

跨平台 Web 网页防火墙构建

Construction of Firewall for Web pages

龚珍 王乘 (华中科技大学数字化工程中心 430074)

摘要:该文探讨了跨平台 Web 网页的安全性问题,利用 php&mysql 技术,提出了构建跨平台 Web 网页防火墙的 IP 地址技术和用户权限验证法,并给出了实现过程,对基于 Web 的应用程序开发和网络数据库的安全技术的研究具有实际意义。

关键词:php mysql

1 前言

随着 Internet 网络技术的发展和普及,越来越多的公司和机构建立了自己的 Web 站点,其应用系统也开始向 Internet 平台转移。如何保证网络数据的安全,防止非法访问者入侵系统,是 Internet 程序开发者所必须考虑的首要问题。为网页设置防火墙的主要目的是为了实现对某些页面的权限访问,从而维护系统安全或保护系统所有者的利益。防火墙的实现可以采用专业的防火墙软件,但价格昂贵;PHP 是一种在服务器上执行的跨平台的免费脚本语言,通过 PHP 与 Mysql Server 相结合,并利用 PHP 内置的 Session,可以设计出简单,高效,可靠的跨平台的网页防火墙。

2 PHP 技术

PHP 是 PHP: Hypertext Preprocessor (超文本预处理器)的缩写,它是一种服务器端的 HTML 脚本/编程语言,是一种面向对象的、独立于架构的、可移植的、动态的脚本语言。PHP 的所有应用程序都是通过 WEB 服务器(如 IIS 或 Apache)和 PHP 引擎程序解释执行完成的,工作过程分以下几步:

(1) 当用户在浏览器地址中输入要访问的 PHP 页面文件名,然后回车就会触发这个 PHP 请求,并将请求传送给支持 PHP 的 WEB 服务器。

(2) WEB 服务器接受这个请求,并根据其后缀进行判断如果是一个 PHP 请求,WEB 服务器从硬盘或内存中取出用户要访问的 PHP 应用程序,并将其发送给 PHP 引擎程序。

(3) PHP 引擎程序将会对 WEB 服务器传送过来的文件从头到尾进行扫描并根据命令从后台读取,处理数据,并动态地生成相应的 HTML 页面。

(4) PHP 引擎将生成 HTML 页面返回给 WEB 服务器。

(5) WEB 服务器再将 HTML 页面返回给客户端浏览器

3 系统实现

3.1 系统功能分析

网站上某些网页如果只提供授权认证,在用 PHP 设计这些网页的防火墙时,通常采用的方法有:IP 地址过滤法,用户权限认证法以及 IP 地址与用户权限验证相结合的方法。IP 地址过滤法就是对浏览者的 IP 地址范围进行限制,设置只允许已授权的 IP(含某些局域网内部某一范围的 IP) 用户访问;用户权限法就是当用户浏览页面时,需要提交正确的帐号和密码才允许访问;IP 地址与用户权限相结合的方法就是要求浏览者拥有已授权的 IP 地址并提交正确的帐号和密码才允许访问。同时也禁止用户在未经过登陆页面的情况下,通过选取“历史记录”中的 URL 地址或者在地址栏中输入记下来的 URL 地址浏览这些网页。

3.2 系统功能实现

依照上述功能要求,设计系统时可在服务器端的 Mysql Server 中建立一个数据库 firewall,数据库中设计一个已授权的用户信息表:userinfo(ip(15), useid(10), usepwd(10)),表中三个字段分别记录已授权的 IP 地址,用户帐号和密码。当浏览器访问系统登陆时,可显示提示信息指导用户进入系统(一般时要求用户输入帐号和密码),然后调用验证页面,判断用户所用的 IP 地址,输入的帐号和密码在表中是否能够找到,若找到表明是合法用户,允许访问下一页,否则认为是非法用户,拒绝访问并给出错误信息。同时系统管理员通过对数据库表的访问来实现对用户的管理,如用户的添加,权限的变更和密码的更改等。

客户端 IP 地址的获取可使用 PHP 内置对象参数 REMOTE_ADDR,其格式为 \$ 变量名 = \$ REMOTE_ADD 这样就可以得到客户端的 IP 地址。如果是合法的 IP 地址,把它存储在服务器中的 \$ HTTP_COOKIE_VARS["变量名"]中,这样

服务器就可以对客户端的 IP 地址的合法性进行验证。

防止非法用户不按顺序而直接利用 URL 跳转访问 Web 页面,可用 Session 对象来进行控制。Session 对象是 PHP 为克服 HTTP 的无状态性而引入的一个服务端对象,可方便的用来保存客户的个性资料。Session 对象的值保存在服务器方,各个客户的 Session 对象相互独立,用户在某个页面中设置的 Session 值在后续页面中均可访问,使用 Session 可以在 PHP 文件中传递数值,字符串等,当用户在应用程序的页间进行跳转时,存储在 Session 对象中的变量不会清除。

4 应用举例

实际应用时可以设计登陆页面 login.php,如果客户没有登录,在进入每个权限访问的页面时强制客户先访问页面 login.php 实现登陆。在登陆页面包括两个方面的内容,如果 IP 地址符合则验证通过;如果 IP 地址不符合则需要用户输入帐号和密码来判断用户时候合法。成功登陆之后自动返回刚才要访问的页面,否则,不允许访问。

系统的主要程序代码如下:

初始化 Session 变量程序

```
<? php
session_start();
session_register("login") 记录客户成功登陆的信息
$login = false;
? >
```

protect.php 需权限访问的页面

```
<? php
if session("login") < > "true" then
header("Location:login.php")
? >
```

login.php 用户登陆页面

```
<html >
<head >
<title > 用户登陆 </title >
</head >
<? php
$IPAddr = $REMOTE_ADDR; 获得客户端地址;
$cn = @mysql_connect('localhost','root','
pwd') or die("不能连接数据库服务器");建立与数据库
的连接
$strSQL = "select * from userinfo where ip = ". $
IPAddr .""; 验证有效性
$result = @mysql_db_query("userinfo", firewall,
cn);
```

```
if( $result! = null) then $login = true
else $strSQL1 = "select * from userinfo where useid
= ". $ useid . "&usepwd = ". $ user . ""
$result1 = @mysql_db_query("userinfo", firewall,
cn);
if( $result1! = null) then $login = true
endif
if session('login') = true then
mysql_close(cn);
else
echo" IP 地址不在域中或输入的帐号与口令有误,请
重新登陆!"
header("Location:login.php")
? >
<p > 请输入帐号和密码 </p >
<form method = "post" action = "login.php" >
<p > 帐号: <input type = "text" name = "useid" >
</p >
<p > 密码: <input type = "password" name = "usr-
pwd" </p >
<p > <input type = "submit" value = "提交" name
= "butt1" >
<input type = "reset" value = "重写" name
= "butt2" >
</p >
</form >
</body >
</html >
```

5 总结

本文讨论了在基于 Web 的应用系统中如何利用 PHP 和 Mysql Server 来建构 Web 页面防火墙,给出了一个具体的实现方法,通过对数据库的操作,使保护功能性更加强大,安全,该方法能够有效地实现对权限页面的保护,对用 PHP 开发网站,维护 Web 站点的安全具有一定的指导作用。

参考文献

- 1 木森林,PHP Web 数据库开发与实例,清华大学出版社,2003。
- 2 卜胜贤,利用 ASP&SQL Server 构建 Web 页面防火墙,微型计算机应用,2004(3)299-301。
- 3 Jesus Castagnetto 等,PHP 高级编程,机械工业出版社,2001。