Dynamic Application Security Testing (DAST)

AUBURN UNIVERSITY

CPSC 4970 Applied Cyber Security

DAST Testing Characteristics

- Programming Language Agnostic
- Fewer False Positives since it looks for known vulnerabilities
- Typically slower at processing
  - Brute force attacks
  - Denial of Service
- Test Execution
  - Should be performed against non-production environments to avoid negatively impacting production environments.
  - New production environments should be tested before going live.
  - DAST can be performed on feature or bug fixing branches to determine if new code introduced a vulnerability. SAST tools perform this automatically.
  - Over time with a complete security testing process (manual, SAST, secure design, etc.), DAST scanning can be considered to be done less frequently.

Penetration vs. Vulnerability Testing

Factor	Vulnerability	Penetration
Description	Scans for and **identifies** potential known vulnerabilities.	Searches for weakness and potential exploits in a system
Automation	Automated	Automated and Manual
Depth vs Breadth	Breadth – can cover large number of known vulnerabilities	Depth – attempts to find weakness in systems to exploit
Frequency	As needed – built into software build pipeline. Can be less frequent after source code maturity	Quarterly, Semi-annual, Annaully
Attack Surface	Application Level	Network, Server, Application Level
Human Involvement	Little knowledge needed since built into automation tools. Internal staff to use tool	Skilled and needed to perform analysis of system for potential weakness – “Ethical Hacker” or 3rd Party
Cost	Low-Med (Tools and Administration)	High – Requires analysis and 3rd Party
Other	Authenticated User Testing	Only non-authenticated
Reporting	A comprehensive or delta list of vulnerabilities, which may include false positives.	Lists vulnerabilities that were successfully exploited and require resolution

DAST Vulnerability Scan Types

- Passive Scan
  - Execute the baseline scan and don’t actively attack the application.

- Active Scan
  - Execute an active scan to attack your application and provide a more comprehensive security report.
  - Non-Authenticated Scan
    - If scripted or configured can test for unprotected resources that should be.
  - Authenticated Scan.
    - Provides DAST tools with credentials to login enabling it to scan protected resources.
    - Some tools can be scripted to test for resources that require different types of permission levels to validate RBAC or ACLs.

Application Stand Alone vs System testing

- Modern apps are trending toward a collection of services vs. single deployed stack
  - Microservice architectures
  - Cloud services

- Application Stand along
  - Test just the piece / component of the overall ‘product’
  - Easier to conduct
  - Easy to connect issues to the proper team

- System Testing
  - Comprehensive picture of the security posture at a product level
  - Harder to connect issues to the proper team
  - Harder to line up versions of the various services
    - Does what you can test match what you want to test?

Where To Test – Prod vs. Non-Prod

- How closely does production environment (“Prod”) match the testing environment?
  - How confident are you this will continue?

- What is the testing scope?
  - Public exposure to unauthenticated attacks?

- Ideal situation
  - Same automation code that builds & launches Prod is used for PreProd
  - Includes all network security devices and tools
  - Allows for completely safe destructive testing
  - PreProd can be removed after testing

AUBURN UNIVERSITY