知識庫文章

AppWall Web 應用程序防火牆 XML/SOAP Web 服務保護 (WAPP) 使用 XML 安全過濾器

應用牆

最佳實踐

最近更新時間 2018 年 3 月 26 日

創建日期

文章編號 BP3528

設想

AppWall XML 安全過濾器解析 POST 請求正文中的 XML 並提取 XML 元素/屬性的鍵/值，以便創建允許的應用程序使用和結構的積極安全模型。

任何篡改 Web 服務應用程序方案、變量或 WSDL 披露的嘗試都會被識別和阻止。
XML 過濾器是針對 XML 外部實體攻擊（又名 OWASP 2017 A4 XXE）的本機保護

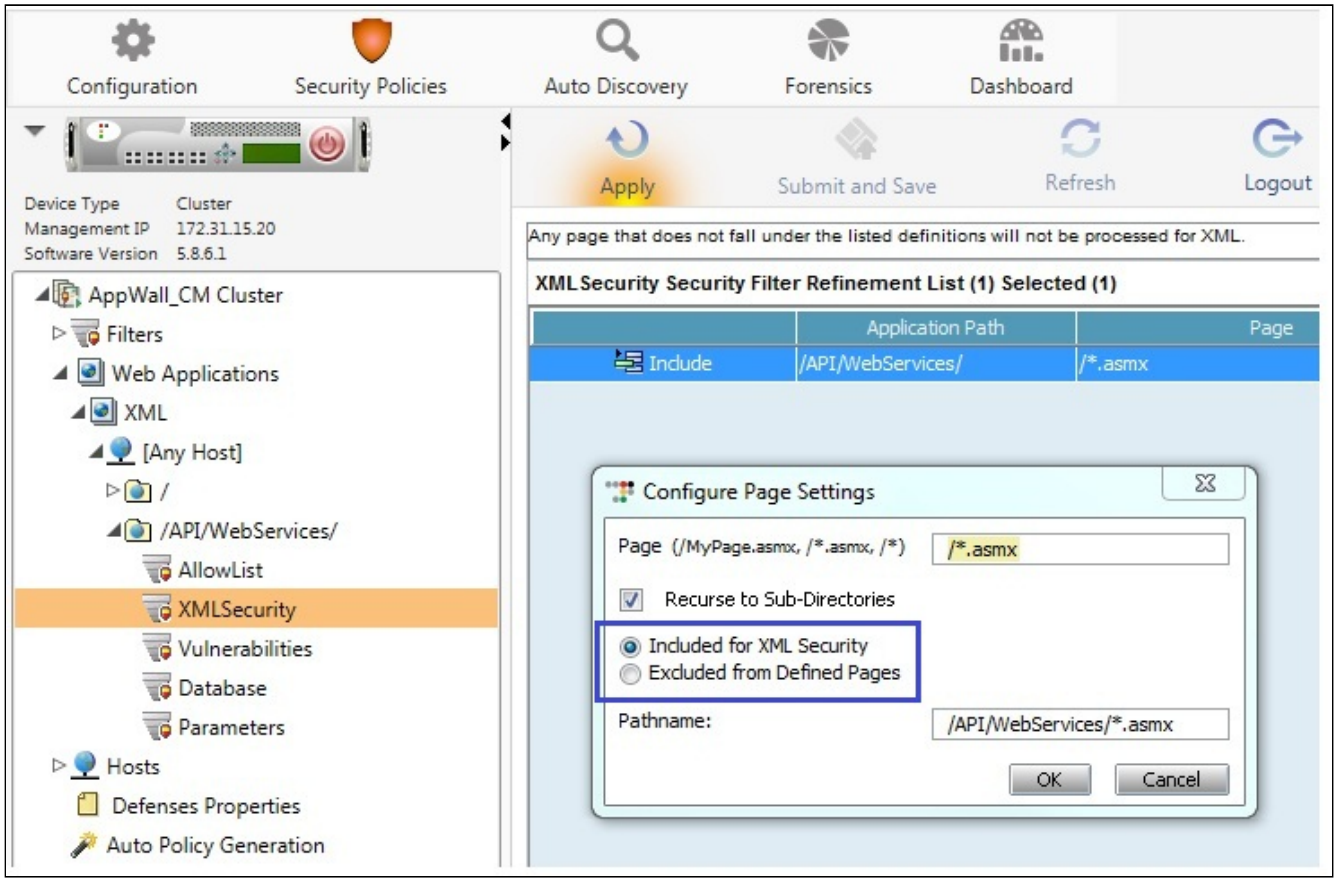
配置

設置 XML 過濾器

1. 從"*安全*"選項卡中，選擇"**過濾器">"Web 應用程序">"應用程序路徑">"將 XML 安全過濾器添加到您的策略"。**
2. 執行以下操作之一：
    a. **為 XML 安全**性選擇包含以指定特定應用程序路徑 (/API/WebServices/) 中的頁面擴展。

或者

b. 選擇**從定義的 頁面**中排除以*排除*指定的頁面擴展名。



The parameters created are passed for validation by subsequent parameter-related security filters defined in the application path.
Other AppWall security filters (Vulnerabilities, Database, and Parameters) are now part of the Web services protection.

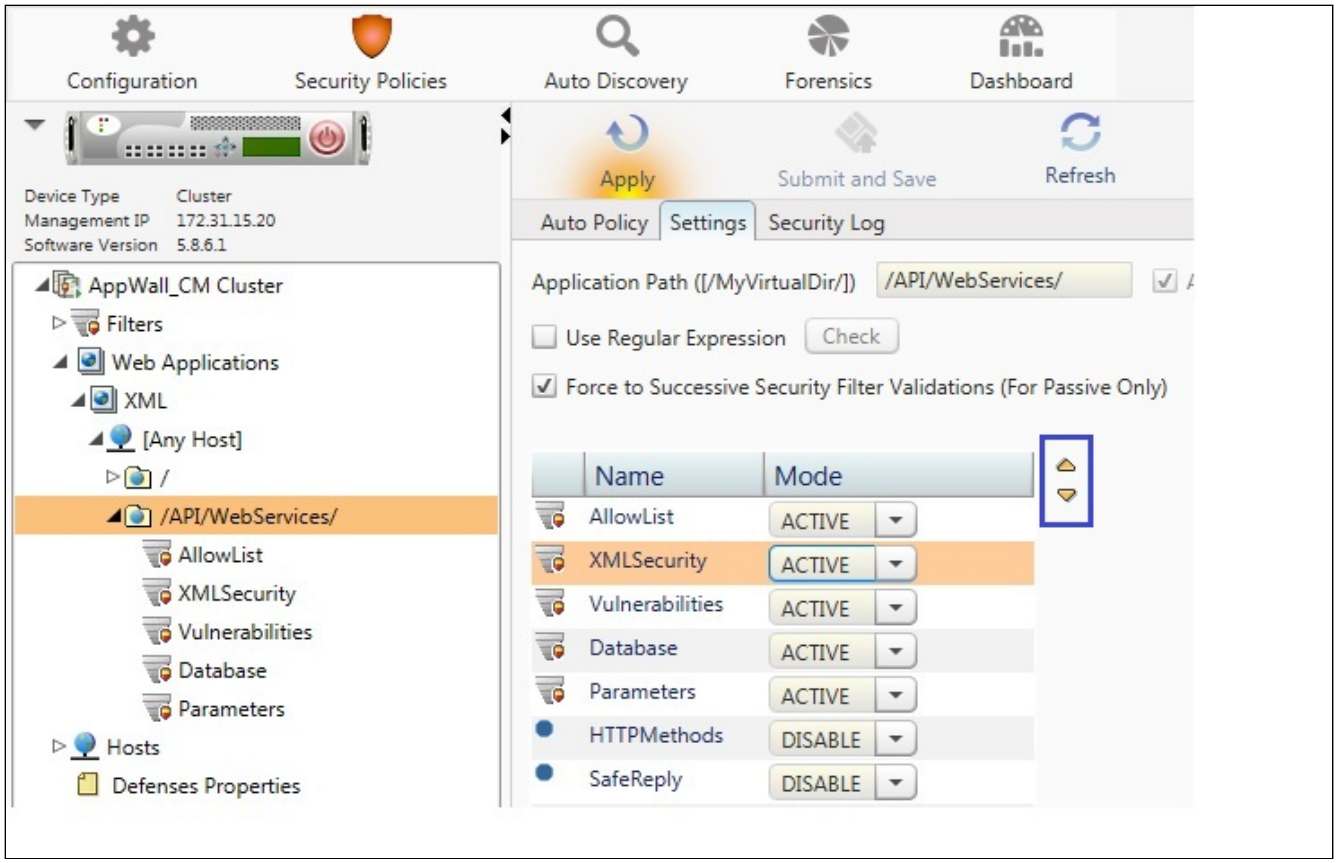
Setting Filter Priority

The XML Security filter should be placed prior to the Vulnerabilities, Database and Parameters

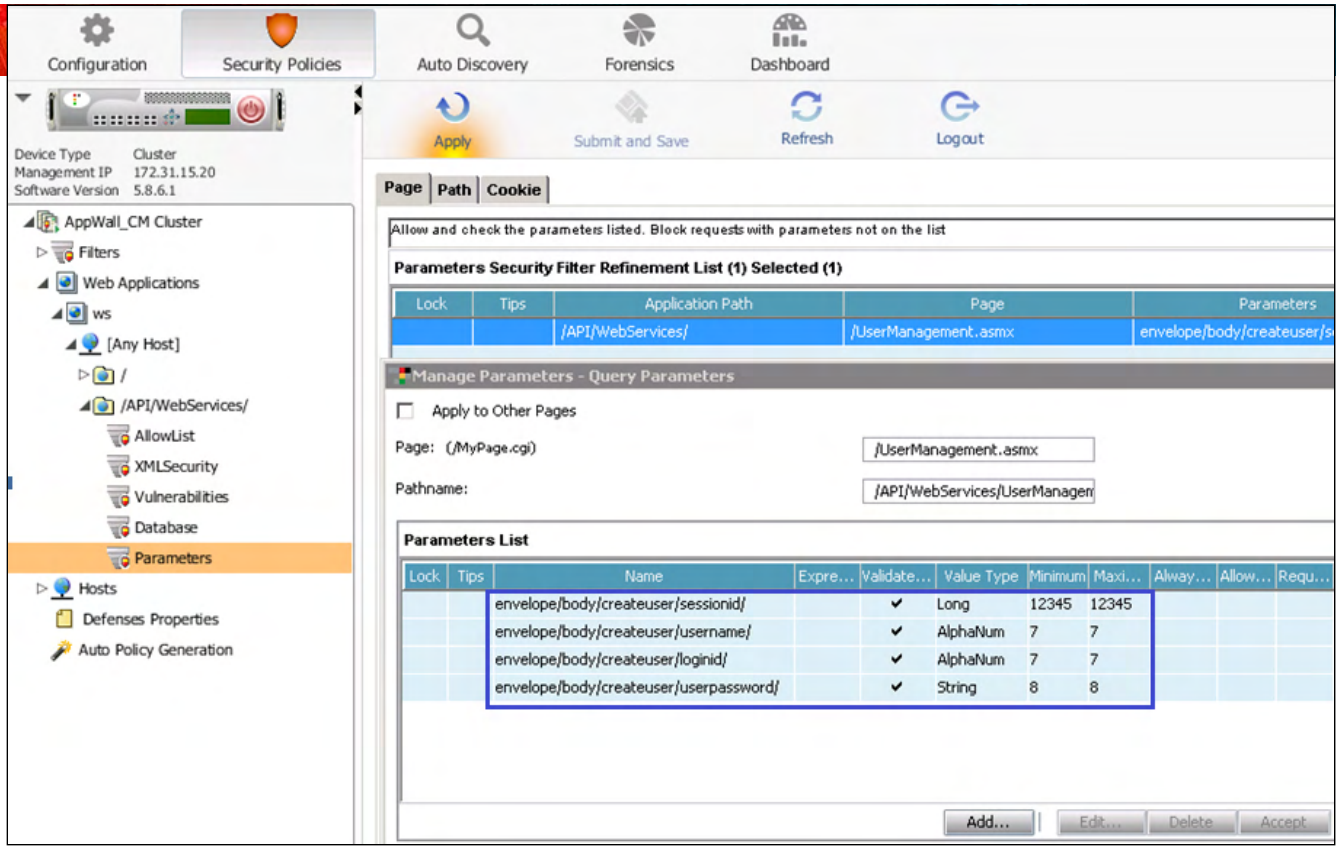
filters.

To set filter priority:

1. From the *Security* tab, select **Filters > Web Applications > XML > Host > API Web Services.**
2. Select the *Setting* tab.
3. Select the filter whose priority you want to change and click the up or down arrow, as shown below:



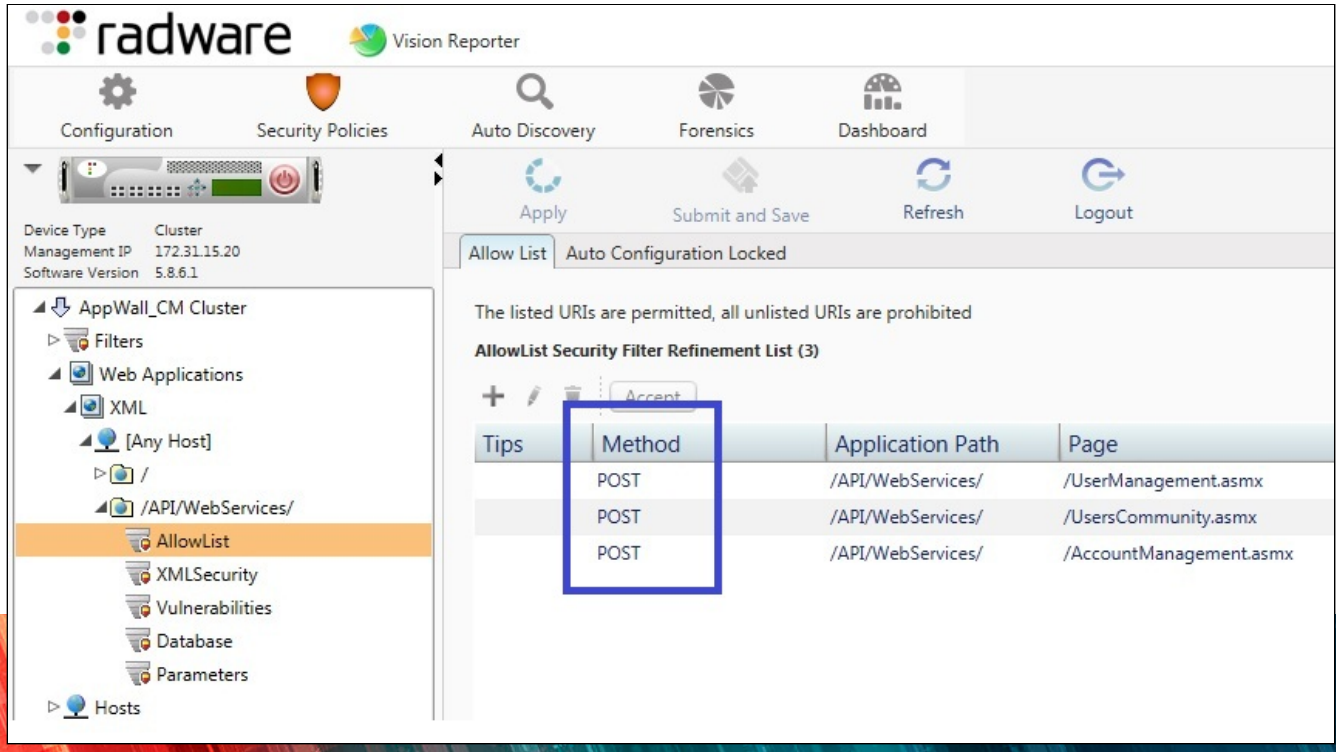
Parameter names are created using the full hierarchy of nested tags and attributes containing each value, and can enforce value type (for example, *integer*, *alpha-num*, and *regex*). Optionally, XML structure can also be enforced by selecting **Enforce Parameter Order**.



After setting and enabling AppWall access to the XML parameters you can utilize **Automatic Configuration** for the Vulnerabilities, Database and Parameters filters for XML requests as well.

Enforcing Non-browser Access (POST requests only)

To enforce non-browser access, use the *Allow List* filter and allow POST methods only.



Optionally, AppWall also enables you to allow, prohibit, or specify access to key/values of XML elements/attributes by defining your application path based on geo-location or specific IP groups, as detailed in the following article (link)

For XML filter to parse also attribute we need to enable “Parse Attributes as Parameters” check box.

For JSON/REST web application, refer the Securing JSON/REST with Radware’s AppWall Web Application firewall article.