Web Security 4D v11 SQL コンポーネント

By Atanas Atanassov, Technical Services Team Member, 4D Inc.

Technical Note 09-23

概要

Web サーバを起動しサイトを立ち上げた瞬間に、インターネットのどこからでもあなたのローカルネットワークを除くことのできる窓を開いたことになります。サイトのパーツごとにユーザアクセスをフィルタすることは重要です。メインページや他の公開ページには通常だれでもアクセスできます。他方、機密情報は守られるべきです。4D v11 SQL には組み込みの Web セキュリティシステムがあります。また開発者独自のカスタマイズされたシステムを使用することもできます。

このテクニカルノートではカスタマイズされた Web セキュリティシステムを作成する方法について、説明およびデモします。セキュリティ領域を構築する助けになるコンポーネントが含まれています。

はじめに

データベースの Web セキュリティを簡潔に説明すると、認証されたユーザのみにデータベースの特定の個所にアクセスを許可するルールに基づき、Web からデータベースへのアクセスに制限を設けることです。Web セキュリティシステムはまたユーザアカウントや、Web サーバが実行されているマシン上のファイルを保護します。基本的なセキュリティの基準には正しく選択されたパスワード、ファイルアクセス権の変更、定期的なデータのバックアップが含まれます。コンピュータのファイルやデータベースに格納されたデータへの悪意のある侵入の可能性を無視することは、ビジネスにとって極めて重大な結果をもたらすかもしれません。

このテクニカルノートでは 4D で利用可能なセキュリティ要素について概観します。コンポーネントとサンプルデータベースが含まれています。コンポーネントは、ユーザが独自のセキュリティ領域やアクセスの認証ルールを作成することを助けます。サンプルデータベースは、データベースの Web セキュリティシステムを構築するために、コンポーネントのインストールと利用方法をデモします。

4D v11 SQL にはユーザ&グループによるセキュリティアクセスシステムが組み込まれています。このシステムを簡単にユーザの Web アクセスに使用できます。他方、これはデータベースにいくつかの制限を課します。まずユーザ名とパスワードをテキストとしてブラウザリクエスト

に渡すので、セキュリティ上の問題となります。またデータベースへの Web アクセスが 4D に定義されたユーザに制限されてしまいます。

On Web Authentication や On Web Connection データベースメソッドを使用して、4D デベロッパは独自のセキュリティシステムを構築できます。セキュリティの設定をどのように保管するか、そしてやってくるリクエストをどのように認証するかを選択できます。バージョン 11 では DIGEST 認証がサポートされ、セキュリティレイヤが追加されました。

Web セキュリティ - 概要

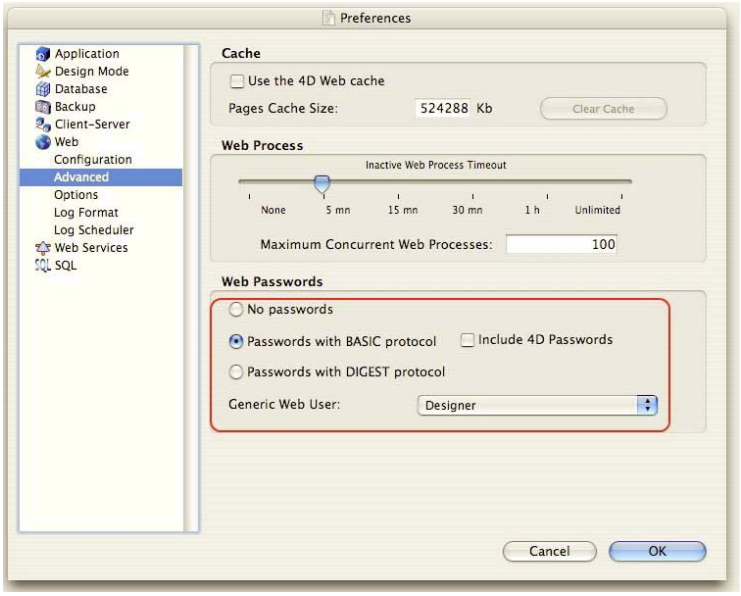
4D の Web セキュリティは以下の要素に基づきます:

- On Web Authentication や On Web Connection データベースメソッド。
- WebFolder - データベース環境設定で設定するデフォルトの Web フォルダ。
- 4DACTION と 4DSCRIPT から利用可能な 4D メソッド。

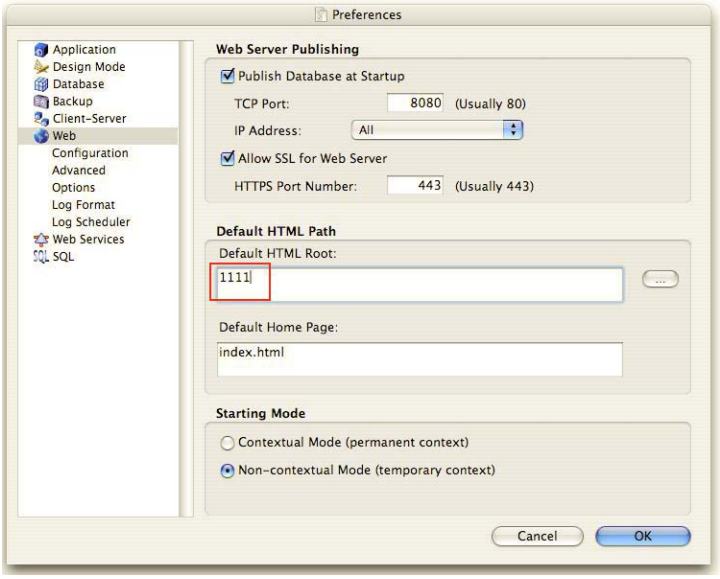
Note: このテクニカルノートではコンテキストモードを取り扱いません。そのため 4DMETHOD は省略されています。

- 4D パスワード管理システムと一般 Web ユーザの定義

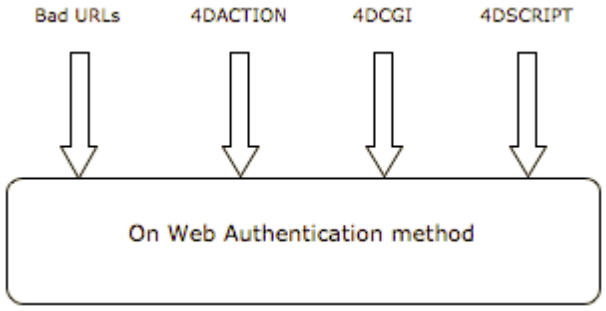
パスワード管理システムの有効化は環境設定から行います。



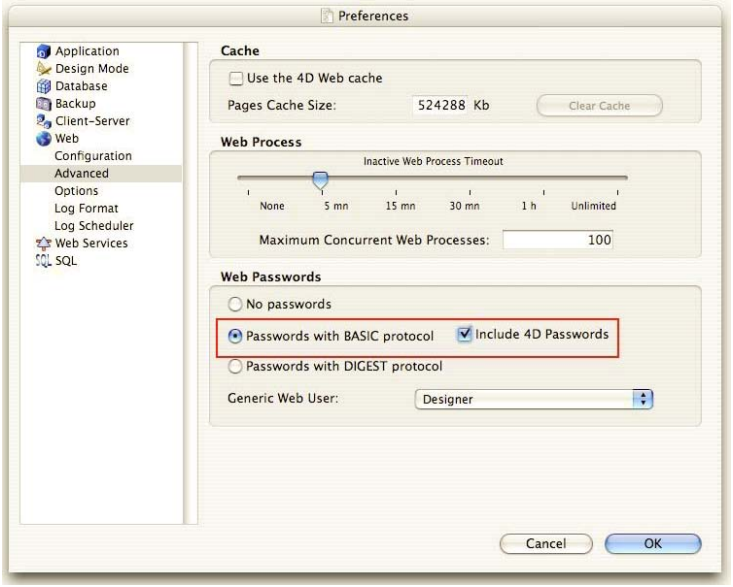
パスワードシステムと On Web Authentication メソッドが有効にされると、すべてのリクエストは On Web Authentication メソッドに送られます。リクエストとは、URL リクエスト、4DACTION、4DSCRIPT、そして 4DCGI です。ただし既に存在するページのリクエストの場合は、On Web Authentication は呼び出されません。そのためこの状況を処理する方法を見つける必要があります。一つの方法はデフォルトの HTML ルートを WebFolder から別な名前にすることです。このようにすると、すべてのリクエストは On Web Authentication に送られます。



リクエストのフローは以下の通りです:



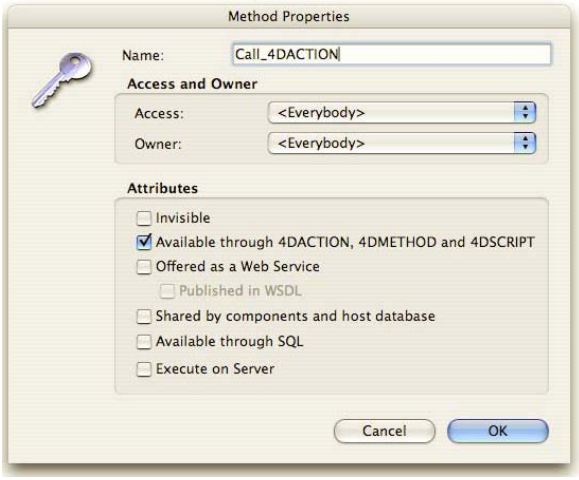
認証は"BASIC"または"DIGEST"に基づいて行われます。ユーザが入力したユーザ名とパスワードはブラウザリクエストにテキストで付加され、On Web Authentication データベースメソッドに渡されます。ユーザ名とパスワードを平文テキストで送信することはセキュリティ上の問題を起こす可能性をはらみますが、そうすることでカスタマイズされたセキュリティシステムおよび 4D 組み込みのシステムで値を検証することが可能になります。組み込みのセキュリティシステムを使用するには、"4D パスワードを含む"オプションをチェックします:



DIGEST モードでは、ユーザパスワードは暗号化されて送信されるため、途中で盗み出して使用することはできません。これによりセキュリティレベルが向上しますが、DIGEST パスワードシステムは 4D のパスワードシステムと互換がありません。DIGEST モードの場合、"4D パスワードを含む"オプションは選択できません。

Note:　DIGEST モードと BASIC モードの切り替えはデータベースの再起動後に行われます。

リクエストは 4DACTION や 4DSCRIPT により 4D のプロジェクトメソッドにアクセスしようとするかもしれません。この場合メソッドを使用できるようにするには、メソッドプロパティ中で"4DACTION、4DMETHOD、および 4DSCRIPT で利用可"オプションが選択されていなければなりません:



Web リクエストを処理するデータベースメソッド

On Web Authentication と On Web Connection データベースメソッドはリクエストを処理し、リクエストされた情報を Web サーバエンジンに渡します。

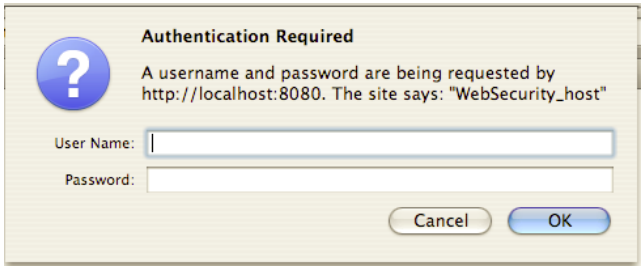
On Web Authentication

このメソッドは 6 つの引数を受け取ります:

$1 - リクエストされた URL
$2 - HTTP ヘッダとボディ
$3 - Web クライアントの IP アドレス
$4 - Web サーバの IP アドレス
$5 - ユーザ名
$6 - ユーザパスワード

Note: パスワードシステムが有効でない場合、$5 と$6 は On Web Authentication メソッドに渡されません。

戻り値$0 はブールです。戻り値が False の場合、認証は失敗し接続は拒否されます。そしてブラウザウィンドウに認証ダイアログが表示されます。



戻り値が True の場合、リクエストは On Web Connection や 4DACTION で呼ばれたメソッドに渡されます。

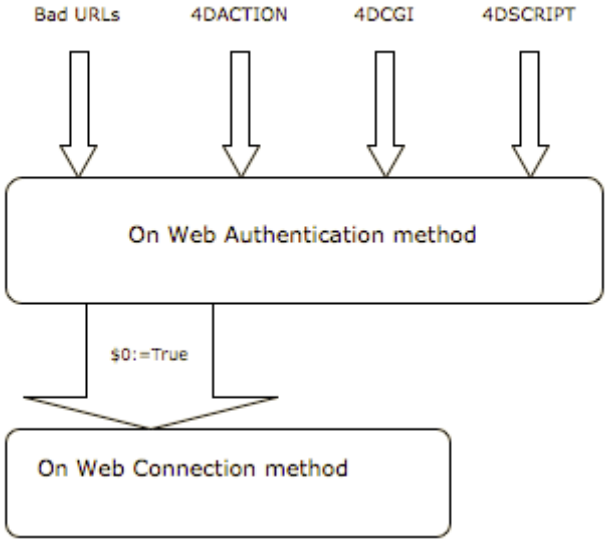
メソッドが最初に呼ばれた時、リクエストにはユーザ名とパスワードが含まれていません。$5 と$6 は空の文字列で、戻り値に False が設定されて認証に失敗します。認証を求めるウィンド

ウが表示され、ユーザはユーザ名とパスワードを入力できます。この時点で、入力された情報が正しければ認証に成功し、On Web Authentication が True を返します。

On Web Connection

このメソッドは Web サーバが、存在しないファイルのリクエストか 4DCGI から始まるリクエストを受け取ったときに呼ばれます。このメソッドも 6 つの引数を受け取ります。これらの引数は On Web Authentication が受け取るものと同じで、明示的に定義する必要があります。

On Web Connection は On Web Authentication が True を返したときに実行されます。



4D 組み込みのセキュリティシステム

4D デベロッパは組み込みのセキュリティシステムを使用して、Web リクエストをフィルタできます。ユーザ名とパスワードはユーザテーブルを使用して検証されます。例えば:

```
    `$users_a - ユーザ名を保持する配列
    `$usersID_a - ユーザ ID を保持する配列
    `$userName - リクエストに含まれるユーザ名($5)
    `$userpassword – リクエストに含まれるパスワード($6)

GET USER LIST($users_a;$usersID_a)
$userPos:=Find in array($users_a;$userName)
If ($userPos>0)
   $4Duser:=Not(Is user deleted($usersID_a{$userPos}))
   If (Validate password($usersID_a{$userPos};$userpassword))
```

```
            $0:=True
    Else
            $0:=False
    End if
Else
    $4Duser:=False
    $0:=False
End if
```

これは簡単なソリューションですが、先に説明した通りセキュリティレベルに劣り、データベースアクセスが登録ユーザに制限されます。これはインターネットに公開されたすべてのデータベースに制限です。

カスタマイズされたセキュリティシステム

カスタマイズされたセキュリティシステムは組み込みシステムより多用途であり、4D デベロッパは様々なタイプの認証を実装できます。またユーザパスワードを保護するために DIGEST プロトコルも使用できます。このときパスワードは On Web Authentication の$6 には渡されません。

以下は DIGEST セキュリティプロトコルを使用してユーザを認証する例です。ユーザ名とパスワードは"Users"テーブルに格納されています:

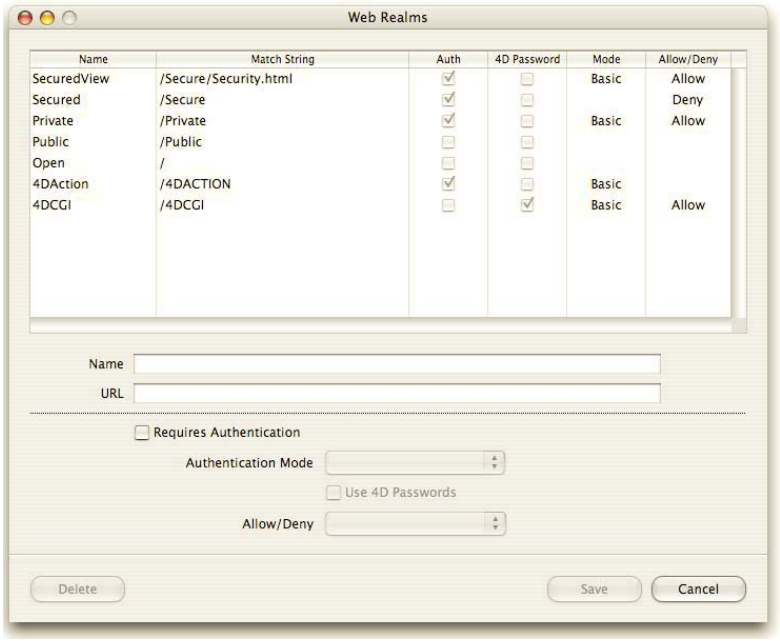
```
$userName:=$5

QUERY([Users];[Users]UserName=$userName)
If (OK=1)
    $0:=Validate Digest Password($userName;[Users]Password)
Else
    $0:=False
End if
```

先に示した通り、カスタマイズされた Web セキュリティシステムは On Web Authentication データベースメソッドに基づいています。すべてのリクエストはこのメソッドに送信されます。認証はセキュリティ領域とそれらの領域にアクセスするためのルールに基づきます。

このテクニカルノートで提供する Web Security コンポーネントはこのような領域とアクセスルールの設定を助けます。

コンポーネントでは *WSec_P_startRealms* プロジェクトメソッドから"Web Realms"フォームが呼ばれます。



必要な情報は:

Name - 領域名を入力。

URL - 領域のパスを入力。すべての 4DACTION、4DSCRIPT、そして 4DCGI リクエストはコンポーネントが処理します。これらのリクエストの URL は大文字であるべきです (例: /4DACTION, /4DSCRIPT, /4DCGI)。

認証モード - Basic, Digest, none から選択します。DIGEST モードを使用するには、データベース環境設定の Web テーマで"DIGEST 認証のパスワード"オプションが選択されている必要があります。

Allow/Deny オプションは特定の領域へのアクセスを許可または拒否します。例えば特定の領域へのすべてのリクエストを拒否しつつ、この領域のファイルやサブフォルダへのアクセス例外を作成できます。

Requires Authentication はユーザにユーザ名とパスワードを尋ねます。

Use 4D Password - このオプションがチェックされていると、ユーザ名とパスワードは 4D に定義されたユーザを対象にして行われます。言い換えれば認証は組み込みのセキュリティシステムを使用して行われます。このオプションは BASIC 認証でのみ使用できます。

コンポーネントのインストール

1. ストラクチャファイルと同階層に Components フォルダを作成し、WebSecurity.4dbase を配置する。
2. Plugins フォルダに 4D Pack プラグインをインストールする。
3. ホストデータベースから *WSec_verify* コンポーネントメソッドを呼び出す。このメソッドは、カスタムの認証ルールを適用する *Authenticate* プロジェクトメソッドをホストデータベースに作成します。サンプルデータベースでは、ユーザ名とパスワードは"Users"テーブルに格納されています。Web リクエストに含まれるユーザ名とパスワードは、このテーブルに含まれるレコードに基づいて認証されます。
4. On Startup データベースメソッドに WSec_install_On_Startup とタイプする。すべての Web セキュリティ設定が起動時にホストデータベースにロードされます。そのため、設定が変更されたらデータベースを再起動する必要があります。
5. On Web Authentication データベースメソッドに WSec_install_On_Web_Authentication とタイプする。
6. On Web Connection データベースメソッドに WSec_install_On_Web_Connection とタイプする。
7. データベース環境設定の Web テーマで、デフォルト HTML ルートフォルダを"WebFolder"以外に変更する。
8. Web サーバを開始する。データベースがポート 8080 で公開されていることを確認してください。

以下は開発者が使用できるメソッドのリストと説明です。

- *WSec_P_startRealms* – このメソッドは Web 領域環境設定フォームを起動します。このフォームで、ユーザは領域を作成し、アクセスを設定できます。
- *WSec_verify* – このメソッドはホストデータベースに開発者のためのフックを作成します。デベロッパはリクエストを認証する方法を実装できます。

サンプルデータベース

WebSecurity_host.4dbase サンプルデータベースにはコンポーネントがインストールされています。コンポーネントのデモのために、いくつかの領域が設定されています。領域はストラクチャファイルと同階層にある WebFolder に作成されます。

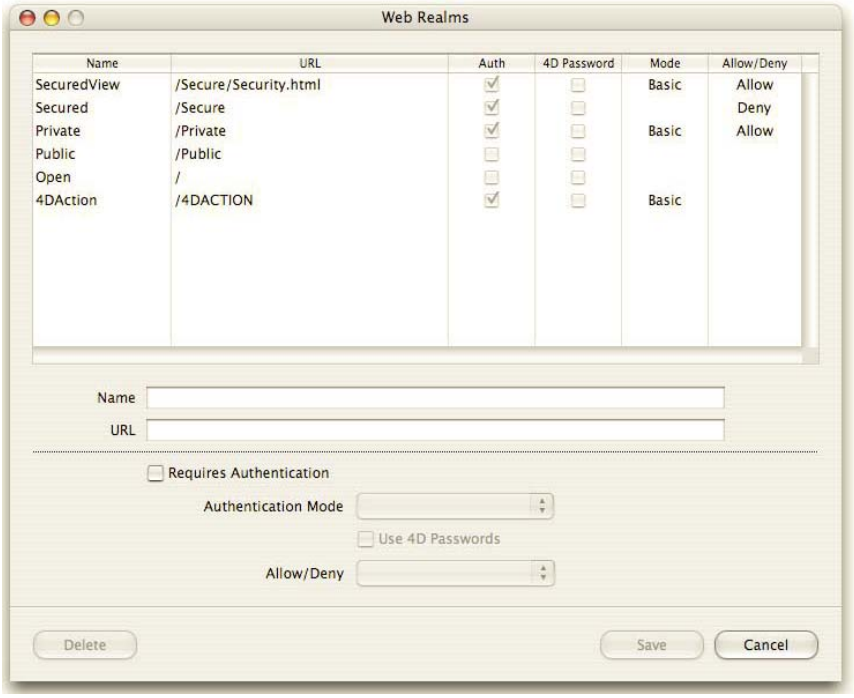
起動時にパスワードの入力を求められます。Designer としてログインしてください。

ユーザリスト	パスワード
Designer	designer
Administrator	administrator
Atanas	atanas

サンプルデータベースには"Users"テーブルが含まれています。ここに Web ユーザの名前とパスワードを登録します。

Web Security メニューから Preferences を選択します。

Web 領域環境設定が表示されます。



Note: *ホストデータベースにメニューを作成するかどうかは任意です。これらのメソッドを呼び出す方法はデベロッパが決定できます。このメニューはデモのために作成されています。*

先に示した通り、いくつかの領域と認証ルールが定義されています。4DACTION、4DCGI、4DSCRIPT などの URL コンポーネントは大文字で入力されています。

ユーザがブラウザからリクエストするのは:

http://hostmachine:8080/Private/private.html

http://hostmachine:8080/Congratulation.html

http://hostmachine:8080/Road_Bikes_Frames.jpg

http://hostmachine:8080/Public/public.html

http://hostmachine:8080/call_4dscript.html

http://hostmachine:8080/4DACTION/Call_4DACTION

Web Security メニューのもう一つのオプション"Install Authenticator"は、Web セキュリティシステムのカスタマイズを可能にするデベロッパフックを作成し、コンポーネントから領域環境設定を取得します。環境設定はインタープロセス配列としてホストデータベースにロードされるので、デベロッパはその状態で使用できます。

まとめ

カスタマイズされた Web セキュリティシステムを 4D に作成することで、組み込みのセキュリティシステムを使用するよりもより多くの利点をユーザに提供できます。4D v11 SQL は、ユーザパスワードを暗号化する新しいセキュリティプロトコルを提供しています。このテクニカルノートで提供されるコンポーネントを使用して領域を作成し、アクセスルールを定義できます。デベロッパフックメソッドを使用すれば独自の認証メカニズムを実装できます。

追加情報:

4D Design Reference (http://www.4d-japan.com/support/documentation.html)

4D Language Reference (http://www.4d-japan.com/support/documentation.html)

接続セキュリティ (http://www.4d-japan.com/docs/CMJ/CMJ02056.HTM)

On Web Authentication データベースメソッド
(http://www.4d-japan.com/docs/CMJ/CMJ02055.HTM)