S. H. E. R. P. A

Web Athletics System

System for ***H***andicapping, ***E***vent ***R***ecording, and ***P***rocessing of ***A***thletics

Operations Manual

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this document is to provide an administration and operational guide to the SHERPA web application. It describes the software requirements; database compatibility issues; and web server security issues.

An installation walk through for a stand-alone or small intranet environment is also provided for first time administrators or evaluation purposes.

1.2 Related Documents

More information on SHERPA is provided in the following documents:

- SHERPA User Guide

1.3 Intended Audience

This document is intended for administrators who will be involved in the maintenance and support of the SHERPA web application. It is also intended for users with a reasonable level of competency, who wish to install and evaluate SHERPA.

2 Software Requirements

The SHERPA web application is a distributed three-tier web database system. It consists primarily of three layers or tiers:

- The client web browser, which acts as the presentation or user interface layer;
- The web server, which acts as the middleware, of which is extended with the use of a server extension program consisting of the business logic; and
- The database server, for persistent storage of business objects.

2.1 Client Web Browser

The SHERPA web application generates HTML web pages dynamically based on data stored in the database. When a client web browser requests to view a web page SHERPA generates the web page in its entirety before sending it. This is done much like a CGI (Common Gateway Interface) application.

Unbeknownst to the client web browser, the generated web page is just like any other static web page.

The web pages generated by SHERPA do not contain any browser specific html tags or any JavaScript.

The only requirement on the web browser is that it must support cookies. The cookies are used to maintain state information for the client. Cookies generated by SHERPA are not persistent, in that they are only held in memory by the client web browser, and are destroyed on termination of the web browser.

This is a great advantage, as the required versions of web browsers needed are vastly broadened. In fact, any web browser on any platform can be used as a client to SHERPA as long as it supports cookies, and the user has not disabled the use of cookies.

Currently Microsoft Internet Explorer 3.x or higher supports cookies, as well as many other browsers such as Netscape Navigator.

2.2 Web Server

The SHERPA web application is an extension program written specifically to extend functionality on the web server. As such, it is on the web server were SHERPA is deployed, and much of the discussion on required software is based here.

The SHERPA web application was written to take advantage of the Microsoft Foundation Classes (MFC) and Microsoft's Internet Server Application Programmers Interface (ISAPI). This choice was made for several reasons, some of which are the ease of distribution of a single extension program, and the high speed of compiled code.

SHERPA communicates to the database server by using Open Database Connectivity (ODBC); this provides a means for database independence. The Microsoft ODBC driver manager and an ODBC driver for your database must be installed on the web server.

This design decision means that your choice of web server is limited to one that supports ISAPI, and the platform it runs on is limited to a Microsoft Windows platform. To the best of the author's knowledge, Microsoft is the only vendor that provides an ISAPI compliant web server.

That is not to say that the Microsoft platform and programmers interface is in any way a limitation, quite the contrary, as MFC, ISAPI and ODBC provide a very powerful and feature rich environment.

2.2.1 Microsoft ISAPI Compliant Web Server

One of the many advantages of using a Microsoft ISAPI web server is that it is freely available, and costs nothing to run. You may even be unaware that it is already installed on your system.

SHERPA will run on any Win32 Microsoft Windows platform, including (but not limited to) Windows 95, 98, Windows NT 4.0 and Windows 2000.

Microsoft Personnel Web Server (PWS) is available for the Windows 9x platforms, and is a good choice as an evaluation or small intranet deployment of SHERPA. PWS4.0 comes bundled with Windows 98 and can be installed from the "\add-ons\pws" folder on the original Windows 98 CD. For Windows 95, you can download PWS from the Microsoft web site. You must install PWS4.0 or higher.

Microsoft Internet Information Server (IIS) is a more robust and feature rich web server designed for use with the Windows NT and 2000 platforms. As such, it is a good choice for a full-blown enterprise deployment of SHERPA on a large intranet or on the Internet.

Windows 2000 comes with IIS5.0, while Windows NT 4.0 usually comes with IIS3.0. The Windows NT 4.0 Option Pack is an additional component that may or may not have come bundled with Windows NT 4.0. The Option Pack consists of (among others) IIS4.0. If you choose to use Windows NT 4.0 to deploy your web server, you must install IIS4.0 rather than IIS3.0. The Windows NT 4.0 Option Pack is also freely available on the Microsoft web site.

More information about Microsoft Internet Information Server can be found at the following web site:

- http://www.microsoft.com/ntserver/web/exec/feature/Datasheet.asp

Personal Web Server 4.0 for Windows 95 is contained in the Windows NT 4.0 Option Pack, which can be downloaded from the following web site:

- http://www.microsoft.com/msdownload/ntoptionpack/askwiz.asp

2.2.2 Microsoft Foundation Class Library & ODBC Driver Manager

To support the SHERPA web application, several run-time libraries are required. These include the Microsoft Foundation Class Library; Microsoft C and C++ Run-Time Libraries; and the Microsoft ODBC Driver Manager.

Included in the distribution of SHERPA are the Microsoft Visual C++ Redistribution Pack, and Data Related Services.

2.2.2.1 Microsoft Visual C++ Redistribution Pack

The Microsoft Visual C++ Redistribution Pack contains all the components for deploying an application that requires the Microsoft Foundation Class Library and C/C++ Run-Time Libraries.

The follows table lists the Versions of Libraries required by SHERPA.

Filename	Version	Description
MFC42.DLL	6.0x.xxxx	Microsoft Foundation Class Library
MSVCRT.DLL	6.0x.xxxx	Microsoft C Run-Time Libraries
MSVCP60.DLL	6.0x.xxxx	Microsoft C++ Run-Time Libraries

Table 1 – Required Libraries for SHERPA

These three DLL files should be located in your windows system folder. If they already exist, then you may only need to install the VC-Redist Pack if your version is older than the version required by SHERPA. For more information, and to download the latest version of the VC-Redist Pack, visit the Microsoft Knowledge Base web site (Article ID: Q259403):

- http://support.microsoft.com/support/kb/articles/Q259/4/03.asp

You can determine the file version by selecting the file, Right-Mouse-Click, select “Properties”, and then select the “Version” tab as illustrated below.

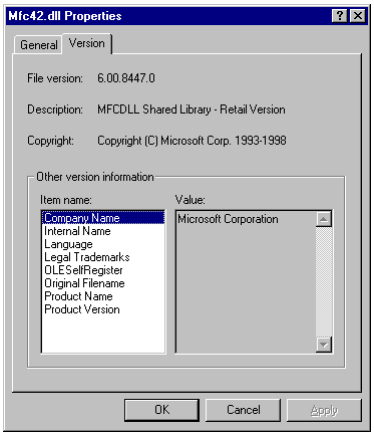

Figure 1 – Version Info for C:\WINDOWS\SYSTEM\MFC42.DLL

2.2.2.2 Data Related Services

Data Related Services for ODBC include:

- MDAC - Microsoft Data Access Components
- DCOM - Distributed Component Object Model

The Microsoft ODBC Driver Manager is installed with MDAC.

In most cases you will not need to install these programs, as they are already on your system, you can check this by going to the Control Panel and opening the “ODBC Data Sources (32bit)” administration applet. Click the “About” tab, if all the file versions displayed in the list are at least version 3.51x.xxxx, then no installation is necessary.

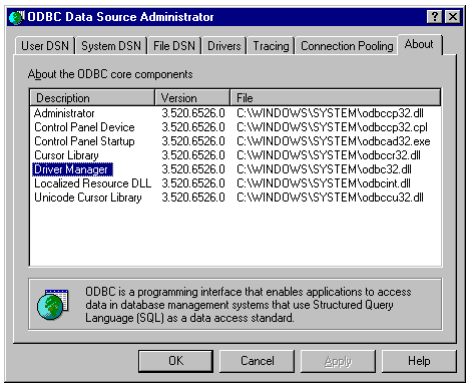

Figure 2 – “ODBC Data Sources (32bit)” Administration Applet

Obviously, if you do not even have the ODBC icon in your Control Panel, then you need to install MDAC (sometimes the case on Windows 95).

You may download the latest version of MDAC from the following site:

- http://www.microsoft.com/data

Windows 95 users should ensure that you have DCOM installed. DCOM must be installed prior to installing MDAC. Note that Windows 2000, Windows NT 4.0, and Windows 98 have DCOM built in.

You can download the DCOM redistributable from the following site:

- http://www.microsoft.com/com

After installing MDAC and or DCOM check the versions of the MFC and C/C++ Run-Time Libraries (outlined above), as these files may be replaced by installing the Data Related Services.

2.3 Database Server

Potentially, you can use any Relational Database Management System (R-DBMS) as your database server, provided that the vendor supplies ODBC drivers. This is usually the case for most database vendors.

The SHERPA web application only uses ODBC to communicate with the database server, all that is required is to install the ODBC drivers on the web server to support the communications to your database server.

For an evaluation or small intranet deployment of SHERPA you may wish to install the database server on the same machine as your web server.

For a full-blown enterprise deployment of SHERPA on a large intranet or on the Internet, and also in terms of scalability, you should install your database server on a separate machine from your web server, this is also facilitates securing the database server behind a firewall. Installing the database server on the web server should only be an interim measure when deploying SHERPA on the Internet.

Installing the database server on a separate machine from the web server also means that you can configure your database server on the platform of your choice.

The only restricting factor in choosing your database server is whether the vendor's R-DBMS complies with the SQL-92 standard. See the following section on Database Compatibility Issues for a more complete discussion of SQL-92 conformance and the requirements by SHERPA.

For evaluation purposes you can use a Microsoft Access (Jet Database Engine) database with SHERPA. The ODBC driver manager installs by default a Microsoft Access ODBC driver that allows you to create a Microsoft Access database even if you don't have Microsoft Access installed.

If you want to evaluate the SHERPA web application in an enterprise environment you may wish to download Microsoft SQL Server – Evaluation Edition.

- http://www.microsoft.com/sql/productinfo/evaluate.htm

Using a robust database server rather than using a Microsoft Access database vastly improves the performance of SHERPA, especially in terms of processing athletics results.

2.4 Summary

Any web browser that supports cookies can be used as a client to the SHERPA web application.

Any SQL-92 compliant R-DBMS on the platform of your choice can be used as the database server for SHERPA, provided that the vendor supplies ODBC drivers.

For evaluation purposes you may choose not to install a database server at all, but rather use a Microsoft Access database, even if you don't have Microsoft Access installed on the system.

Any ISAPI compliant web server installed on any Microsoft Windows Win32 platform can be used as the SHERPA web server, provided that you check or upgrade your versions of ODBC and MFC; and that your database server's ODBC drivers are installed on the web server.

Evaluating SHERPA with a Microsoft Access database and an ISAPI web server will cost you nothing, as all are freely available.

3 Database Compatibility Issues

The SHERPA web application handles some very complex functions for processing and calculating handicaps on athletic results. Part of the processing is handled internally by the system, while part is handled by issuing SQL statements to the database server.

While much of the SQL written was as simple as possible, it was inevitable that complex SQL statements are used in processing the athletic results. All the SQL that SHERPA issues to the database server is ensured to be SQL-92 compliant, and as long as the database server implements the SQL-92 specification, everything will function correctly.

The conformance of SQL-92 by some database venders is the issue that is at stake. It is a known fact that all most all database venders do not implement the full SQL-92 specification, and that some implement more of the specification than others. Adherence to the SQL-92 specification involves three levels; entry, intermediate, and full.

In terms of SHERPA, most SQL is simple enough to comply with entry level SQL-92 specification, but the noticeable exception is the use of the "OUTER JOIN" and "INNER JOIN" operators, which is part of the intermediate SQL-92 specification.

An example of the SQL-92 OUTER JOIN operator is as follows:

```
SELECT * FROM (a LEFT JOIN b ON (a.x = b.x));
```

or

```
SELECT * FROM (a LEFT JOIN b USING (x));
```

Although Oracle supports the use of outer joins, it does not support the SQL-92 OUTER JOIN operator but rather its own proprietary form:

```
SELECT * FROM a, b WHERE a.x = b.x (+);
```

As is with Informix:

```
SELECT * FROM a, OUTER b WHERE a.x = b.x;
```

Microsoft SQL Server does support the SQL-92 OUTER JOIN operator, even though it does not implement the full SQL-92 specification, as does the Microsoft Access Jet database engine.

These two R-DBMS's have been fully tested with the SHERPA application and are fully compatible and recommended.

There are other R-DBMS's that support the SQL-92 OUTER JOIN operator, but have not been tested with SHERPA.

Your choice of database server is limited to one that adheres the SQL-92 intermediate specification, or at least implements the SQL-92 OUTER JOIN operator.

4 Web Server Security Issues

4.1 Windows 2000 Security Policies

When deploying your Web Server on the Windows 2000 platform, you should be aware of the tighter security policies that are placed on the Web Server. Internet Information Server (IIS) on both Windows NT and 2000 is configured with a default login that has sufficient privileges to access resources such as HTML pages for serving to a client Web Browser. Usually this login is named "IUSR_<computer name>", and is created by the IIS installation.

The SHERPA web application uses the Windows Registry on the Web Server to store configuration information such as ODBC settings. On Windows NT 4.0 the IIS login has sufficient privileges to read and write to the Windows Registry, while on Windows 2000 this login does not have write permissions.

It is necessary to configure the IIS login with permission to write to the Windows Registry, at least until you are satisfied with the SHERPA installation. Once SHERPA has been configured, writing to the Windows Registry is usually no longer necessary.

Consult the Windows 2000 Documentation and the Internet Information Server Documentation for more details on Security and Permissions.

4.2 HTTP Network Traffic

The SHERPA web application uses cookies extensively. It validates a user's login every time a web page is generated, using cookie information. This section tries to explain some security issues which may be raised with this method of user validation, and the associated network traffic of clear text passwords.

4.2.1 Cookies

Most web browsers today support the use of cookies. A cookie is merely small piece of information stored on the client by the web browser. Before a cookie can be stored it must be received from the web server. This can be very useful for example, if a web page has an option for changing its default colour scheme, the colour preference can be stored as a cookie on the client. A person visiting the web page for a second time (perhaps a week later) will not have to change their colour preference, as it will be remembered with the use of the cookie.

Every time a client web browser requests a web page from the server, it issues a HTTP GET command. Every time the client web browser issues this command, information is provided in the HTTP header of the request, for example "REMOTE_ADDR" is the IP address of the remote host making the request. A cookie is sent with the HTTP header in the same manner.

Cookies also have a number of settings, one of which is the expiry date. A persistent cookie is stored to the disk on the client only when the expiry date has a value; this is so the cookie information can be retrieved at a later date.

A temporary cookie (one that has no expiry date) is not stored on the disk, but rather in the web browser's memory address space. This means that the cookie is discarded when the browser is terminated.

4.2.2 User Validation

The method by which the SHERPA web application validates users is with temporary cookies. When the user logs on to Athletics System their login name and password is stored as a cookie by the user's browser. Every subsequent request for a new web page requires the user's login/password cookie to be sent and validated again.

SHERPA uses the Win32 Crypto API to encrypt passwords. By default, encryption is turned off, but is easily enabled from the SHERPA Options module, Cryptography page. When encryption is enabled, the password cookie will be encrypted for all subsequent requests for new web pages.

Encryption of the password cookie does not prevent the password being transmitted in plain text when the user first enters their password at login, i.e. the cookie has not yet been set. This means that a password is initially sent in plain text, and can be exploited by a malicious user.

One method by which to circumvent this problem is to encrypt all transmissions by using Secure Sockets Layer (SSL).

The SHERPA web application has several types of user roles, enabling different users to access certain privileged areas of the SHERPA system. When an administrator logs on, they can access all or most areas of the SHERPA system. Any web pages generated by SHERPA are sent across the Internet in plain text as part of the HTML web page. The web page may contain such private information as a person's home address or telephone number. A malicious user by means of eavesdropping could obtain this information.

If you consider that the transmission of data between the web server and web browser is sufficiently private, then you should consider encrypting it by using SSL.

4.2.3 Encrypting Data with Secure Sockets Layer (SSL)

The Secure Sockets Layer protocol provides communications privacy over networks by using a combination of public key cryptography and bulk data encryption for data privacy. By using this protocol, clients and servers can communicate in a way that prevents eavesdropping, tampering, or message forgery.

4.2.4 Simplified Overview of Secure Sockets Layer (SSL)

Cryptographic keys are created at the same time in pairs: a public key and a private key. The public key is given to anyone. The private key is kept and safeguarded by the server. Both keys are required for any exchange of information.

The web browser encrypts data (such as HTML) by using the server's public key. The encrypted data is sent to the server. The data is decrypted by the server, which uses its private key. The data can be decrypted only with the private key, held by the server.

4.2.5 Enabling Secure Sockets Layer (SSL)

To enable SSL, you must obtain a X.509 server certificate. You can acquire a server certificate from a trusted third party Certificate Authority (CA) such as VeriSign. An un-trusted server certificate can also be created if you configure your web server to be its own CA. In such a case your web server is not any less secure than if you had a trusted certificate, but rather the certificate is not known or trusted by the client web browser and subsequently the web browser will ask the user if the certificate should be trusted or not.

For more information about using SSL with IIS, see the Internet Information Server Installation and Administration Guide.

The trade off in protecting sensitive information with encryption is reduced performance. Because SSL uses complex encryption, and because encryption requires considerable processor resources, it takes much longer to retrieve and send data from SSL-enabled directories.

5 Windows Registry

The SHERPA web application stores all of it settings in the Windows Registry. All items stored here (except one) can be directly manipulated from SHERPA in either the Options module or the Maintenance module. The registry key where settings are stored is:

- \HKLM\Software\Darian\WebAthl

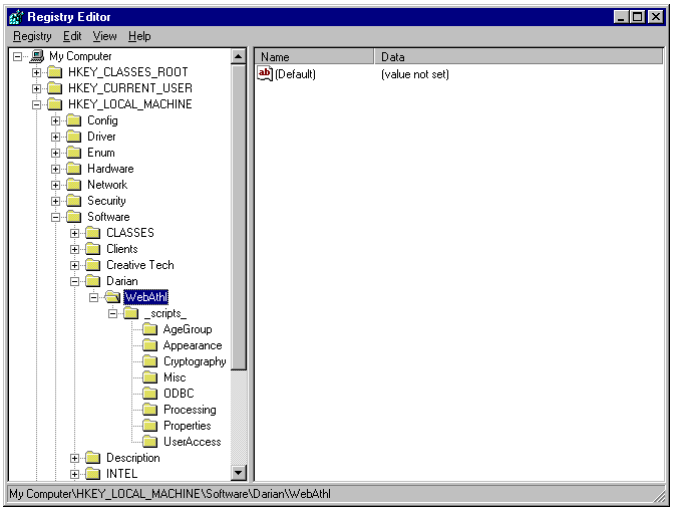

Figure 3 – Windows Registry Editor

5.1 Cryptography

The only option that is not configurable from SHERPA is the Cryptography password. Manipulating the Windows Registry directly is the only way to modify it.

By default, user names and passwords are stored in the database in clear text. Enabling Cryptography from the Options module configures SHERPA to encrypt the passwords before storing them in the database.

When Cryptography is enabled, the Maintenance module allows all passwords to be encrypted and decrypted. This is important if you want to change the Cryptography password in the registry. The Cryptography password is used as the decryption key for user passwords in the database. If the key is changed in the registry, all currently encrypted passwords in the database will become unreadable. If you wish to change the Cryptography password, then you must first ensure that all passwords in the database are decrypted first, from the Maintenance module. After changing the Cryptography password, you can then re-encrypt all user passwords with the new key.

5.2 Cryptographic Implementation

Encryption is the process of encoding data into cipher, a form unreadable without a decoding key. Decryption is the reverse process of converting encoded data to its original un-encoded, plaintext form. To encode plaintext, an encryption key is used to impose an encryption algorithm onto the data. To decode a cipher, a user must possess the appropriate decryption key.

Symmetric encryption is the approach whereby the same key is used for encoding and decoding data. This key is known as a Session key.

SHERPA uses symmetric encryption for encoding user passwords for storage in the database as well as the user login cookie. The Cryptographic password stored in the Windows Registry is used to derive a Session key, which is then used to encode the user password.

The Microsoft Base Cryptographic Provider is used along with a Hashing algorithm based on the MD5 Message Digest to derive a Session key. A Data Encryption algorithm based on the RC2 64-bit Symmetric Block Cipher is then used to encrypt the user password.

The Session key derived using the MD5 hashing algorithm implemented by the Microsoft Base Cryptographic Provider is by default 40-bits in length.

The above-mentioned cryptographic algorithms are well known and can be reviewed in detail in any reference on cryptography.

5.3 Multiple Instances of the SHERPA Web Application

It is very easy to configure multiple instances of the SHERPA web application. By doing this you are able to run SHERPA with multiple (and completely separate) databases.

For example, you may wish to host more than one sporting club on the same web server. Each club will have it own series of events, members and financial management.

SHERPA stores its configuration information in the Windows Registry according to the URL that accesses it. For example, if you hit the web site by using http://localhost/scripts/MyAthleticsClub/WebAthl.DLL, then the configuration information in the registry is stored under the key "\HKLM\Software\Darian\WebAthl_scripts_MyAthleticsClub_". You may have a second sporting club, which accesses the site by using the URL http://localhost/scripts/MyCyclingClub/WebAthl.DLL, in which case the configuration information is stored in the registry under the key "\HKLM\Software\Darian\WebAthl_scripts_MyCyclingClub_". Each instance of SHERPA is configured independently with separate databases and settings. This is also very useful for hosting both a production and test database from the same web server.

The only requirements for hosting multiple sites are that the WebAthl.DLL is accessed from two different URL's. This can be accomplished by either copying the WebAthl.DLL to two different physical directories on the web server, or by aliasing a second virtual directory to the first physical directory.

Each organisation or sporting club is required to hold a sperate license. So in terms of licensing, when you host more than one site, you must obtain separate licenses for each site.

6 Licensing Information

The SHERPA web application runs in two modes; registered, and evaluation or unregistered mode. When running in evaluation mode, there are no restrictions on the functionality available, the only restrictions is on the amount of data permitted to be processed in the database.

These restrictions are as follows:

- 2 Series (of Events)
- 10 Events per Series
- 100 People

Of course, you can manually load the database with more data, but the SHERPA web application will not process this extra data.

We believe that this restriction is enough to give you a flavour as to the functionality that the SHERPA web application can provide for your club, but not enough storage to process more than a few months worth of sporting events.

Once you have installed and configured SHERPA, and are satisfied that it meets your club's requirements, you are then encouraged to purchase an "unlock" license key.

7 Installation Walk Through for a Stand-Alone or Small Intranet Environment

This section will guide you through a sample installation of the SHERPA web application on Windows 98 with a Microsoft Access database.

An installation on Windows NT or 2000 is fairly similar, except that security issues are involved.

Please read the Software Requirements section for detailed information on why certain software is installed.

7.1 Software Pre-Install

For the purposes of this guide, I reformatted my hard disk drive and performed a clean install of Windows 98.

I then upgraded the system by installing the latest versions (at the time) of the following software (in order):

- Internet Explorer 5.5
- DCOM 98 version 1.3 for Windows 98
- MDAC version 2.6
- MDAC Jet 4.0 service pack 3 (for MS Access ODBC Jet Drivers)
- Personal Web Server 4.0
- Microsoft Visual C++ Redistribution Pack

Note: All the above software was downloaded off the Microsoft web site (outlined in the Software Requirements section).

Note: If you wish to install on Windows 95, you may need to apply the WinSock2 update (also available on the Microsoft web site).

Note: If you wish to install on Windows 95, you must install DCOM 95 rather than DCOM 98.

Note: If you wish to install on Windows NT or 2000, then there is no need to install DCOM at all, as it is built in to the operating system.

Note: Not all of the above software is required; it depends on your system and what it currently installed. As a minimum you must have PWS4.0 and the ODBC Driver Manager (MDAC) installed in the Control Panel, with the ODBC drivers you wish to use. Also required is version 6.x of the MFC and C/C++ Run-Time libraries (outlined in the Software Requirements section).

7.2 Configuring the Web Server

Configuring the web server is relatively simple, in that you only need to copy the "WebAthl.DLL" file into a virtual folder that allows the "execute" permission. This is discussed below.

There are several folders created by the PWS installation.

- \InetPub
- \InetPub\wwwroot\
- \InetPub\scripts\

By default, the Web Server configures the folder "\InetPub\" for storage of html documents. The "\InetPub\wwwroot\" folder is where static web pages can be stored, and usually has "read" permissions. The "\InetPub\scripts\" folder is where CGI and executable programs can be stored, and usually has "execute" permission without "read" permissions. These folders and permissions can be managed from the Personnel Web Manager (installed by PWS).

The physical folders on disk are mapped to virtual folders on the web site. For example, browsing to the URL http://localhost/ will map the root virtual folder to the "\InetPub\wwwroot\" physical folder, while http://localhost/scripts is mapped to "\InetPub\scripts\".

The SHERPA web application is contained entirely in the "WebAthl.DLL" file. It is an executable program, and as such should only be placed in folder on the web server that has "execute" permission.

Depending on how you want to configure your web site, you may want to copy the "WebAthl.DLL" file into the "\InetPub\scripts\" folder, but you can put it any virtual folder that you allocate the "execute" permission.

If you open up your web browser and enter the URL http://localhost/scripts/WebAthl.DLL, you should see the SHERPA splash page. There should be an error message at the bottom of the page prompting you to configure the database connection.

7.3 Configuring the Database

Several simple steps are involved in configuring the database and the ODBC connection to the database. These will vary slightly depending on the database server you wish to use. It generally consists of providing a Data Source Name to connect your database through ODBC. This section will outline how to configure the Microsoft Access ODBC connection.

From the "Control Panel", open the "ODBC Data Sources (32bit)" administration applet. Choose the "System DSN" tab.

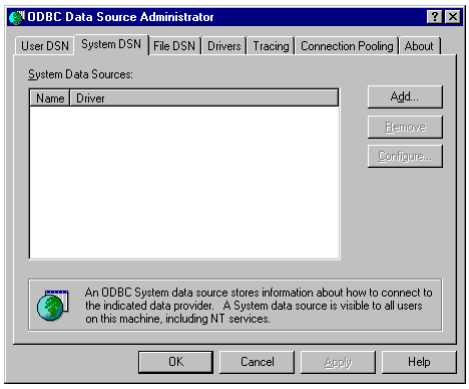

Figure 4 – "ODBC Data Sources (32bit)" Administration Applet

There are three types of Data Sources that can be created: User; System; and File. It is important to choose the System DSN as this allows the Web Server service to access the Data Source.

Click the "Add" button from the "System DSN" tab.

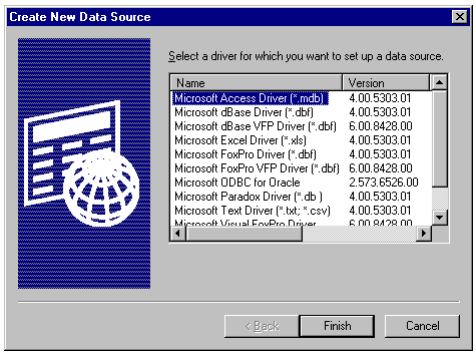

Figure 5 – "Create New Data Source" Dialog Box

From the "Create New Data Source" dialog box, choose the "Microsoft Access Driver (*.mdb)" and click "Finish".

The "ODBC Microsoft Access Setup" dialog box should appear.

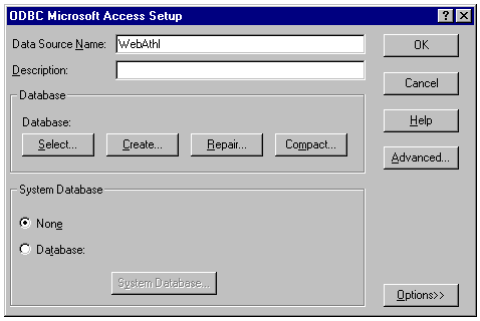

Figure 6 – "ODBC Microsoft Access Setup" Dialog Box

Provide a “Data Source Name” of your choice. If you already have an Access database that you wish to connect to choose the “Select” button and locate your database file. Otherwise, choose the “Create” button, to create a new database.

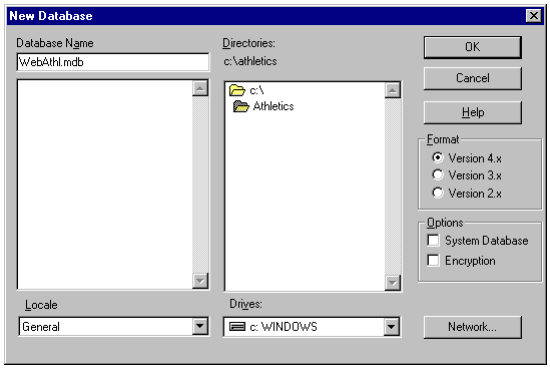

Figure 7 – “New Database” Dialog box

Choose a location where you wish your database to lie, and enter a name for it.

Notice the different Versions of the database that can be created. Depending on the version of MDAC you have installed and the version of the Microsoft Access driver you have, you may need to choose Version 3.x. If you have installed all the latest versions of MDAC and the Microsoft Access driver, then you can use a Version 4.x database. Microsoft Access 2000 can open a Version 4.x database, and Microsoft Access 97 can open a Version 3.x database.

Click “OK” to create the new database.

Figure 8 – “Success” Dialog Box

Confirm the “Success” dialog box, and notice the name of the your new database in the “ODBC Microsoft Access Setup” dialog box.

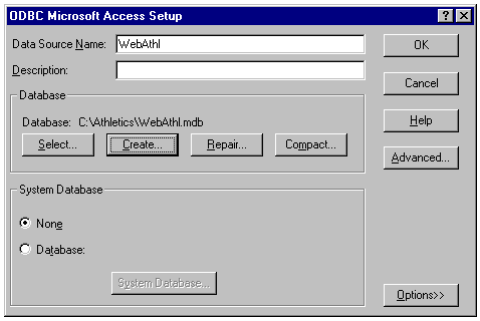

Figure 9 – “ODBC Microsoft Access Setup” Dialog Box

You may also notice the “Repair” and “Compact” buttons. These can be used to maintain the database periodically. Compacting the database should be done regularly as Microsoft Access, keeps a log of all the transactions processed on the database. If you do not compact the database to clear the logs, then it will continue to grow.

Click “OK” to create the new Data Source.

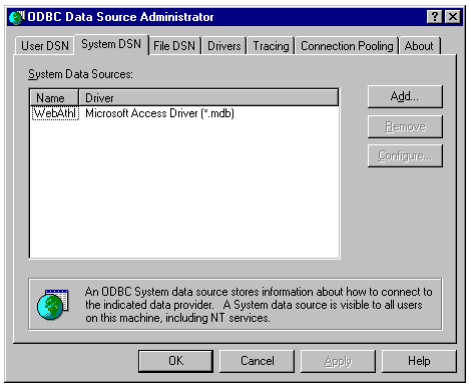

Figure 10 – “ODBC Data Sources (32bit)” Administration Applet

Notice your new Data Source and the driver it is using. You can configure it at any time in the future by returning to the “ODBC Data Sources (32bit)” administration applet.

That’s it; you’ve successfully created a new empty database and provided it with an ODBC Data Source Name.

7.4 Configuring SHERPA for ODBC

This section explains how to configure the SHERPA web application with an ODBC database. It is simply a matter of providing the ODBC details in the SHERPA ODBC Setup Page.

After successfully configuring the Web Server and creating an ODBC Data Source Name, you can now link the two together using SHERPA. Open up your web browser and enter the URL http://localhost/scripts/WebAthl.DLL, you should see the SHERPA splash page. There should be an error message at the bottom of the page prompting you to configure the database connection.

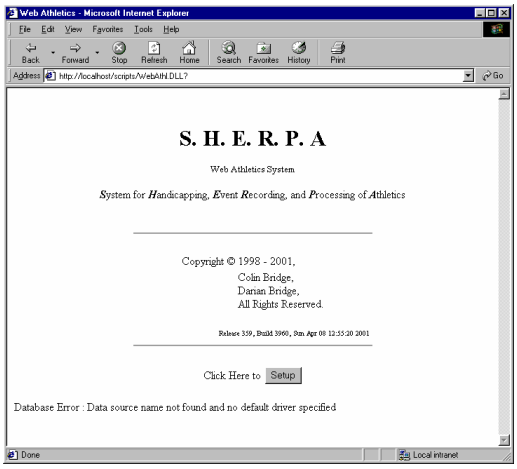

Figure 11 – SHERPA Splash Page

The SHERPA web application checks for a database configuration when it is invoked. Normally the "Click Here to [Start]" button will be displayed, but only if the database configuration is valid. The "Click Here to [Setup]" button will be displayed, when the database configuration is invalid.

The "Click Here to [Start]" button links to the "Start Menu" page while the "Click Here to [Setup]" button links to the "ODBC Setup" page. Click it.

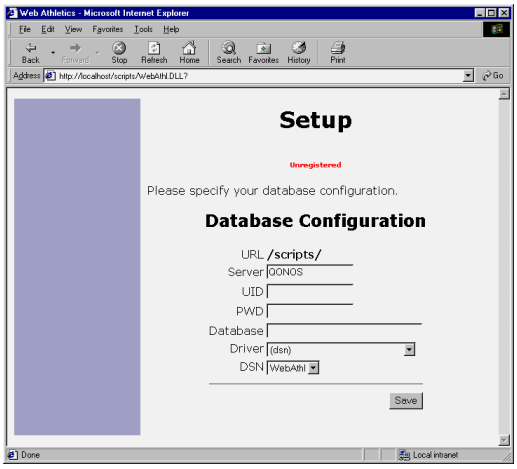

Figure 12 – SHERPA ODBC Setup Page

The "ODBC Setup" page contains several fields that are required to configure SHERPA for connecting to the ODBC Data Source.

The following table describes each of the fields on the "ODBC Setup" page.

Field	Description
URL	The Virtual Directory where the WebAthl.DLL is located.
Server	The name of the computer where the database is installed. By default, SHERPA will obtain the Windows Name of the web server. This can also be an IP address, or a Fully Qualified Domain Name (FQDN).
UID	The Login Name used to connect to the database. SHERPA also uses this user name for the super user login. If you do not require a Login Name to connect to the database, then you can still enter a name here for SHERPA to use as the super user login.
PWD	The Password associated with the above Login Name.
Database	The Name of the database. Leave this empty when using a Data Source Name (it will be copied from the DSN you select).
Driver	The Driver to use when connecting to the database. The list is obtained from the ODBC driver manager on the web server. Select (dsn) when using a Data Source Name.
DSN	The Data Source Name to use when connecting to the database. The list is obtained from the currently configured Data Sources on the web server.

Table 2 – "ODBC Setup" Page Fields

When using an ODBC configured Data Source Name, you merely need to choose it from the list. If it is not there, then you may have created a User DSN rather than a System DSN (the web server may be a different user than the user associated with the DSN).

For the Microsoft Access database you created earlier, you should see the Data Source Name in the DSN select box. Select it, and also choose (dsn) in the Driver select box.

Normally with a Microsoft Access database, you don't need a login name or password to connect to it. But this is configurable. In any case, you should supply a login name and password to SHERPA, for the super user to use. If you don't supply any login name or password, then super user can login with an empty login name and password.

Click the "Save" button on the "ODBC Setup" page and SHERPA will try to establish the database connection. SHERPA will report any invalid connection attributes and allow you to try again. Otherwise, SHERPA will confirm your settings and allow you to continue to the "Start Menu" page.

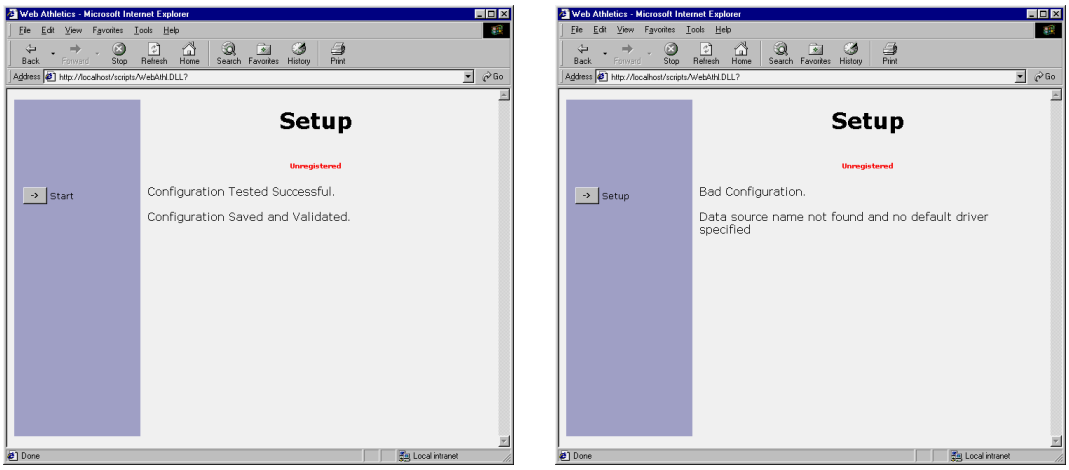

Figure 13 – SHERPA ODBC Success and Failures Pages

After successful configuration, you should login as the super user and create all the database tables and views from the Maintenance Module.

More discussion on maintaining the database can be found in the SHERPA User Guide.

Congratulations, you've successfully installed and configured the SHERPA web application.