防 Web 攻击的登录窗口程序设计*

王命全,张祖莲,李景林
(新疆气象局 新疆兴农网信息中心,新疆 乌鲁木齐 830002)

摘 要:目前网络安全问题已是大家普遍关注的问题,网络黑客攻击给很多单位造成巨大的损失。如何减少网络攻击已是很多相关研究人员重点研究方向。系统登录窗口是绝大多数用户使用系统的首要入口,也是黑客攻击的主要目标。所以如何设计好登录窗口,对一个系统的安全来说至关重要。本文从 10 个方面考虑如何设计登录界面。

关键词:网络安全;登录窗口;Web 攻击;黑客攻击;程序设计

中图分类号:TP393 **文献标识码**:A **文章编号**:1674-7720(2014)05-0005-03

Design of login window program against Web attacks

Wang Mingquan, Zhang Zulian, Li Jinglin
(Information Center of Xinjiang Develop Agriculture Net, Xinjiang Bureau of Meteorology, Urumqi 830002, China)

Abstract: Network security is generally concerned problem currently, the network hacker attacks to many units result in huge losses. How to reduce cyber attacks have been a lot of focus on the direction of researchers. System login page is the primary entrance of users to use the system, and is also the main target of hacker attacks. So it is critical on a system's security, which how to design a good login page. This article consider how to design a login page from ten aspects.

Key words: network security; login window; Web attacks; hacking; programming

目前网络攻击现象十分严重,给很多企业和单位造成很大程度的破坏。网络安全问题一直是很多单位重视的问题。目前所有交互性系统或用户查询系统类,都需要涉及到登录窗口。网络攻击者也主要是攻破登录窗口这个界面,才能进入应用系统,进行操作相关的数据或应用程序。可见登录窗口对系统的作用是至关重要的。现在 Web 系统直接部署在网络上,任何人都可以访问到,安全问题是很多系统担心的问题。

本文的防 Web 攻击登录窗口设计主要从程序设计角度来讲,针对一般的 Web 系统,例如论坛、留言等用户能自己登录后发布信息的窗口。对于银行等安全性要求极高的系统来说,除了本身的 Web 设计外,还必须借助其他如 U 盾等外界硬件设备来保证其足够安全性。

1 关于提高 Web 安全性的相关研究

1.1 借用外界硬件设备来提高安全性

(1)基于可信平台模块(TPM)的用户登录可信认证。该认证方式是利用 PC 机 USB 接口外接 TPM,将用户的身份信息、相关的密钥信息等存储在 TPM 中,并利用 USBKEY 技术、动态的口令技术来确保用户身份的真实可信[1];(2)用户登录端程序嵌入到还原程序当中通信代理服务,用户端和服务器端分开响应[2]。

以上的研究主要从硬件来考虑,对于一般的论坛类系统不可能让每个用户发篇帖子还要单独配置相关的硬件。

1.2 主要用软件设计来提高安全性

(1)以著名的 RSA 算法和 DES 算法为基础,提出一种互补性的混合数据加密方案及其实现过程[3];(2)安全减少用户登录次数,在分布式环境中基于 Web 服务的用户单点登录机制,使得用户只需登录一次即可完成复杂业务[4]。

1.3 程序配合数据库设置

过滤特殊字符,分配数据库账户权限,正确使用存储过程,确保输入的合法性,对敏感数据加密存储,严格进行错误处理[5]。此研究主要从软件设计上考虑,用户可以借鉴,设计考虑的并不全面,对于不同的攻击不一

*基金项目:新疆维吾尔自治区农村服务体系建设(新财农[2013]61 号)

定能很好地预防。关于数据库设置,对于网络管理员来说,可以借鉴。

本文主要从软件设计方面来考虑不同用户不同需要及各种有关预防策略。

2 程序设计

登录窗口要设计好,首先考虑的方面要全,攻击者不可能用所有的方法去试探,但仅用其中的部分要素就可以。本文将列出一部分常见的实用的攻击及预防的策略。

(1)防 SQL 注入漏洞攻击

目前很多登录程序在设计上存在一个很大的隐患就是直接写 SQL 语句进行验证登录,即黑客输入任意的用户名、密码后,只要在后面输入"'1'or'1'='1'"成为选择语句,验证就会轻松通过,进入后台,访问数据库。换一种方法去验证用户名和密码,就可以有效地预防这类现象。

代码例如:

```
conn.Open();                                    //打开数据库
SqlCommand cmd=conn.CreateCommand();
cmd.CommandText = "select*from 用户表 where 用户名=@UserName and 密码=@pwd";
cmd.Parameters.Add (new SqlParameter ("UserName", txtUserName.Text));
cmd.Parameters.Add (new SqlParameter ("pwd", txtpwd.Text));
```

(2)加入输入密码次数

目前电脑配置也越来越高,很多相关黑客破解密码的软件,黑客会用一个配置较好的主机去破解用户名的密码,直到破解为止,计算机的运行速度特别快,一般数字密码很快就会破解。因此在登录窗口要设置用户登录输入密码的次数,如输入密码次数不超过 3 次,这样才能大大减少被破解的机会。如果用户登录成功,错误次数会自动清零。以免影响正常用户的正常登录。

核心代码例如:

```
DataTable dt=SqlHelp.ExecuteDataTable ("select* from 用户表 where 用户名=@UserName and 密码=@pwd",
new SqlParameter ("UserName", uid.Text)); new SqlParameter("pwd", pwd.Text));
if (dt.Rows.Count <=0) {MessageBox.Show ("用户名不存在!"); return;}
else
{
DataRow row=dt.Rows[0];
int errorTimes=Convert.ToInt32(row["ErrorTimes"]);
if(errorTimes>=3)
{MessageBox.Show("登录错误次数过多!"); return;}
string dbpassword=Convert.ToString(row["Password"]);
if(dbpassword==pwd.Text)
{MessageBox.Show("登录成功!");
SqlHelp.ExecuteNonQuery ("Update 用户表 Set ErrorTimes=0 where 用户名=@UserName",}
else {SqlHelp.ExecuteNonQuery ("Update 用户表 Set ErrorTime =ErrorTimes +1 where UserName =@UserName", new SqlParameter("UserName", pwd.Text));
MessageBox.Show("密码错误!");}
}
```

(3)限制同一 IP 多次申请注册

如果用户一直注册,当作攻击的一种类型,当申请次数达到一定数据,该用户不能再申请。主要由浏览器缓存暂时存下用户的相关信息如 IP 等,用于记录用户申请帐户次数。

核心代码:

```
Form frmRequestAnAccount =CacheManager.Instance.GetForm(assemblyName, IP);    //获取 IP 申请用户名次数
If(frmRequestAnAccount.ShowDialog()==DialogResult.OK)
                                                //次数达到某一限制,弹出对话框
{this.btnRequestAnAccount.Enabled=false;}
                                                //禁止该用户再申请帐户
```

(4)判断当前用户是否在线,为 false 方可注册

```
BaseSystemInfo.CheckOnLine=false;   //当前用户若不在线
BaseSystemInfo.AllorNullPassword=true;          //可以注册
```

(5)核实是否记录日志

```
BaseSystemInfo.RecordLog=true;                  //确定记录
```

(6)重要的应用登录后写入注册表

输入正确用户名和密码后,写入注册表,即使该用户暂时没权限,发生异常,则写入 XML。

核心代码如下:

```
If(this.chkRememberPassword.Checked)
{registryKey.SetValue (BaseConfiguration.CURRENT_USERNAME, SecretUtil.Encrypt (userInfo.Username));
registryKey.SetValue (BaseConfiguration.CURRENT_PASSWORD, SecretUtil.Encrypt (this.txtPassword.Text));}
Else
{registryKey.SetValue (BaseConfiguration.CURRENT_USERNAME, string.Empty);
registryKey.SetValue (BaseConfiguration.CURRENT_PASSWORD, string.Empty);}
```

(7)对键盘上的回车进行处理

相关代码(用户按键盘 Enter 也可以登录):

```
if(e.KeyChar==13)
{If(this.CheckInput())          //检查输入的有效性
{This.Login();                  //用户登录}
}
```

(8)多语言加载,如果有外籍人员

```
ResourceManagerWrapper.Instance.LoadResources
```

```
(Application.StartupPath+@"\语言包路径\");
                                    //从当前指定的语言包读取信息
```

(9)添加验证码

目前网络上有多种验证码,稍加修改,明白其中的成图原理,都可以改成自己常用的开发语言进行使用。

例如下面生成验证码相关核心代码:

```
int fSize=FontSize;
int fWidth=fSize+Padding;
int imageWidth =(int) (code.Length*fWidth) +4 + Padding*2;
int imageHeight=fSize*2+Padding;
System.Drawing.Bitmap image=new System.Drawing.Bitmap(imageWidth,imageHeight);
Graphics g=Graphics.FromImage(image);
g.Clear(BackgroundColor);
Random rand=new Random();
if(this.Chaos)                    //给背景添加随机生成的燥点
{Pen pen=new Pen(ChaosColor,0);
int c=Length*10;
for(int i=0;i<c;i++)
{int x=rand.Next(image.Width);
int y=rand.Next(image.Height);
g.DrawRectangle(pen,x,y,1,1);}
}
int left=0,top=0,top1=1,top2=1;
int n1=(imageHeight-FontSize-Padding*2);
int n2=n1/4;top1=n2;top2=n2*2;Font f;Brush b;
int cindex,findex;
for(int i=0;i<code.Length;i++)
                                    //随机字体和颜色的验证码字符
{cindex=rand.Next(Colors.Length-1);
findex=rand.Next(Fonts.Length-1);
f=newSystem.Drawing.Font(Fonts[findex],
fSize,System.Drawing.FontStyle.Bold);
b=new System.Drawing.SolidBrush(Colors[cindex]);
if(i%2==1){top=top2;}
else{top=top1;}left=i*fWidth;
g.DrawString(code.Substring(i,1),f,b,left,top);}
                                    //画一个边框 边框颜色为 Color.Gainsboro
g.DrawRectangle (new Pen (Color.Gainsboro,0),0,0,
image.Width-1,image.Height-1);
g.Dispose();
                                    //产生波形
image=TwistImage(image,true,8,4);
return image;
```

(10)客户端和服务器端都验证,防止黑客禁掉客户端程序

登录是用户进入系统的首要窗口,攻破登录,对非法用户操作数据就很容易了,开发 Web 程序时应当重视登录窗口的设计,做好程序代码的安全性检查,设置好服务器和数据库的安全,虽然没有绝对的安全,但各种方面小心防范,就可以从很大程度上保证 Web 服务器的安全。

本文从以上 10 个方面考虑防 Web 攻击登录窗口设计,设计的登录窗口系统已在实际系统中使用一年半时间,目前发现攻击的次数越来越少。随着网络的发展,可能有更多的情况需要考虑,本文将不断优化改进。

参考文献

[1] 谭良,周明天.一种新的用户登录可信认证方案的设计与实现[J].计算机应用,2007,27(5):1070-1072.

[2] 王书海,刘明生,肖众.机房管理系统用户登录认证方案设计[J].实验室研究与探索,2008,24(2):37-38.

[3] 伍华健.公开密钥密码体系在网络安全中的应用研究[J].微计算机信息,2006,22(43):14-17.

[4] 胡毅时,怀进鹏.基于 Web 服务的单点登录系统的研究与实现[J].北京航空航天大学学报,2004,30(3):236-239.

[5] 郜激扬.基于 Web 服务的数据库注入攻击与防范[J].华北水利水电学院学报,2008,29(1):89-91.

(收稿日期:2013-11-04)

作者简介:

王命全,男,1986 年生,硕士研究生,工程师,主要研究方向:网格计算,云计算。

张祖莲,女,1984 年生,硕士研究生,工程师,主要研究方向:网络安全,信息检索。

李景林,男,1957 年生,大学本科,高级工程师,主要研究方向:气象生态气候,农业信息服务。