# Best Practices: Keeping Your Web Application Secure

https://campus.barracuda.com/doc/67174832/

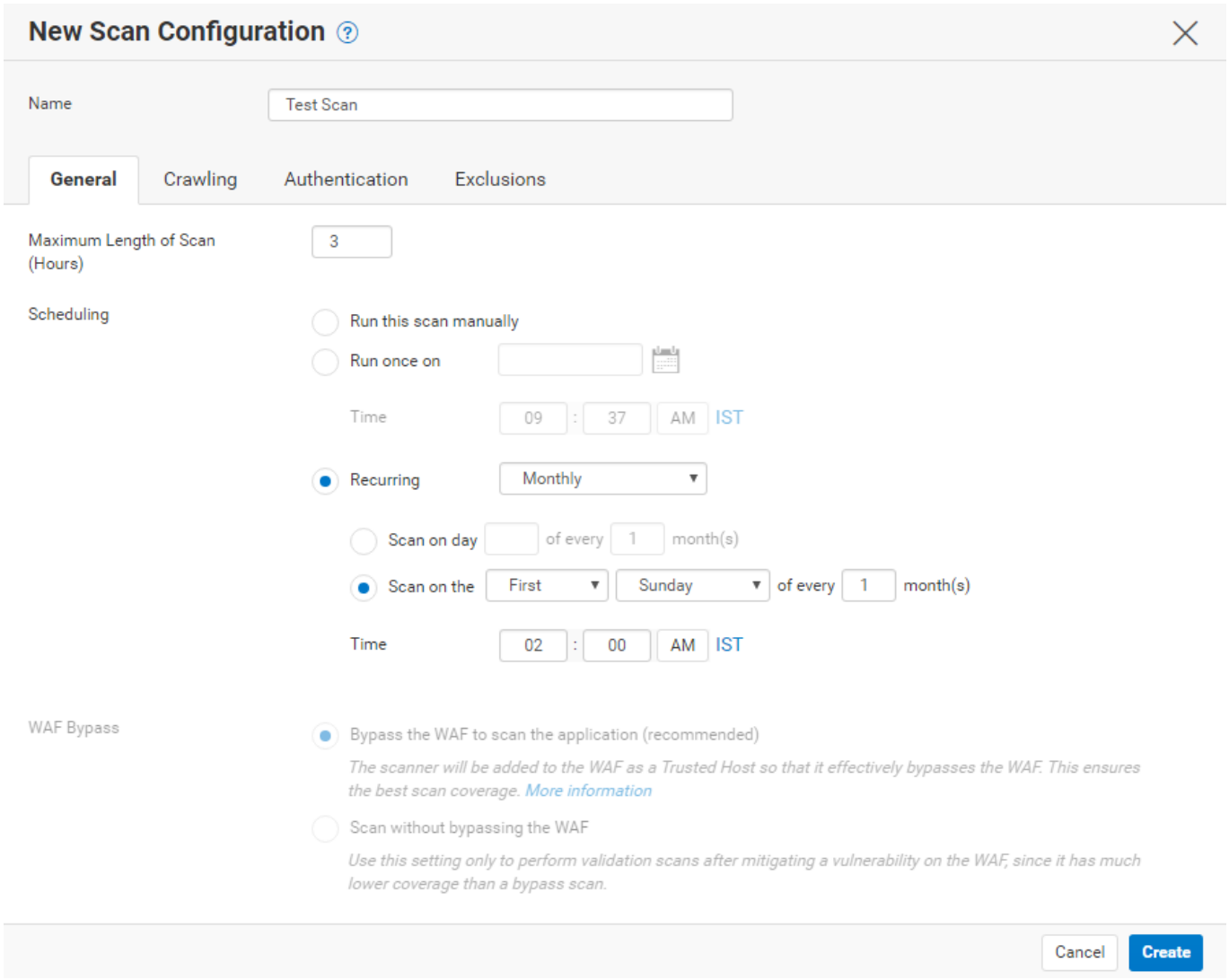
This article explains how to use the Barracuda Vulnerability Remediation Service to keep your application secure after deployment.

## Scan Applications Periodically

The web application threat landscape is constantly evolving. New threats are constantly being discovered. To keep your application secure, scan your applications periodically to search for new threats.

> Barracuda recommends scanning your applications monthly.

You can use the Barracuda Vulnerability Remediation Service to scan your applications on a set schedule. For example, in the **New Scan Configuration** dialog below, we have configured the scan to run on the first Sunday of each month at 2:00 AM.




For additional information, refer to Actions on Existing Scans and Web Applications.

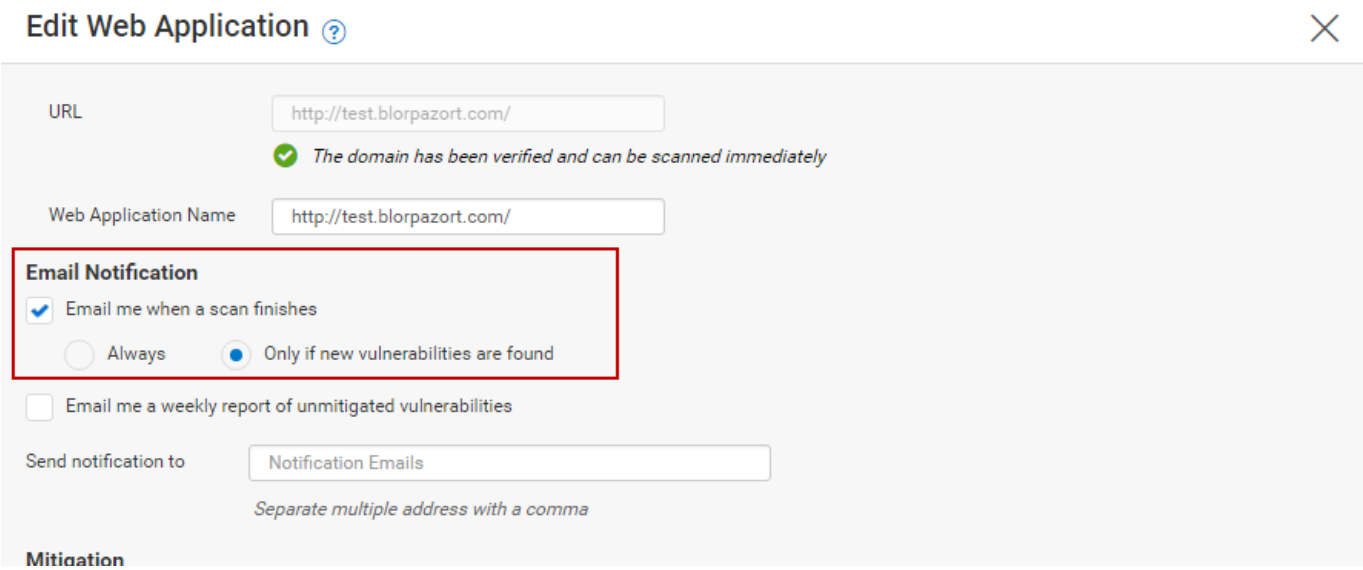
## Scan Applications After Updates

In addition to scheduled periodic scans, it is important to scan your applications whenever you deploy new versions or make changes to the configuration. To quickly run a scan, navigate to the **Scanner > Web Applications** page, locate the scan you want to run, and click **Run Now**.

### Enable Email Notifications

You can configure the Barracuda Vulnerability Remediation Service to send a notification to your email address whenever a new vulnerability is found during web application scans. This automatic email serves as an alert that the scanner found something new, so you do not have to check each

scan. When you add or edit a web application on the **Scanner > Web Applications** page, select that you want to be notified when a scan finishes only if new vulnerabilities are found, as shown here:




For additional information, refer to How to Create a New Web Application Scan.

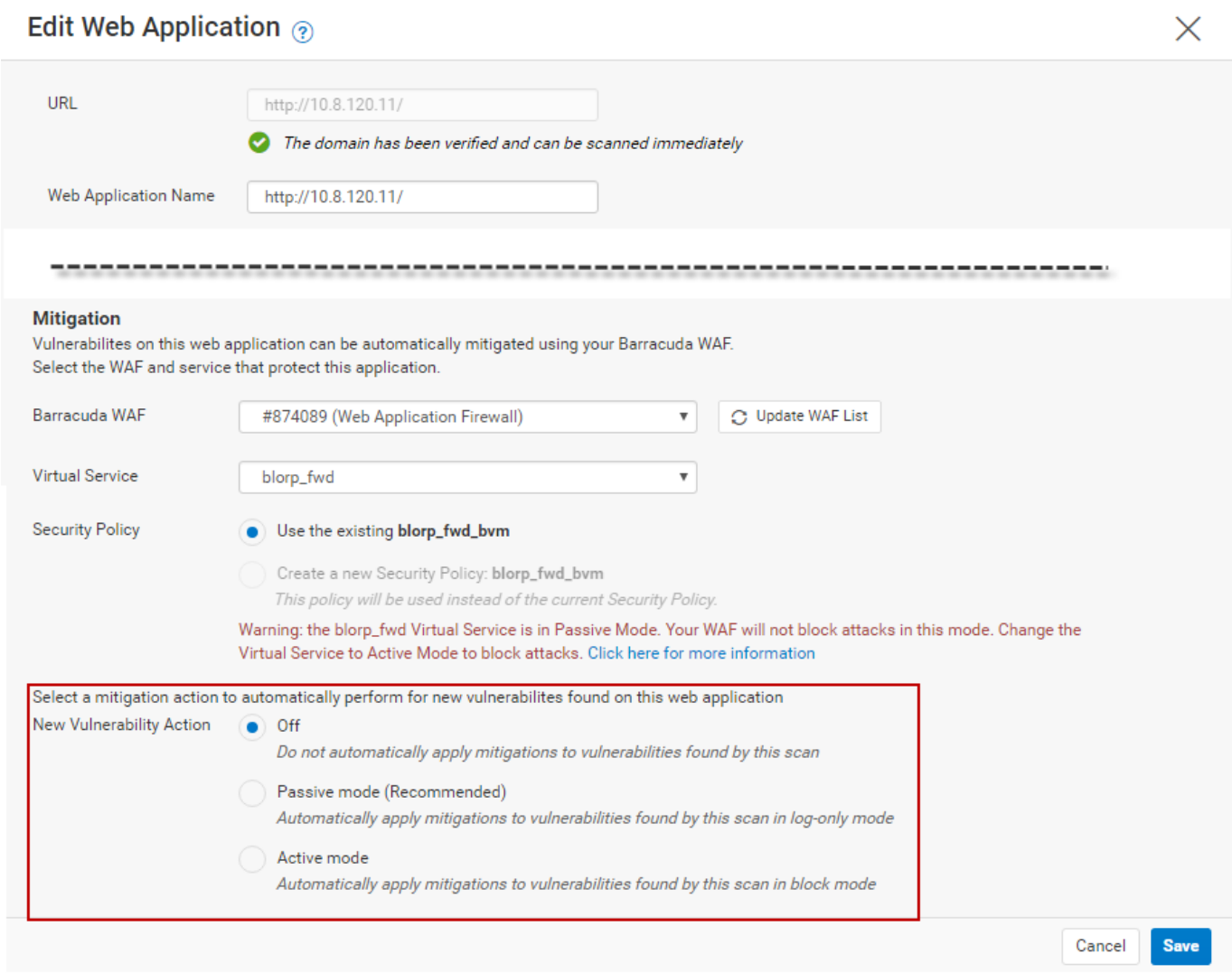
## Automatic Remediation Policy

The Barracuda Vulnerability Remediation Service works in tandem with the Barracuda Web Application Firewall to automatically take action when a new vulnerability is discovered during a scan of your web application.

You can configure three possible actions when you add or edit the web application from the **Scanner > Web Applications** page:

- **Off** – Vulnerability Remediation Service notifies you if you have enabled email notifications, but takes no further action.
- **Passive Mode** – (Recommended) Vulnerability Remediation Service automatically applies security policy changes to your Web Application Firewall in passive mode. This logs violations, but does not block them, so no behavior changes on your site.
- **Active Mode –** Vulnerability Remediation Service automatically applies security policy changes to your Web Application Firewall in active mode. This blocks violations immediately.

Barracuda strongly recommends that you select automatic remediation in **Passive Mode**. Passive Mode allows you to manually audit the policy changes and verify no false positives are logged. After verifying, you can deploy the fix in Active Mode.




For additional information, refer to How to Create a New Web Application Scan and Vulnerabilities.

## Recommended Workflow

Integrating the recommendations made earlier, Barracuda recommends the following workflow to keep your web applications secure:

1. When you configure your web applications:
    1. **Enable email notifications** to be sent when new vulnerabilities are discovered.
    2. Configure them to **scan automatically every month**.
    3. Select **Passive Mode** for your automatic remediation policy.
2. Run a **manual scan** every time you make significant changes to your application.
3. When a new vulnerability is discovered and you receive an email, wait 1-2 business days, then log in and look at the logs for that particular vulnerability, since it was fixed in Passive Mode. If

you do not see any false positives or other issues, **fix the vulnerability in Active Mode**.

## Figures