F5 Rules for AWS WAF - Web Exploits OWASP Rules
Getting Started Guide
F5 Web Exploits OWASP for AWS WAF is found in the AWS Marketplace and helps your organization guard against attacks that are part of the OWASP Top 10 threats, including cross-site scripting, SQL injection, path traversal, and predictable resource. It offers integration with AWS WAF that makes it easy to deploy, in just a few clicks, without changes to your infrastructure. F5 Web Exploits OWASP for AWS WAF also offers rules that are written, managed, and updated regularly by F5 security experts, so you never need to worry about manually updating versions to protect against emerging vulnerabilities.
Subscribing to F5 Web Exploits OWASP for AWS WAF

Step 1  Locate F5 Web Exploits OWASP for AWS WAF in AWS Marketplace. Select the **Continue to Subscribe** button.

Step 2  Select the **Subscribe** button.

Steps 3 of 3
Step 3: Select the **Set Up Your Account** button.

Part 1 Complete

Part -2: Demonstration Guide for F5 Web Exploits OWASP for AWS WAF

Steps 1 - 2 of 19
Part - 2: Demonstration Guide for F5 Web Exploits OWASP for AWS WAF

**Step 1**
After subscribing to F5 Web Exploits OWASP for AWS WAF, you are taken to the AWS WAF and AWS Shield page. Select the Go to AWS WAF button.

![AWS WAF and AWS Shield](image)

**Step 2**
Select Configure Web ACL at the next page.

![Configure Web ACL](image)

Steps 3 - 4 of 19
Step 3  You will see general information about the ACL concepts on the next page. Select the Next button.

Step 4  Enter a name for your ACL.

Steps 5 - 6 of 19
**Step 5** Select the **Region** you want to apply the ACL to.

**Step 6** At the next page, you see an option to **create conditions**.

Steps 7 - 8 of 19
Step 7
For this demonstration, we will skip creating custom conditions and select the **Next** button.

Step 8
Select **AWS WAF** from the drop-down menu.

Steps 9 - 10 of 19
Step 9  
Select the **Add Rule to Web ACL** button.

Step 10  
For this demonstration, we will leave the default override selection of **No Override**.
**Step 11** Select *allow* under the default action and choose the **Review and Create** button.

**Step 12** Review the information you have selected and click the **Confirm and Create** button.

**Steps 13 - 14 of 19**
Step 13
You then see the ACL is created.

Step 14
You can edit the ACL.

Steps 15 - 16 of 19
Step 15  And add in Rule group exceptions by adding rule identifiers.

Step 16  The Request tab will show you data being ingested from AWS Kinesis Firehose that matches the rules.

Steps 17 - 18 of 19
Step 17  You can enable logging by selecting the **Logging** tab.
Note: You will need to have a Delivery Stream set up with Amazon Kinesis Data Firehose prior to setting up logging for the F5 Web Exploits OWASP Rules for AWS WAF. We do not cover this set up in this demonstration.

Step 18  Select your Firehose and choose the **Create** button.

Steps 19 of 19
Step 19  You will see a message that **logging is enabled**.

AWS WAF sends logs for this web ACL to the following Amazon Kinesis Data Firehose.

<table>
<thead>
<tr>
<th>Logging</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kinesis Data Firehose stream</td>
<td>aws-waf-logs-cybrary1234</td>
</tr>
<tr>
<td>Redacted Fields</td>
<td>None</td>
</tr>
</tbody>
</table>
Thank you.

For more information, visit https://amzn.to/32rWnHa