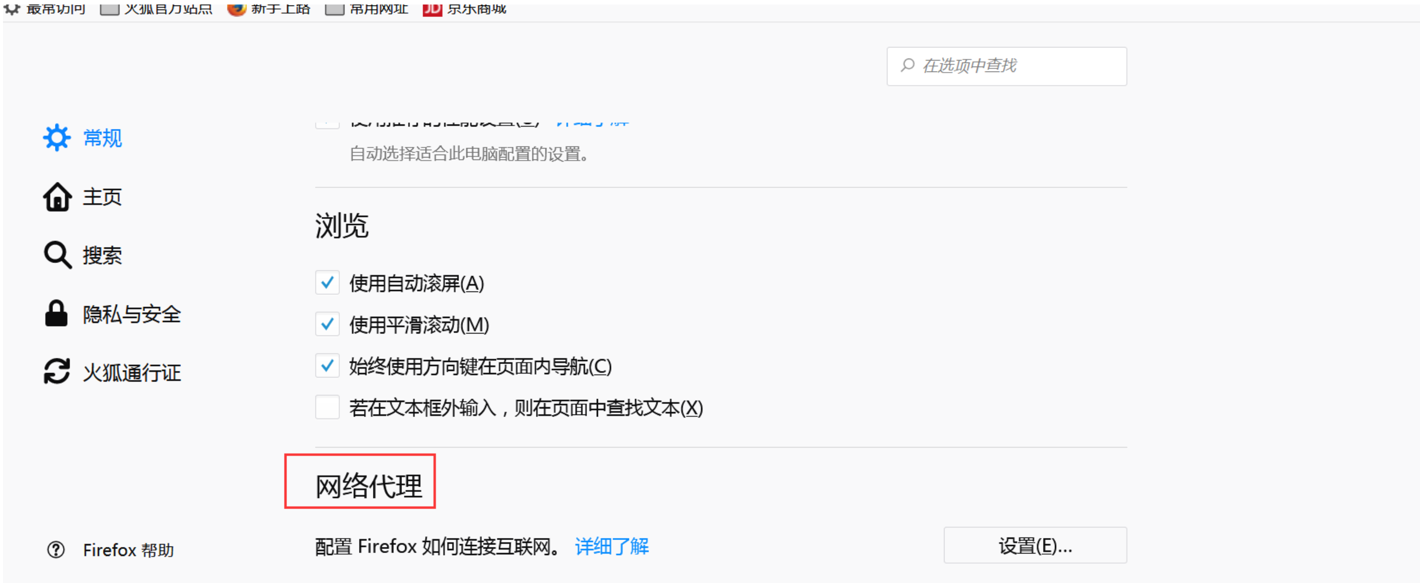
```php
<?php

    if (isset($_GET['Change'])) {//$_POST和$_GET皆为接收用户的数据的

        // Checks the http referer header
        if ( eregi ( "127.0.0.1", $_SERVER['HTTP_REFERER'] ) ){        //$_POST和$_GET

            // Turn requests into variables
            $pass_new = $_GET['password_new'];
            $pass_conf = $_GET['password_conf'];

            if ($pass_new == $pass_conf){
                $pass_new = mysql_real_escape_string($pass_new);
                $pass_new = md5($pass_new);

                $insert="UPDATE `users` SET password = '$pass_new' WHERE user = 'admi
                $result=mysql_query($insert) or die('<pre>' . mysql_error() . '</pre>

                echo "<pre> Password Changed </pre>";
                mysql_close();
            }

            else{
                echo "<pre> Passwords did not match. </pre>";
            }

        }

    }
?>
```



CSRF漏洞分析

- low级别的CSRF源码，利用mysql_real_escape_string()函数对$pass_new和$pass_conf变量进行了过滤，可以防止SQL注入，但无法阻止CSRF攻击。
- medium级别的CSRF源码，在获取$pass_new和$pass_conf这两个变量之前，先利用if语句以及eregi()函数来判断"$_SERVER['HTTP_REFERER']"的值是否是127.0.0.1。

可以设置代理:



□ 使用推荐的性能设置(U) 详细了解

自动选择适合此电脑配置的设置。

浏览

☑ 使用自动滚屏(A)

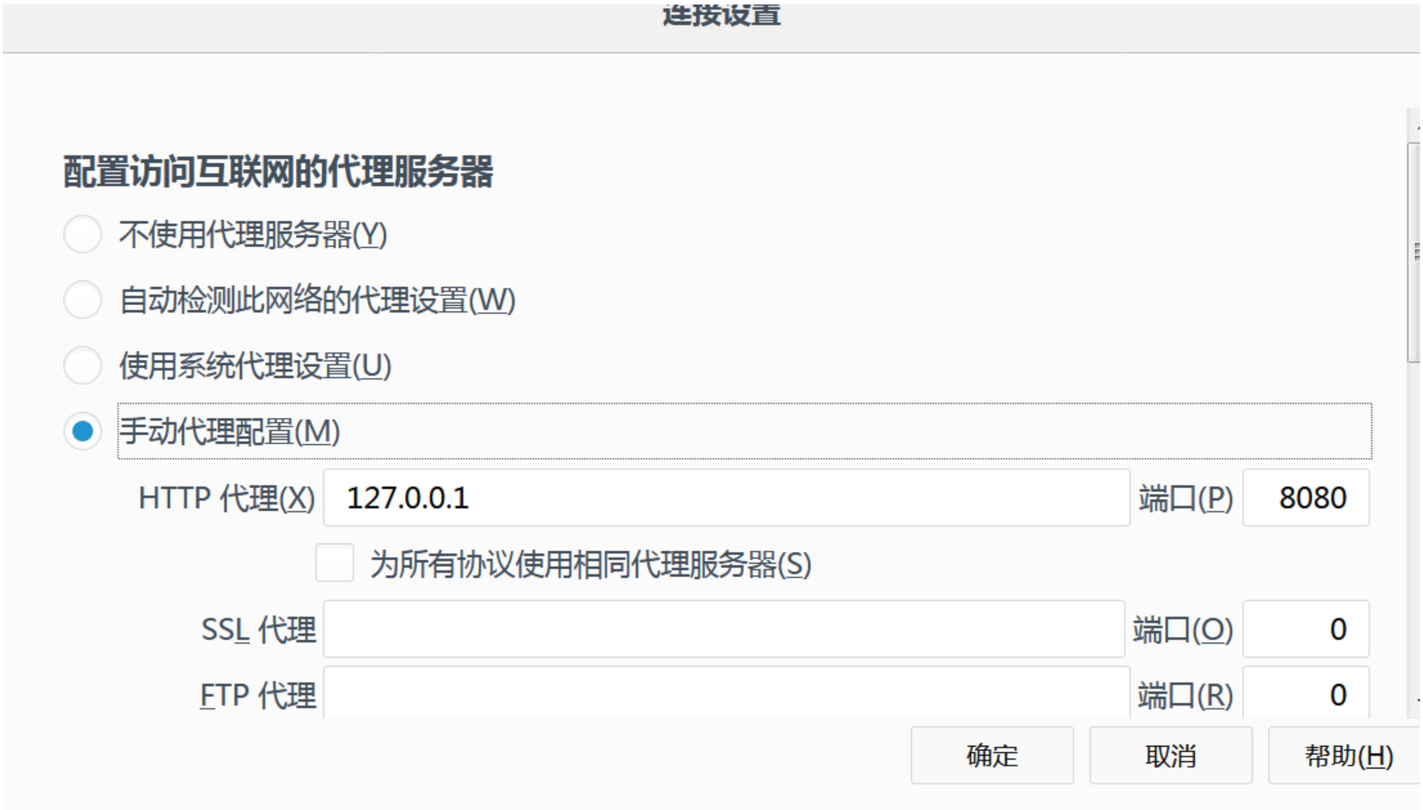
☑ 使用平滑滚动(M)

☑ 始终使用方向键在页面内导航(C)

□ 若在文本框外输入，则在页面中查找文本(X)

网络代理

配置 Firefox 如何连接互联网。 详细了解



配置访问互联网的代理服务器

○ 不使用代理服务器(Y)

○ 自动检测此网络的代理设置(W)

○ 使用系统代理设置(U)

● 手动代理配置(M)

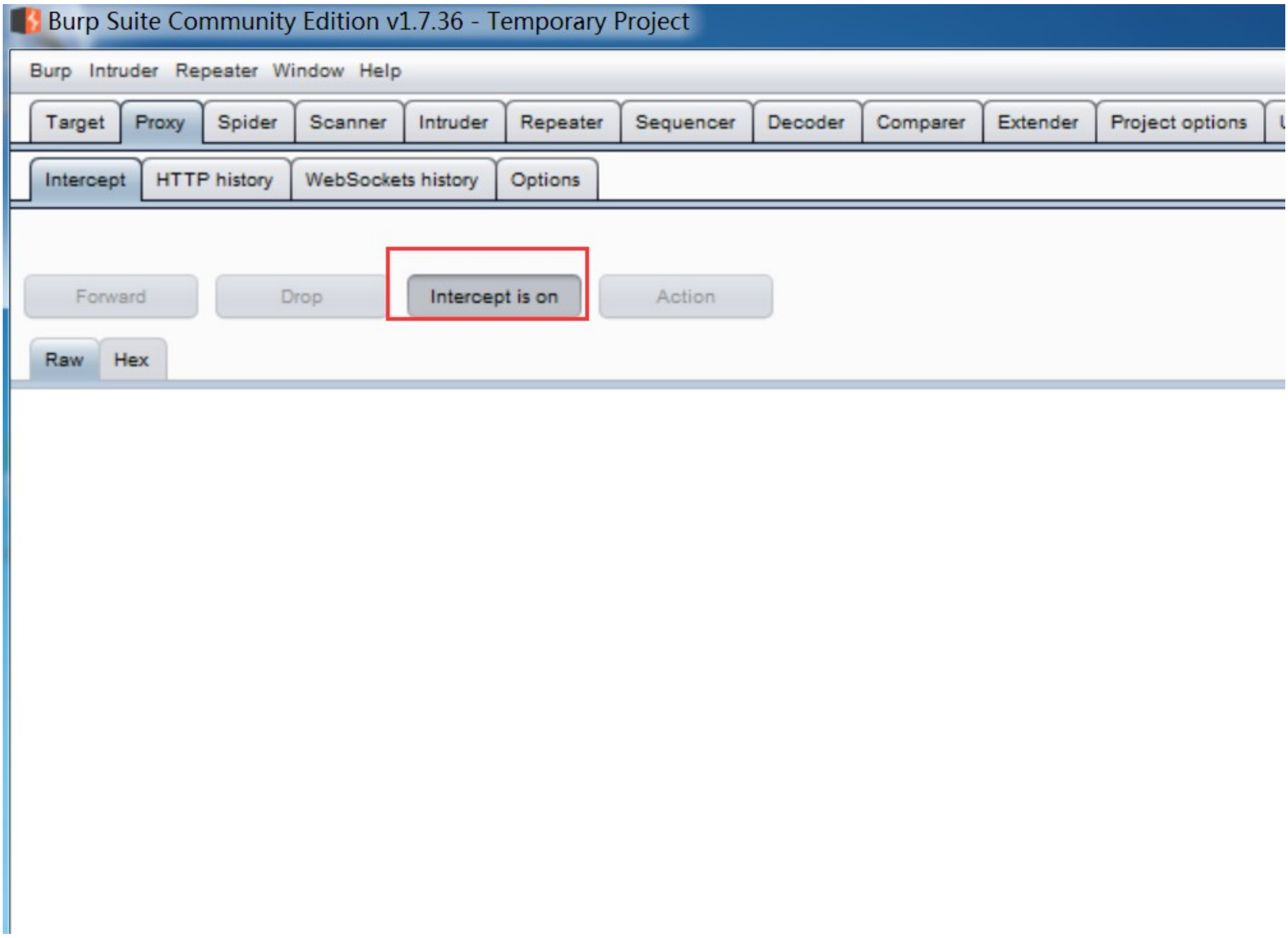
HTTP 代理(X) 127.0.0.1 端口(P) 8080

□ 为所有协议使用相同代理服务器(S)

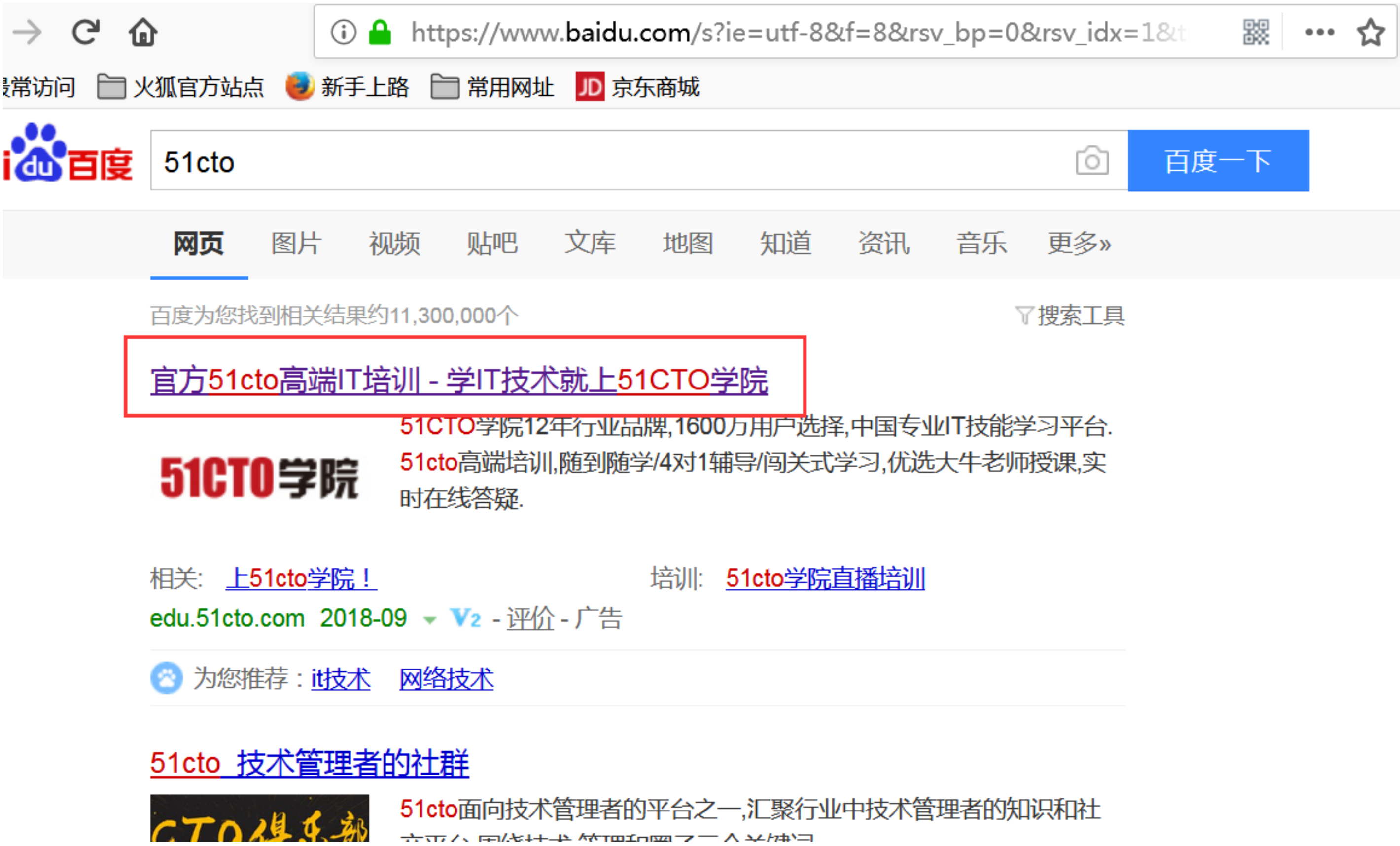
SSL 代理 端口(O) 0

FTP 代理 端口(R) 0

打开burp suite:


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Raw
Hex

点击一个链接:


https://www.baidu.com/s?ie=utf-8&f=8&rsv_bp=0&rsv_idx=1&t
常访问 火狐官方站点 新手上路 常用网址 京东商城
51cto
百度一下
网页 图片 视频 贴吧 文库 地图 知道 资讯 音乐 更多»
搜索工具

百度为您找到相关结果约11,300,000个

官方51cto高端IT培训 - 学IT技术就上51CTO学院

51CTO学院12年行业品牌,1600万用户选择,中国专业IT技能学习平台.51cto高端培训,随到随学/4对1辅导/闯关式学习,优选大牛老师授课,实时在线答疑.

相关: 上51cto学院！ 培训: 51cto学院直播培训

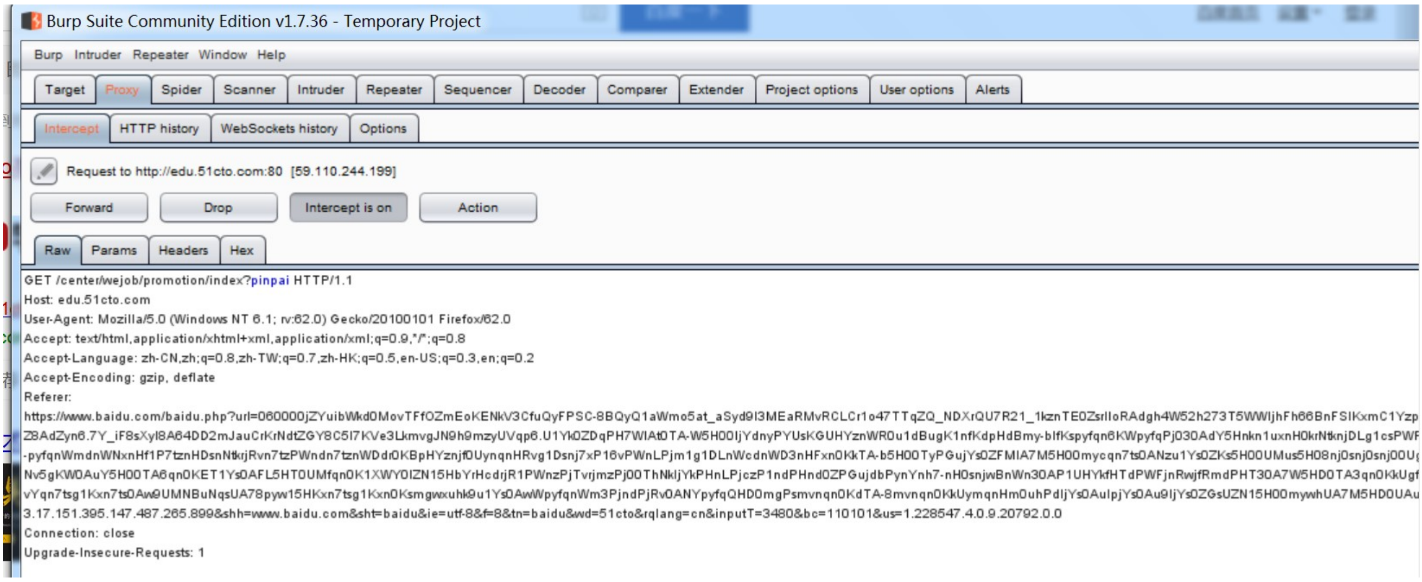
edu.51cto.com 2018-09 - 评价 - 广告

为您推荐：it技术 网络技术

51cto_技术管理者的社群

51cto面向技术管理者的平台之一,汇聚行业中技术管理者的知识和社

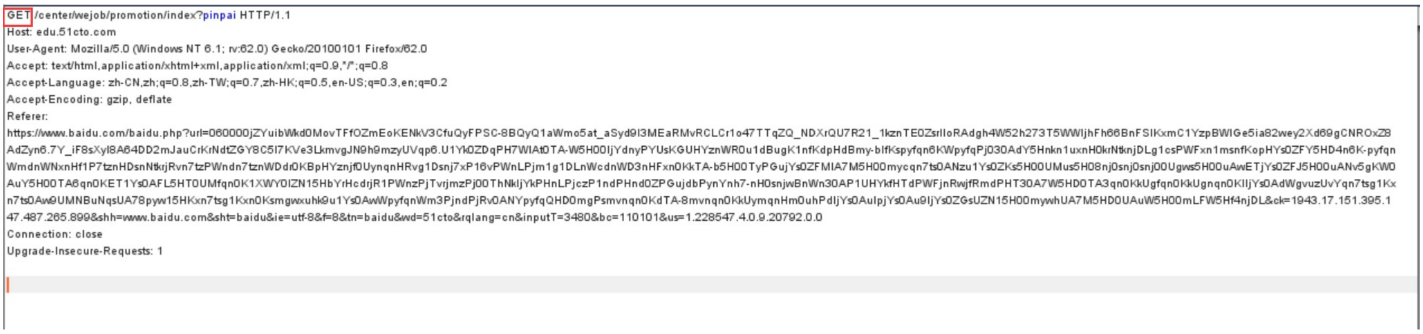
再来看一下burpsuite:


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Raw Params Headers Hex

Request to http://edu.51cto.com:80 [59.110.244.199]

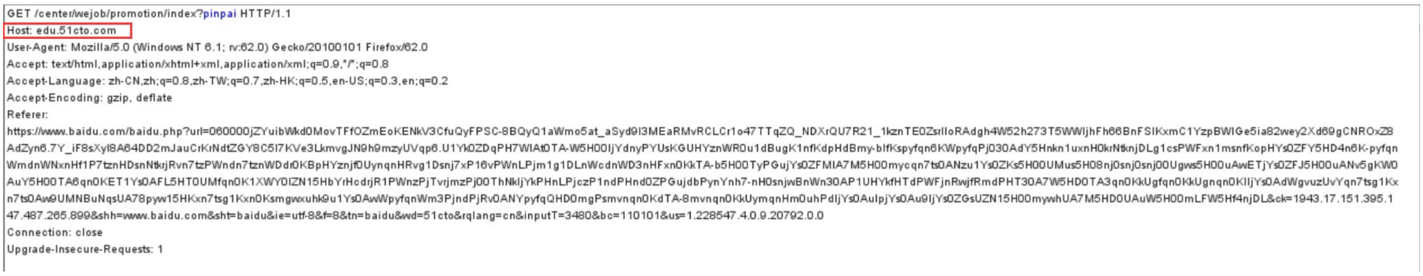
```
GET /center/wejob/promotion/index?pinpai HTTP/1.1
Host: edu.51cto.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer:
https://www.baidu.com/baidu.php?url=060000jZYuibWkd0MovTFfOZmEoKENkV3CfuQyFPSC-8BQyQ1aWmo5at_aSyd9I3MEaRMvRCLCr1o47TTqZQ_NDXrQU7R21_1kznTE0ZsrlloRAdgh4W52h273T5WWljhFh66BnFSIKxmC1Yzp
Z8AdZyn6.7Y_iF8sXyl8A64DD2mJauCrKrNdtZGY8C5I7KVe3LkmvgJN9h9mzyUVqp6.U1Yk0ZDqPH7WIAt0TA-W5H00IjYdnyPYUsKGUHYznWR0u1dBugK1nfKdpHdBmy-blfKspyfqn6KWpyfqPj030AdY5Hnkn1uxnH0krNtknjDLg1csPWF
-pyfqnWmdnWNxnHf1P7tznHDsnNtkrjRvn7tzPWndn7tznWDdr0KBpHYznjf0UynqnHRvg1Dsnj7xP16vPWnLPjm1g1DLnWcdnWD3nHFxn0KkTA-b5H00TyPGujYs0ZFMIA7M5H00mycqn7ts0ANzu1Ys0ZKs5H00UMus5H08nj0snj0snj00U
Nv5gKW0AuY5H00TA6qn0KET1Ys0AFL5HT0UMfqn0K1XWY0IZN15HbYrHcdrjR1PWnzPjTvrjmzPj00ThNkljYkPHnLPjczP1ndPHnd0ZPGujdbPynYnh7-nH0snjwBnWn30AP1UHYkfHTdPWFjnRwjfRmdPHT30A7W5HD0TA3qn0KkUgf
vYqn7tsg1Kxn7ts0Aw9UMNBuNqsUA78pyw15HKxn7tsg1Kxn0KsmgwxuhK9u1Ys0AwWpyfqnWm3PjndPjRv0ANYpyfqQHD0mgPsmvnqn0KdTA-8mvnqn0KkUymqnHm0uhPdljYs0AulpjYs0Au9IjYs0ZGsUZN15H00mywhUA7M5HD0UAu
3.17.151.395.147.487.265.899&shh=www.baidu.com&sht=baidu&ie=utf-8&f=8&tn=baidu&wd=51cto&rqlang=cn&inputT=3480&bc=110101&us=1.228547.4.0.9.20792.0.0
Connection: close
Upgrade-Insecure-Requests: 1
```

http协议头的信息:



```
GET /center/wejob/promotion/index?pinpai HTTP/1.1
Host: edu.51cto.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer:
https://www.baidu.com/baidu.php?url=060000jZYuibWkd0MovTFfOZmEoKENkV3CfuQyFPSC-8BQyQ1aWmo5at_aSyd9I3MEaRMvRCLCr1o47TTqZQ_NDXrQU7R21_1kznTE0ZsrlloRAdgh4W52h273T5WWljhFh66BnFSIKxmC1YzpBWIGe5ia82wey2Xd69gCNROxZ8
AdZyn6.7Y_iF8sXyl8A64DD2mJauCrKrNdtZGY8C5I7KVe3LkmvgJN9h9mzyUVqp6.U1Yk0ZDqPH7WIAt0TA-W5H00IjYdnyPYUsKGUHYznWR0u1dBugK1nfKdpHdBmy-blfKspyfqn6KWpyfqPj030AdY5Hnkn1uxnH0krNtknjDLg1csPWFxn1msnfKopHYs0ZFY5HD4n6K-pyfqn
WmdnWNxnHf1P7tznHDsnNtkrjRvn7tzPWndn7tznWDdr0KBpHYznjf0UynqnHRvg1Dsnj7xP16vPWnLPjm1g1DLnWcdnWD3nHFxn0KkTA-b5H00TyPGujYs0ZFMIA7M5H00mycqn7ts0ANzu1Ys0ZKs5H00UMus5H08nj0snj0snj00Ugws5H00uAwETjYs0ZFJ5H00uANv5gKW0
AuY5H00TA6qn0KET1Ys0AFL5HT0UMfqn0K1XWY0IZN15HbYrHcdrjR1PWnzPjTvrjmzPj00ThNkljYkPHnLPjczP1ndPHnd0ZPGujdbPynYnh7-nH0snjwBnWn30AP1UHYkfHTdPWFjnRwjfRmdPHT30A7W5HD0TA3qn0KkUgfqn0KkUgnqn0KIljYs0AdWgvuzUvYqn7tsg1Kx
n7ts0Aw9UMNBuNqsUA78pyw15HKxn7tsg1Kxn0KsmgwxuhK9u1Ys0AwWpyfqnWm3PjndPjRv0ANYpyfqQHD0mgPsmvnqn0KdTA-8mvnqn0KkUymqnHm0uhPdljYs0AulpjYs0Au9IjYs0ZGsUZN15H00mywhUA7M5HD0UAuW5H00mLFW5Hf4njDL&ck=1943.17.151.395.1
47.487.265.899&shh=www.baidu.com&sht=baidu&ie=utf-8&f=8&tn=baidu&wd=51cto&rqlang=cn&inputT=3480&bc=110101&us=1.228547.4.0.9.20792.0.0
Connection: close
Upgrade-Insecure-Requests: 1
```

这是用用get方法传递的消息;



```
GET /center/wejob/promotion/index?pinpai HTTP/1.1
Host: edu.51cto.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer:
https://www.baidu.com/baidu.php?url=060000jZYuibWkd0MovTFfOZmEoKENkV3CfuQyFPSC-8BQyQ1aWmo5at_aSyd9I3MEaRMvRCLCr1o47TTqZQ_NDXrQU7R21_1kznTE0ZsrlloRAdgh4W52h273T5WWljhFh66BnFSIKxmC1YzpBWIGe5ia82wey2Xd69gCNROxZ8
AdZyn6.7Y_iF8sXyl8A64DD2mJauCrKrNdtZGY8C5I7KVe3LkmvgJN9h9mzyUVqp6.U1Yk0ZDqPH7WIAt0TA-W5H00IjYdnyPYUsKGUHYznWR0u1dBugK1nfKdpHdBmy-blfKspyfqn6KWpyfqPj030AdY5Hnkn1uxnH0krNtknjDLg1csPWFxn1msnfKopHYs0ZFY5HD4n6K-pyfqn
WmdnWNxnHf1P7tznHDsnNtkrjRvn7tzPWndn7tznWDdr0KBpHYznjf0UynqnHRvg1Dsnj7xP16vPWnLPjm1g1DLnWcdnWD3nHFxn0KkTA-b5H00TyPGujYs0ZFMIA7M5H00mycqn7ts0ANzu1Ys0ZKs5H00UMus5H08nj0snj0snj00Ugws5H00uAwETjYs0ZFJ5H00uANv5gKW0
AuY5H00TA6qn0KET1Ys0AFL5HT0UMfqn0K1XWY0IZN15HbYrHcdrjR1PWnzPjTvrjmzPj00ThNkljYkPHnLPjczP1ndPHnd0ZPGujdbPynYnh7-nH0snjwBnWn30AP1UHYkfHTdPWFjnRwjfRmdPHT30A7W5HD0TA3qn0KkUgfqn0KkUgnqn0KIljYs0AdWgvuzUvYqn7tsg1Kx
n7ts0Aw9UMNBuNqsUA78pyw15HKxn7tsg1Kxn0KsmgwxuhK9u1Ys0AwWpyfqnWm3PjndPjRv0ANYpyfqQHD0mgPsmvnqn0KdTA-8mvnqn0KkUymqnHm0uhPdljYs0AulpjYs0Au9IjYs0ZGsUZN15H00mywhUA7M5HD0UAuW5H00mLFW5Hf4njDL&ck=1943.17.151.395.1
47.487.265.899&shh=www.baidu.com&sht=baidu&ie=utf-8&f=8&tn=baidu&wd=51cto&rqlang=cn&inputT=3480&bc=110101&us=1.228547.4.0.9.20792.0.0
Connection: close
Upgrade-Insecure-Requests: 1
```

host是目标网站;

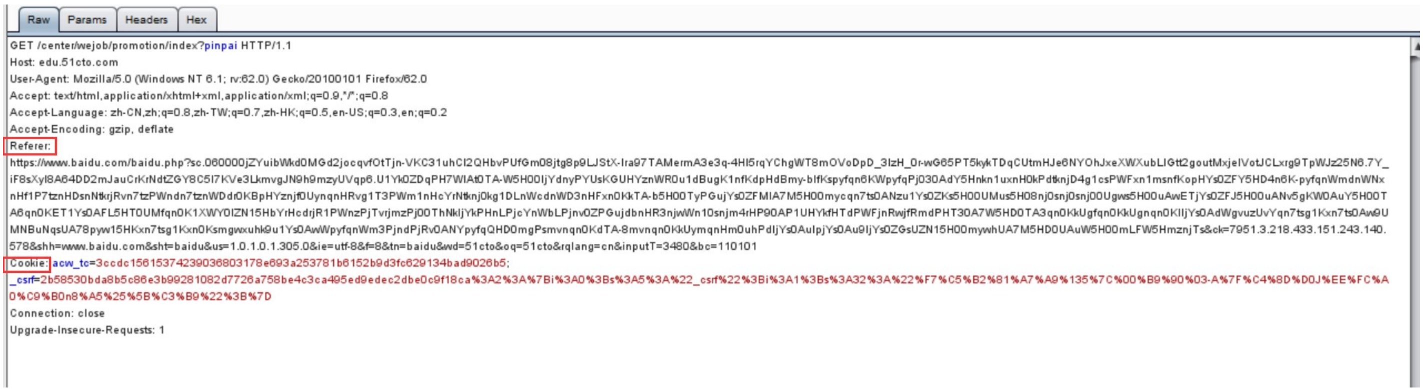
User-agent:这是客户端的浏览器的信息;

Accept:访问的网页类型;

Accept-Language:访问的网页的语言!

refer，有的还有cookie;

再次访问的时候就有了:

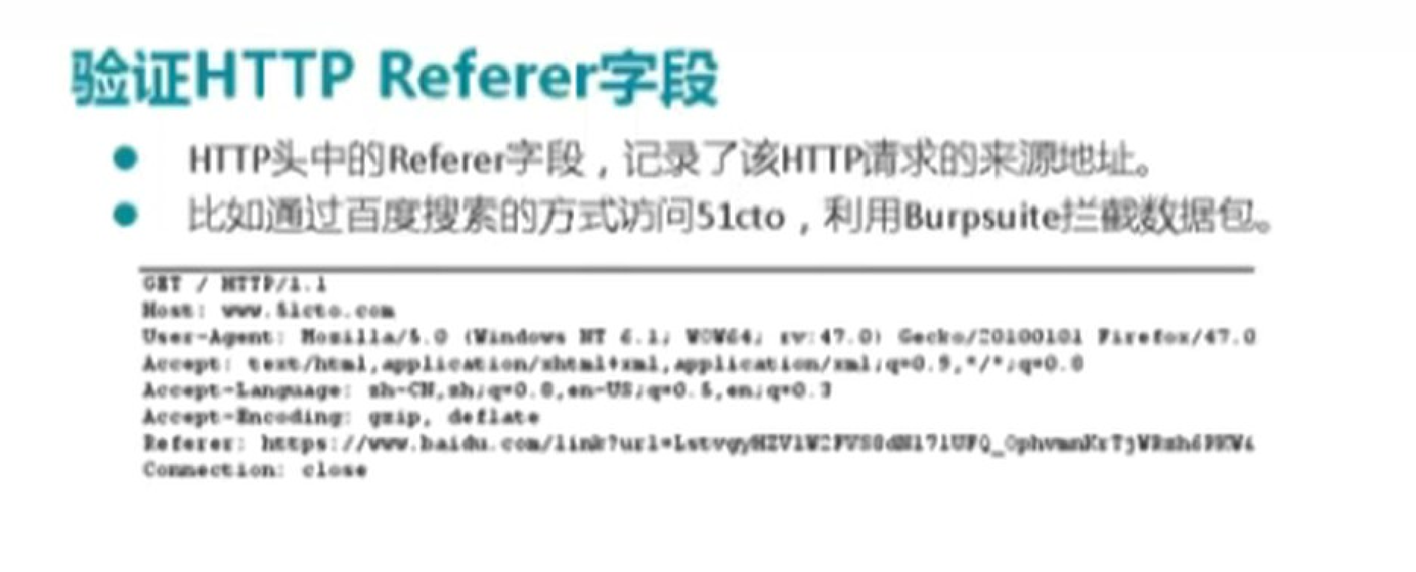


```
GET /center/wejob/promotion/index?pinpai HTTP/1.1
Host: edu.51cto.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer:
https://www.baidu.com/baidu.php?sc.060000jZYuibWkd0MGd2jocqvfOtTjn-VKC31uhCI2QHbvPUfGm08jtg8p9LJStX-lra97TAMermA3e3q-4HI5rqYChgWT8mOVoDpD_3IzH_0r-wG65PT5kykTDqCUtmHJe6NYOhJxeXWXubLIGtt2goutMxjelVotJCLxrg9TpWJz25N6.7Y_
iF8sXyl8A64DD2mJauCrKrNdtZGY8C5I7KVe3LkmvgJN9h9mzyUVqp6.U1Yk0ZDqPH7WIAt0TA-W5H00IjYdnyPYUsKGUHYznWR0u1dBugK1nfKdpHdBmy-blfKspyfqn6KWpyfqPj030AdY5Hnkn1uxnH0kPdtknjD4g1csPWFxn1msnfKopHYs0ZFY5HD4n6K-pyfqnWmdnWNx
nHf1P7tznHDsnNtkrjRvn7tzPWndn7tznWDdr0KBpHYznjf0UynqnHRvg1T3PWm1nHcYrNtknj0kg1DLnWcdnWD3nHFxn0KkTA-b5H00TyPGujYs0ZFMIA7M5H00mycqn7ts0ANzu1Ys0ZKs5H00UMus5H08nj0snj0snj00Ugws5H00uAwETjYs0ZFJ5H00uANv5gKW0AuY5H00T
A6qn0KET1Ys0AFL5HT0UMfqn0K1XWY0IZN15HbYrHcdrjR1PWnzPjTvrjmzPj00ThNkljYkPHnLPjcYnWbLPjnv0ZPGujdbnHR3njwWn10snjm4rHP90AP1UHYkfHTdPWFjnRwjfRmdPHT30A7W5HD0TA3qn0KkUgfqn0KkUgnqn0KIljYs0AdWgvuzUvYqn7tsg1Kxn7ts0Aw9U
MNBuNqsUA78pyw15HKxn7tsg1Kxn0KsmgwxuhK9u1Ys0AwWpyfqnWm3PjndPjRv0ANYpyfqQHD0mgPsmvnqn0KdTA-8mvnqn0KkUymqnHm0uhPdljYs0AulpjYs0Au9IjYs0ZGsUZN15H00mywhUA7M5HD0UAuW5H00mLFW5HmznjTs&ck=7951.3.218.433.151.243.140.
578&shh=www.baidu.com&sht=baidu&us=1.0.1.0.1.305.0&ie=utf-8&f=8&tn=baidu&wd=51cto&oq=51cto&rqlang=cn&inputT=3480&bc=110101
Cookie: acw_tc=3ccdc15615374239036803178e693a253781b6152b9d3fc629134bad9026b5;
_csrf=2b58530bda8b5c86e3b99281082d7726a758be4c3ca495ed9edec2dbe0c9f18ca%3A2%3A%7Bi%3A0%3Bs%3A5%3A%22_csrf%22%3Bi%3A1%3Bs%3A32%3A%22%F7%C5%B2%81%A7%A9%135%7C%00%B9%90%03-A%7F%C4%8D%D0J%EE%FC%A
0%C9%B0n8%A5%25%5B%C3%B9%22%3B%7D
Connection: close
Upgrade-Insecure-Requests: 1
```

你要 访问host这个 目标网站,你是从哪个网站开启 访问的;你访问目标网站之前,你是从哪个网站过去的,访问之前的那个页面就叫做referer;

```
https://www.baidu.com/baidu.php?sc.060000jZYuibWkd0MGd2jocqvfOtTjn-VKC31uhCI2QHbvPUfGr
```

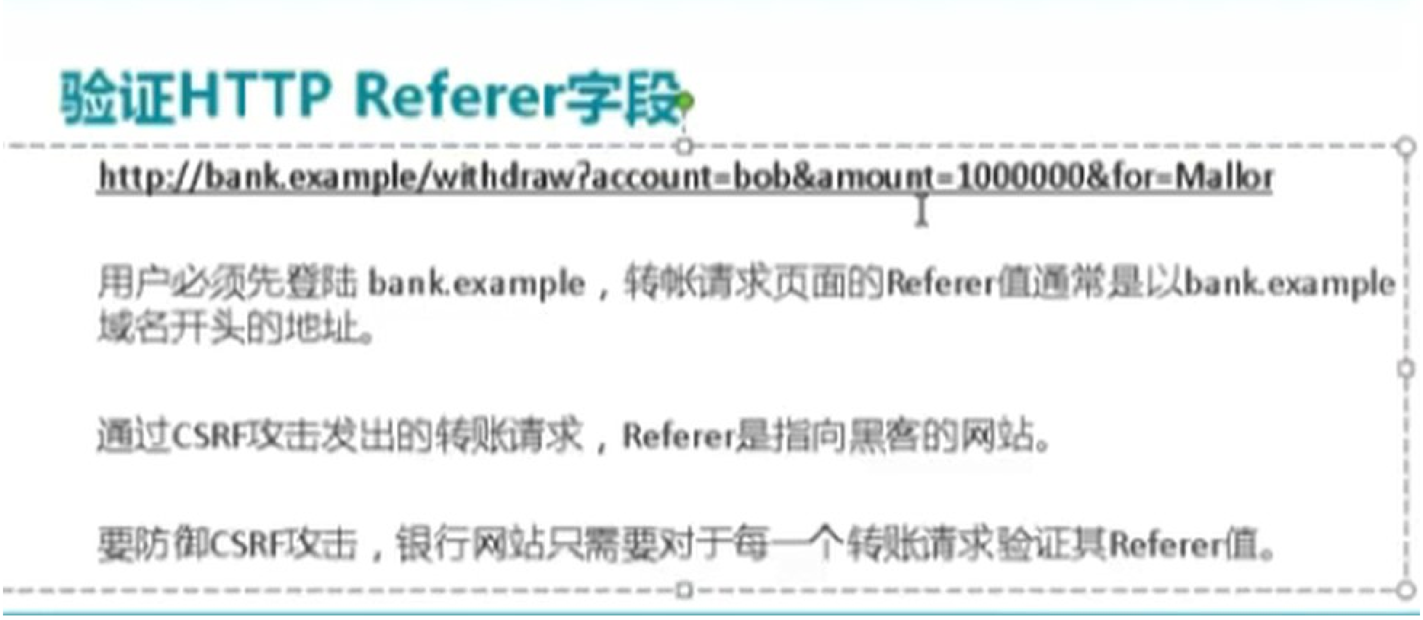
referer就指明了你在访问某一个网站的时候是从哪一个网站过去的;



验证HTTP Referer字段

- HTTP头中的Referer字段，记录了该HTTP请求的来源地址。
- 比如通过百度搜索的方式访问51cto，利用Burpsuite拦截数据包。

```
GET / HTTP/1.1
Host: www.51cto.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://www.baidu.com/link?url=LstvgyHZV1WZFVS0dHl71UFQ_OphvmnKrTjWEshdPNW4
Connection: close
```



验证HTTP Referer字段

http://bank.example/withdraw?account=bob&amount=1000000&for=Mallor

用户必须先登陆 bank.example，转帐请求页面的Referer值通常是以bank.example域名开头的地址。

通过CSRF攻击发出的转账请求，Referer是指向黑客的网站。

要防御CSRF攻击，银行网站只需要对于每一个转账请求验证其Referer值。

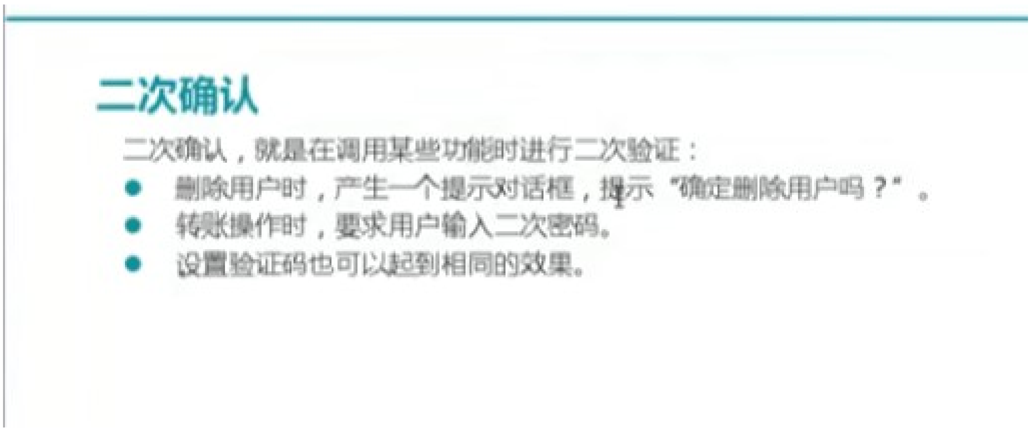
验证其referer值即可！

其实referer也是可以伪造的！！ 这是一个缺陷！！

另外,有的单位他不用referer，因为他怕泄露内部信息！！

High CSRF Source

二次验证即可！



二次确认

二次确认，就是在调用某些功能时进行二次验证：

- 删除用户时，产生一个提示对话框，提示“确定删除用户吗？”。
- 转账操作时，要求用户输入二次密码。
- 设置验证码也可以起到相同的效果。

```php
<?php

    if (isset($_GET['Change'])) {

        // Turn requests into variables
        $pass_curr = $_GET['password_current'];
        $pass_new = $_GET['password_new'];
        $pass_conf = $_GET['password_conf'];

        // Sanitise current password input
        $pass_curr = stripslashes( $pass_curr );
        $pass_curr = mysql_real_escape_string( $pass_curr );
        $pass_curr = md5( $pass_curr );

        // Check that the current password is correct
        $qry = "SELECT password FROM `users` WHERE user='admin' AND password='$pass_cu
        $result = mysql_query($qry) or die('<pre>' . mysql_error() . '</pre>' );

        if (($pass_new == $pass_conf) && ( $result && mysql_num_rows( $result ) == 1 )
            $pass_new = mysql_real_escape_string($pass_new);
            $pass_new = md5($pass_new);

            $insert="UPDATE `users` SET password = '$pass_new' WHERE user = 'admin';"
            $result=mysql_query($insert) or die('<pre>' . mysql_error() . '</pre>' );

            echo "<pre> Password Changed </pre>";
            mysql_close();
        }

        else{
            echo "<pre> Passwords did not match or current password incorrect. </pre>"
        }

    }
?>
```