Web Application Scan Results in XML

Web application scan results may be downloaded in XML format from the WAS scan history list. The web application scan results in XML format contains the same content as the web application scan results in other supported formats (PDF, HTML, MHT and CSV).

The scan results report includes summary and detailed results. The report summary in the header section provides summary information about the scan, including the user who requested the scan, the scan mode (discovery or vulnerability), the time when the scan was initiated, the target web application, and how long the scan took to complete. The detailed results include detected vulnerabilities (vulnerability scans only), sensitive content, and information gathered.

The service associates the "webapp_scan.dtd" with web application scan results XML output. The "webapp_scan.dtd" describes the markup declarations for the report elements (element types, attribute lists, entities, and notations). This DTD can be found at the API Server URL appropriate for your account location.

Account Location	API Server URL
US Platform	https://qualysapi.qualys.com/webapp_scan.dtd
EU Platform	https://qualysapi.qualys.eu/webapp_scan.dtd
@Customer Platform	https://qualysapi.<customerbaseURL>/webapp_scan.dtd

DTD for Web Application Scan Results

A recent "webapp_scan.dtd" is shown below.

```
<!-- QUALYS WEB APPLICATION SCAN DTD -->

<!ELEMENT WEB_APPLICATION_SCAN (ERROR | (HEADER, SUMMARY, RESULTS))>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

<!-- GENERIC HEADER -->
<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>

<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)>
<!ELEMENT ADDRESS (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT USER_INFO (NAME, USERNAME, ROLE)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT ROLE (#PCDATA)>

<!-- SUMMARY -->
<!ELEMENT SUMMARY (SCAN_SUMMARY, VULN_SUMMARY?,SENSITIVE_CONTENT_SUMMARY)>
<!ELEMENT SCAN_SUMMARY (SCAN_INFO*)>
<!ELEMENT SCAN_INFO (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>

<!ELEMENT VULN_SUMMARY (VULN_GROUP*)>
<!ELEMENT VULN_GROUP (TITLE, SEVERITY_5, SEVERITY_4, SEVERITY_3, SEVERITY_2,
                      SEVERITY_1, TOTAL)>
<!ELEMENT SEVERITY_1 (#PCDATA)>
```

```
<!ELEMENT SEVERITY_2 (#PCDATA)>
<!ELEMENT SEVERITY_3 (#PCDATA)>
<!ELEMENT SEVERITY_4 (#PCDATA)>
<!ELEMENT SEVERITY_5 (#PCDATA)>
<!ELEMENT TOTAL (#PCDATA)>

<!ELEMENT SENSITIVE_CONTENT_SUMMARY (SENSITIVE_CONTENT_GROUP*)>
<!ELEMENT SENSITIVE_CONTENT_GROUP (TITLE, TOTAL)>

<!-- RESULTS -->
<!ELEMENT RESULTS (VULN_LIST?, SENSITIVE_CONTENT_LIST?, INFO_LIST?)>

<!ELEMENT VULN_LIST (VULN*)>
<!ELEMENT VULN (GROUP, QID, TITLE, VULN_INSTANCES)>
<!ELEMENT VULN_INSTANCES (VULN_INSTANCE*)>
<!ELEMENT VULN_INSTANCE (HOST, PORT, URI, AUTHENTICATED?, FORM_ENTRY_POINT?, PARAMS,
                         FINDINGS)>
<!ELEMENT AUTHENTICATED (#PCDATA)>
<!ELEMENT FORM_ENTRY_POINT (#PCDATA)>
<!ELEMENT SENSITIVE_CONTENT_LIST (SENSITIVE_CONTENT*)>
<!ELEMENT SENSITIVE_CONTENT (GROUP, QID, TITLE, SENSITIVE_CONTENT_INSTANCES)>
<!ELEMENT SENSITIVE_CONTENT_INSTANCES (SENSITIVE_CONTENT_INSTANCE*)>
<!ELEMENT SENSITIVE_CONTENT_INSTANCE (HOST, PORT, URI, CONTENT?, FINDINGS)>

<!ELEMENT INFO_LIST (INFO*)>
<!ELEMENT INFO (QID, TITLE, RESULT)>

<!ELEMENT GROUP (#PCDATA)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT HOST (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT URI (#PCDATA)>
<!ELEMENT CONTENT (#PCDATA)>
<!ELEMENT PARAMS (#PCDATA)>
<!ELEMENT FINDINGS (FINDING*)>
<!ELEMENT FINDING (PAYLOAD?, RESULT)>
<!ELEMENT PAYLOAD (#PCDATA)>
<!ELEMENT RESULT (#PCDATA)>
```

XPaths for Web Application Scan Results

This section describes the XPaths for the web application scan results output (webapp_scan.dtd).

XPath	element specifications / notes
/WEB_APPLICATION_SCAN	(ERROR | (HEADER, SUMMARY, RESULTS))
/WEB_APPLICATION_SCAN/ERROR	(#PCDATA)
	An error description.
attribute: number	An error number (implied)
/WEB_APPLICATION_SCAN/HEADER	
	(NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO)
/WEB_APPLICATION_SCAN/HEADER/NAME	(#PCDATA)
	A scan title specified by the user who launched the scan.
/WEB_APPLICATION_SCAN/HEADER/GENERATION_DATETIME	(#PCDATA)
	The date and time when the web application scan was launched.
/WEB_APPLICATION_SCAN/HEADER/COMPANY_INFO	
	(NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)

XPath	element specifications / notes
/WEB_APPLICATION_SCAN/HEADER/COMPANY_INFO/NAME (#PCDATA)	
	The company name associated with the account used to launch the scan.
/WEB_APPLICATION_SCAN/HEADER/COMPANY_INFO/ADDRESS (#PCDATA)	
	The street address associated with the account used to launch the scan.
/WEB_APPLICATION_SCAN/HEADER/COMPANY_INFO/CITY (#PCDATA)	
	The city associated with the account used to launch the scan.
/WEB_APPLICATION_SCAN/HEADER/COMPANY_INFO/STATE (#PCDATA)	
	The state associated with the account used to launch the scan.
/WEB_APPLICATION_SCAN/HEADER/COMPANY_INFO/COUNTRY (#PCDATA)	
	The country associated with the account used to launch the scan.
/WEB_APPLICATION_SCAN/HEADER/COMPANY_INFO/ZIP_CODE (#PCDATA)	
	The zip code associated with the account used to launch the scan.
/WEB_APPLICATION_SCAN/HEADER/USER_INFO	
	(NAME, USERNAME, ROLE)
/WEB_APPLICATION_SCAN/HEADER/USER_INFO/NAME (#PCDATA)	
	The name of the user who launched the scan.
/WEB_APPLICATION_SCAN/HEADER/USER_INFO/USERNAME (#PCDATA)	
	The user login of the user who launched the scan.
/WEB_APPLICATION_SCAN/HEADER/USER_INFO/ROLE (#PCDATA)	
	The user role assigned to the user who launched the scan: Manager, Unit Manager, Scanner or Reader.
/WEB_APPLICATION_SCAN/SUMMARY	
	(SCAN_SUMMARY, VULN_SUMMARY, SENSITIVE_CONTENT_SUMMARY)
/WEB_APPLICATION_SCAN/SUMMARY/SCAN_SUMMARY (SCAN_INFO*)	
/WEB_APPLICATION_SCAN/SUMMARY/SCAN_SUMMARY/SCAN_INFO (KEY, VALUE)	
/WEB_APPLICATION_SCAN/SUMMARY/SCAN_SUMMARY/SCAN_INFO/KEY (#PCDATA)	
	A scan summary parameter name. The parameter “Status” identifies a scan status code. The parameter “Message” identifies a scan status message when applicable.
/WEB_APPLICATION_SCAN/SUMMARY/SCAN_SUMMARY/SCAN_INFO/VALUE (#PCDATA)	
	A scan summary parameter value. See “Web Application Scan Status” for information on WAS scan status codes and messages.
/WEB_APPLICATION_SCAN/SUMMARY/VULN_SUMMARY (VULN_GROUP*)	
/WEB_APPLICATION_SCAN/SUMMARY/VULN_SUMMARY/VULN_GROUP	
	(TITLE, SEVERITY_5, SEVERITY_4, SEVERITY_3, SEVERITY_2, SEVERITY_1, TOTAL)
/WEB_APPLICATION_SCAN/SUMMARY/VULN_SUMMARY/VULN_GROUP/TITLE (#PCDATA)	
	A vulnerability group title.
/WEB_APPLICATION_SCAN/SUMMARY/VULN_SUMMARY/VULN_GROUP/SEVERITY_1 (#PCDATA)	
	The number of severity 1 vulnerabilities found in a vulnerability group.
/WEB_APPLICATION_SCAN/SUMMARY/VULN_SUMMARY/VULN_GROUP/SEVERITY_2 (#PCDATA)	
	The number of severity 2 vulnerabilities found in a vulnerability group.
/WEB_APPLICATION_SCAN/SUMMARY/VULN_SUMMARY/VULN_GROUP/SEVERITY_3 (#PCDATA)	
	The number of severity 3 vulnerabilities found in a vulnerability group.
/WEB_APPLICATION_SCAN/SUMMARY/VULN_SUMMARY/VULN_GROUP/SEVERITY_4 (#PCDATA)	
	The number of severity 4 vulnerabilities found in a vulnerability group.
/WEB_APPLICATION_SCAN/SUMMARY/VULN_SUMMARY/VULN_GROUP/SEVERITY_5 (#PCDATA)	
	The number of severity 5 vulnerabilities found in a vulnerability group.
/WEB_APPLICATION_SCAN/SUMMARY/VULN_SUMMARY/VULN_GROUP/TOTAL (#PCDATA)	
	The total number of vulnerabilities found in a vulnerability group, including all severity levels.

XPath	element specifications / notes
/WEB_APPLICATION_SCAN/SUMMARY/SENSITIVE_CONTENT_SUMMARY	
	(SENSITIVE_CONTENT_GROUP*)
/WEB_APPLICATION_SCAN/SUMMARY/SENSITIVE_CONTENT_SUMMARY/SENSITIVE_CONTENT_GROUP	
	(TITLE, TOTAL)
/WEB_APPLICATION_SCAN/SUMMARY/SENSITIVE_CONTENT_SUMMARY/SENSITIVE_CONTENT_GROUP/TITLE	
	(#PCDATA)
	A sensitive content group title.
/WEB_APPLICATION_SCAN/SUMMARY/SENSITIVE_CONTENT_SUMMARY/SENSITIVE_CONTENT_GROUP/TOTAL	
	(#PCDATA)
	The total number of sensitive content detections found in a sensitive content group.
/WEB_APPLICATION_SCAN/RESULTS	
	(VULN_LIST?, SENSITIVE_CONTENT_LIST?, INFO_LIST?)
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST	(VULN*)
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN	(GROUP, QID, TITLE, VULN_INSTANCES)
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/GROUP	
	The title of a vulnerability group: XSS (for cross-site scripting), SQL (for SQL injection), PATH (for path-based vulnerability), or INFO (for other vulnerability information).
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/QID	(#PCDATA)
	A QID detected in a vulnerability group.
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/TITLE	(#PCDATA)
	A title for a vulnerability in a vulnerability group.
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/VULN_INSTANCES	(VULN_INSTANCE*)
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/VULN_INSTANCES/VULN_INSTANCE	
	(HOST, PORT, URI, AUTHENTICATED?, FORM_ENTRY_POINT?, PARAMS, FINDINGS)
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/VULN_INSTANCES/VULN_INSTANCE/HOST	(#PCDATA)
	A host on which a vulnerability instance was detected.
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/VULN_INSTANCES/VULN_INSTANCE/PORT	(#PCDATA)
	A port on which a vulnerability instance was detected.
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/VULN_INSTANCES/VULN_INSTANCE/URI	(#PCDATA)
	A URI on which a vulnerability instance was detected.
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/VULN_INSTANCES/VULN_INSTANCE/AUTHENTICATED	
	(#PCDATA)
	When the vulnerability was detected by an authenticated scan, the title of the authentication record used for the scan.
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/VULN_INSTANCES/VULN_INSTANCE/FORM_ENTRY_POINT	
	(#PCDATA)
	When the vulnerability was detected by exploiting a form, the URL where the form was discovered.
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/VULN_INSTANCES/VULN_INSTANCE/PARAMS	(#PCDATA)
	Parameters used by the scanning engine to detect a vulnerability instance.
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/VULN_INSTANCES/VULN_INSTANCE/FINDINGS	(FINDING*)
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/VULN_INSTANCES/VULN_INSTANCE/FINDINGS/FINDING	
	(PAYLOAD?, RESULT)
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/VULN_INSTANCES/VULN_INSTANCE/FINDINGS/FINDING/PAYLOAD	(#PCDATA)
	A payload for a vulnerability instance.
/WEB_APPLICATION_SCAN/RESULTS/VULN_LIST/VULN/VULN_INSTANCES/VULN_INSTANCE/FINDINGS/FINDING/RESULT	(#PCDATA)
	A scan test result for a vulnerability instance.

XPath	element specifications / notes
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST (SENSITIVE_CONTENT*)	
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT	(GROUP, QID, TITLE, SENSITIVE_CONTENT_INSTANCES)
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT/GROUP	The title of a sensitive content group: CUSTOM (for custom sensitive content detection), SSN-US (for social security number detection - United States only), and CC (for credit card number detection).
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT/QID (#PCDATA)	A QID detected in a sensitive content group.
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT/TITLE (#PCDATA)	A title for a sensitive content detection in the sensitive content group.
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT/SENSITIVE_CONTENT_INSTANCES	(SENSITIVE_CONTENT_INSTANCE*)
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT/SENSITIVE_CONTENT_INSTANCES /SENSITIVE_CONTENT_INSTANCE	(HOST, PORT, URI, CONTENT?, FINDINGS)
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT/SENSITIVE_CONTENT_INSTANCES /SENSITIVE_CONTENT_INSTANCE/HOST (#PCDATA)	A host on which a sensitive content instance was detected.
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT/SENSITIVE_CONTENT_INSTANCES /SENSITIVE_CONTENT_INSTANCE/PORT (#PCDATA)	A port on which a sensitive content instance was detected.
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT/SENSITIVE_CONTENT_INSTANCES /SENSITIVE_CONTENT_INSTANCE/URI (#PCDATA)	A URI on which a sensitive content instance was detected.
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT/SENSITIVE_CONTENT_INSTANCES /SENSITIVE_CONTENT_INSTANCE/CONTENT (#PCDATA)	A custom sensitive content value, as defined in the web application profile.
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT/SENSITIVE_CONTENT_INSTANCES /SENSITIVE_CONTENT_INSTANCE/FINDINGS (FINDING*)	
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT/SENSITIVE_CONTENT_INSTANCES /SENSITIVE_CONTENT_INSTANCE/FINDINGS/FINDING (PAYLOAD?, RESULT)	
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT/SENSITIVE_CONTENT_INSTANCES /SENSITIVE_CONTENT_INSTANCE/FINDINGS/FINDING/PAYLOAD (#PCDATA)	A payload for a sensitive content instance for a custom sensitive content detection. For other detections, no payload is returned by the scanning engine.
/WEB_APPLICATION_SCAN/RESULTS/SENSITIVE_CONTENT_LIST/SENSITIVE_CONTENT/SENSITIVE_CONTENT_INSTANCES /SENSITIVE_CONTENT_INSTANCE/FINDINGS/FINDING/RESULT (#PCDATA)	A scan test result for a sensitive content instance.
/WEB_APPLICATION_SCAN/RESULTS/INFO_LIST (INFO*)	
/WEB_APPLICATION_SCAN/RESULTS/INFO_LIST/INFO (QID, TITLE, RESULT)	
/WEB_APPLICATION_SCAN/RESULTS/INFO_LIST/INFO/QID (#PCDATA)	A QID for an information gathered.
/WEB_APPLICATION_SCAN/RESULTS/INFO_LIST/INFO/TITLE (#PCDATA)	A title for an information gathered.
/WEB_APPLICATION_SCAN/RESULTS/INFO_LIST/INFO/RESULT (#PCDATA)	Scan test results for an information gathered.

Web Application Scan Status

The scan status returned by the scanning engine for each web application scan includes a status code and additional status message if appropriate.

Status Code	Status Message	Description	Scan Results
Canceled	Scan has been canceled	The scan was canceled successfully.	Partial
Finished	<None>	The scan completed successfully. For a vulnerability scan: The full scan results include vulnerability detection data, if any. For a discovery scan: The full scan results include discovery detection data, if any.	Full
Finished	No host alive	The scanning engine did not find the host to be up and running.	Empty
Finished	Time limit exceeded	The scan duration exceeded the time limit.	Partial
Finished	No web application detected	The scanning engine did not detect the target web application.	Information Gathered only