

Information Assurance Best Practices

Information Assurance* refers to measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. In this release, WebFOCUS has been enhanced with a number of new security capabilities that emphasize strategic risk management and defend against malicious hacker attacks. This level of security is critical for externally-facing Web-based Business Intelligence applications. Release 7.6.10 has achieved Level 3 Application Security Verification Standards low risk security certification against the industry's most important security vulnerabilities and threats as defined by the Open Web Application Security Project (OWASP). For more information about Information Assurance and OWASP, click on this link: http://www.owasp.org/index.php/Main_Page.

*Source: U.S. Government's National Information Assurance Glossary Superset of Security Integration.

Documentation

This document is intended to be used as a reference. Settings and controls are fully documented in the following manuals and technical memos:

- ❑ *WebFOCUS and ReportCaster Installation and Configuration for z/OS Version 7 Release 6.2 and Higher* DN4500818.0909
- ❑ *WebFOCUS and ReportCaster Installation and Configuration for i5/OS Version 7 Release 6.1 and Higher* DN4500819.0909
- ❑ *WebFOCUS and ReportCaster Installation and Configuration for UNIX Version 7 Release 6.1 and Higher* DN4500815.0909
- ❑ *WebFOCUS and ReportCaster Installation and Configuration for Windows Version 7 Release 6.1 and Higher* DN4500816.0909
- ❑ *WebFOCUS Security and Administration Version 7 Release 6.1 and Higher* DN4500790.0909

- ❑ *ReportCaster Development and Administration Version 7 Release 6.1 and Higher* DN4500787.0909
- ❑ *Server Installation WebFOCUS Reporting Server* DN4500929.0909
- ❑ *Technical Memo #4558: Configuring Basic Authentication for z/OS Version 7 Release 6.2 and Higher* DN4500649.0507
- ❑ *Technical Memo #4673: IBM Tivoli WebSEAL Integration with WebFOCUS Version 7 Release 6.9* DN4500954.0509
- ❑ *Technical Memo #4653: Installing and Configuring Apache Tomcat on z/OS for WebFOCUS and ReportCaster Version 7 Release 6.2 and Higher* DN4500883.0707

Open Web Application Security Project (OWASP)

The Open Web Application Security Project (OWASP) is an open community organization that is dedicated to improving the security of application software. All of the OWASP information, tools, documents, and forums are free to anyone interested in learning about Web-based security and how to improve it within their environments.

The OWASP Top Ten Project provides a list of Web vulnerabilities, as well as remediation steps to eliminate them.

These top ten vulnerabilities are listed as:

- ❑ Injection
- ❑ Cross Site Scripting (XSS)
- ❑ Broken Authentication and Session Management
- ❑ Insecure Direct Object References
- ❑ Cross Site Request Forgery (CSRF)
- ❑ Security Misconfiguration
- ❑ Failure to Restrict URL Access
- ❑ Unvalidated Redirects and Forwards
- ❑ Insecure Cryptographic Storage
- ❑ Insufficient Transport Layer Protection

OWASP also provides an Application Security Verification Standard (ASVS) document, which outlines a standard that can be implemented to test for Web application security vulnerabilities.

For additional information on the Top Ten Project and the ASVS document, visit the OWASP Web site at www.owasp.org.

Software Development Life Cycle

Information Builders Business Intelligence Products Group has taken information from the OWASP Top Ten list, the Application Security Verification Standard (ASVS) document, and other open source documentation, and has integrated this information utilizing a full Software Development Life Cycle (SDLC) approach that targets these Web vulnerabilities within our product.

Our SDLC approach utilizes, but is not limited to:

- ❑ Developer code review
- ❑ Static code analysis tools
- ❑ Unit, validation, integration, regression, and functional testing
- ❑ Defenses for Injection, XSS, CSRF, Session Fixation, and others
- ❑ Automated notification of introduced vulnerabilities
- ❑ Application penetration testing using third-party tools
- ❑ Web hacking techniques, ethical hacking
- ❑ Raised security awareness
- ❑ Best practices
- ❑ Secured defaults
- ❑ Third-party security audits
- ❑ Customer input

For specific information regarding Application Servers and DBMS support, see the *WebFOCUS and ReportCaster Installation and Configuration* manual for your specific platform, as well as the *Server Installation WebFOCUS Reporting Server* manual.

Network Infrastructure

External users must connect to Internet servers in order to run applications and retrieve data. Allowing connections is unavoidable so it is really important that connections are secured to prevent malicious attacks. In terms of security, servers are of two types, trusted and untrusted. Trusted servers are typically hosted in the internal or private network behind a firewall. Untrusted servers are typically in the demilitarized zone (DMZ).

Enterprise customers can secure the untrusted servers with a reverse proxy by allowing only the reverse proxy to communicate to the untrusted servers. Customers may choose to isolate Internet servers from trusted servers by hosting only the reverse proxy in the demilitarized zone (DMZ) and hosting trusted servers on their internal network.

This security layer prevents malicious users from communicating directly to Web servers. Instead, they can only access the reverse proxy. Reverse proxies also limit exposure to real machine names, providing additional security.

WebFOCUS Settings

The following list includes WebFOCUS specific configuration settings, as well as recommendations to further secure a WebFOCUS application.

Depending on application specific requirements, all of these configuration options may or may not be required or used in the final application security design. As stated in the *WebFOCUS Security and Administration* manual, “Customers may need to prototype one or more configuration scenarios before arriving at the optimal solution.”

- ❑ Use SSL Version 3.0 or TLS to encrypt all sensitive data between the client browser and the Web/application servers, using ciphers of 128-bit encryption or higher.
- ❑ Use an external security provider to enforce logon policies for a named user environment.
- ❑ Remove or protect diagnostic .jsp files used to obtain additional information about the configuration: about.jsp, aboutreportcaster.jsp, jvmstatus.jsp, properties.jsp, source.jsp, and wfsysinf.jsp. These files are held in the root of the WebFOCUS Web application.
- ❑ Use one of the AES encryption mechanisms for TCP/IP communication from the WebFOCUS Client to the WebFOCUS Reporting Server.
- ❑ Run the WebFOCUS Client and the WebFOCUS Reporting Server on separate physical machines, with a firewall or RESTRICT_TO_IP in between.
- ❑ Implement File Permissions for WebFOCUS and ReportCaster. See Chapter 14 of the *WebFOCUS Security and Administration* manual.
- ❑ PROTECT IBIF_adhocfex and IBIF_raw in production. For example:

```
<SET> IBIF_adhocfex( PROTECT )
```

See Chapter 14 of the *WebFOCUS Security and Administration* manual. This setting will not allow these variables to be set from a browser. The following development tools need this to be enabled:

- ❑ Editors in Dashboard, Managed Reporting Applet environment, and Developer Studio
- ❑ My InfoAssist
- ❑ Procedure Viewer

- ❑ WebFOCUS Autoprompting with FIND
- ❑ OLAP requests
- ❑ Data Server section
- ❑ Running within Report Assistant
- ❑ Enable validation and control of variables.
`<SET> variablename(option)`
These options allow you to specify a type and format for variables that can be sent on a URL.
See Chapter 10 of the *WebFOCUS Security and Administration* manual.
- ❑ Enable the WebFOCUS encryption option for:
 - ❑ WebFOCUS cookies
 - ❑ Managed Reporting passwords
 - ❑ Business Intelligence Dashboard public passwords
 - ❑ Business Intelligence Dashboard WebFOCUS Reporting Server credentials
 - ❑ Tickets used in a trusted Managed Reporting sign-on
See Chapter 9 of the *WebFOCUS Security and Administration* manual.
- ❑ Set MR_ANONYMOUS_RUN_ACCESS to NO
This prevents access to procedures for users not logged into Managed Reporting.
See Chapter 6 of the *WebFOCUS Security and Administration* manual.
- ❑ Set WF_proj_list_from_wfrs to YES
This restricts the list of application folders seen in Developer Studio based on the APP PATH setting on the Reporting Server.
See Chapter 4 of the *WebFOCUS Security and Administration* manual.
- ❑ CACHE_CONTROL NO-CACHE
Browser caching is disabled. No files will be created on disk in the Temporary Internet folder of the user.
- ❑ Disable Redirection within the mime.wfs file for certain formats.
No files will be created on disk in the ibi/temp directory for these formats.

Note that redirection is still needed for some formats, such as on demand pages and images. In that case, use REDIRECT_COOKIE=ON.

- ❑ Enable IBI_COOKIE_SECURE=Y in cgivars.wfs for WebFOCUS.
- ❑ Set WF_COOKIE_EXPIRATION in cgivars.wfs and <session-timeout> in the WebFOCUS Web application Web deployment descriptor, web.xml, to the same value.

WebFOCUS Administration Consoles

It is important to secure the WebFOCUS Administration Consoles immediately after the installation as described below.

WebFOCUS Client Administration Console

The WebFOCUS Client Administration Console is accessible from the WebFOCUS Welcome Page and is packaged with a default administration user ID of admin. This default can be changed so that anyone accessing the WebFOCUS Client Administration Console must provide valid credentials. There are several options for securing the WebFOCUS Client Administration Console:

- ❑ WEB and WEBHDR. Can be used if the user ID is populated in an HTTP header variable.
- ❑ EDA and EDA (with input box). Can be used if the WebFOCUS Reporting Server is enabled with a security mode of LDAP, DBMS, or OPSYS.
- ❑ J2EE roles. This is described in Technical Memo 4606, which can be downloaded from the Technical Documentation Library Web site.

WebFOCUS Reporting Server

The WebFOCUS Reporting Server Web Console by default is unsecured. Immediately after installation it should be secured using a security mode that is suited to your overall solution.

The security modes PTH, OPSYS, DBMS, and LDAP secure the Web Console. Users attempting to gain access to the Web Console must provide valid credentials.

WebFOCUS ReportCaster Settings

The ReportCaster Distribution Server usually runs within a secured network environment, and encrypting these communication parameters is not usually necessary. If encryption from the Distribution Server to Managed Reporting is needed and encryption of the data to and from the WebFOCUS Reporting Server is needed, follow these steps:

JSSE Caster

Set to YES within the ReportCaster configuration. This enables the use of SSL from the ReportCaster Distribution Server communicating to the Managed Reporting Repository to schedule MR procedures.

JSSE Servlet

Set to YES within the ReportCaster configuration. This enables the use of SSL for the applet scheduling tools to retrieve MR procedures.

Set 3DES encrypt connection to WFRS, with the following additional parameter on the WebFOCUS Reporting Server JDBC URL:

```
jdbc:eda:\machine:port;server=;ENCRYPTION=1;
```

For additional information regarding these settings, see the *ReportCaster Development and Administration Version 7 Release 6.1 and Higher* manual.

Enable IBI_COOKIE_SECURE=Y in the web.xml file for ReportCaster.

WebFOCUS Reporting Server Security

For additional information, see the *Server Administration Manual*.

- ❑ Install the WebFOCUS Reporting Server on a separate physical machine than the WebFOCUS Client.

- ❑ RESTRICT_TO_IP restricts incoming communications.

Configure the Reporting Server to accept incoming connections from a restricted list of hosts for the TCP/IP and HTTP connections. Use this and/or set up a firewall in between the WebFOCUS Client and the WebFOCUS Reporting Server.

- ❑ Use SSL to encrypt all data between the client browser and the HTTP Listener for the WebFOCUS Reporting Server.

- ❑ Use 3DES encryption for TCP/IP communication from the WebFOCUS Client to the WebFOCUS Reporting Server.

- ❑ SET OPSYSCMD=OFF to disable operating system commands.

If applications do not require operating system commands, this should be disabled. See Chapter 14 of the *WebFOCUS Security and Administration* manual.

- ❑ SET DPT=OFF to disable the Direct Passthru option.

If application requirements do not require direct SQL Passthru, this should be disabled.

See Chapter 14 of the *WebFOCUS Security and Administration* manual.

- ❑ SET HTMLENCODE=ON to encode the HTML output that is data.

This setting will disable the rendering of HTML tags within a browser when these tags are stored within the actual data, or created using a DEFINE or COMPUTE command.

- ❑ Encrypt Master Files on the WebFOCUS Reporting Server.

- ❑ Encrypt WebFOCUS Reporting Server FOCEXECs.
- ❑ SET DEFECHO=NONE. This setting will disable echo output, so information regarding WebFOCUS code cannot be returned to the browser. This feature is planned for a post-769 release.
- ❑ SET EMGSRV=OFF. This setting will disable any FOCUS error messages.
- ❑ Use DBA for Master Files for which you want to restrict access. See Chapter 6 of the *WebFOCUS Security and Administration* manual and Chapter 11 of the *Describing Data With WebFOCUS Language* manual.

WebFOCUS Open Portal Services

The WebFOCUS Client can be configured to accept connections only from the Portal Server host machine (IP) that is hosting the Open Portal Services Gateway. When specifying the list of allowable machines, you must use the IP, not the host name.

The following excerpt was taken from the *WebFOCUS Open Portal Services* manual.

For additional security, you can define and provide a value for the RESTRICT_WOAS_TO_IP parameter when configuring your servlet engine. When you add the RESTRICT_WOAS_TO_IP parameter, you must provide an IP of the portal server where WebFOCUS is being hosted. This parameter increases security for the portal environment because it allows you to use only validated connections from the IP you specify. You can also provide multiple addresses by separating each IP with a comma character (,).

The following is a section of code in the `.../webapps/webfocus76/WEB-INF/web.xml` file that can be updated.

```
<context-param>
  <!-- Directory where the webserver can locate the html files. -->
  <param-name>USE_GATEWAY</param-name>
  <param-value>yes</param-value>
</context-param>
<context-param>
  <!-- Directory where the webserver can locate the html files. -->
  <param-name>RESTRICT_WOAS_TO_IP</param-name>
  <param-value>12.34.56,127.0.0.1</param-value>
</context-param>
```

WebFOCUS Reporting Best Practices

To avoid introducing vulnerabilities, application developers need to keep the following in mind when coding WebFOCUS applications:

- ❑ SET HTMLENCODE=ON, where appropriate and not utilized for techniques.
- ❑ Avoid echoing user-supplied data within responses.

- ❑ CHKFMT for parameter validation. For CHKFMT usage, see [CHKFMT Parameter Validation](#) on page 9.
- ❑ QUOTEDSTRING to eliminate injection flaws. For QUOTEDSTRING usage, see [Creating a Standard Quote-Delimited String](#) on page 10.
- ❑ SQL Passthru requests should use stored procedures.

CHKFMT Parameter Validation

The syntax for CHKFMT is

```
CHKFMT(numchar, string, 'mask', outfield)
```

where:

numchar

Integer

Is the number of characters you want to compare against the mask.

string

Alphanumeric

Is the character string to be checked. This can be the character string enclosed in single quotation marks, or the field that contains the character string.

'mask'

Alphanumeric

Is the mask, which contains the comparison characters enclosed in single quotation marks.

Some characters in the mask are generic and represent character types. If a character in the string is compared to one of these characters and is the same type, it matches. Generic characters are:

<i>A</i>	Any of the letters A-Z (uppercase or lowercase).
<i>9</i>	Any of the digits 0-9.
<i>X</i>	Any of the letters A-Z or digits 0-9.
<i>\$</i>	Any character.

Any other character in the mask represents only that character. For example, if the third character in the mask is B, the third character in the string must be B to match.

outfield

Integer or Alphanumeric

Is the name of the field that contains the result, or the format of the output value enclosed in single quotation marks.

Note: In Dialogue Manager, the format must be specified. In Maintain, the name of the field must be specified.

Creating a Standard Quote-Delimited String

Character strings must be enclosed in single quotation marks to be handled by most database engines. In addition, embedded single quotation marks are indicated by two contiguous single quotation marks. Quotation marks are required around variables containing delimiters, which include spaces and commas.

The QUOTEDSTRING suffix on a Dialogue Manager variable applies the following two conversions to the contents of the variable:

- ❑ Any single quotation mark embedded within a string is converted to two single quotation marks.
- ❑ Single quotation marks are added around the string.

Dialogue Manager commands differ in their ability to handle character strings that are not enclosed in single quotation marks and contain embedded blanks. An explicit or implied -PROMPT command can read such a string. The entire input string is then enclosed in single quotation marks when operated on by .QUOTEDSTRING.

Note: When using the -SET command to reference a character string, ensure the character string is enclosed in single quotes to prevent errors.

Syntax: **How to Create a Standard Quote-Delimited Character String**

&var.QUOTEDSTRING

where:

&var

Is a Dialogue Manager variable.

Example: Creating a Standard Quote-Delimited Character String

The following example shows the results of the QUOTEDSTRING suffix on input strings.

```
-SET &A = ABC;
-SET &B = 'ABC';
-SET &C = O'BRIEN;
-SET &D = 'O'BRIEN';
-SET &E = 'O''BRIEN';
-SET &F = O''BRIEN;
-SET &G = OBRIEN';
-TYPE ORIGINAL = &A QUOTED = &A.QUOTEDSTRING
-TYPE ORIGINAL = &B QUOTED = &B.QUOTEDSTRING
-TYPE ORIGINAL = &C QUOTED = &C.QUOTEDSTRING
-TYPE ORIGINAL = &D QUOTED = &D.QUOTEDSTRING
-TYPE ORIGINAL = &E QUOTED = &E.QUOTEDSTRING
-TYPE ORIGINAL = &F QUOTED = &F.QUOTEDSTRING
-TYPE ORIGINAL = &G QUOTED = &G.QUOTEDSTRING
```

The output is:

```
ORIGINAL = ABC          QUOTED = 'ABC'
ORIGINAL = ABC          QUOTED = 'ABC'
ORIGINAL = O'BRIEN     QUOTED = 'O''BRIEN'
ORIGINAL = O'BRIEN     QUOTED = 'O''BRIEN'
ORIGINAL = O'BRIEN     QUOTED = 'O''BRIEN'
ORIGINAL = O''BRIEN    QUOTED = 'O''''BRIEN'
ORIGINAL = OBRIEN'     QUOTED = 'OBRIEN'''
```

Note: The -SET command will remove single quotes around a string. Notice in the example above that the result of -SET &B = 'ABC' was changed to ORIGINAL = ABC (as shown in the output), prior to the QUOTEDSTRING conversion.

Example: Converting User Input to a Standard Quote-Delimited Character String

The following -TYPE command accepts quoted or unquoted input and displays quoted output.

```
-TYPE THE QUOTED VALUE IS: &E.QUOTEDSTRING
```

The output is:

The screenshot shows a terminal window with the following content:

```
E      : |o'brien|
Submit
Reset
```

THE QUOTED VALUE IS: 'o''brien'

Example: Using Quote-Delimited Strings With Relational Data Adapters

The following procedure creates an Oracle table named SQLVID from the VIDEOTRK data source.

```
TABLE FILE VIDEOTRK
SUM CUSTID EXPDATE PHONE STREET CITY STATE ZIP
  TRANSDATE PRODCODE TRANSCODE QUANTITY TRANSTOT
BY LASTNAME BY FIRSTNAME
WHERE LASTNAME NE 'NON-MEMBER'
ON TABLE HOLD
END
-RUN
CREATE FILE SQLVID
-RUN
MODIFY FILE SQLVID
FIXFORM FROM HOLD
DATA ON HOLD
END
```

Consider the following SQL Translator request:

```
SET TRACEUSER = ON
SET TRACEON = STMTRACE//CLIENT
SQL
SELECT *
FROM SQLVID WHERE LASTNAME = &1.QUOTEDSTRING;
END
```

When this request is executed, you must enter a last name, in this case, O'BRIEN:

```
PLEASE SUPPLY VALUES REQUESTED

1=
O'BRIEN
```

In the generated SQL request, the character string used for the comparison is correctly enclosed in single quotation marks, and the embedded single quote is doubled:

```
SELECT SQLCOR01.CIN , SQLCOR01.LN , SQLCOR01.FN ,
SQLCOR01.EXDAT , SQLCOR01.TEL , SQLCOR01.STR , SQLCOR01.CITY ,
SQLCOR01.PROV , SQLCOR01.POSTAL_CODE , SQLCOR01.OUTDATE ,
SQLCOR01.PCOD , SQLCOR01.TCOD , SQLCOR01.NO , SQLCOR01.TTOT
FROM SQLVID SQLCOR01 WHERE SQLCOR01.LN = 'O''BRIEN';
```

The following input variations are translated to the correct form of quoted string demonstrated in the trace.

```
'O'BRIEN'
'O''BRIEN'
```


