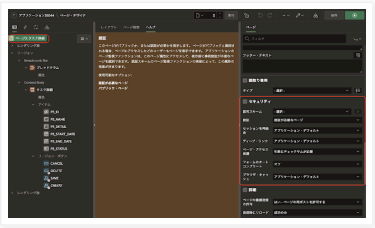
日日是Oracle APEX

Oracle APEXを使った作業をしていて、気の付いたところを忘れないようにメモをとります。

2020年7月1日水曜日

特定のページへの直リンクによるアクセス(2) - ページの保護について

Oracle APEXのアプリケーションに含まれるページの保護は、ページのプロパティに含まれるセキュリティのセクションに纏まっています。



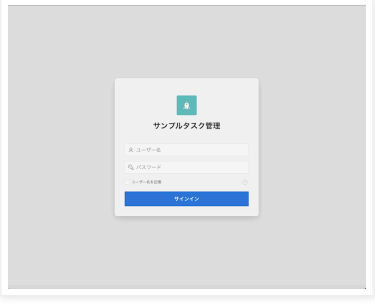
今回は以下の直リンクを機能させるために、セキュリティのいくつかの設定を解除することで、その設定内容の理解を深めることを目標としています。

https://apex.oracle.com/pls/apex/f?p=demo-tasks:task:::::P3_ID:1

タスク詳細画面でタスクのID(P3_ID)が1のを選択した以下のページが表示されるようにします。

認証

Oracle APEXのアプリケーションが開始していないブラウザから上記のURLへアクセスします。タスク詳細ページを指定しましたが、ログイン・ページにリダイレクトされます。



これはセキュリティにある**認証**の属性が**認証が必要なページ**に設定されているためです。

では、**認証**の属性を認証が必要なページから**パブリック・ページ**に切り替え、再度同じURLでアクセスします(クッキーを初期化するためブラウザは再起動してください)。セッション・ステートの保護違反が発生します。

ページ・アクセス保護（ページのプロパティ）

これは**ページ・アクセス保護**の項目が、**引数にチェックサムが必要**、となっているためです。ページ・アクセスの保護には厳しい順番で、URLアクセスなし、引数をサポートしない、引数にチェックサムが必要、制限なし、の４種類の設定が可能です。

- **URLアクセスなし**、を設定するとブラウザからのアクセスをすべて禁止します。設定されたページはOracle APEXのコンポーネントであるブランチを通してアクセスされます。
- **引数をサポートしない**、を設定すると、ここで指定しているP3_IDというような引数の指定自体が禁止されます。
- **引数にチェックサムが必要**、を設定するとURLにチェックサムの指定を含むことが要求されます。チェックサムの指定がない場合は、上記のエラーになります。

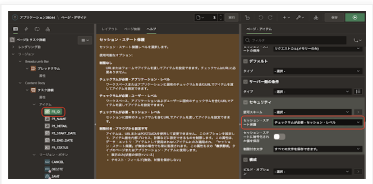
ページ・アクセス保護の項目を**制限なし**に切り替え、再度ブラウザを初期化したのち直リンクでのアクセスを行います。

ページ・アクセス保護の項目を**制限なし**に変更したにもかかわらず、同じエラーが発生します。これは引数として与えられているP3_IDがチェックサムで保護されているためです。

ページ・アクセス保護の設定は、URLに引数が含まれているか、チェックサムが含まれているかを検証します。だたし、チェックサム自体はページ・アイテムを保護するものであるため、ページ・アイテムの設定を参照します。

セッション・ステート保護（ページ・アイテムのプロパティ）

ページ・アイテム**P3_ID**を選択し、**セキュリティ**に属するプロパティを確認します。**セッション・ステート保護**の項目が**チェックサムが必要 - セッション・レベル**となっていることが確認できると思います。



それぞれのページ・アイテムへのセッション・ステート保護には厳しい順で、制限付き - ブラウザから設定不可、チェクサムが必要 - セッション・レベル、チェックサムが必要 - ユーザー・レベル、チェクサムが必要 - アプリケーション・レベル、制限なし、になります。

制限付き - ブラウザから設定不可の場合、リンクに含まれることやサブミット時に送信されるデータに含まれることも禁止されます。チェックサムは、そもそも与えられるページ・アイテムP3_IDの値１が変更されることを防ぎます。チェックサムが含まれているとリンクは以下のようになります。

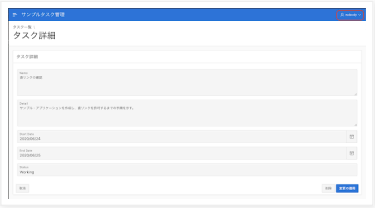
https://apex.oracle.com/pls/apex/f?p=demo-tasks:task:::::P3_ID:1&cs=3vJed02HiANkep22cwG4JFv-Jfp690PkYweG1IBUClQ0T29kRU83H6yFvF_RLGgxP38jCxvutH9ql0m4z

P3_IDの値１からチェックサムが生成されているので、チェックサムを変更せず、P3_IDの値だけを変更すると以下のエラーが発生します。

上記開発者画面でのエラーの表示で、エンド・ユーザーの場合では、さきほどのセッション・ステートの保護違反の画面が表示されます。

- **アプリケーション・レベル**の保護では値の変更が行われなくてもアプリケーションが変更されるとエラーになります。このレベルの保護で生成されたURLは、値の変更を行わなければ、ユーザーにかかわらず有効です。Oracle APEXではパブリック・ブックマーク(PUBLIC_BOOKMARK)と指定することがあります。
- **ユーザー・レベル**はそれに加えて、ユーザーが異なるとエラーになります。このレベルの保護で生成されたURLは、そのURLが生成されたときに認証されていたユーザーに対してのみ有効です。ユーザーが異なると対象ページへのアクセスはエラーになります。Oracle APEXではプライベート・ブックマーク(PRIVATE_BOOKMARK)と指定することがあります。
- **セッション・レベル**ではセッションが異なってもエラーになります。このレベルの保護で生成されたURLにアクセスできるのは、認証されたセッションが有効な期間に制限されています。ブックマークとしては使えません。Oracle APEXではセッション(SESSION)と指定することがあります。

ページ・アイテムP3_IDの**セッション・ステート保護**を**制限なし**へ変更し、再度、直リンクでアクセスします。今度はタスク詳細画面が表示されます。



ディープ・リンク

チェックサムによる保護を解除したので、再度、ページの**認証**の設定を**認証が必要なページ**に戻します。

再度、直リンクでアクセスします。今度は変更した設定の通りに、ユーザー認証が要求されます。

ユーザー名とパスワードを入力し、サインインを実行します。サインイン後は**ホーム・ページが開きます**。

ユーザー認証が完了したのち、指定したページを開くようにするには、**ディープ・リンク**を**有効**にします。デフォルトは**アプリケーション・デフォルト**の設定になっていますが、通常これは**無効**に設定されています。

ディープ・リンク（を禁止すること）によって、認証されたセッションが存在しない状態で、ページを指定したアクセスができないようにしています。

これで、直リンクへのアクセスが可能になりました。解除したセキュリティは以下になります。

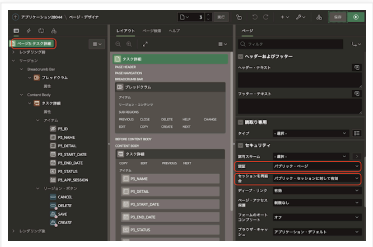
1. ページのプロパティである**ページ・アクセス保護**を**制限なし**へ変更
2. ページ・アイテムのプロパティである**セッション・ステート保護**を**制限なし**へ変更
3. ページのプロパティである**ディープ・リンク**を**有効**へ変更

セッションを再結合

通常、直リンクはセッションIDを含みません。そのため、直リンクからOracle APEXのアプリケーションをアクセスした際には、必ず新しいセッションが開始されます。すでにセッションがあると、それらのセッションは無効になります。また、仮にURLにセッションIDが含まれていても、Oracle APEXがセッションを維持するために使用しているクッキーの値に含まれているセッションIDと一致しない場合、セッションは無効とされ認証が要求されます。

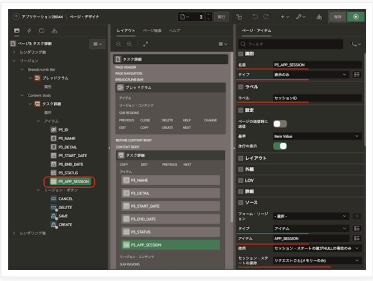
セッションを再結合を有効にすると、直リンクにセッションIDが含まれない場合、またはセッションIDが0のときに、すでにOracle APEXのセッションとして有効なクッキーがあると、そのセッションを利用します。非常に危険な設定なので、デフォルトでは**無効**になっています。また、**すべてのセッションに対して有効**の設定は認証されたセッションを含むため、開発者が設定できないよう、通常はインスタンスのレベルで設定が禁止されています。

ですので、直リンクの対象ページの**認証**を**パブリック・ページ**にし、**セッションを再結合**を**パブリック・セッションに対して有効**とすることで効果を確認してみます。



新規にセッションが開始されているかどうかを目視で確認できるように、ページ・アイテムをひとつ追加します。

追加するページ・アイテムは**名前**を**P3_APP_SESSION**とし、**タイプ**を**表示のみ**とします。**ラベル**は**セッションID**とします。情報を表示するためにのみ使用するので、**ページの送信時に送信**はOFFにします。**ソース**の**タイプ**は**アイテム**で、**アイテム**としてセッションIDを保持している組み込みのアイテムである**APP_SESSION**を指定します。**セッション・ステート**の保持は**リクエストごと(メモリーのみ)**とします。



セッションIDを含まないURLにてアクセスして、セッションIDの数値を確認します。

セッションIDが変化しないことが確認できます。ページのプロパティの**セッションを再結合**を**無効**に変更し、同様にURLアクセスを行うと、今度はセッションIDがアクセスごとに変更されることが確認できるはずです。

パブリック・ページの場合は、セッションが新規かどうかでセキュリティ上のリスクに大きな違いはでてきません。すでにページはパブリックで認証なしでアクセスできるためです。認証が必要なページの場合は、認証がスキップされるため、危険度は大幅に異なります。

例えば電子メールに直リンクが埋め込まれている場合、すでにブラウザでそのアプリケーションを使用中（認証が完了している）であれば、その直リンクをクリックすると認証なしで、かつ、すでに開始済みのセッションとして処理が実行されます。**セッションを再結合**が**無効**であれば、新たにユーザー認証が要求され、それまでのセッションは中断されます。

危険かどうかはアプリケーション自体にも依存しますが、**セッションを再結合**を**すべてのセッションに対して有効**にはしないことがお勧めです。

以上で直リンクを有効にするための設定を通した、ページを保護する機能の説明は終了です。この記事で説明していない、アプリケーション・デフォルトの設定箇所などの説明は、また記事を分けて説明します。

続く

Yuji N. 時刻: 18:06

共有

‹ ホーム ›

ウェブ バージョンを表示

自己紹介

Yuji N.

日本オラクル株式会社に勤務していて、Oracle APEXのGroundbreaker Advocateを拝命しました。
こちらの記事につきましては、免責事項の参照をお願いいたします。

詳細プロフィールを表示