

1. Overview of N-Stalker Scan Profiles

1.1. Development & QA Scan Profile

This profile is recommended to check for development & QA issues on Web Applications. It is the recommended analysis for the first step of Web Application Secure Development Life-cycle.

Here are the security checks enabled in this profile (see section 1.3.3 for more details):

- **Custom Design Errors**
- **Confidentiality Exposure Checks**
- **Cookie Exposure Checks**
- **File & Directory Exposure Checks**

1.2. Infrastructure & Deploy Scan Profile

This profile is recommended to check for Deployment issues of Web Applications. It is the recommended analysis for the second step of Web Application Secure Development Life-cycle.

When finishing the deployment of Web Applications, this policy profile will assist you to ensure Web Server infrastructure is secured and cannot expose applications, even when those are already tested for security flaws.

Here are the security checks enabled in this profile (see section 1.3.3 for more details):

- **Web Server Exposure**
- **Web Signature Attacks (35,000 attack database)**
- **File & Directory Exposure Checks**

1.3. Audit & Pen-test Scan Profile

This profile is recommended to check for multiple vulnerabilities on Web Applications, ranging for development to infrastructure issues. It is the recommended analysis for the third step of Web Application Secure Development Life-cycle.

This is the most complete policy profile and should assist you on creating policies for periodic security tests against your Web Application.

All security checks are enabled in this profile (see section 1.3.3 for a complete list):

- **Custom Design Errors**
- **Web Server Exposure**
- **Web Signature Attacks (35,000 attack database)**
- **Confidentiality Exposure Checks**
- **Cookie Exposure Checks**
- **File & Directory Exposure Checks**

Note: These profiles may not be available in your N-Stalker Web Application Security Scanner Edition. All profiles are available in Enterprise Edition. Please contact N-Stalker Support Team for more information.