Applicatie Security Testen

Testen van software (AST) kan manueel gebeuren, bijvoorbeeld door een peer review, en geautomatiseerd door security test tools. Deze tools zijn weer te verdelen in 2 categorieën met elk hun eigen aanpak; Black-box en White-box.

Black box

- Bij black-box testen wordt een **live** applicatie aan een onderzoek naar kwetsbaarheden onderworpen, zonder kennis van de code.
- Ook wel **DAST**, Dynamic Application Security Testing genoemd.
- Proberen om misbruik te maken van een applicatie, net als een hacker.
- Onderzoeken van buiten naar binnen.

- Snel inzicht en makkelijk toe te passen, vergt weinig tot geen aanpassingen van de organisatie.
- Onderzoekt de **runtime** omgeving van de applicatie (http/https verkeer).
- Test ook de interfaces van derden.
- Er is geen toegang tot de code nodig.
- Vind kwetsbaarheden door **misbruik** te maken **van functionaliteit**.
- Een korte leercurve.

- Een DAST oplossing kan niet precies aangeven waar in de code de kwetsbaarheid zit.
- Zegt weinig over de kwaliteit van programmeren, of in hoeverre het programmeren voldoet aan algemene standaarden of richtlijnen.

Black-box only

- Environment configuration issues
- Patch level issues
- Runtime privileges issues
- Authentication issues
- Protocol parser issues
- Session management issues
- Issues in 3rd party web components
- Cross-site request forgery
- Malware analysis

White box

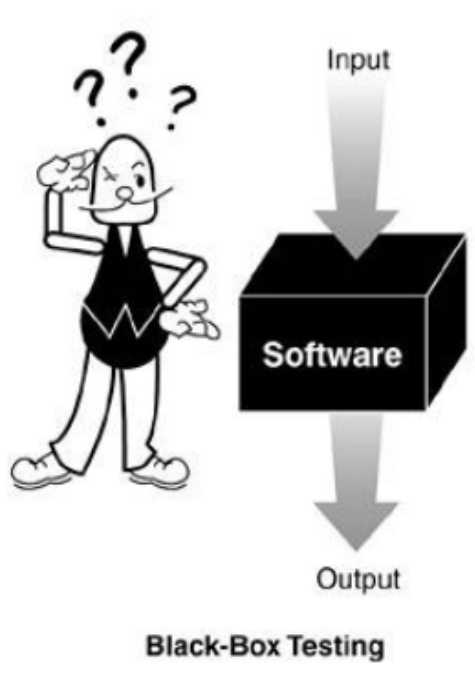
- Static Application Security Testing is het proces waarbij broncode, binaries of byte code van een applicatie aan een onderzoek naar kwetsbaarheden wordt onderworpen.
- Ook wel **SAST**, Static Application Security Testing genoemd.
- Wordt uitgevoerd tijdens het bouwen van de applicatie, onderdeel van de staande **SDLC**.
- Onderzoekt de kwaliteit van de code.
- Onderzoek van binnen naar buiten.

- Geeft precies aan waar in de code het mankement zit.
- Voordat de applicatie in productie gaat is de kwetsbaarheid ontdekt.
- Vroeg in de **ontwikkelfase** herstellen van issues bespaart enorm veel geld

- Vind geen kwetsbaarheden buiten de code om of in interfaces van derden.
- Vind geen kwetsbaarheden in de infrastructuur.
- Vergt aanpassingen van **development** in organisatie, processen en mensen.

White box only

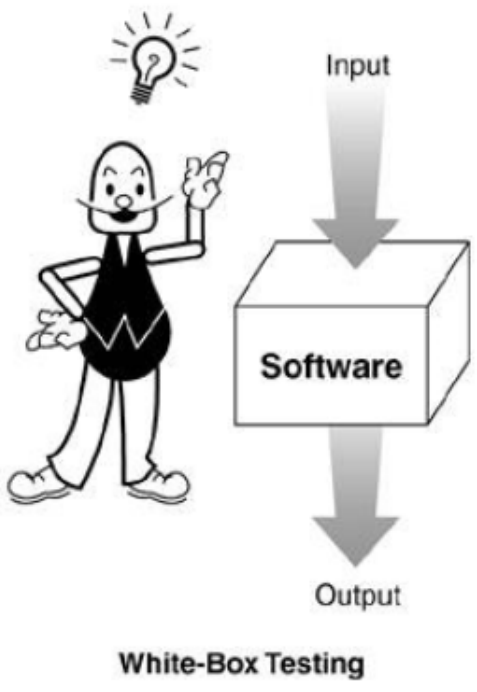
- Null pointer dereference
- Threading issues
- Code quality issues
- Issues in dead code
- Insecure crypto functions
- Issues in back-end application code
- Complex injection issues
- Issues in non-web applications



Black-Box Testing

Black & White box

- SQL Injection
- Cross Site Scripting
- HTTP Response Splitting
- OS Commanding
- LDAP Injection
- XPath Injection
- Path Traversal
- Buffer Overflows
- Format String Issues



White-Box Testing

FACT

IAST

SAST en DAST samen geeft het beste resultaat. De beste oplossing is te vinden bij leveranciers die beide technieken optimaal integreren met **IAST** oftewel Integrated Application Security Testing.

Mythe: SAST levert minder false positives op.

Noch SAST, noch DAST resulteert in minder false positives. Alleen een menselijk oordeel kan bepalen of een kwetsbaarheid een false positive is. Elke organisatie zal haar eigen unieke **risicoanalyse** moeten uitvoeren.

Mythe: manueel testen levert betere resultaten op dan geautomatiseerd.

De kwaliteit van manueel testen is voornamelijk afhankelijk van de menselijke factor. De kwaliteit van geautomatiseerd testen is afhankelijk van het ontwikkelteam wat er achter zit. Wederom beide aanpakken gecombineerd levert het beste resultaat op.

Contact

+31 (0)6 532 33 269
info@sebyde.nl
www.sebyde.nl/contact

© 2014 Sebyde bv