Alibaba Cloud Web Application Firewall

ベストプラクティス

Document Version20190920

目次

1 Web 脆弱性の保護の提案.....1
1.1 Apache Struts2 REST プラグインの DoS 脆弱性に対する保護のベストプラクティス (CVE-2018-1327)..... 1
1.2 WordPress の DoS 脆弱性に対する保護のベストプラクティス (CVE-2018-6389)..... 2
2 配信元サーバーの保護.....5
3 Web アプリケーション保護のためのベストプラクティス.....9
4 悪意のあるクローラーの阻止.....13

1 Web 脆弱性の保護の提案

1.1 Apache Struts2 REST プラグインの DoS 脆弱性に対する保護のベストプラクティス (CVE-2018-1327)

HPE (Hewlett Packard Enterprise) の 2 人のセキュリティエキスパート (Yevgeniy Grushka 氏と Alvaro Munoz 氏) が、Apache Strust2 REST プラグインに DoS の脆弱性を発見しました。 Struts REST プラグインで XStream ライブラリハンドラーを使用すると、攻撃者は悪意のある XML リクエストを作成して DoS 攻撃を開始します。

脆弱性番号

CVE-2018-1327

脆弱性の名前

Apache Struts2 REST プラグイン DoS 脆弱性 (S2-056)

脆弱性の説明

S2-056 脆弱性が Apache Struts2 REST プラグインに存在します。 XStream コンポーネントを使用して XML 形式のパケットを逆シリアル化し、データコンテンツを検証しない場合、攻撃者は悪意のある XML データを送信してアプリケーションにリモート DoS 攻撃を開始します。

悪意のある攻撃者が大量の攻撃リクエストを開始すると、アプリケーションの置かれる CPU リソースが急速に一杯になります。

この脆弱性の詳細については、『公式の脆弱性の公開』をご参照ください。

影響範囲

Struts 2.1.1 ~ Struts 2.5.14.1

公式ソリューション

Apache Struts をバージョン 2.5.16 にアップグレードします。

防御アドバイス

Apache Struts のバージョンをアップグレードしてこの脆弱性を解決しない場合は、WAF の HTTP ACL ポリシーとカスタム HTTP フラッド保護機能を使用して業務を保護することを推奨します。

- HTTP ACL ポリシーを使用して、特定の XML データ (`com . sun . xml . internal . ws . encoding . xml . XMLMessage $ XmlDataSou rce`) を含む POST リクエストを制限し、この脆弱性を利用して開始された DoS 攻撃リクエストをブロックします。たとえば、次のルールを設定して Apache Strust REST プラグインの XStream ライブラリのアプリケーションページを使用する攻撃リクエストをブロックします。

- カスタム HTTP フラッド保護機能を使用して、同一 IP アドレスに対して Apache Strust REST プラグインの XStream ライブラリのアプリケーションページを使用するリクエストの頻度を制限します。 たとえば、次のルールを設定して指定したページへのリクエスト頻度が 5 秒ごとに 100 回を超えないことを確認します。

HTTP ACL ポリシーとカスタム HTTP フラッド保護機能の紹介については、「HTTP ACL ポリシー」と「カスタム HTTP フラッド保護」をご参照ください。

1.2 WordPress の DoS 脆弱性に対する保護のベストプラクティス (CVE-2018-6389)

2018 年 2 月 5 日、セキュリティ研究者らが WordPress に関する DoS (サービス拒否) の脆弱性 (CVE-2018-6389) を公開しました。 WordPress バージョン 3.x ~ 4.x はこの脆弱性の影響を受けます。 悪意のある攻撃者は、1 回のリクエストで WordPress に複数の JavaScript ファイルをロードすることでサーバーリソースを使い切り、DoS がトリガーされます。

Alibaba Cloud WAF はこの脆弱性の影響を受けません。 ただし、Web サイト業務で WordPress を使用している場合は、適切な保護ルールを設定することを推奨します。

脆弱性の説明

この脆弱性は *load - scripts . php* ファイル内にあります。 *load - scripts . php* とは WordPress CMS 用の組み込みスクリプトです。 *load - scripts . php* ファイルは、 `name` パラメーターを `load` パラメーターに渡して、必要な JavaScript ファイルを選択的に呼び出します。 name パラメーターは コンマ (,) で区切ります。

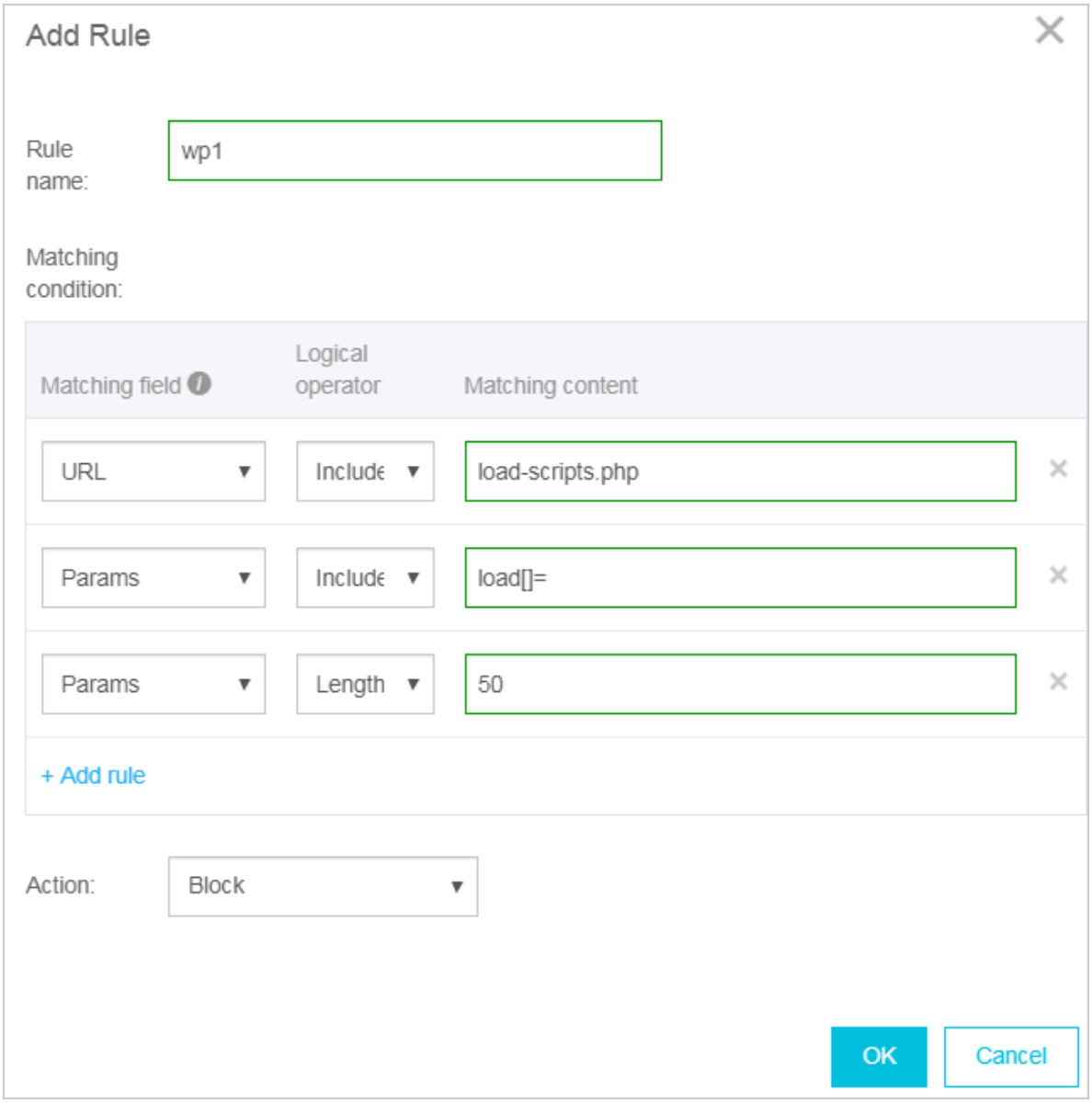
たとえば、 `https :// example . com / wp - admin / load - scripts . php ? c = 1 & amp ; load []= jquery - ui - core , editor & amp ; ver = 4 . 9 . 1` リクエストにアップロードされた JavaScript ファイルは、 *jquery - ui - core* と *editor* です。

`script - loader . php` ファイル内に定義された 181 個の JavaScript ファイルは、単一のリクエストでロードすることができるため、悪意のある攻撃者は権限付与されたログインなしで多数のリクエストを送信します。 これによりサーバーの負荷が増大し、DoS 攻撃が開始されます。

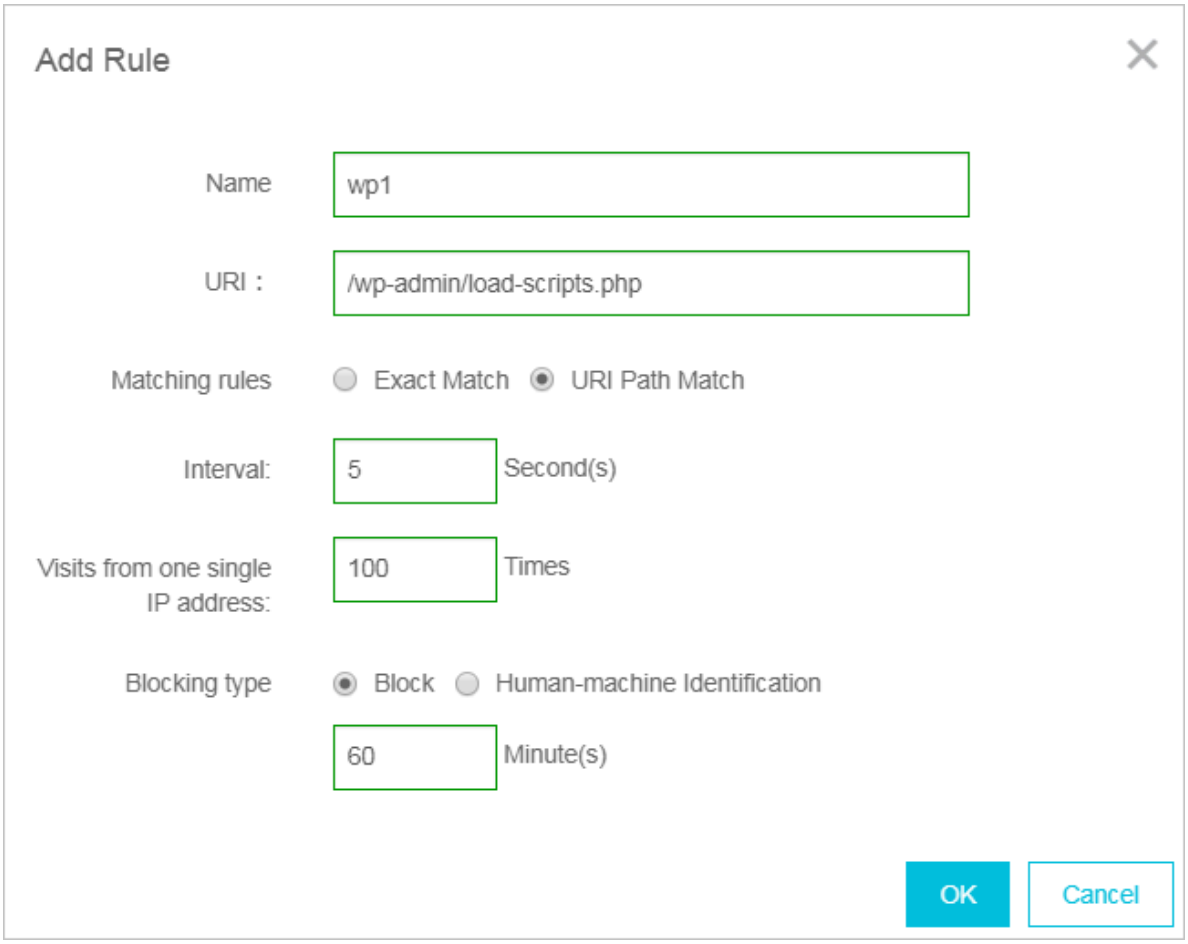
防御アドバイス

HTTP ACL ポリシーとカスタム HTTP フラッド保護を使用して、WordPress Web サイト業務を保護することを推奨します。

- HTTP ACL ポリシーを介して `load - scripts . php` ファイルに渡すパラメーターの数を制限します。 たとえば、次のルールを設定して、 `load - scripts . php` ファイルに渡すパラメーターの最大長を 50 文字までに制限します。



- カスタム HTTP フラッド保護によって、同一 IP アドレスからの `load-scripts.php` ファイルに対するリクエストの頻度を制限します。 たとえば、次のルールを設定して、`load-scripts.php` ファイルへの同一 IP からのリクエストの最大頻度を制限します。



HTTP ACL ポリシーとカスタム HTTP フラッド保護の紹介については、「HTTP ACL ポリシー」と「カスタム HTTP フラッド保護」をご参照ください。

2 配信元サーバーの保護

配信元サーバーの IP アドレスが公開されている場合、攻撃者はそれを悪用して Alibaba Cloud WAF を迂回し、配信元サーバーに対して直接配信元攻撃を開始する可能性があります。 このような攻撃を防ぐには、配信元サーバーにセキュリティグループ (ECS 配信元) またはホワイトリスト (SLB 配信元) を設定します。

> 注 :
> 本ページで説明されている設定は必須ではありません。 ただし、IP 公開によって発生する可能性があるリスクを排除するために設定することを推奨します。

次のように、配信元サーバーにこのようなリスクがあるかどうかを確認します。

Telnet を使用して、Alibaba Cloud 以外のホストから配信元サーバーのパブリック IP アドレスのリスナーポートへの接続を確立します。 接続が成功したかどうかを確認します。 接続に成功した場合、配信元サーバーは露出のリスクに直面しています。 ハッカーはパブリック IP アドレスを取得すると、WAF を迂回して配信元サーバーに到達可能です。 接続に失敗した場合、配信元サーバーは安全です。

たとえば、WAF が有効な配信元サーバ IP のポート 80 と 800 への接続をテストします。 接続が正常に確立された場合、配信元サーバーは安全ではありません。

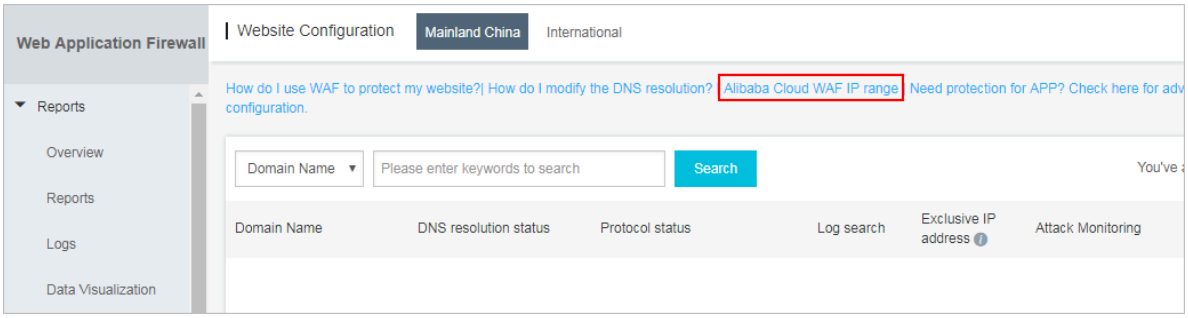
```
Last login: Tue Jul 31 13:48:10 on ttys000
[                          l$ telnet 4            80 ]
Trying (          )5...
Connected to (          5.
Escape character is '^]'.
^ZConnection closed by foreign host.
```

注記

セキュリティグループの設定には一定のリスクがあります。 次の点を考慮します。

- 配信元サーバー (ECS または SLB インスタンス) でホストされているすべてのドメイン名が Alibaba Cloud WAF にデプロイされていることを確認します。
- WAF で検査されたトラフィックがスタンバイルートを介して配信元サーバーに返される Alibaba Cloud WAF クラスター障害の場合、配信元サーバーでセキュリティグループポリシーが有効になっていると、サイトへのアクセスが影響を受けます。
- Alibaba Cloud WAF の IP アドレスを拡張する場合、配信元サーバーでセキュリティグループポリシーが有効になっていると、訪問者に 5xx エラーページが頻繁に返されることがあります。

1. Alibaba Cloud WAF コンソールにログインします。
2. [管理] > [Web サイト設定] ページに移動します。
3. [Alibaba Cloud WAF IP 範囲] をクリックして WAF IP アドレスを表示します。



4. [Alibaba Cloud WAF IP 範囲] ダイアログボックスで、[IP リストのコピー] をクリックします。

5. 配信元サーバーのアクセス制御を設定して WAF IP アドレスのみを許可します。

   - ECS 配信元の場合

     a. ECS インスタンスリストに移動し、配信元インスタンス見つけ、[管理] をクリックします。

     b. 左側のナビゲーションウィンドウで、[セキュリティグループ]をクリックします。

     c. 操作するセキュリティグループを探し、[ルールの追加] をクリックします。

     d. [セキュリティグループルールの追加] をクリックし、次の設定を完了して最も優先度の高い WAF IP アドレスを許可します。

        - NIC: インターネットネットワーク
        - ルールの方向: Ingress
        - アクション: 許可
        - プロトコル種別: カスタム TCP
        - 権限付与タイプ: Ipv4 CIRD ブロック
        - ポート範囲: 80/443
        - 権限付与オブジェクト: 手順 4 でコピーした WAF IP アドレスを貼り付けます。
        - 優先度: 1

     e. 別のセキュリティグループルールを追加し、次のように設定して、優先順位が最も低いアクセスをすべてブロックします。

        - NIC: インターネットネットワーク
        - ルールの方向: Ingress
        - アクション: 禁止
        - プロトコル種別: カスタム TCP
        - ポート範囲: 80/443
        - 権限付与タイプ: Ipv4 CIRD ブロック
        - 権限付与オブジェクト: 0.0.0.0/0
        - 優先度: 100

      注 :

配信元インスタンスが他の IP またはアプリケーションと対話する場合は、対応するルールを追加してアクセスを許可する必要があります。

- SLB 配信元の場合

  SLB インスタンスの設定は ECS と似ています。 WAF IP アドレスをホワイトリストに追加します。 詳細は、「アクセス制御の設定」をご参照ください。

  - アクセス制御リストの作成
  - WAF IPアドレスを IP ホワイトリストに追加
  - IP ホワイトリストの有効化

3 Web アプリケーション保護のためのベストプラクティス

本ページでは、Alibaba Cloud Web Application Firewall (WAF) の Web アプリケーション保護のためのベストプラクティスについて説明します。 シナリオ、保護ポリシー、保護効果、およびルール更新という 4 つの側面を紹介します。

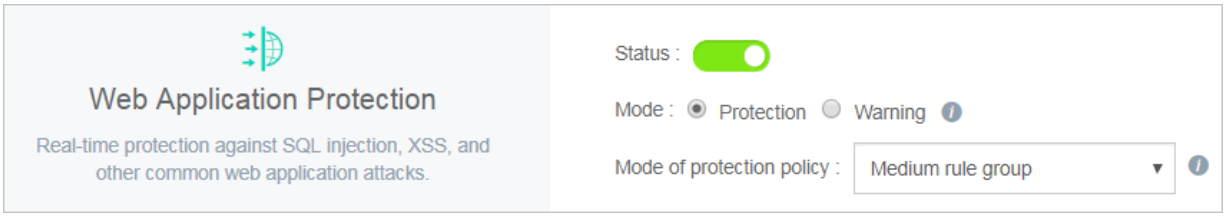
シナリオ

WAF は、SQL インジェクション、XSS、リモートコマンド実行、Webshell アップロードなどの Web 攻撃に対する保護を提供します。 Web 攻撃の詳細については、「OWASP 2017 Top 10」をご参照ください。

> 注：
> サーバー侵入を引き起こすホスト層サービスのセキュリティ問題 (Redis や MySQL への不正アクセスなど) は、WAF の対象外です。

保護ポリシー

保護用 WAF に Web サイトを追加後、Web Application Firewall コンソール にログインし、[管理] > [Web サイト設定] に移動します。 次の図に示すように、保護するドメインを選択して、[ポリシー] をクリックして Web アプリケーション攻撃の保護ステータスを表示します。



Web アプリケーション保護機能が有効になり、標準モードの保護ポリシーがデフォルトで使用されます。 この機能では、

・ ステータス

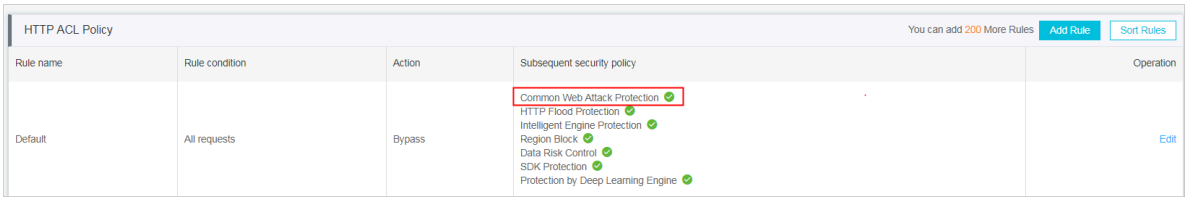
- 有効は、Web アプリケーション保護が有効であることを示しています。
- 無効は、Web アプリケーション保護が無効であることを示しています。

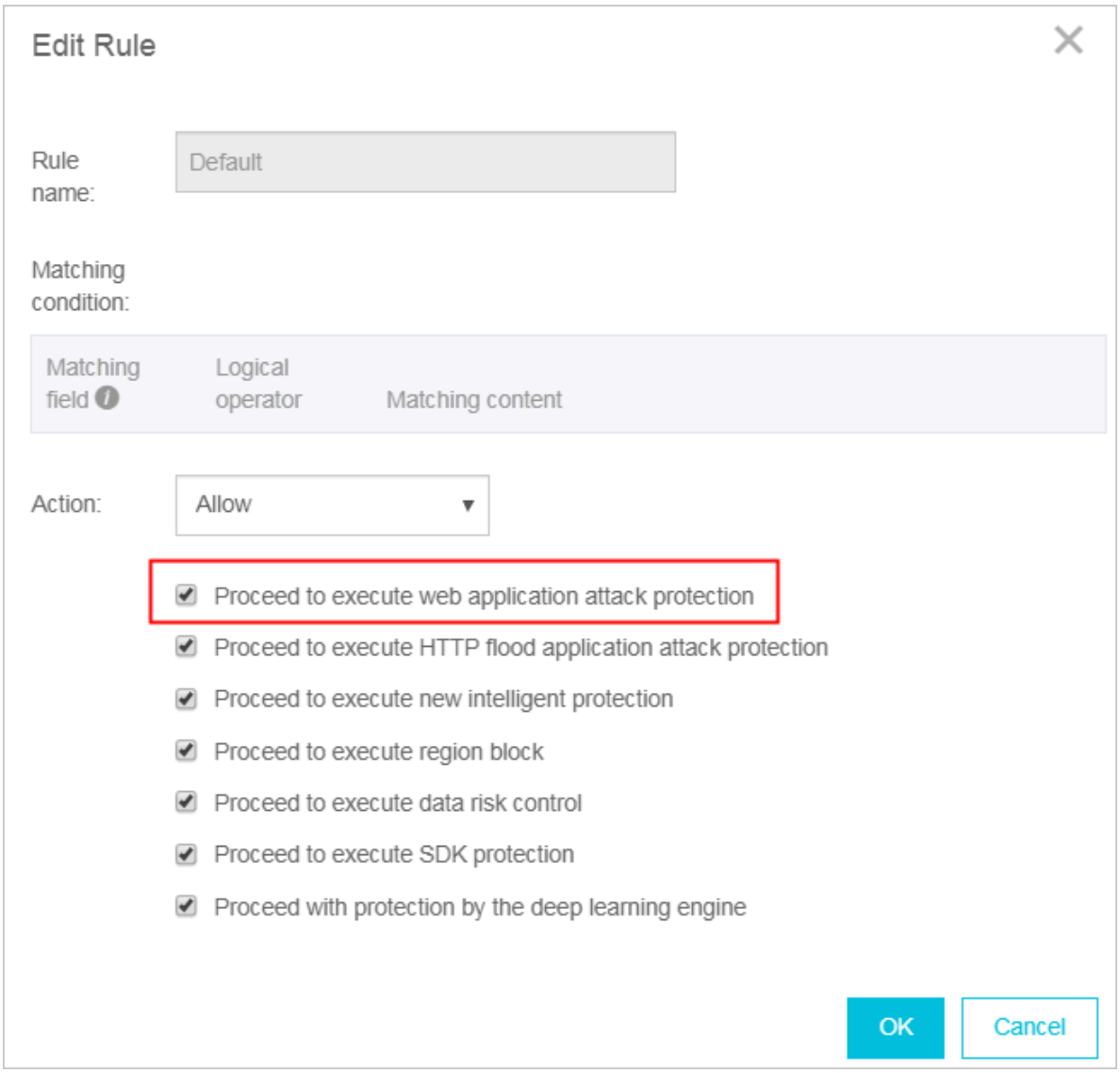
- モード: 保護モードと警告モードがあります。
  - 保護モードは、WAF が悪意のあるリクエストを自動的にブロックし、Web 攻撃を受けているときにバックエンドで攻撃ログをログすることを示します。
  - 警告モードは、Web 攻撃を受けているときに WAF が悪いのあるリクエストをブロックしていないことを示します。 WAF は攻撃をバックエンドでログするだけです。
- 保護ポリシーのモード: 保護モードには、"緩い"、"標準"、"厳しい" の 3 つがあります。 この設定は、保護が有効になって初めて有効になります。
  - 緩い: 明らかな攻撃特性を持ったリクエストのみをブロックします。
  - 標準: 迂回特性を持った一般的な攻撃リクエストをブロックします。
  - 厳しい: 複雑な迂回特性を持った攻撃リクエストをブロックします。

使い方の提案:

- 自身の業務トラフィック特性が明確でない場合は、まず警告モードに切り替えて観察することを推奨します。 通常、Web 保護機能を 1 ~ 2 週間観察してから警告モードで攻撃ログを分析することを推奨します。
  - 通常のトラフィックがブロックされていることを示す記録が見つからない場合は、保護モードに切り替えて保護を有効にします。
  - 通常の業務トラフィックが攻撃ログに見つかった場合は、Alibaba Cloud セキュリティエキスパートに連絡して問題を解決します。
- PHPMyAdmin と開発テクノロジフォーラムを保護用 WAF に追加すると、WAF はこれらのサイトをブロックする可能性があります。 Alibaba Cloud セキュリティエキスパートに連絡して問題を解決することを推奨します。
- 業務運用においては、次の点に注意する必要があります。
  - 元の SQL 文と JavaScript コードを通常業務の HTTP リクエストに渡さないでください。
  - `www . example . com / abc / update / mod . php  set = 1` などの通常業務の URL のパスとして特別なキーワード (UPDATE や SET など) を使用しないでください。
  - 業務にファイルをアップロードする必要がある場合は、50 Mbpsを超えるファイルを Web を介して直接アップロードしないでください。 OSS または他の方法を使用してファイルをアップロードすることを推奨します。

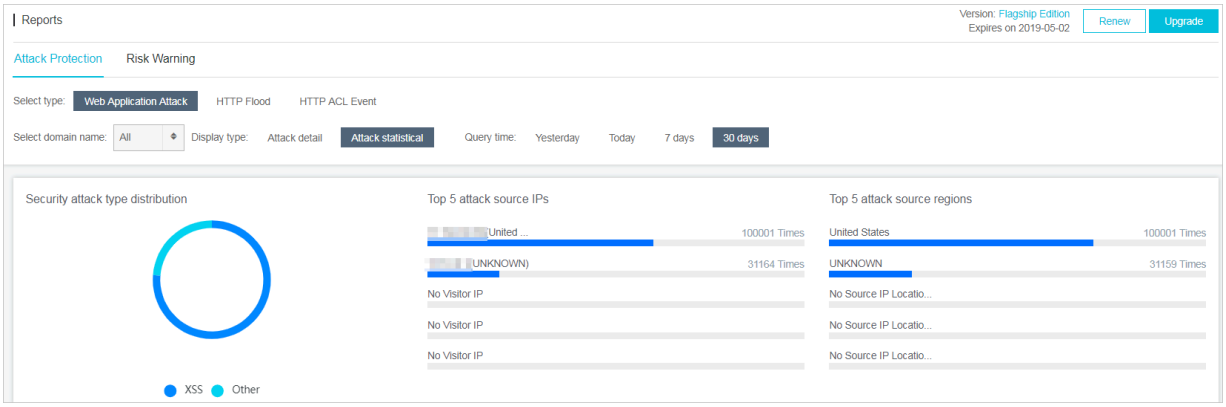
- Web アプリケーション保護を有効にした後、HTTP ACL ポリシーのデフォルトルールで一般的な Web 攻撃保護を無効にしないでください。



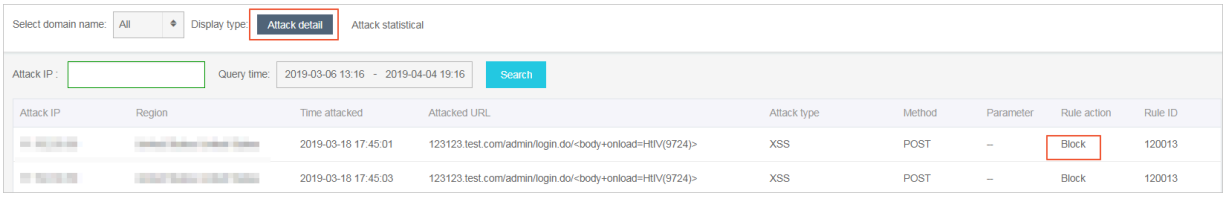


保護結果

Webアプリケーション保護を有効にしたら、次の図に示すように、[レポート] > [レポート] ページでブロックされた攻撃のログを表示します。



昨日、今日、過去 7 日間、および先月の攻撃の詳細を表示します。 次の図に示すように、[攻撃の詳細] をクリックして攻撃情報を表示します。



スクリーンショットに表示されているログは、WAF によってブロックされた SQL インジェクション攻撃リクエストです。

> 注：
> WAF が通常の業務トラフィックをブロックしていることがわかった場合は、影響を受ける URL にホワイトリストを設定して、Alibaba Cloud セキュリティエキスパートに連絡して解決策を見つけることを推奨します。

ルール更新

パブリックネットワーク上の既知の脆弱性や未公開のゼロデイ脆弱性について、Alibaba Cloud WAF は保護ルールを更新し、タイムリーに保護速報をリリースします。

Web Application Firewall コンソール にログインします。 次の図に示すように、[概要] > [セキュリティ] ページに移動して、最新の保護速報を表示します。

> 注：
> Web 攻撃には通常、複数の概念実証 (POC) があります。 Alibaba Cloud のセキュリティエキスパートは、脆弱性の原理を徹底的に分析し、公開されている Web 保護ルールが公開、未公開の脆弱性の突破口すべてを確実にカバーできるようにします。

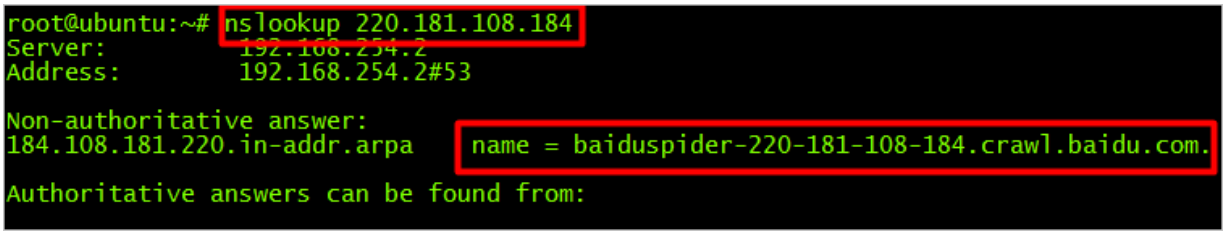
4 悪意のあるクローラーの阻止

本ページでは、悪意のあるクローラーの特徴と、 WAF を使用してクローラーをブロックする方法について説明します。

注意すべきことは、プロフェッショナルのクローラーが、 Web サイト管理者の設定したクロール防止ポリシーを回避するよう絶えずクロール方法を変更していることです。 固定したルールを適用して完全な保護を実現することは不可能です。 さらに、クロール防止は、自身の業務の特性と強い関連性があります。 したがって、理想に近い結果を得るためには、保護ポリシーを定期的に見直して更新する必要があります。

悪意のあるクローラーの識別

一般的に、通常のクローラーには xxspider のユーザーエージェントに似たマークが付いています。 定期的にリクエストし、URL と時間は比較的分散しています。 正当なクローラーに対して逆 nslookup または tracert を実行すると、常に正当なソースアドレスが見つかります。 たとえば、次の図は Baidu クローラーレコードを示します。

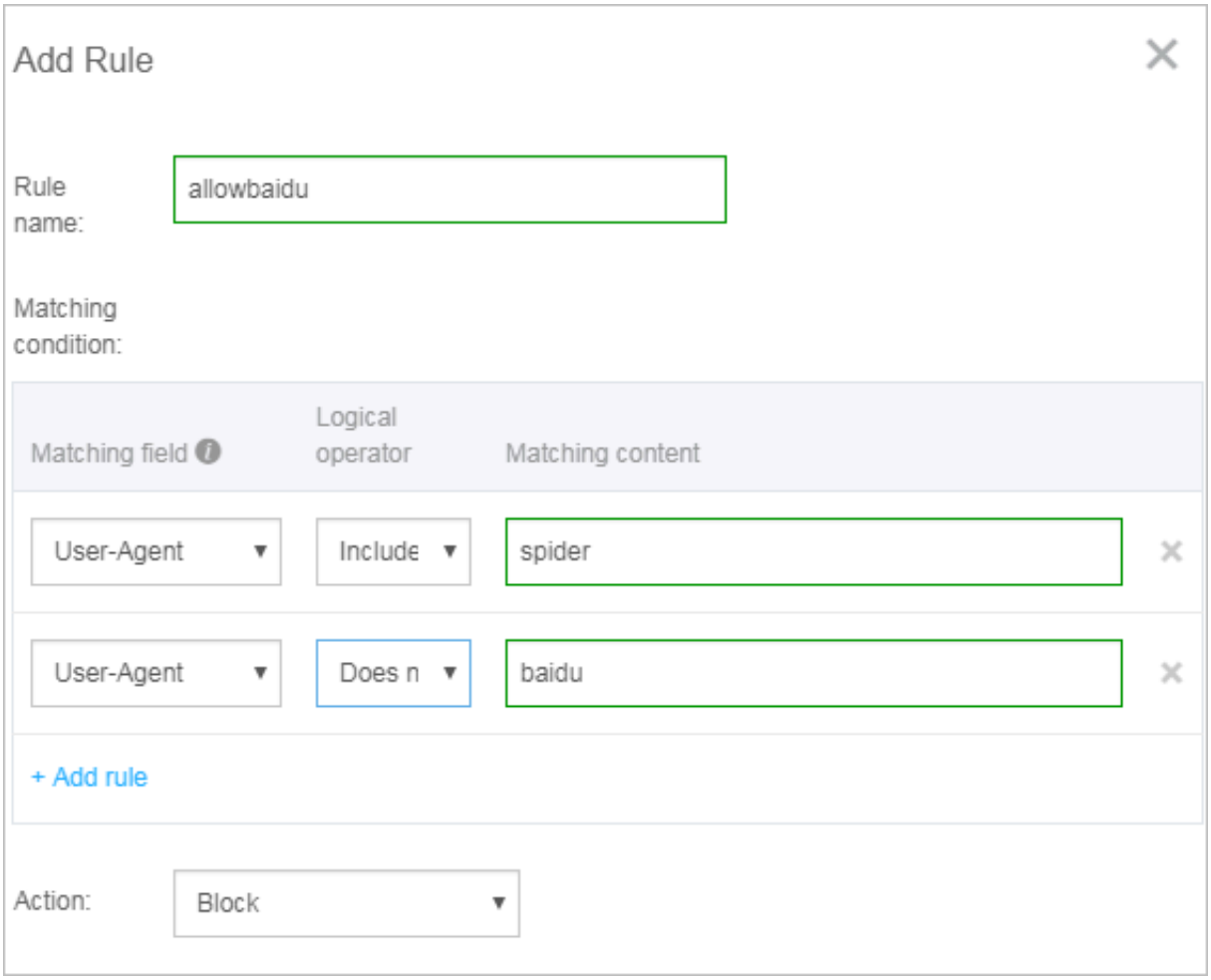


ただし、悪意のあるクローラーは、特定の期間中にドメイン名の特定の URLやインターフェイスに対し、大量のリクエストを送信することがあります。 これは、クローラーを装った HTTP フラッド攻撃、またはサードパーティを装ったターゲット機密情報をクロールするクローラーである可能性があります。 悪意のあるクローラーが送信したリクエストの数が十分に多い場合、通常、CPU 使用率の急上昇、Web サイトを開けない、およびサービスの中断を引き起こします。

WAF は悪意のあるクローラーに対してWAF セキュリティレポートを行い、前日のクローラーリクエストについて警告します。 実際の事業状況に基づいて以下のルールを 1 つ以上設定して、対応するクローラーリクエストをブロックします。

HTTP ACL ポリシーを設定して特定のクローラーをブロック

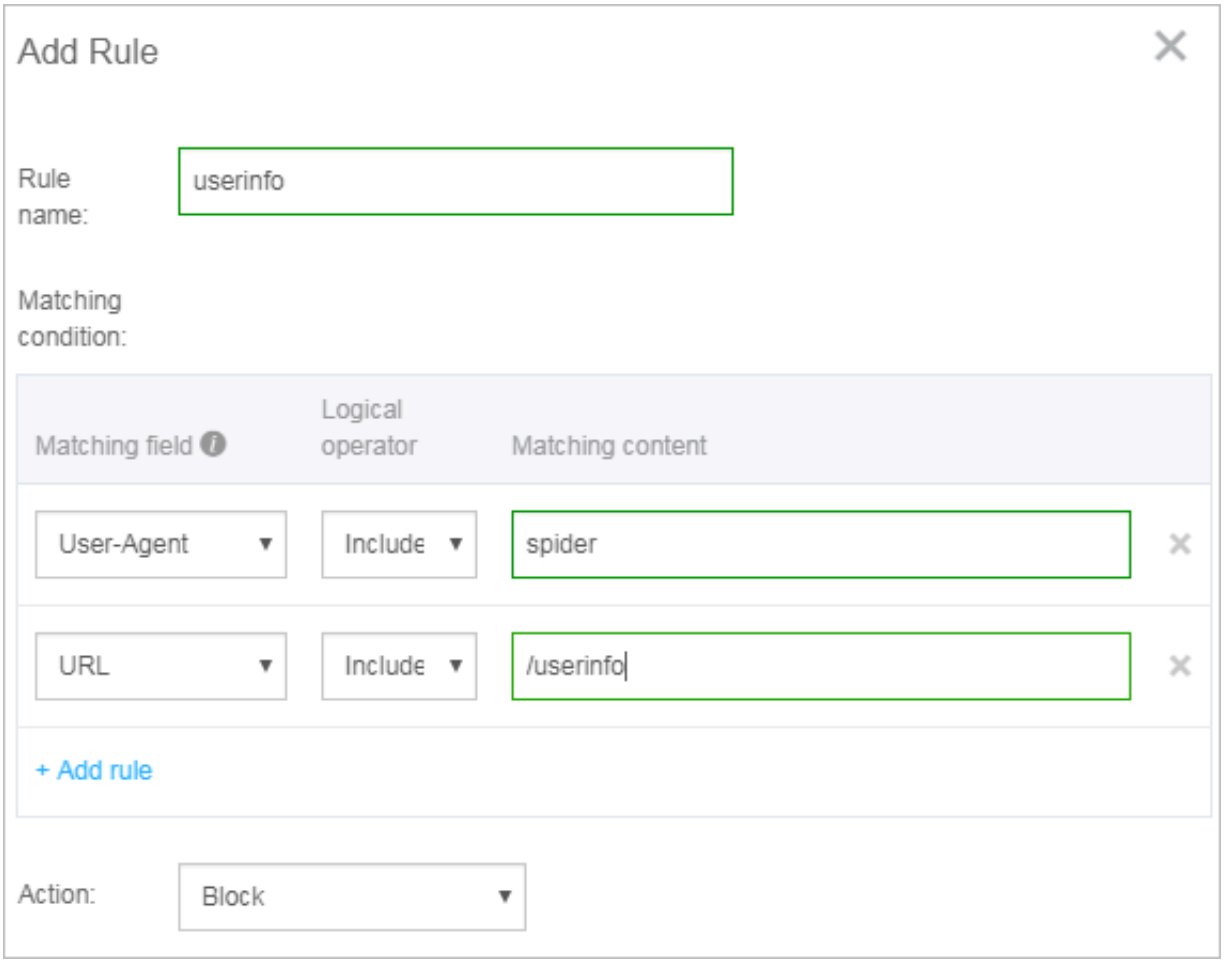
HTTP ACL ポリシーを設定して、ユーザーエージェント、URL、およびその他のキーワードを使用して悪意のあるクローラーリクエストをフィルターして除外します。 たとえば、次の設定では Baidu クローラーのみを許可し、他のクローラーをフィルターして除外します (キーワードの大文字と小文字は区別されません)。



注：

ルール内の複数の条件は ”AND” 論理関係によってつなぐため、ルールを有効にするには、リクエストがルールの条件をすべて満たす必要があります。

次の設定を使用して、すべてのクローラーが `/userinfo` ディレクトリ配下のコンテンツにアクセスできないようにします。



カスタム HTTP フラッドポリシーを設定して悪意のあるリクエストをブロック

カスタム HTTP フラッド保護ルールを使用して、一定のアクセス頻度でいくつかの特定 URL のブロックルールを設定可能です。