# 浅析验证码在B/S系统安全性中的应用

坤燕昌，曾大海

（西昌学院， 四川 西昌 615013）

【摘 要】 本文分析了验证码在B/S系统安全性中的关键作用，介绍了验证码的类型，探讨了验证码在B/S系统安全性中的具体应用。

【关键词】 验证码；B/S系统；安全性；应用

【中图分类号】TP309.2 【文献标识码】A 【文章编号】1673-1891(2005)03-0079-02

随着WWW应用的发展，在Web中出现了动态Web文档，即B/S程序(基于浏览器/服务器的程序)，伴随而来的就是B/S系统的安全性问题。B/S系统的安全性涉及两方面，即服务器程序与B/S程序，本文仅从B/S程序方面论述验证码在B/S系统中的安全性应用。

## 1 验证码在B/S系统安全性中的关键作用

验证码可用于防止他人对程序进行暴力破解而造成系统不安全。在浏览器中如需输入用户名与密码才能登录某个Web服务，即使用户名与密码中含有特殊字符，但该用户名一旦被他人获取，就可对密码进行猜解，而用户名也可进行猜解。因此，应采取安全措施进行防范。目前B/S系统的安全防范措施不胜枚举，使用验证码即是其中之一。如果登录某个Web服务时需要输入随机产生的一个验证码，可使他人猜解密码不能轻易实现。

使用验证码还能够防止他人使用一些广告软件发布大量的垃圾信息。例如，在我馆主页的留言本中，曾出现过大量的广告信息，这给正常管理带来了较大难度，经过分析发现，此类广告都是通过软件自动加上去的，使用验证码技术后，自动添加广告的软件便失效，从而避免了垃圾信息的发布。

## 2 验证码的类型及其在B/S系统安全性中的应用

验证码可分为数字验证码、汉字验证码或混合型验证码以及图片验证码。

### 2.1 数字验证码及其安全性应用

最早出现的验证码是纯数字的，称为数字验证码。当用户进入WWW登陆页面时，在服务器上随机产生一个数字字符串，并将此字符串传送到浏览器，用户输入用户名与密码的同时，要求输入刚才随机产生的数字字符串，若没有输入随机产生的字符串或所输字符串与刚才产生的字符串不符，即判断此次登陆动作无效，重新产生新的验证码，要求进行重新登陆。这时，可不再对用户名与密码进行验证。

在一般的系统中，验证码的位数通常为4位，4位数字可以完全相同，如此，要猜准验证码的几率就是：$1/10\times10\times10\times10$，即$1/10^4$，当用户登陆失败后，再一次进入登陆页面时，又会产生一个新的验证码。如为了提高安全性，也可以产生5位、6位，甚至更多位数的验证码，但这使正常用户登陆时非常麻烦，影响其网络利用效率。

### 2.2 汉字验证码和混合型验证码及其安全性应用

如既要提高安全性，又不增加验证码位数，可在所要随机产生的字符串中加入其它字符。例如在验证码字符串中加入汉字字符。中国的汉字数量非常多，猜准一位验证码的几率是几千分之一，要猜准4位显然非常难。虽然要随机产生数字较为简单，要随机产生汉字，相对困难些。

目前常用的一种汉字编码是GB2312码。GB2312码是中华人民共和国国家汉字信息交换用编码，全称《信息交换用汉字编码字符集——基本集》，由国家标准总局发布，1981年5月1日实施，通行于大陆，此编码也用于新加坡等地。

GB2312码收录简化汉字及符号、字母、日文假名等共7445个图形字符，其中汉字占6763个。

收稿日期：2005-07-06

作者简介 坤燕昌(1972- )，女，在读硕士，从事计算机、网络、存储的管理与维护以及文献检索课教学等工作。

GB2312码规定：对任意一个图形字符都采用两个字节表示，每个字节均采用七位编码表示，习惯上称第一个字节为“高字节”，第二个字节为“低字节”。GB2312-80包含了大部分常用的一、二级汉字和9区的符号。该字符集是几乎所有的中文系统和国际化的软件都支持的中文字符集，这也是最基本的中文字符集，其编码范围为高位0xA1-0xFE，低位0xA1-0xFE，汉字从0xB0A1开始，结束于0xF7FE。因此，随机产生一个0xB0A1到0xF7FE之间的数字，并将此数字所对应的汉字送往客户端，即形成汉字验证码。在汉字验证码中加入字母、数字等字符则形成混合型验证码，该验证码可使B/S系统安全性更高。

用上述方法产生的验证码会以代码的方式传送到浏览器端，用户可以直接从他的浏览器端HTML代码中提取出验证码，所设验证码形同虚设。如不以代码的方式传送出验证码，将随机产生的验证码写入一幅图片中，并将此图片数据发送至浏览器端，用户就不能从HTML代码当中提取出验证码，从而避免用户从浏览器端提取出验证码。

### 2.3 图片验证码及其安全性应用

图片验证码分数字图片验证码与字符（包括汉字）图片验证码。要实现图片验证码，必须非常熟悉一种图片格式，这样才能将所需的验证码字符加入到图片当中去。在此笔者以BMP文件格式为例阐述将所需数据加入到图像当中的原理。

BMP文件格式分为四个部分：一、图像文件头，二、图像信息头，三、调色板数据（彩色表），四、图像数据。按BMP的格式将数据写入到浏览器端，这样，在浏览器端就可以看到一幅BMP格式的图像。

BMP是位图，所需随机验证码要以点阵的形式在图像数据中加入，在不同的点有不同的颜色，这时，在所产生的BMP位图当中即可看出随机产生的验证码。由于验证码与图片是一整体，图片上的数据又是以随机的方式产生的，所以就无法从浏览器端提取出验证码信息。

目前使用的OCR软件能够从图像信息当中提取出文字信息，针对此可采取在所需图像信息中加入一些与字符点阵无关的其它无用的点，即杂点，杂点越多，识别出验证码的可能性就越小。但需注意，一定要将杂点控制好，不能过多，否则用肉眼可能无法看出验证码。

## 3 验证码在B/S系统中应用时需注意的问题

验证码在B/S系统中应用时需注意以下几个方面，即：(1)当网络用户一进入登陆页面时，就需要产生验证码。(2)对验证码的验证应该在所有信息验证的前面，这样可以节约服务器资源。(3)在对验证码的验证中，无论是网络用户提交的验证码，还是服务端所保存的验证码，都不允许出现空验证码。(4)当验证到网络用户所提交的信息不正确时，就应即刻产生新的验证码或将服务端的验证码信息置空。否则，网络用户只需进入登陆页面一次，即可得到验证码，便可直接用该验证码进行登陆用户名和密码的猜解。

参考文献：

〔1〕万里威，李成友.网络通信中的数据安全技术〔J〕.网络安全技术与应用，2002(7)，P58~62.

〔2〕沙布拉尼尔Ⅱ.验证码能实现验证功能吗？〔J〕.黑客防线，2004(11)，P34~37.

〔3〕非常感觉.轻松绕过登录表单〔J〕.黑客防线，2004(11)，P49~51.

〔4〕http://www.douzi.org/weblog/archives/000018.html.

# Initial Study on Application of Validate Code in the Browser/Server System Security

KUN Yan-chang，ZENG Da-hai

(*Xichang College, Xichang 615013, Sichuan*)

**Abstract**：This paper analyses in the browser server system security from the aspects of key action，sorts，and so on. And discusses the practical application in its system as well.

**Key words**：Validate code；Browser server system；Security；Application