Acunetix v12 Spec List

acunetix

Acunetix Web Vulnerability Scanner v12 features

Protocol Support

Transport Support

HTTP 1.1	Yes
HTTP 1.0	Yes
TLS1.1 or above	Yes
HTTP Keep-Alive	Yes
HTTP compression	Yes
HTTP user agent configuration	Yes
Detection of mobile friendly version of website	Yes

Proxy Support

HTTP 1.0 proxy	Yes
HTTP 1.1 proxy	Yes

Authentication

Full support for a variety of Authentication Schemes

Basic	Yes
Digest	Yes
HTTP negotiate	Yes
NTLM Authentication	Yes

HTML Form-based

Automated	Yes
Scripted	Yes
Non-Automated	Yes
Single sign on	Yes
Client SSL certificates	Yes
OAuth-based authentication§	Yes

Session Management

Comprehensive Session Management Capabilities

Start a new session	Yes
Session token refresh	Yes
Session expired	Yes
Reacquire session tokens	Yes

Acunetix v12 Spec List

acunetix

Session Management Token Type Support

HTTP cookies	Yes
HTTP parameters	Yes
HTTP URL path	Yes

Session Token Detection Configuration

Automatic session token detection	Yes
Manual session token configuration	Yes

Session Token Refresh Policy

Fixed session token value	Yes
Login process provided token value	Yes
Dynamic token value	Yes

Crawling

Web Crawler Configuration

Define a starting URL	Yes
Define additional hostnames *(or IPs)*	Yes
Manual Crawling	Yes

Define exclusions for

Specific hostnames *(or IPs)*	Yes
Specific URLs or URL patterns	Yes
Specific file extensions	Yes
Specific parameters	Yes
Limit redundant requests	Yes
Supporting concurrent sessions	Yes
Specify request delay	Yes
Define maximum crawl depth	Yes
Training the crawler	Yes

Web Crawler Functionality

Identify newly discovered hostnames	Yes
Support automated form submission	Yes
Detect error pages/custom 404 responses	Yes

Redirect Support

Follow HTTP redirects	Yes
Follow meta refresh redirects	Yes
Follow JavaScript redirects	Yes
Identify and accept cookies	Yes
Support AJAX applications	Yes

Acunetix v12 Spec List

acunetix

Crawl Preseeding using

Web Crawler Configuration

HTTP Archives (HAR) Files	Yes
Fiddler Exports (.saz)	Yes
Burp Saved Items and Burp State Files	Yes
Acunetix Sniffer Log (.slg)	Yes

Parsing

Web Content Types

HTML4	Yes
HTML5 - Advanced HTML5 Parsing via Acunetix DeepScan technology	-
that implements a rendering engine that is in widespread use	Yes
JavaScript	Yes
VBScript	Yes
XML	Yes
Plaintext	Yes
Java Frameworks *(e.g. Spring, Struts and JavaServer Faces)*	Yes
Flash	Yes - Limited
CSS	Yes
Web Services (WSDL)	Yes
Ruby on Rails	Yes
CRUD	Yes
REST APIs *(including support for WADL & Swagger/OpenAPI)*	Yes

Character Encoding Support

ISO-8859-1	Yes
UTF-7	Yes
UTF-8	Yes
UTF-16	Yes
Parser tolerance	Yes
Extraction of dynamic content	Yes

Testing

Testing Configuration

Host names or IPs	Yes
URL patterns	Yes
File extensions	Yes
Web Parameters	Yes
Cookies	Yes
JSON Parameters	Yes

Acunetix v12 Spec List

acunetix

XML Parameters	Yes
HTTP headers	Yes
XML	Yes

Brute Force Prevention

Lack of account lockout	Yes
Different login failure message	Yes
Insufficient authentication	Yes
Weak password recovery	Yes
Lack of SSL on login pages	Yes
Auto-complete enabled on pass parameters	Yes

Authorization

Credential/Session Prediction

Sequential session token	Yes
Non-Random session token	Yes

Insufficient Authorization

Forcefully browse to "logged-in" URL	Yes
Forcefully browse to high-privilege URL	Yes
HTTP verb tampering	Yes
Insufficient session expiration	Yes

Session Fixation

Failure to generate new session ID	Yes
Permissive session management	Yes

Session Weaknesses

Session token passed in URL	Yes
Session cookie not set with secure attribute	Yes
Session cookie not set with HTTPOnly	Yes
Session cookie not sufficiently random	Yes
Site does not force SSL connection	Yes
Site uses SSL but references insecure objects	Yes
Site supports weak SSL ciphers	Yes

Client-side Attacks

FContent spoofing	Yes
Test for DNS vulnerabilities	Yes

Cross-Site Scripting

Reflected cross-site scripting	Yes
Persistent cross-site scripting	Yes

Acunetix v12 Spec List

acunetix

DOM-based cross-site scripting	Yes
Cross-frame scripting	Yes
HTML injection	Yes
Cross-site request forgery	Yes
Clickjacking	Yes

Injection Attacks

Format string attack	Yes
LDAP injection	Yes
OS command injection	Yes
SQL injection	Yes
Blind SQL injection	Yes
SSL injection	Yes
XPath injection	Yes
HTTP header injection/response splitting	Yes
Remote file includes	Yes
Local file includes	Yes
Potential malicious file uploads	Yes

Information Disclosure

Directory indexing	Yes
XML External Entity (XXE)	Yes

Information Leakage

Sensitive information in code comments	Yes
Detailed application error messages	Yes
Backup files	Yes
Include file source code disclosure	Yes
Path traversal	Yes
Predictable resource location	Yes
Insecure HTTP methods enabled	Yes
WebDAV enabled	Yes
Default web server files	Yes
Testing and diagnostics pages	Yes
Front page extensions enabled	Yes
Internal IP address disclosure	#Yes
Support for Google Hacking Database (GHDB)	Yes
Server Side Request Forgery (SSRF)	Yes
WordPress Specific Vulnerabilities	Yes, over 1200 vulnerabilities
Port Scanning (Test for Open Ports)	Yes

Malware

Detection of links to sites hosting malware	
Detection of Trojan Shell Scripts	

Testing Customization

Modify existing tests	Deprecated
Create new tests	Deprecated

Acunetix v12 Spec List

acunetix

Advanced Scan Control Capabilities

Native Scan Scheduler that does not rely on OS Scheduler	-
e.g. Windows Scheduler or Unix Cron) with Dedicated Scheduler	-
Application and Optimized Task Queuing.	Yes
Pause and resume scans	Yes
View real-time status	Yes
Define re-usable scan configuration templates	Yes
Run multiple scans simultaneously	Yes
AcuSensor Agent deployment for enhanced vuln detection and	-
verification, down to the line of code in the web application	Yes - .NET, PHP & Java
Support multiple users	Yes
Regular updates for the application	Yes
Easy to compare the results (dedicated module to compare the	-
results is available)	Yes

Command & Control

Scan Control Capabilities

Schedule scans	Yes
Pause and resume scans	Yes
Vew real-time status	Yes
Define re-usable scan configuration templates	Yes
Run multiple scans simultaneously	Yes
Support multiple users	Yes
Remote/distributed scanning	Yes

Remote/distributed scanning

Command line interface	Yes
Web-based interface	Yes

Extensibility & Interoperability

Scan API	Yes
Integrates with bug-tracking systems	Yes

Technical Detail Report

Full request and response data	Yes
List of all hosts and URLs	Yes
Delta Report	Yes

Compliance Report

OWASP Top 10	Yes
WASC Threat Classification	Yes
SANS Top 20	Yes
Sarbanes-Oxley (SOX)	Yes
PCI DSS	Yes
HIPAA	Yes
NIST 800-53	Yes

Acunetix v12 Spec List

acunetix

Advisories for Each Unique Vulnerability Type

Vulnerability description	Yes
CVE or CWE ID	Yes
Severity level	Yes
CVSS version 2 Score	Yes
Remediation guidance	Yes
Remediation code example(s)	Yes

Report Customization

Add custom notes	Yes
Mark vulnerabilities as false positives	Yes

Adjust the Risk Level

CVSS score	Yes
Severity level or other risk quantifiers	Yes
Report vulns according to content location	Yes

Report Format

PDF	Yes
HTML	Yes
XML	Yes

Manual Testing Tools for the Verification of Results

HTTP Packet Sniffer	Yes
HTTP Request Editor	Yes
HTTP Fuzzing Tool	Yes
Blind SQL Injection Exploit Tester	Yes
BruteForce / Authentication Tester	Yes
Text Encoding Tool	Yes
Dedicated tool to scan the sub-domains (Sub-domain Scanner)	Yes
Target Finder, allowing the scanner to easily find web servers on the network	- Yes

Custom Criteria

Use this section for custom criteria you may have for your organization

Integrates with Integrating system (Jenkins)	Yes
JSON injection	Yes
XML injection	Yes
Deploy in enterprise internal network	Yes
Distributed deployment.	Yes
Local technical support service	Yes
Scan speed	Yes
Support for recorded HTTP request/response message input for Fuzz source	- Yes
Swagger yaml file for Fuzz source (optional)	Yes