BUUCTF WEB EASY_BYPASS1

原创

显哥无敌 于 2021-10-17 14:25:30 发布 64 收藏

分类专栏： BUUCTF 文章标签： web安全

本文链接：https://blog.csdn.net/qq_41696858/article/details/120810606

打开场景，直接给了源码，代码审计，没啥好说的，两个get，一个post，很常规的md5数组绕过，post过去的passwd 数字字符弱相等

```php
$flag='MRCTF{xxxxxxxxxxxxxxxxxxxxxxxx}';
if(isset($_GET['gg'])&&isset($_GET['id'])) {
 $id=$_GET['id'];
 $gg=$_GET['gg'];
 if (md5($id) === md5($gg) && $id !== $gg) {
  echo 'You got the first step';
  if(isset($_POST['passwd'])) {
   $passwd=$_POST['passwd'];
   if (!is_numeric($passwd)) {
    if($passwd==1234567) {
     echo 'Good Job!';
     highlight_file('flag.php');
     die('By Retr_0');
    } else {
     echo "can you think twice??";
    }
   } else {
    echo 'You can not get it !';
   }
  } else {
   die('only one way to get the flag');
  }
 } else {
  echo "You are not a real hacker!";
 }
} else {
 die('Please input first');
}
```

给一个payload：?id[]=1&gg[]=2

post:passwd=1234567a

参考视频链接：https://www.bilibili.com/video/BV1Pv411u7QR?spm_id_from=333.999.0.0