南邮tip sql.php_南京邮电大学 CTF Write Up

原创

谢谢你快来 于 2021-03-09 18:25:51 发布 31 收藏
文章标签： 南邮tip sql.php

这次来看看某著名大学——

(Ps:因本人较懒，所以做题时都是手工＋度娘，几乎没有用到浏览器以外的工具，如有更好的办法，欢迎留言告知~)

Web

签到题

直接查看源代码吧。。

key在哪里？
nctf{flag_admiaanaaaaaaaaaaa}

Flag:nctf{flag_admiaanaaaaaaaaaaa}

md5 collision

直接给了源码，来看看

```
$md51 = md5('QNKCDZO');

$a = @$_GET['a'];

$md52 = @md5($a);

if(isset($a)){

if ($a != 'QNKCDZO' && $md51 == $md52) {

echo "nctf{*****************}";

} else {

echo "false!!!";

}}

else{echo "please input a";}
```

发现利用的是MD51=MD52来跳出flag，而且还给了个参数a，那么只需要让参数a的值经过MD5加密后与字符串QNKCDZO经过加密后的MD5值相等就好了。加密后发现是0E开头的密文，即PHP解析0E开头的md5漏洞。详情参照：?a=s878926199a(自行百度，数不胜数)，即

签到题2

口令是11位数的zhimakaimen，输入会发现这个输入框限制输入长度为10位数，本人Firefox浏览器直接按F12(或鼠标单击右键审查元素)找到这一行：

style="background-image:url… type="password">

maxlength="10"的10改成>=11，再输入就可以提交口令了。

Flag:nctf{follow_me_to_exploit}

这题不是web

既然不是web，源码和头文件也没有任何提示信息，就把这张图下载下来，改为txt格式打开，Ctrl+F快速查找，发现flag在文末。。还真的不是WEB啊

Flag:nctf{photo_can_also_hid3_msg}

层层递进

没啥思路。。。就右键查看源代码，跟随底部链接，依次访nctf{javascript_aaencode}

打开是乱码，习惯性用转码工具(Alt->查看->文字编码->Unicode)转换一下发现是一对堆表情，明显是JS加密，直接F12贴进控制台跑一下，Flag就出来了~

Flag:nctf{javascript_aaencode}

单身二十年

查看源码，点击，Flag直接出来了。。

Flag:nctf{yougotit_script_now}

php decode

因为PHP环境没有配置好还是什么原因，据说eval函数可以执行php代码，但我将他写好放进本地根目录的时候打开会报错，所以也就没做留着以后填坑

文件包含

LFI漏洞，自行百度补充。

学到了一点猥琐的知识，在服务器端的.php文件无法直接显示，用base64加密(read=convert.base64-encode)后拿到密文再解密，就可以看到源码了。

asdf

```
error_reporting(0);

if(!$_GET[file]){echo 'click me? no';}

$file=$_GET['file'];

if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){

echo "Oh no!";

exit();

}

include($file);

//flag:nctf{edulcni_elif_lacol_si_siht}

?>
```

Flag:nctf{edulcni_elif_lacol_si_siht}

单身一百年也没用

和单身二十年一样，看源码，点击 结果却跳转到了

/no_key_is_here_forever.php，猜想是用了重定向，F12查看网络，就能发现index.php这个包，果然是302重定向，查看响应没有东西，那么应该在头文件了，果然，不出所料~

响应头：

Server: sae

Date: Sat, 13 Jan 2018 08:17:43 GMT

Content-Type: text/html

Content-Length: 0

Connection: keep-alive

flag: nctf{this_is_302_redirect}

Location: http://chinalover.sinaapp.com/web8/no_key_is_here_forever.php

Via: 1566

Flag: nctf{this_is_302_redirect}

Download~!

不能做，留着以后填坑~

COOKIE

先弄明白COOKIE是个什么东西，验证身份用的对吧？那么然后去看请求包，F12网络，发现请求头和响应头之间的基情：

Host: chinalover.sinaapp.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Cookie: Login=0

Connection: keep-alive

Upgrade-Insecure-Requests: 1

DNT: 1

Cache-Control: max-age=0

Server: sae

Date: Sat, 13 Jan 2018 08:27:49 GMT

Content-Type: text/html

Transfer-Encoding: chunked

Connection: keep-alive

Via: 15146

Set-Cookie: Login=0

Content-Encoding: gzip

cookie:Login=0，题目给的有Tips啊，0==not，按照程序员的思维(不要问为什么，嘿嘿嘿)，那么1==yes，改之，出Flag.

Flag:nctf{cookie_is_different_from_session}

MYSQL

按照提示进去robots.txt后转码看到如下内容：

别太开心，flag不在这，这个文件的用途你看完了？

在CTF比赛中，这个文件往往存放着提示信息

TIP:sql.php

```
if($_GET[id]) {

mysql_connect(SAE_MYSQL_HOST_M . ':' .
SAE_MYSQL_PORT,SAE_MYSQL_USER,SAE_MYSQL_PASS);

mysql_select_db(SAE_MYSQL_DB);

$id = intval($_GET[id]);

$query = @mysql_fetch_array(mysql_query("select content from ctf2 where id='$id'"));

if ($_GET[id]==1024) {

echo "

no! try again

";
}

else{

echo($query[content]);

}

}

?>
```

好了，TIP又出来了，进去sql.php看看，什么都没有，回来看到这一行

```
if ($_GET[id]==1024) {
```

echo "

no! try again

";
}

/sql.php?id=1024后提示try again，换到/sql.php?id=1025后提示no more。。虽然不懂原理，但是猥琐的试了一波/sql.php?id=1024.5，哈哈，成功拿到Flag~

后来才知道重点是这儿

if ($_GET[id]==1024) {

echo "

no! try again

";
}

else{

echo($query[content]);

}

要求提交的ID在值上==1024，但又不能是1024，否则就会try again。。任意的小数都可以~ ~ Wpsec的基友们记不记得某浪想要的998？同一个道理~

/x00

(膜拜大佬，不甘心这道题，看了Writeup恶补一番知识才弄明白，此题writeup直接拖)

view-source:

if (isset ($_GET['nctf'])) {

if (@ereg ("^[1-9]+$", $_GET['nctf']) === FALSE)

echo '必须输入数字才行';

else if (strpos ($_GET['nctf'], '#biubiubiu') !== FALSE)

die('Flag: '.$flag);

else

echo '骚年，继续努力吧啊~';

}

这里ereg有两个漏洞

1.%00截断及遇到%00则默认为字符串的结束

2.当ntf为数组时它的返回值不是FALSE

所以有两个方法拿flag

1.令id=1%00%23biubiubiu

2.令nctf为数组，即nctf[]=1

Flag:nctf{use_00_to_jieduan}

伪装者

改了X-Forwarded-For没用，不用改Referer，应该是服务器出问题了，看了writeup后发现思路也没错。。自行补充XFF和Referer和UA在HTTP协议中的作用吧。。

Header

直接F12看头文件，Flag就在里面。

Date: Sun, 14 Jan 2018 10:42:18 GMT

Server: Apache/2.2.15 (CentOS)

X-Powered-By: PHP/5.3.3

Flag: nctf{tips_often_hide_here}

Content-Length: 132

Connection: close

Content-Type: text/html; charset=UTF-8

Flag:nctf{tips_often_hide_here}

bypass again

打开见到

if (isset($_GET['a']) and isset($_GET['b'])) {

if ($_GET['a'] != $_GET['b'])

if (md5($_GET['a']) === md5($_GET['b']))

die('Flag: '.$flag);

else

print 'Wrong.';

}

GET可以接受数组 但md5()不能加密数组内的数据，所以令a和b分别为数组，可以绕过，所以在url里加入index.php?a[]=1&b[]=2，即可看到Flag

Flag: nctf{php_is_so_cool}

综合题

一大堆，是jother编码，控制台跑一下出来1bc29b36f623ba82aaf6724fd3b16718.php，贴入URL发现被耍了==，TIP在头里，查看头文件发现

Server: sae

Date: Sat, 13 Jan 2018 08:47:08 GMT

Content-Type: text/html

Transfer-Encoding: chunked

Connection: keep-alive

tip: history of bash

Via: 1566

Content-Encoding: gzip

百度一波history of bash，发现某大佬文章.bash_history，贴入url发现

zip -r flagbak.zip ./*

再次下载，发现被损坏无法解压。。常规思路，改为txt格式发现Flag~

Flag:nctf{bash_history_means_what}

Re

Hello，RE!

因为工具的不兼容。。RE的题就没做。。

Pwn

When did you born？

提取码错误。。

Stack Overflow

不会做，留着以后搞~

Crypto

easy!

丢Base64解密，秒出。。

Flag:nctf{this_is_base64_encode}

Keyboard

题目就是键盘，看提示也是键盘，那么就从键盘入手，会发现形状是字母areuhack，

题目也说了加上nctf{}。。

Flag:nctf{areuhack}

异性相吸

提取码错误，以后填坑吧

Misc

全部提取码错误。。就先放着吧