第十届全国大学生信息安全竞赛一道Web题的Writeup

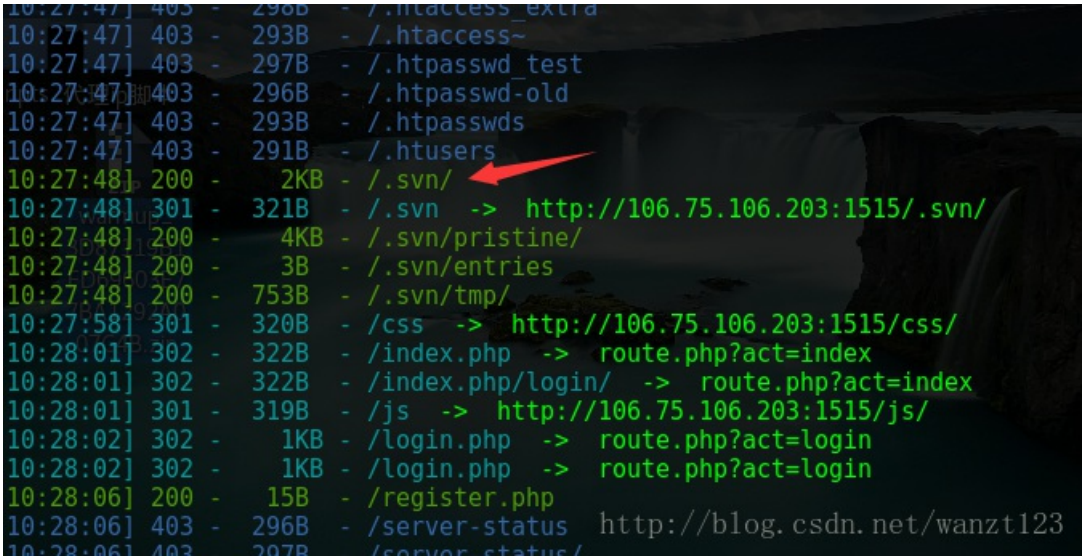
原创

Brucetg 于 2017-07-15 17:01:44 发布 6038 收藏 2
分类专栏： CTF

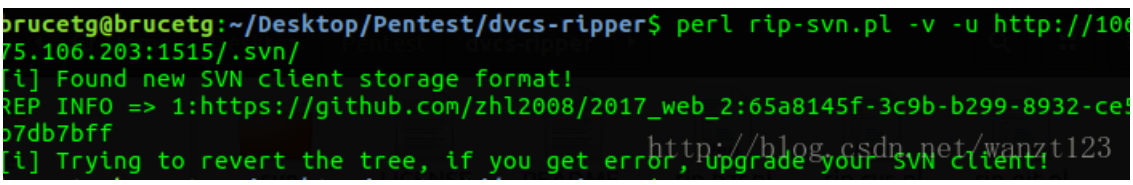
wanna to see your hat?

http://106.75.106.203:1515/

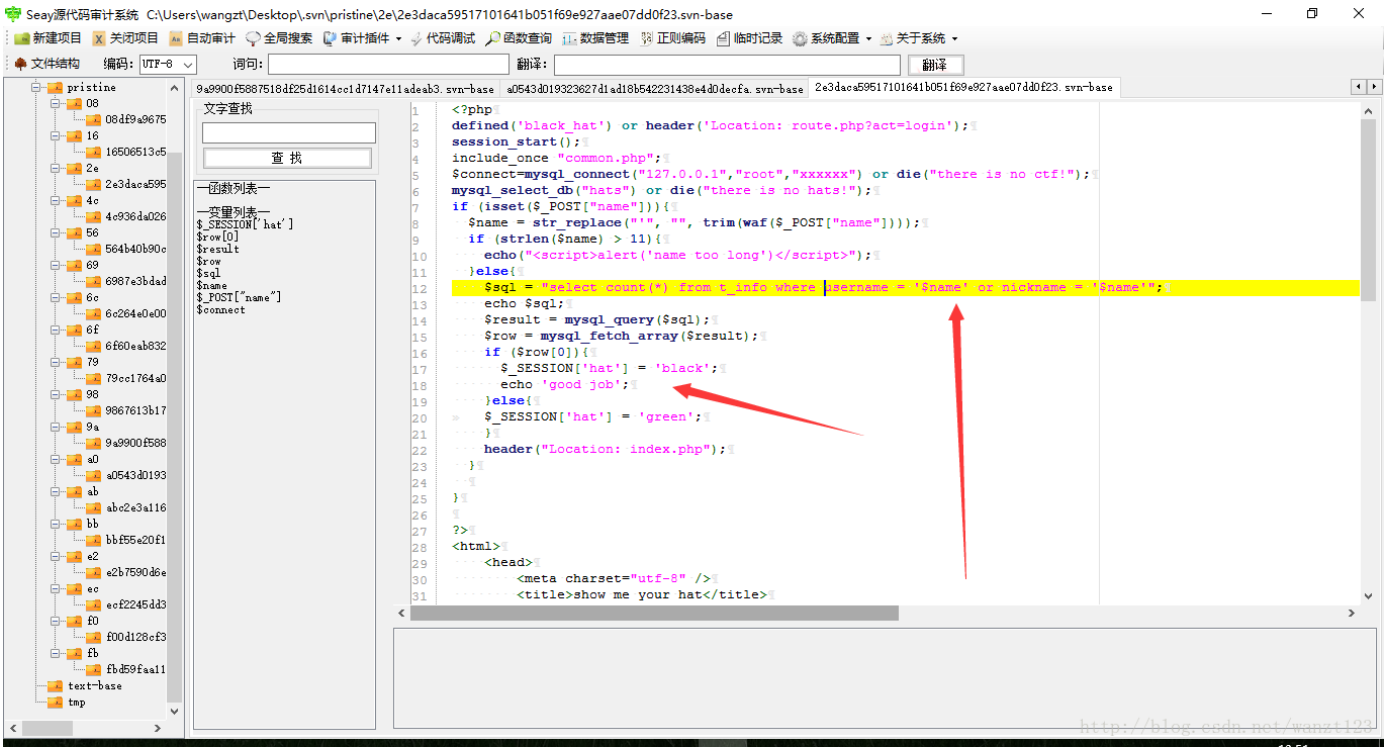
svn文件泄露



使用dvcs-ripper将泄露文件下载下来：



进行代码审计：



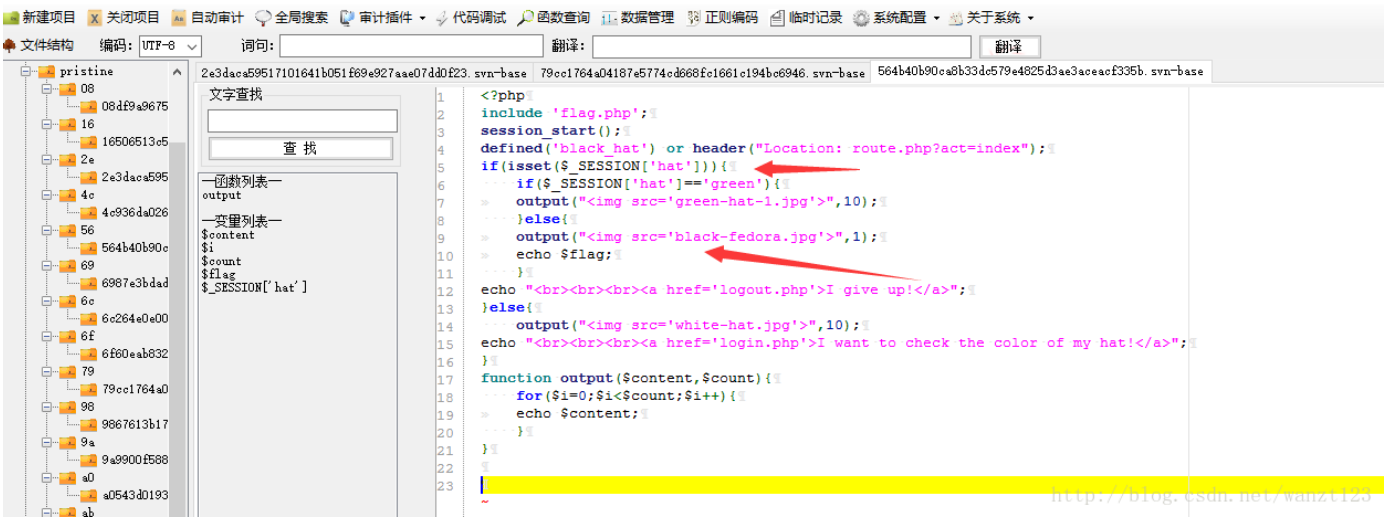
关键代码：

```
$name = str_replace("'","", trim(waf($_POST["name"])));
 if (strlen($name) >11){
  echo("<script>alert('name toolong')</script>");
 }else{
  $sql = "select count(*) from t_info where username ='$name' or nickname = '$name'";
  echo $sql;
  $result = mysql_query($sql);
  $row = mysql_fetch_array($result);
  if ($row[0]){
   $_SESSION['hat']= 'black';
   echo 'good job';
  }else{
```

```
    $_SESSION['hat']= 'green';
}
```

name字段长度不能大于11，只要查询语句返回不为空,就执行：

```
$_SESSION['hat']= 'black';
    echo 'good job';
```

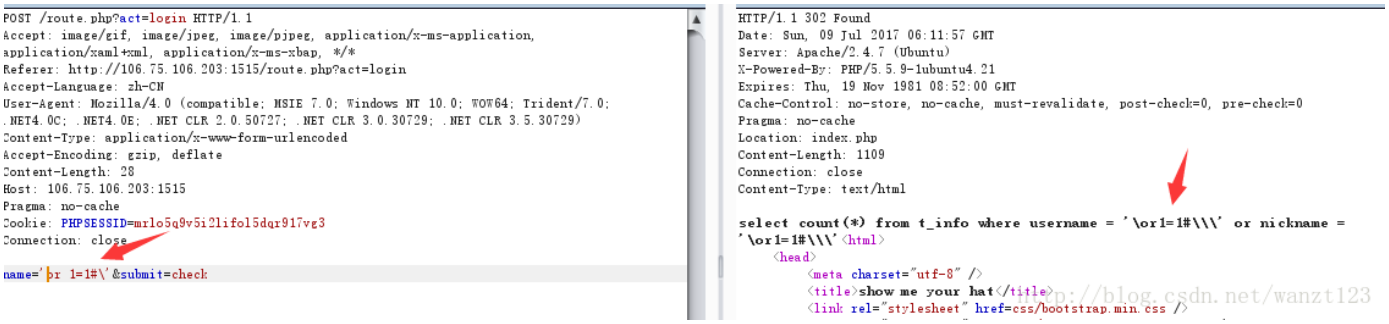


关键代码：

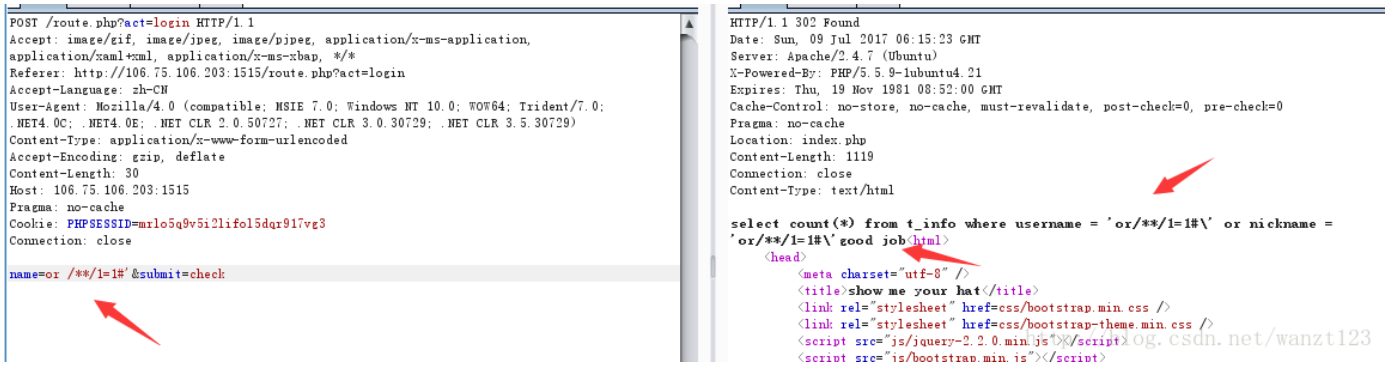
```
if(isset($_SESSION['hat'])){
    if($_SESSION['hat']=='green'){
    output("<imgsrc='green-hat-1.jpg'>",10);
    }else{
    output("<imgsrc='black-fedora.jpg'>",1);
    echo $flag;
    }
```

如果SESSION中存在hat字段，并且其值不等于green，就输出flag，而设置session的地方就是第一处关键代码所在的地方。

而我们不知道哪个name值返回不为空，猜测存在注入，burp抓包：



发现name字段可以注入，不过过滤了很多，经测试发现过滤了空格，%df也被替换了，尝试使用注释绕过，提示good job，说明payload有效，故最终payload为：or /**/1=1#'



在login页面输入框中输入 or/**/1=1#' 即得到flag。