安全地使用 TurboCMS

一、使用 Windows 验证替代基于表单的验证

TurboCMS 本身是一套基于 WEB 的应用。通常情况下，TurboCMS 使用数据库保存所有帐号信息，并使用基于 Web 的表单来对用户进行验证。

众所周知，基于 WEB 的表单使用 HTTP 协议，其数据在网络上以明文方式进行传递。因此，攻击者只要使用在合适的地方使用 Sniffer 工具，即可以截获正常用户的帐号信息，从而冒充正常用户进入系统。

TurboCMS 本身的日志也是记录在数据库中，对于攻击者而言，其如果能进入到 TurboCMS 系统，则其操作日志也存在可能。因此，在系统审计方面，使用 TurboCMS 本身的用户验证其安全性也不高。

使用 SSL 对往返的信息进行加密是一个解决办法。但是，我们仍然强烈建议使用基于 Windows 的验证方式。

TurboCMS 系统本身可以与 Windows 的帐号进行集成。从而设置 TurboCMS 使用基于 Windows 的验证，以获得更高的系统安全特性。

与 Windows 验证进行集成包括两方面，一是帐号信息的同步，二是验证的切换和转移。

TurboCMS 设计为可以单方向的同步 Windows 域中的帐号。具体操作步骤：

1、安装 Windows 域控制器，可以在 TurboCMS 服务器上安装，也可以在单独的服务器上安装，然后让 TurboCMS 服务器加入到域里。

2、在 TurboCMS 系统中，系统管理视图，系统设置，设置 ADPath，设置域的路径，例如：dc=turbocms,dc=com

3、在 TurboCMS 系统的用户管理中，右键，选择“同步 WindowsAD”，将域里的帐号信息同步到 TurboCMS 系统中，系统会提示同步哪些数据。

4、在 TurboCMS 系统中，为同步进来的用户设置用户组，并赋予相应的权限。注意，如果以后 AD 中新加了用户，则这些用户在第一次登陆 TurboCMS 时，可以自动进行同步，但是仍然需要为其设置用户组，新的用户才能正常使用 TurboCMS 系统。

在帐号信息同步到 TurboCMS 系统之后，就可以设置验证了。步骤如下：

1、 在 TurboCMS 服务器上，打开 Internet Information Service 管理器，找到站点 TurboCMS，属性， 目录安全性，编辑，去掉“启用匿名访问”前的勾，在“集成 Windows 验证”前打上勾，按确认。

2、 以浏览器打开 TurboCMS 系统，IE 会弹出如下图的对话框，提示输入用户名和密码，在这里输入帐号，按确认即可自动进入 TurboCMS 系统。

注意，在与 Windows 验证进行集成后，原来 TurboCMS 的帐号仍然可以使用，如果有需要使用原来的帐号进行登陆，则可以在登陆 TurboCMS 后，点界面右上方的“退出登陆”即可回到原有的 Web 登陆方式。

另外，需要注意的是，尽管在同步了帐号后，在 TurboCMS 里可以看到域中的帐号，但是在 TurboCMS 里对这些帐号的修改将是无效的。所有对帐号的修改和设置应当在 AD 里去进行。

二、使用两个 IIS 站点

TurboCMS 本身是一套基于 Web 的应用。在 TurboCMS 系统安装的时候，安装程序会在 IIS 里创建一个名为“TurboCMS 例子站点”的 IIS 站点，并将 TurboCMS 作为一个应用部署在这个站点之下，同时，TurboCMS 所维护的第一个站点也将直接使用这个站点来进行。就是说，默认情况下，TurboCMS 里所管理的第一个站点与 TurboCMS 应用本身是在同一个站点下。

这样实现的好处是方便安装，并让用户可以快速上手使用 TurboCMS，但是这样也带来一些潜在的安全隐患。

假设攻击者来自 TurboCMS 的正常用户，例如一个普通的编辑，他是一个技术的精通者，他希望使用一些手段将自己的权限提升为系统管理员，那么他可能通过精心构造的一些包含 javascript 的 HTML 代码作为文章的内容提交到系统中，那么他可能通过 XSS（交叉站点脚本攻击）达到目的。

我们有一个假设，那就是在系统中，除了超级管理员以外，别的用户均不可信任，因此，来自内部的攻击也应当尽量避免。

一个必要的步骤是通过设置，将 TurboCMS 本身所在的站点与 TurboCMS 所维护的站点分离开。

具体的步骤如下：

1、 在 IIS 管理器里查看站点“TurboCMS 例子站点”的属性，记录下其指向的路径。

2、 在 IIS 管理器里新建一个站点，与“TurboCMS 例子站点”指向同一个目录，设置其“默认内容文档”。并取消该站点的一切执行许可，包括 ASP 的执行。我们假设通过 CMS 所维护的站点主要是为了维护内容，因此对于站点里的 ASP 等脚本不需要在 TurboCMS 里进行预览。我们可以使用端口，或 IP 地址来区分这个新的站点与“TurboCMS 例子站点”。

3、 将“TurboCMS 例子站点”站点的目录指向一个空的目录。

4、 在数据库 TurboCMS 中，打开表 Site，找到字段 ip 和 port，将其修改为刚创建的站点使用的配置。

注意，做了以上的设置后，即便是 TurboCMS 服务器拥有多个 IP 地址，我们将只能使用一个 IP 地址来访问 TurboCMS，这个 IP 地址应当与“TurboCMS 例子站点”里的 IP 地址完全一致（这一点与 TurboCMS 维护多个站点时是类似的）。

三、使用 SSL

使用 SSL 来加密传输的数据对于提高系统的安全性有很大的提升。加密的用户名和密码可以保护用户的帐号。如果用户发表的信息本身是需要保密的，SSL 更加迫切。

使用 http://www.microsoft.com/china/technet/security/guidance/secmod30.mspx 里介绍的步骤设置 IIS 使用 SSL 证书。

注意，如果尚没有证书，可以到 microsoft 或 Verisign 申请。如果使用自己的证书服务器，则需要在每一个客户端上设置信任自己的证书服务器。

四、删除 TurboCMS 里不必要的文件。

我们在第一步里已经设置使用基于 Windows 的验证，因此，TurboCMS 本身的用户管理功能可以不再使用。以下文件可以删除：

/cms/usermanager/prenewuser.asp
/cms/usermanager/newuser.asp
/cms/usermanager/predeluser.asp
/cms/usermanager/deluser.asp
/cms/groupmanage/group/prenewuser.asp
/cms/groupmanage/group/newuser.asp
/cms/groupmanage/group/predeluser.asp
/cms/groupmanage/group/deluser.asp

五、IIS 的安全设置

设置错误处理信息为一段固定的话，而不是详细的错误信息。

如果 CMS 位于防火墙内，则用以下方法设置 IIS，禁止 IIS 将自己的 IP 地址暴露到外网。

To set the **UseHostName** property, follow these steps:

1. Click **Start**, click **Run**, type **cmd**, and then click **OK** to open a command prompt.
2. Change to the folder where the Adsutil.vbs tool is located. By default, this folder is the following:
   %SYSTEMROOT%\Inetpub\AdminScripts
3. Type the following command, where *x* is your site identifier:
   cscript adsutil.vbs set w3svc/*x*/UseHostName true

To set the **SetHostName** property, follow these steps:

1. Click **Start**, click **Run**, type **cmd**, and then click **OK** to open a command prompt.
2. Change to the folder where the Adsutil.vbs tool is located. By default, this folder is the following:
   %SYSTEMROOT%\Inetpub\AdminScripts
3. Type the following command, where *x* is your site identifier and *hostname* is the alternate host name that you want to use:
   cscript adsutil.vbs set w3svc/*x*/SetHostName *hostname*

您可以通过将以下注册表值设置为 1，以便从 IIS 6 中删除服务器横幅：
HKLM\SYSTEM\CurrentControlSet\Services\HTTP\Parpameters\DisableServerHeader

六、其他安全设置

进行其他必要的安全设置，以保证操作系统和网络平台本身的安全性。