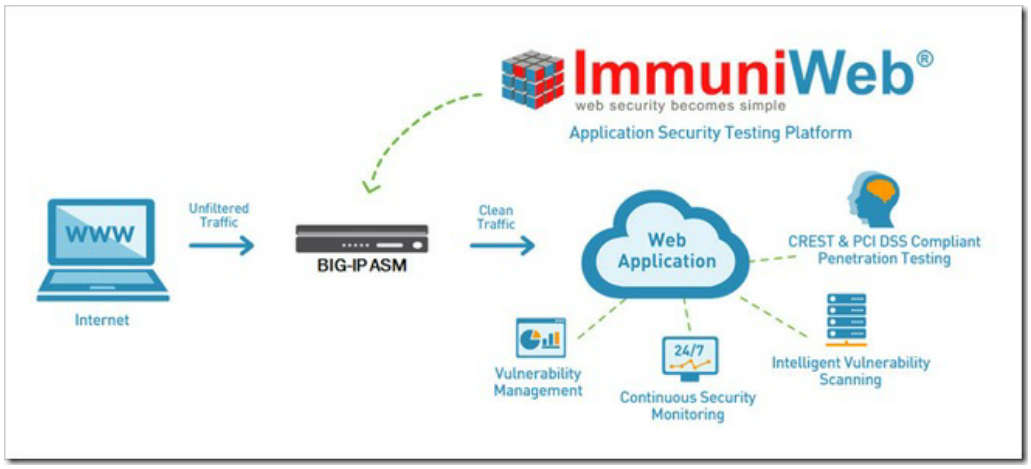
BIG-IP ASM Integration with ImmuniWeb

John Wagnon, 2017-24-04

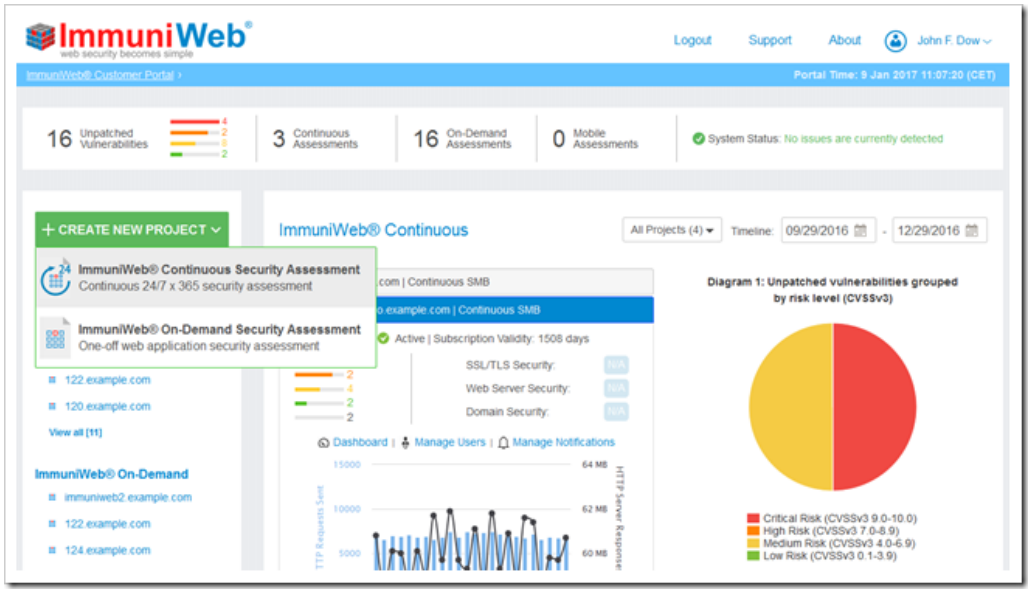
I've got good news and bad news and more good news. The good news is that you have amazing web applications that do great things for you and your customers every day. The bad news is that those web applications are under attack. The unfortunate reality of the world we live in is that web applications are getting attacked by someone, somewhere every day. It never stops…and it never will. While that's bad news, I mentioned that I have other good news as well. The other good news is that you have the opportunity to identify all the vulnerabilities in your web applications and then customize a Web Application Firewall security policy using the details of the vulnerability scan.

High-Tech Bridge is a world-class web security company that specializes in machine learning for web and mobile applications security testing. Their application security testing platform, ImmuniWeb, combines machine learning technology, intelligent automation, and human intelligence to detect the most sophisticated web application vulnerabilities. They offer continuous and on-demand application security testing. ImmuniWeb Continuous provides 24/7 vulnerability scanning and application change detection, manual validation of the results, and just-in-time penetration testing. ImmuniWeb On-Demand leverages the same technology as ImmuniWeb Continuous, but is designed for precise scope security testing during a specific timeframe. ImmuniWeb also offers a mobile security testing option that performs SAST and DAST testing of mobile applications for iOS and Android, encryption and privacy validation, as well as thorough security testing of the mobile backend, such as web services and APIs.

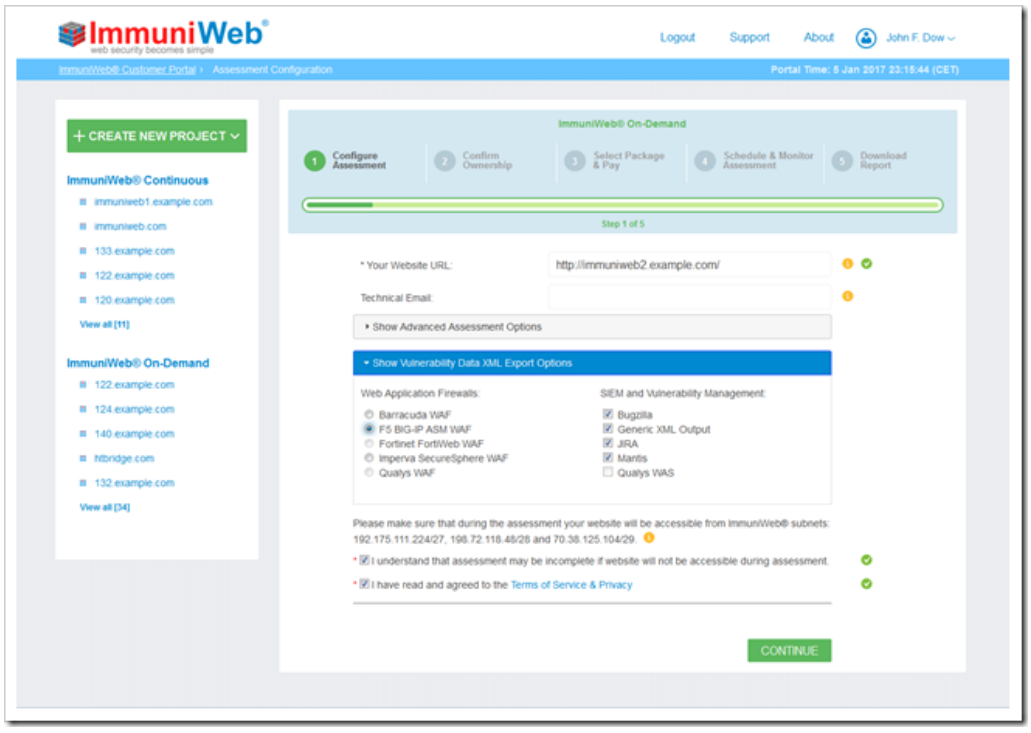
Regardless of which assessment option(s) you choose, you can import the results of the assessments directly into the BIG-IP Application Security Manager (ASM) and customize a security policy from the results. The following diagram shows a representation of the overall approach:



In order to import the results of the ImmuniWeb assessment into your BIG-IP ASM, you start in the ImmuniWeb portal by logging in and selecting "Create New Project" on the left side of the screen. You can either choose the "Continuous Security Assessment" or the "On-Demand Security Assessment" from the drop down menu. The following screenshot shows the details:

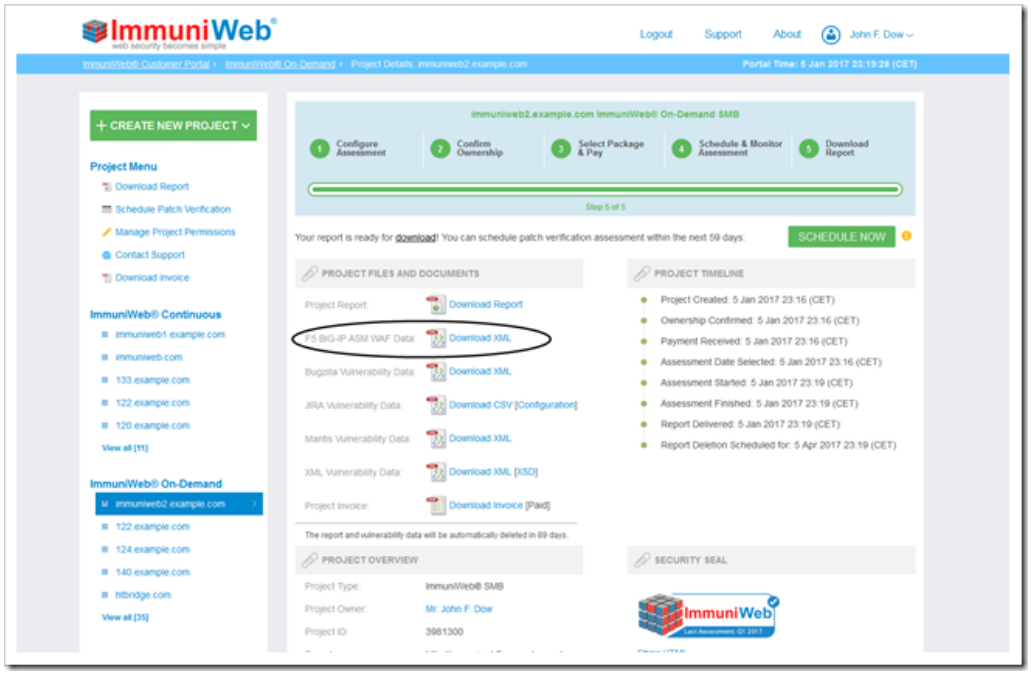


Once you select your option for security assessment, you will need to configure the assessment to let ImmuniWeb know you want the data to be exported in a format for the BIG-IP ASM. You will need to input the website URL for the applications you want to assess, and then you will need to select the “Show Vulnerability Data XML Export Options” and choose “F5 BIG-IP ASM WAF” as the Web Application Firewall option. You will have an opportunity to select several other SEIM and Vulnerability Management options as well. The following screenshot shows the details:



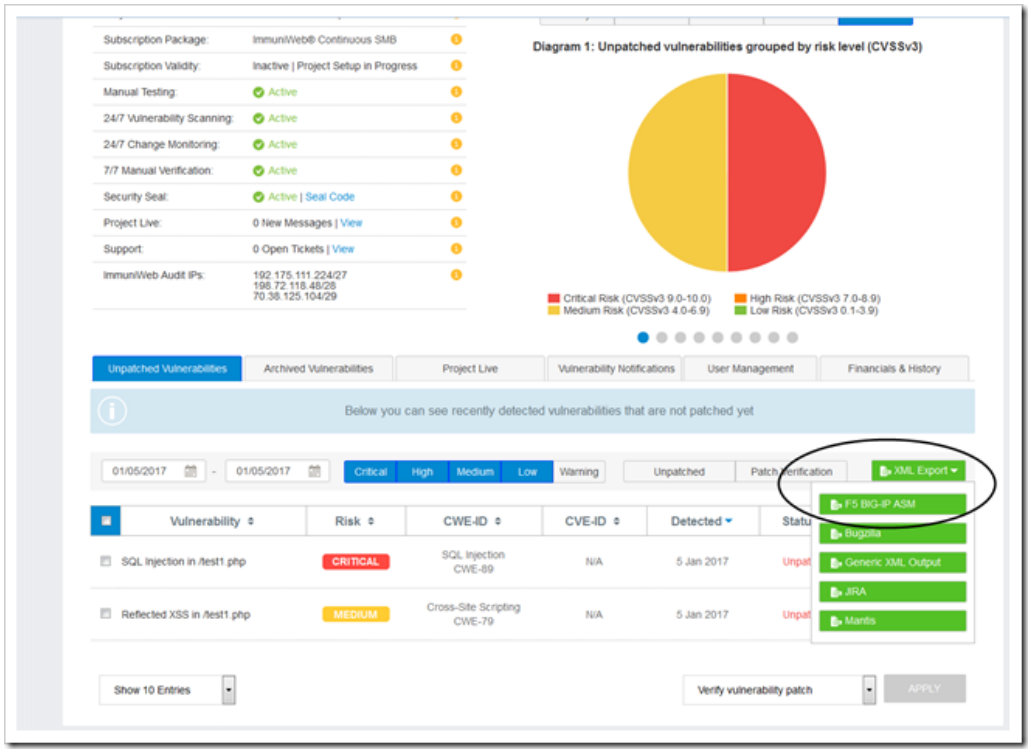
On-Demand Assessment

If you choose the On-Demand assessment option, ImmuniWeb will assess your applications and then create a list of findings for you to download and export into your BIG-IP ASM. Depending on the options you chose when configuring the assessment details, you will have more than one XML file available to download. Choose the “F5 BIG-IP ASM WAF Data” XML file as shown in the screenshot below.



Continuous Assessment

If you choose the Continuous Assessment option, ImmuniWeb will be continuously assessing your applications so you won't be waiting for the assessment to complete the way you would with the On-Demand option. For Continuous Assessment projects, you will be able to view unpatched or archived vulnerabilities any time ImmuniWeb detects there are vulnerabilities in your applications. The screenshot below shows the various tabs that you can use to view the detected vulnerabilities (unpatched and archived), and it also shows where you can download the exportable XML results file that you will use to load into your BIG-IP ASM.



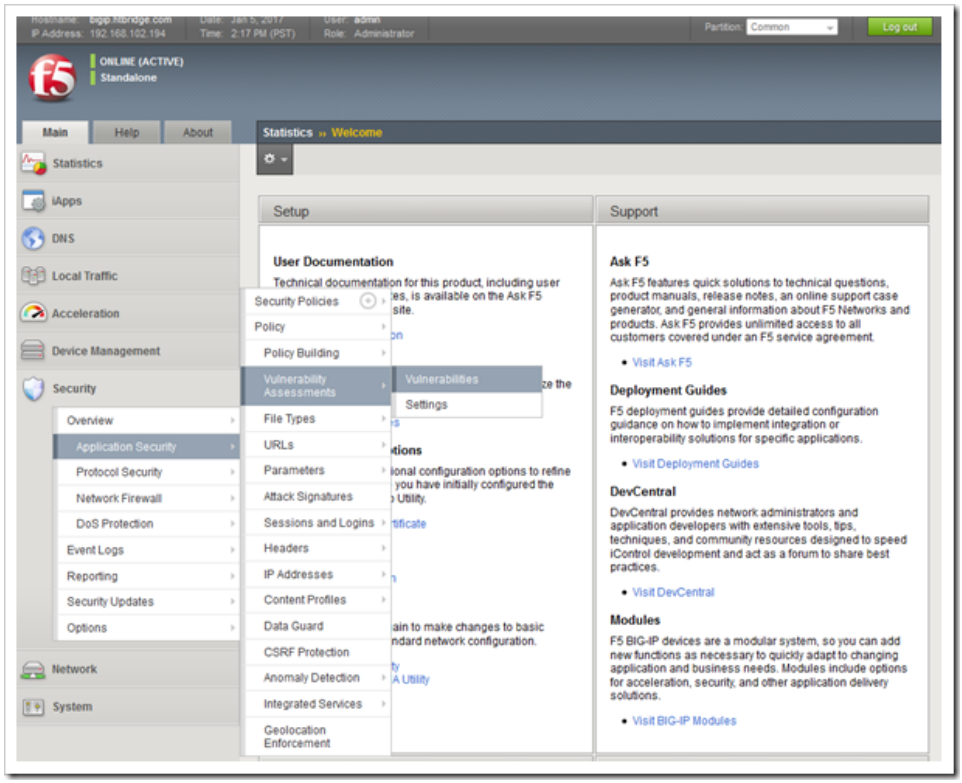
Importing to BIG-IP ASM

Regardless of which assessment you choose (On-Demand or Continuous), ultimately you will import the resulting XML file into your BIG-IP ASM so that it can protect your applications from the vulnerabilities found in the assessment. Really powerful and precise stuff!

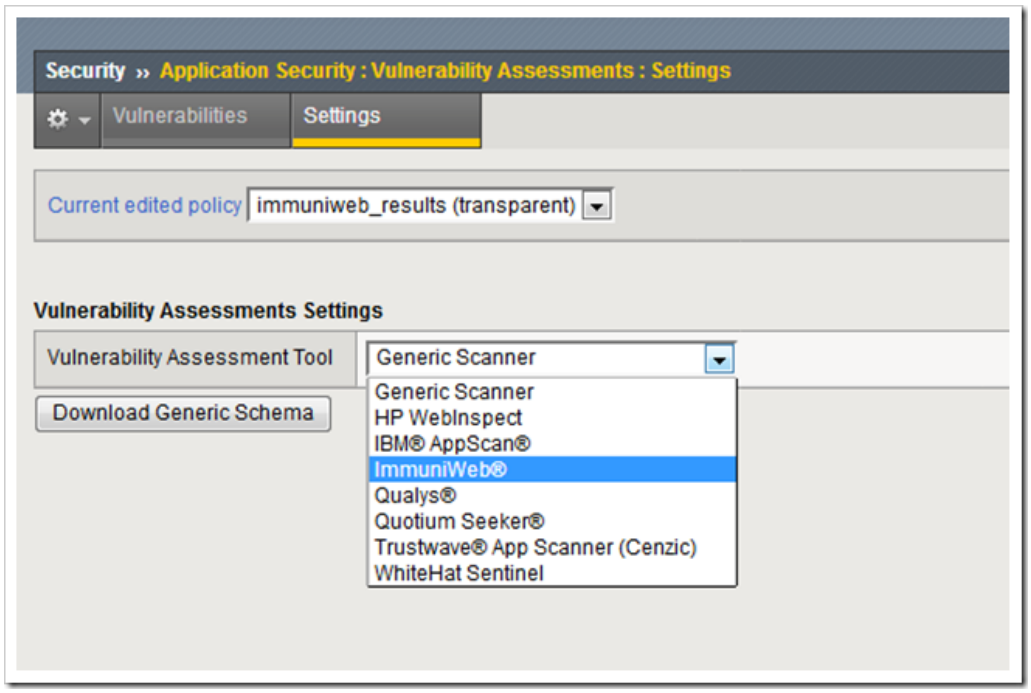
You simply download the XML file from the ImmuniWeb portal and save it in a secure location (local hard drive, network drive, etc). One of the reasons you need to save it in a secure location is that it holds the information for all current vulnerabilities in your web applications. That's not something you want any bad guys to get their hands on! Another good idea is to delete the file from the chosen storage location after you import it into the BIG-IP ASM. That way, there's less risk of someone finding it later and using the information against you. Anyway, after you download the XML file to a secure location, you are ready to login to your BIG-IP ASM and navigate to the page to import the file.

The BIG-IP ASM allows you to do a couple of things with respect to vulnerability data. First, you can import the data and associate it with an existing security policy. Second, you can tell the ASM exactly what scanner you used to get the vulnerability data. The ASM comes pre-loaded with the intelligence to handle several industry-leading scanners, and ImmuniWeb is (of course) one of those scanners. You can appreciate the fact that each industry scanner handles vulnerability scanning in slightly different ways, so it's very nice to be able to tell the ASM that you are importing results from a specific scanner versus another (in this case, ImmuniWeb). That way, the ASM can fully engage the data from the results because it knows exactly what format, style, etc the ImmuniWeb results will bring.

The way to configure these settings and import the XML file into the BIG-IP ASM is pretty simple and straightforward. Navigate to **Security > Application Security > Vulnerability Assessments**. You'll notice in the following screenshot that you have two options at this point: **Vulnerabilities** and **Settings**. The **Vulnerabilities** path will take you to a screen that shows you the exact vulnerability data that has been loaded into the BIG-IP ASM for the specific security policy you are viewing. The **Settings** path will allow you to select which scanner you will be importing results from…so as to allow the ASM to more specifically handle the vulnerability results.

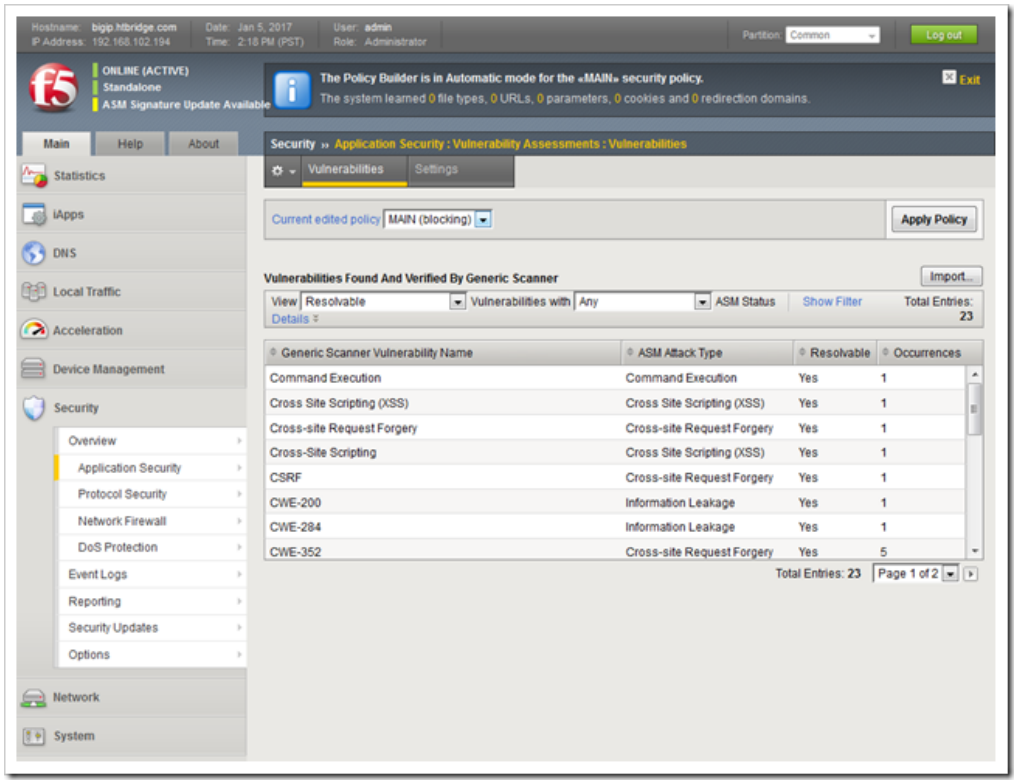


When you select **Settings**, you will see the following screen. Notice that it allows you to select the exact scanner from which you will be importing scan results. If your scanner is not included in the list, you should choose “Generic Scanner” as your option. Starting in version 13.1, ImmuniWeb will be one of the options in the list, so be on the lookout when you upgrade to version 13.1!! Also, notice that it allows you to select the current security policy that will be modified by these scan results.



When you select **Vulnerabilities**, you will see the following screen. Notice that, like in the Settings screen, you can view and select the security policy that will be modified by these scan results. Also, notice that any current vulnerabilities that have been loaded into the BIG-IP ASM for this specific security policy will be shown. The name of the vulnerability is listed, the ASM attack type associated with that vulnerability is listed, the resolvable status is listed, and the number of occurrences for that vulnerability is listed.

To import the new vulnerability data from the XML file you saved earlier, you click the “Import” button on the upper/right portion of the screen. A pop-up window will appear and you will be able to browse to the location where you saved the XML file. Simply browse to the file and then click the “Import” button. The ASM will import the new vulnerabilities and add them to the current list. Don’t forget to hit the “Apply Policy” button as well so that all these updates will be applied to the currently selected security policy.



Well, that's it! As you can see, ImmuniWeb and BIG-IP ASM can combine to provide a very powerful way of protecting your critical web applications by protecting the exact areas where your applications are vulnerable. This precision allows you to keep your security policy extremely efficient and doesn't add undue overhead and bulk.

Related Resources

- Learn more about the F5 and High-Tech Bridge technology alliance partnership
- Technology Webinar: ImmuniWeb Application Security Platform

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com