



ホワイトリスト型 Web Application Firewallのススメ

昨今見られる高度化する SQL インジェクション、クロスサイト・スクリプティング攻撃の特徴

従来の SQL インジェクション攻撃、クロスサイト・スクリプティング攻撃では、GET メソッドや POST メソッドのパラメータ（クエリー）部分に、攻撃用文字列（SQL インジェクションであれば「'or'1='1」など）を埋め込むのが一般的でした。しかしながら、昨今の SQL インジェクション攻撃、クロスサイト・スクリプティング攻撃では、例えば以降に挙げるような高度化する攻撃の特徴が散見されます。これらは、WAF 等の防御システムを回避するための手法でもあり、特にブラックリスト（シグニチャー）型の WAF をすり抜ける場合があります。

● 高度化する攻撃の特徴その1

SQL インジェクション攻撃を実行するための文字列が Cookie に埋め込まれている場合があります。

従来、GET メソッドや POST メソッドのパラメータ（クエリー）部分に攻撃用文字列を埋め込むことで Web アプリケーションに渡していましたが、Cookie 値として攻撃用文字列が渡されることがあります。Web アプリケーションによっては、Cookie でパラメータが受け取れる実装になっており、この場合、攻撃が成功してしまう可能性があります。

● 高度化する攻撃の特徴その2

SQL インジェクション攻撃を実行するための文字列に「%」が含まれている場合があります。

IIS/ASP では、下記のように攻撃用文字列中に余計な「%」が入っていた場合、「%」を除去してしまうため、攻撃が成功してしまう可能性があります。

【SQL インジェクション攻撃の文字列に「%」が含まれる例】

```
' un%ion se%lect password from data wh%ere '1'='1
```

● 高度化する攻撃の特徴その3

クロスサイト・スクリプティング攻撃を実行するための文字列が UTF-7 でエンコードされている場合があります。

charset（文字コード）が不明瞭な Web アプリケーションの場合、下記のように UTF-7 で攻撃用文字列がエンコードされ、攻撃が成功してしまう可能性があります。

【クロスサイト・スクリプティング攻撃の文字列が UTF-7 でエンコードされた例】

```
+ADw-script+AD4-alert(document.cookie)+ADsAPA-/script+AD4-
```

↓デコードすると下記のようなスクリプトになります。

```
<script>alert(document.cookie);</script>
```



以上の特徴は、散見される様々な高度化する攻撃の一部に過ぎません。

このような攻撃に対し、恒久的に対策を行うには、Citrix NetScaler Application Firewall (以下 CitrixWAF) に実装されている下記に挙げるようなホワイトリスト型の機能をご使用いただくことを推奨いたします。

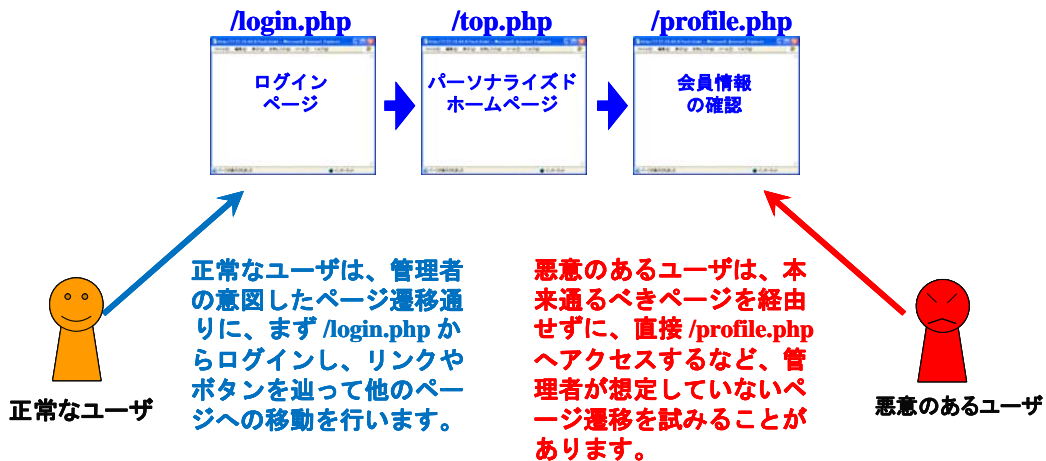
Citrix Application Firewall に実装されたホワイトリスト系の機能

● Start URL

StartURL とはユーザが訪問可能な URL を設定しておく機能です。不正なページ遷移を検知し、攻撃を防御することが可能となります。

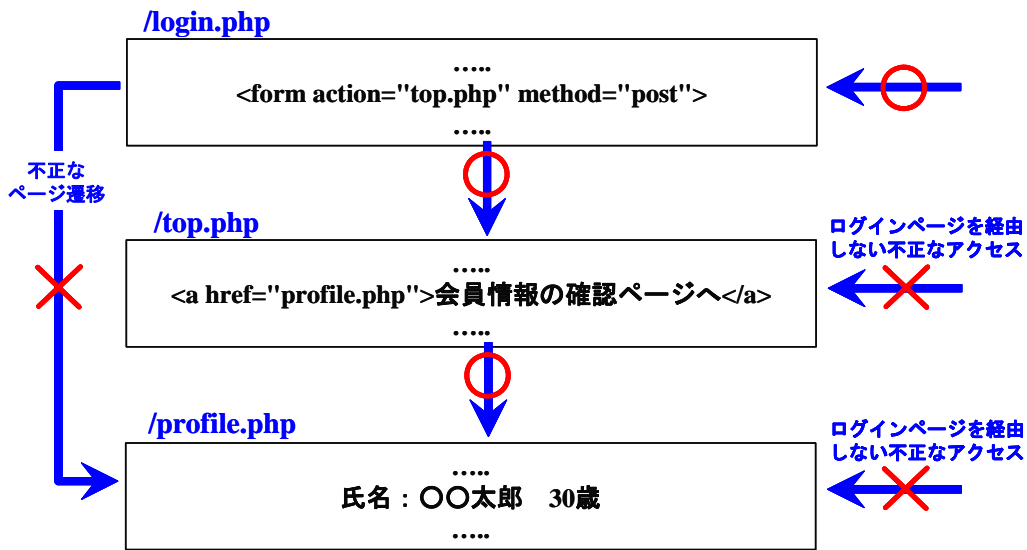
- ・ 高度なホワイトリスト機能
 - 設定工数を減らし、導入時間を大幅に短縮
 - 設定時のミスによる誤検知を大幅に削減
- ・ CitrixWAF の独自機能

下記のようなページ遷移を想定した Web アプリケーションがあると仮定します。最初にユーザ名、パスワードの入力を行いログインし、パーソナライズされたページ内のメニューからリンクを辿り、会員情報の確認を行うとします。もし悪意のあるユーザが他人の会員情報を閲覧しようと、ログインページを経由せずに会員情報確認ページ(/profile.php)へ直接アクセスしようとした場合、WAF はそれを悪意のあるアクセスとして検知する必要があります。

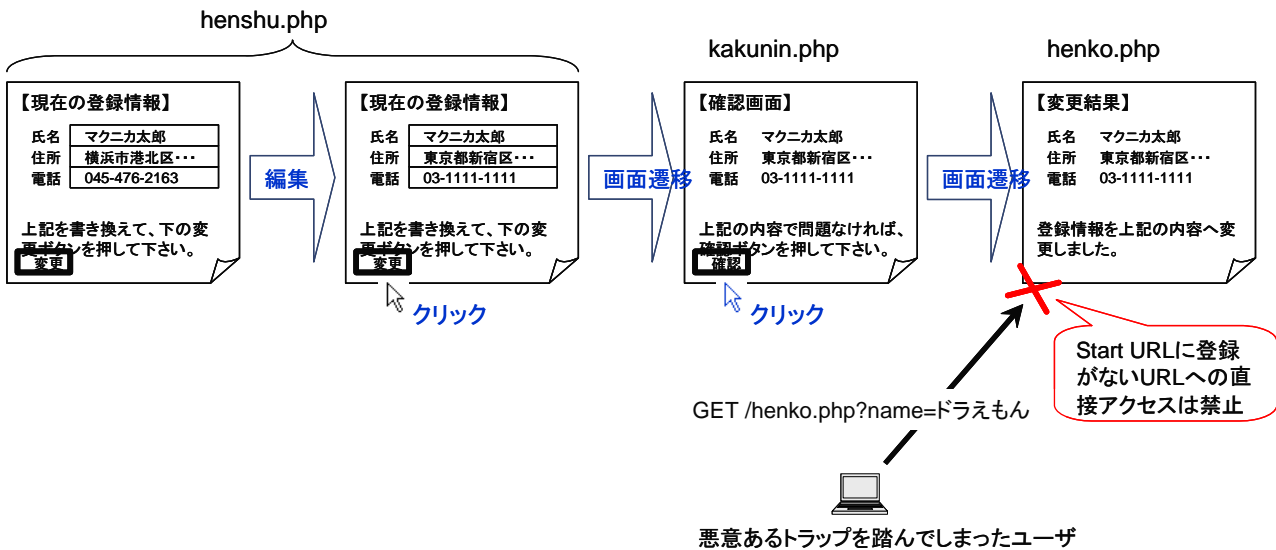


では、CitrixWAF ではどのようにセッション追跡を行っているのでしょうか。

CitrixWAF はページ内の HTML ソースを解析し、そこに埋め込まれたリンク先 URL を読み取ることで、次に遷移できるページ URL を限定することができます。



例えば、住所などの登録情報を変更する機能を想定します。1 ページ目で現在の登録情報が入力欄に埋め込まれて表示され、その入力欄の必要な部分を書き換えてボタンを押すと 2 ページ目で確認画面となり、「変更」ボタンを押すと変更が処理されて 3 ページ目が表示されるという典型的な構成を想定します。ここで、不正なトラップ（スクリプト）を踏ませて、3 ページ目に直接飛ばされ、ユーザが意図しない変更操作をさせられてしまうのが CSRF の一例です。



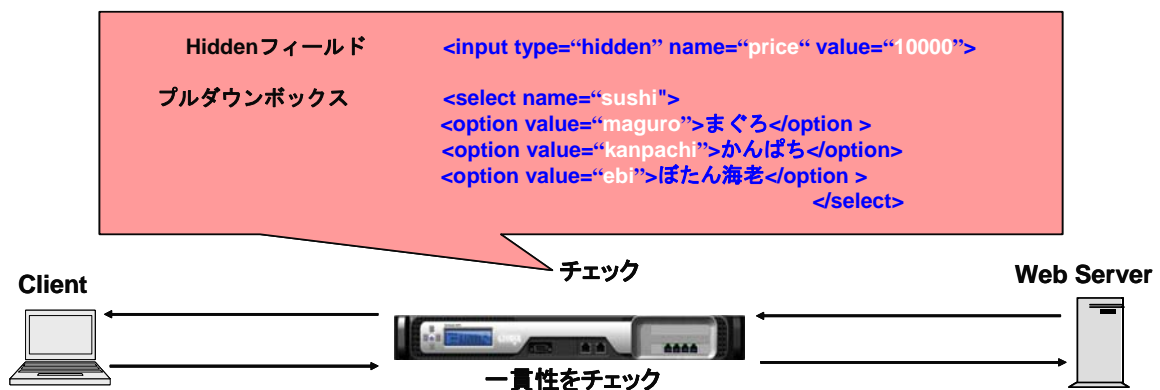
Start URL の機能を使って、1 ページ目の URL (henshu.php)、もしくはもっと手前のページの URL をエントリーポイントとして指定しておくことで、それ以降のページに直接遷移することを禁止することが可能です。



● Form Field Consistency Check

- ・双方向の通信を精査し、自動的にパラメータの一貫性をチェックして、クライアント側での不正改ざんを防ぐ。
- ・ゼロデイアタックも防御可能。
- ・ CitrixWAF の独自機能

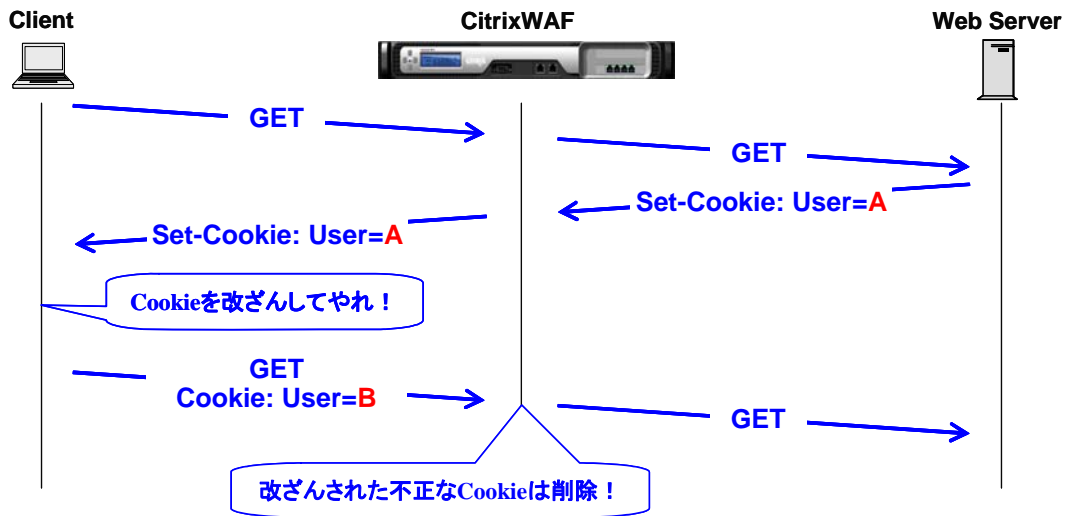
CitrixWAF はサーバから返された HTML の中身を全て精査します。そこに Hidden のような Read-Only のパラメータがある場合、次に来るクライアントからのリクエストで、同一のパラメータ名と値があるか検査します。ラジオボタン、チェックボックス、プルダウンボックスのような場合でも、値が精査したものと一致するか検査します。もし HTML になかったパラメータ名や値が含まれていると、不正アクセス（パラメータ不正変更）と見なされ、事前に指定したエラーページへリダイレクトされます。テキストボックスのように値が未定の場合でも、パラメータ名の不正変更がないかはチェックされます。このパラメータの一貫性チェックはデフォルトで動作しています。



● Cookie Consistency Check

- ・双方向の通信を精査し、自動的に Cookie 値の一貫性をチェックして、クライアント側での不正改ざんを防ぐ。
- ・ CitrixWAF の独自機能

CitrixWAF はサーバから返された Set-Cookie ヘッダをモニターし、次回以降のリクエストに同じ Cookie が付いていることを期待します。もし異なる Cookie が付いていた場合、Cookie が改ざんされたと判断し、その不正な Cookie を削除します。この Cookie の一貫性チェックはデフォルトで動作しています。



ブラックリスト（シグニチャー）型 WAF では十分でない！

ブラックリスト型では、一般的なアプリケーションでブロックしたほうがよいであろうパターンをパターンマッチでブロックするためのリストでのマッチングになりますので、攻撃者からの一般的なアプリケーションに対する不正な入力値をブロックすることができます。

しかしながら、実際のアプリケーションではアプリケーション毎にそれぞれ URL（ディレクトリ構造）や使用するパラメータ、Cookie などが異なり、全てをパターン化しブラックリストで防ぐことができません。そのため、ホワイトリストでアプリケーション毎のアプリケーションで許可すべき通信パターンだけをリスト化し、それ以外をブロックすることでアプリケーションの安全性を高めることができるのです。

Citrix WAF のホワイトリスト設定は簡単！

未知の攻撃に強いホワイトリスト型の WAF を導入しても、Web アプリケーションに組み込まれているパラメータ（Hidden、ラジオボタン、チェックボックス、プルダウンなど）、リンク、クッキー情報は数千、数万と存在し、そのすべての値を手動で正確にホワイトリスト化することは不可能とっていいかもしれません。

CitrixWAF であればサーバから返された HTML の中身を全て精査し、リアルタイム且つ全自動でホワイトリストを有効にします。このことにより管理者が手動でホワイトリスト作成することがなくなります。また、コンテンツが更新された場合であっても自動的にホワイトリストを作成する CitrixWAF であれば追加作業を必要としません。



また、現在 CitrixWAF を購入されているお客様は、ライセンス費用の追加なしでホワイトリスト機能の利用が可能です。そのため、すでに CitrixWAF/ 旧 Teros WAF をご利用いただいているお客様におかれましてもホワイトリストを利用されることをお勧めします。

最新の NetScaler シリーズではホワイトリスト機能を利用することでのパフォーマンス劣化はほとんどありません。

弊社エンジニアによるコンサルティング・支援サービスもご提供しておりますので、CitrixWAF の導入をご検討の方、もしくは、旧 Teros/ NetScaler をご利用のお客様でホワイトリスト機能をご利用希望のお客様はぜひお問い合わせください。

<Citrix 製品お問い合わせ先>

マクニカネットワークス株式会社 Citrix 製品担当

TEL : 045-476-2010 FAX : 045-476-2060

E-mail : citrix_sales@cs.macnica.net

製品詳細 : <http://www.macnica.net/citrix/waf.html/>