Which Vulnerabilities does Acunetix WVS Check for?

Acunetix WVS automatically checks for the following vulnerabilities among others:

- Version Check
  - Vulnerable Web Servers
  - Vulnerable Web Server Technologies – such as "PHP 4.3.0 file disclosure and possible code execution.
- Web Server Configuration Checks
  - Checks for Web Servers Problems – Determines if dangerous HTTP methods are enabled on the web server (e.g. PUT, TRACE, DELETE)
  - Verify Web Server Technologies

- Parameter Manipulation

  - Cross-Site Scripting (XSS)
  - SQL Injection
  - Code Execution
  - Directory Traversal
  - File Inclusion
  - Script Source Code Disclosure
  - CRLF Injection
  - Cross Frame Scripting (XFS)
  - PHP Code Injection
  - XPath Injection
  - Path Disclosure (Unix and Windows)
  - LDAP Injection
  - Cookie Manipulation
  - Arbitrary File creation (AcuSensor Technology)
  - Arbitrary File deletion (AcuSensor Technology)
  - Email Injection (AcuSensor Technology)
  - File Tampering (AcuSensor Technology)
  - URL redirection
  - Remote XSL inclusion
  - DOM XSS

- MultiRequest Parameter Manipulation

  - Blind SQL/XPath Injection

- File Checks

  - Checks for Backup Files or Directories - Looks for common files (such as logs, application traces, CVS web repositories)
  - Cross Site Scripting in URI

    - Checks for Script Errors

- File Uploads
    - Unrestricted File uploads Checks

- Directory Checks
    - Looks for Common Files (such as logs, traces, CVS)
    - Discover Sensitive Files/Directories
    - Discovers Directories with Weak Permissions
    - Cross Site Scripting in Path and PHPSESSID Session Fixation.
    - Web Applications
    - HTTP Verb Tampering

- Text Search
    - Directory Listings
    - Source Code Disclosure
    - Check for Common Files
    - Check for Email Addresses
    - Microsoft Office Possible Sensitive Information
    - Local Path Disclosure
    - Error Messages
    - Trojan shell scripts (such as popular PHP shell scripts like r57shell, c99shell etc)

- Weak Passwords
    - Weak HTTP Passwords

- GHDB Google Hacking Database
    - Over 1200 GHDB Search Entries in the Database

- Port Scanner and Network Alerts
    - Port scans the web server and obtains a list of open ports with banners
    - Performs complex network level vulnerability checks on open ports such as:
        - DNS Server vulnerabilities (Open zone transfer, Open recursion, cache poisoning)
        - FTP server checks (list of writable FTP directories, weak FTP passwords, anonymous access allowed)
        - Security and configuration checks for badly configured proxy servers
        - Checks for weak SNMP community strings and weak SSL cyphers
        - and many other network level vulnerability checks!

- Other web vulnerability checks
    - Cross-site request forgery (CSRF)

- Other vulnerability tests may also be peformed using the advanced penertation testing tools provided, including:

    - Input Validation (also performed automatically)
    - Authentication attacks (also performed automatically)
    - Buffer overflows
    - Blind SQL injection (also performed automatically)
    - Sub domain scanning