Qualys WAS 4.5 New Features

As a follow-up to our recent major release WAS 4.3, we have added a few new features, tweaks and clarifications in WAS 4.5 to allow further optimizations of scans as well as deliver some optimizations to Progressive Scanning in particular. Customers can also now receive more comprehensive CSV reporting on their scans. This allows customers to continue to deliver targeted web application security metrics to all the stakeholders while ensuring a successful web application security program meets the protection of all organizational demands.

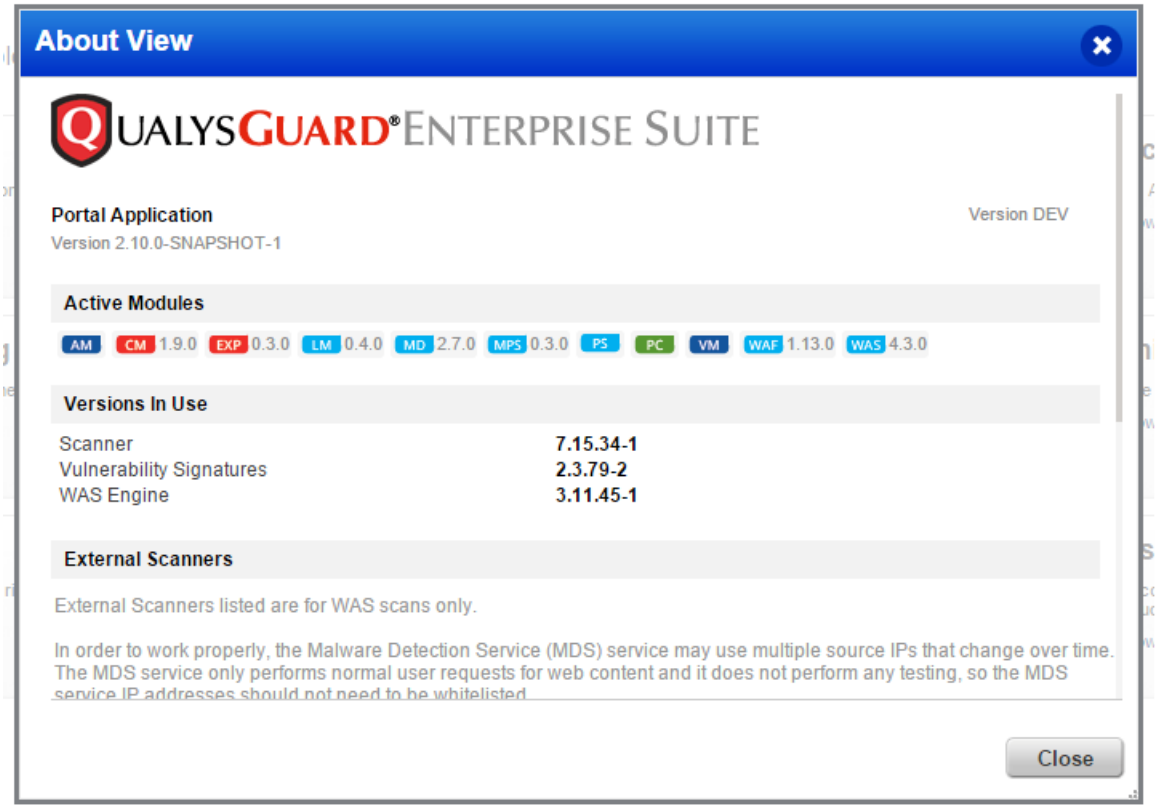
Feature highlights include:

- **Display WAS Engine Version in the WAS UI**
- **Condense and clarify CSV reporting**
- **Additional Progressive Scanning option for a single scan when in multi-scan mode**
- **Increased default scan error threshold values while still allowing customization**

Display WAS Engine Version in the WAS UI

Previously, we were only able to see the WAS scan engine version in the scan report. Users needed a way to easily display the WAS engine version in the UI.

Now, through the About panel available in the UI, users can access this information easily by clicking the About link in bottom-right corner or from the Help top-right menu that includes a new section called “Versions In Use” that displays the versions of Scanner, WAS engine, and Vulnerability signatures.



Condense and Clarify CSV Reporting

A WAS report when exported to CSV previously, had information truncated into two rows that made it difficult for proper reading and use. Manual adjustments were required to make information easily readable and readily usable. We have changed this!

Web Application CSV Reports

The report will now display each vulnerability and sensitive content using one single line, with following headers:

Vulnerability Header - one payload per vulnerability

```
"Web Application Name","VULNERABILITY","ID","QID","Url","Param","Form Entry Point","Access Path","Authentication","Status","Ignored","Ignore Reason","Ignore Date","Ignore User","Ignore Comments","First Time Detected","Last Time Detected","Last Time Tested","Times Detected","Payload #1","Request Method #1","Request URL #1","Request Headers #1","Response #1","Evidence #1"
```

Sensitive Content Header - one payload per sensitive content

```
"Web Application Name","SENSITIVE CONTENT","ID","QID","Content","Url","Param","Form
Entry Point","Access Path","Authentication","Status","Ignored","Ignore Reason","Ignore
Date","Ignore User","Ignore Comments","First Time Detected","Last Time Detected","Last
Time Tested","Times Detected","Payload #1","Request Method #1","Request URL
#1","Request Headers #1","Response #1","Evidence #1"
```

Or if a user selects to display all results in the Display step of report generation dialog:

Vulnerability Header - All payloads per vulnerability

```
"Web Application Name", "VULNERABILITY", "ID", "QID", "Url", "Param", "Form Entry
Point", "Access Path", "Authentication", "Status", "Ignored", "Ignore Reason", "Ignore
Date", "Ignore User", "Ignore Comments", "First Time Detected", "Last Time Detected",
"Last Time Tested", "Times Detected","Payload #1","Request Method #1","Request URL
#1","Request Headers #1","Response #1","Evidence #1","Payload #2","Request Method
#2","Request URL #2","Request Headers #2","Response #2","Evidence #2","Payload
#3","Request Method #3","Request URL #3","Request Headers #3","Response #3","Evidence
#3","Payload #4","Request Method #4","Request URL #4","Request Headers #4","Response
#4","Evidence #4","Payload #5","Request Method #5","Request URL #5","Request Headers
#5","Response #5","Evidence #5"
```

Sensitive Content Header - All payloads per sensitive content

```
"Web Application Name", "SENSITIVE CONTENT", "ID", "QID", "Content", "Url", "Param",
"Form Entry Point", "Access Path", "Authentication", "Status", "Ignored", "Ignore
Reason", "Ignore Date", "Ignore User", "Ignore Comments", "First Time Detected", "Last
Time Detected", "Last Time Tested", "Times Detected","Payload #1","Request Method
#1","Request URL #1","Request Headers #1","Response #1","Evidence #1","Payload
#2","Request Method #2","Request URL #2","Request Headers #2","Response #2","Evidence
#2","Payload #3","Request Method #3","Request URL #3","Request Headers #3","Response
#3","Evidence #3","Payload #4","Request Method #4","Request URL #4","Request Headers
#4","Response #4","Evidence #4","Payload #5","Request Method #5","Request URL
#5","Request Headers #5","Response #5","Evidence #5"
```

Scan CSV Reports

The report will now display each vulnerability and sensitive content using one single line, with following headers:

Vulnerability Header - one payload per vulnerability

```
"VULNERABILITY","ID","Detection ID","QID","Url","Param","Form Entry Point","Access
Path","Authentication","First Time Detected","Last Time Detected","Last Time
Tested","Times Detected","Payload #1","Request Method #1","Request URL #1","Request
Headers #1","Response #1","Evidence #1"
```

Sensitive Content Header - one payload per sensitive content

```
 "SENSITIVE_CONTENT", "ID", "Detection ID", "QID", "Content", "Url", "Param", "Form
Entry Point", "Access Path", "Authentication","First Time Detected","Last Time
Detected","Last Time Tested","Times Detected","Payload #1","Request Method
#1","Request URL #1","Request Headers #1","Response #1","Evidence #1"
```

Or if the user selected to display all results in the Display step of report generation dialog:

Vulnerability Header - All payloads per vulnerability

```
"VULNERABILITY","ID","Detection ID","QID","Url","Param","Form Entry Point","Access
Path","Authentication","First Time Detected","Last Time Detected","Last Time
Tested","Times Detected","Payload #1","Request Method #1","Request URL #1","Request
Headers #1","Response #1","Evidence #1","Payload #2","Request Method #2","Request URL
#2","Request Headers #2","Response #2","Evidence #2","Payload #3","Request Method
#3","Request URL #3","Request Headers #3","Response #3","Evidence #3","Payload
#4","Request Method #4","Request URL #4","Request Headers #4","Response #4","Evidence
#4","Payload #5","Request Method #5","Request URL #5","Request Headers #5","Response
#5","Evidence #5"
```

Sensitive Content Header - All payloads per sensitive content

```
"SENSITIVE_CONTENT","ID","Detection ID","QID","Content","Url","Param","Form Entry
Point","Access Path","Authentication","First Time Detected","Last Time Detected","Last
Time Tested","Times Detected","Payload #1","Request Method #1","Request URL
#1","Request Headers #1","Response #1","Evidence #1","Payload #2","Request Method
#2","Request URL #2","Request Headers #2","Response #2","Evidence #2","Payload
#3","Request Method #3","Request URL #3","Request Headers #3","Response #3","Evidence
#3","Payload #4","Request Method #4","Request URL #4","Request Headers #4","Response
#4","Evidence #4","Payload #5","Request Method #5","Request URL #5","Request Headers
#5","Response #5","Evidence #5"
```

Additional Progressive Scanning option for a single scan when in multi-scan mode

When using the multi-scan option previously, and selecting any single Web Application with the Progressive Scanning setting enabled from Web Application > Create Scan/Schedule, the Progressive Scanning option was not auto-enabled based on web application setting.

This behavior was previously supported only for an account where multi-scan is not enabled.

This behavior has now been corrected when a single web application is selected as a target and inherits the setting correctly as it should.

Increased default scan error threshold values while still allowing customization

Through thorough testing, our WAS team has found that the proper default scan error thresholds should be changed as this would be the best default setting for most common web applications. Customization of these settings still remains user configurable.

The default value for "timeout_errors_threshold" is 100.
For "unexpected_errors_threshold", the default value is 300.