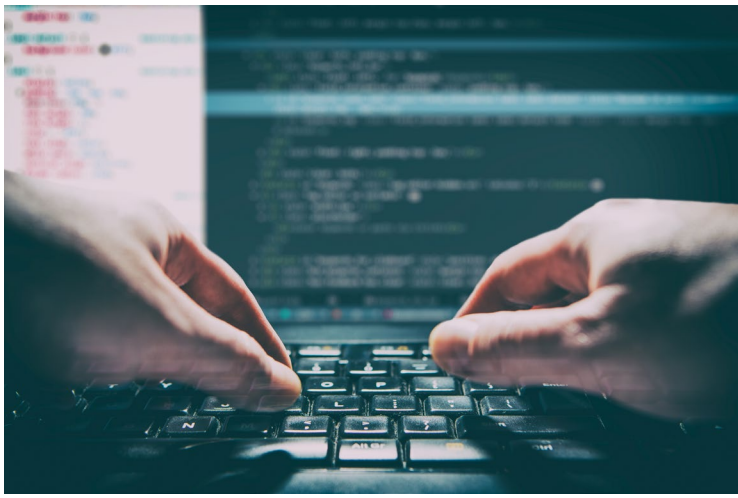
Contrast SECURITY

WHITE PAPER

Révolutionner le DAST avec l'IAST : une nouvelle ère pour la sécurité des applications

Introduction

Le test dynamique de sécurité des applications (DAST) constitue depuis des dizaines d'années une technique clé pour la sécurité des applications (AppSec). C'est également l'une des principales méthodes pour découvrir et traiter les vulnérabilités dans les applications logicielles. Mais malgré son adoption généralisée, cette approche a ses limites. Les outils DAST existants envoient des attaques à partir d'un point externe et tentent ensuite de déterminer si ces attaques ont réussi en se basant sur les réponses HTTP. Bien qu'efficace dans certaines circonstances, cette méthode n'offre pas d'informations détaillées sur ce qui se passe à l'intérieur du code et passe donc souvent à côté de véritables vulnérabilités.



Le besoin crucial de visibilité interne et d'analyses sur le comportement du code témoigne d'une problématique urgente au sein du secteur de l'AppSec : Pour garantir une protection fiable, nous avons besoin d'un outil qui ne se contente pas d'opérer en périphérie, mais comprend également les mécanismes internes d'une application. C'est le seul moyen de rassembler les données nécessaires pour identifier avec précision les véritables vulnérabilités, sans exception, et sans faux positifs.

Contexte : comprendre le DAST

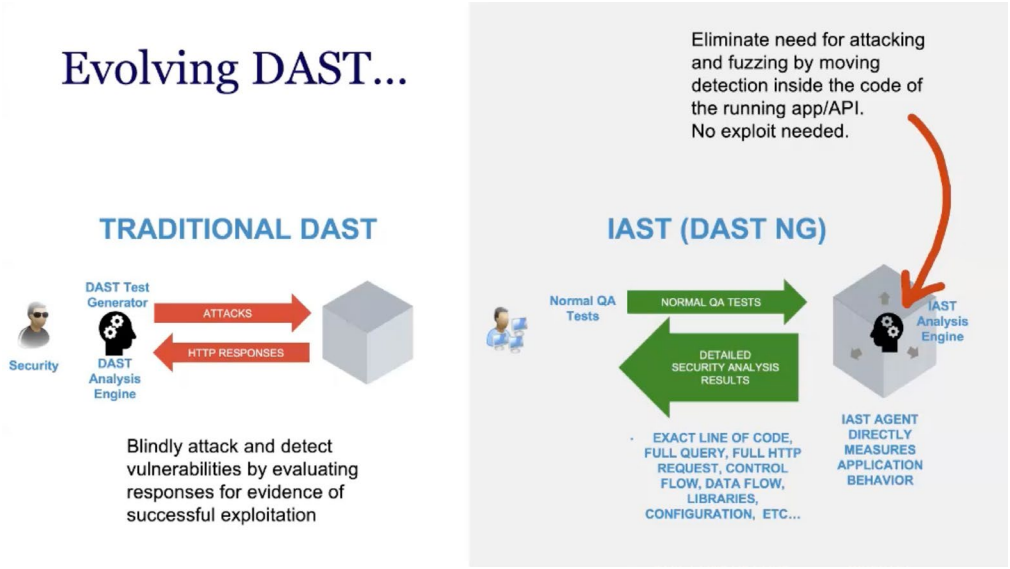
Il existe de nombreuses descriptions du DAST. Communément, on définit le DAST comme une méthodologie de tests de sécurité qui implique l'analyse d'une application en cours d'exécution. Aux États-Unis, le National Institute of Standards and Technology (NIST) souligne l'importance des tests dynamiques dans une de ses publications [cf. Special Publication 800-53 (Rev. 5), under Security Assessment (SA-11), guideline 8]. Cette ligne directrice du NIST recommande d'effectuer une analyse dynamique du comportement des composants logiciels en réponse à diverses entrées et conditions, insistant ainsi sur l'importance du DAST en AppSec. Toutefois, le NIST reconnait qu'il existe de nombreuses façons d'analyser une application en cours d'exécution.

La méthode DAST fonctionne souvent de l'extérieur vers l'intérieur : elle identifie les failles de sécurité en simulant des attaques, inspecte les réponses HTTP et observe les réactions de l'application. Cette approche externe est synonyme d'une incapacité à comprendre les nuances et contextes complexes du code exécuté. Cela limite l'efficacité et la précision du DAST, en particulier lorsqu'il s'agit d'applications modernes et sophistiquées.

DAST nouvelle génération : l'avènement du test interactif de sécurité applicative (IAST)

Compte tenu des limites du DAST traditionnel, une nouvelle version de cette méthodologie suscite un intérêt croissant : le test interactif de sécurité des applications (IAST). L'IAST est une forme de test d'AppSec qui analyse les applications en cours d'exécution, de l'intérieur vers l'extérieur. L'IAST utilise l'instrumentation pour surveiller les opérations internes d'une application, les interactions avec les bibliothèques, les connexions avec les systèmes backend, et bien plus encore. Le tout en temps réel, pendant que l'application est utilisée.

Contrairement au type d'analyse externe du DAST, l'approche IAST permet de mieux comprendre le comportement et les interactions du code, au-delà de ce que les réponses HTTP peuvent détecter et révéler. Cette visibilité accrue permet une identification plus pointue des vulnérabilités et offre un niveau de précision inégalé, comparé au DAST traditionnel et aux tests statiques de sécurité des applications (SAST).



La variante IAST du DAST révolutionne les tests d'AppSec grâce à une visibilité et une précision sans précédent. La contextualisation offerte par l'approche inversée de l'IAST permet des tests de sécurité nettement supérieurs. Ces derniers fournissent des résultats précis et exploitables en temps réel et garantissent ainsi une sécurité applicative robuste et exhaustive. Les DAST de type IAST peuvent identifier un bien plus large éventail de vulnérabilités que les DAST traditionnels, notamment un chiffrement faible qui ne serait pas forcément repérable depuis l'extérieur de l'application. En outre, les IAST ne signalent que les comportements vulnérables qui se produisent dans l'application en cours d'exécution, ce qui garantit une très grande précision.

Il est important de noter que les DAST de type IAST sont capables de détecter les vulnérabilités, même si celles-ci ne sont pas exploitées. Le trafic d'application ordinaire peut être analysé pour trouver les vulnérabilités complexes, contrairement au fuzzing et aux attaques d'exploits. De quoi mettre à la portée de tous le DAST, habituellement réservé aux experts en AppSec. Les développeurs peuvent détecter instantanément des vulnérabilités dans leur code lorsqu'ils effectuent leurs tests de qualité habituels. Tous les tests d'assurance qualité (QA), y compris les cas de tests automatisés, peuvent désormais servir à la fois aux tests de QA et de sécurité.

Contrast Assess : une nouvelle ère pour l'AppSec

Le besoin d'un outil de test AppSec complet allant plus loin que le DAST traditionnel a conduit au développement de solutions innovantes telles que Contrast Assess. Cet outil avancé offre une approche unique en matière de tests de sécurité avec une méthode DAST de type IAST qui permet une évaluation plus précise et plus détaillée des vulnérabilités des applications.

Contrast Assess fonctionne en intégrant l'instrumentation de sécurité dans le code de l'application. Contrast a initié l'utilisation de l'instrumentation pour la sécurité. Contrairement au DAST traditionnel, qui analyse les réponses HTTP, Contrast analyse l'application en cours d'exécution. La technique d'instrumentation est utilisée depuis des dizaines d'années sur le marché de la performance et constitue la base d'outils tels que New Relic, AppDynamics et DataDog.

Contrairement aux outils DAST traditionnels qui n'ont aucune vue sur l'intérieur du code, Contrast Assess contrôle le flux de contrôle, le flux de données, l'utilisation des bibliothèques et les fonctions dangereuses pendant l'exécution du logiciel. Par exemple, Contrast peut détecter lorsque des données non fiables sont utilisées de manière dangereuse, notamment lorsqu'elles sont ajoutées directement à une requête SQL sans application des défenses appropriées. Cette capacité de détection est hautement précise et peut détecter une vulnérabilité non exploitée.

Contrast Assess réinvente le modèle DAST de manière innovante. À l'instar des outils DAST traditionnels, Contrast analyse les applications en cours d'exécution, mais il dirige l'analyse vers le code. Il identifie les vulnérabilités avec plus de précision et offre un retour d'information en temps réel aux développeurs. Contrast ne nécessite aucun balayage ou exploit.

Le tableau de bord AppSec fourni par Contrast fournit des descriptions très détaillées des vulnérabilités, y compris la requête HTTP, les lignes de code concernées et le flux de données exact à travers une application ou une interface de programmation d'applications (API). Contrairement aux solutions DAST traditionnelles qui nécessitent un scanner centralisé avec une planification complexe, Contrast propose une approche distribuée et peut fonctionner en parallèle sur des centaines ou des milliers d'applications, pour détecter les failles de sécurité pendant le développement, le pipeline, l'assurance qualité ou même la production.

Grâce à sa capacité à fournir des informations exploitables sur les vulnérabilités potentielles, Contrast Assess constitue un outil puissant pour les développeurs, en les aidant à comprendre et à corriger les problèmes de code rapidement et efficacement. Les temps de réaction sont accélérés, ce qui rend le processus d'AppSec plus efficace et plus rentable.

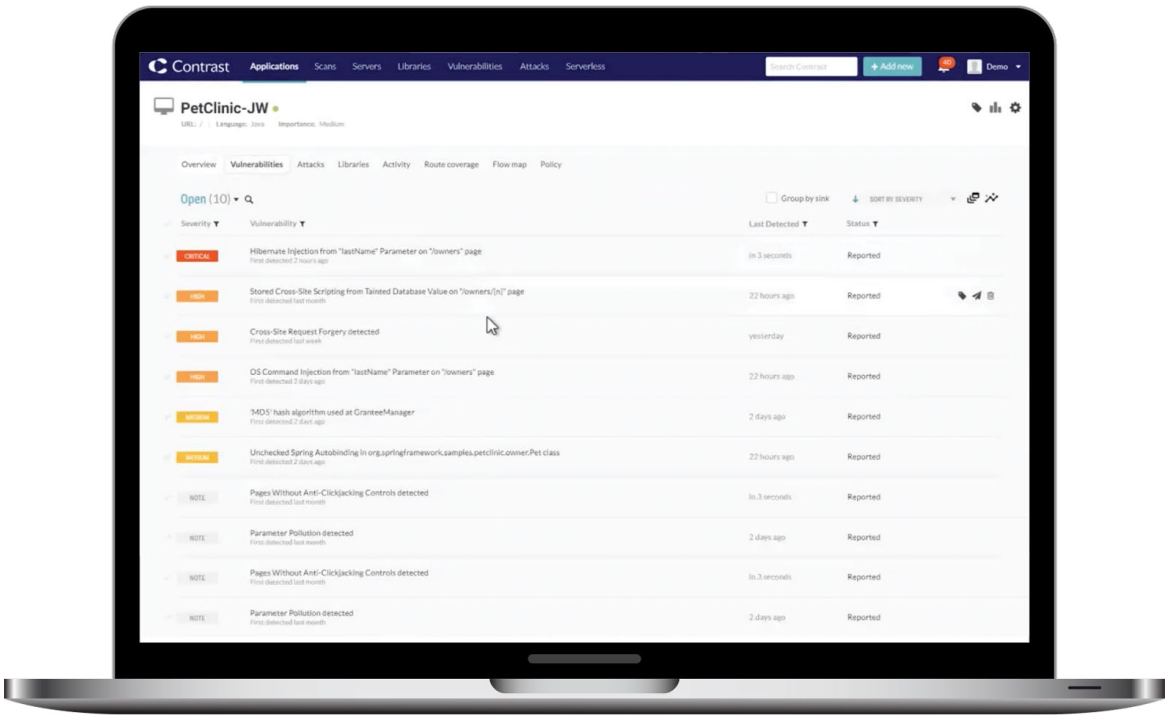
Contrast Assess représente une nouvelle ère pour l'AppSec, une avancée remarquable dans le domaine des tests de sécurité. Ce bond en avant en matière de méthodologie d'AppSec permet aux organisations de protéger plus efficacement leurs applications logicielles en s'appuyant sur les points forts du DAST traditionnel et en y ajoutant de nouvelles capacités puissantes. Ce faisant, Contrast propose une approche supérieure pour garantir la sécurité applicative et répondre aux exigences DAST.

Un autre type de DAST : Contrast Assess en action

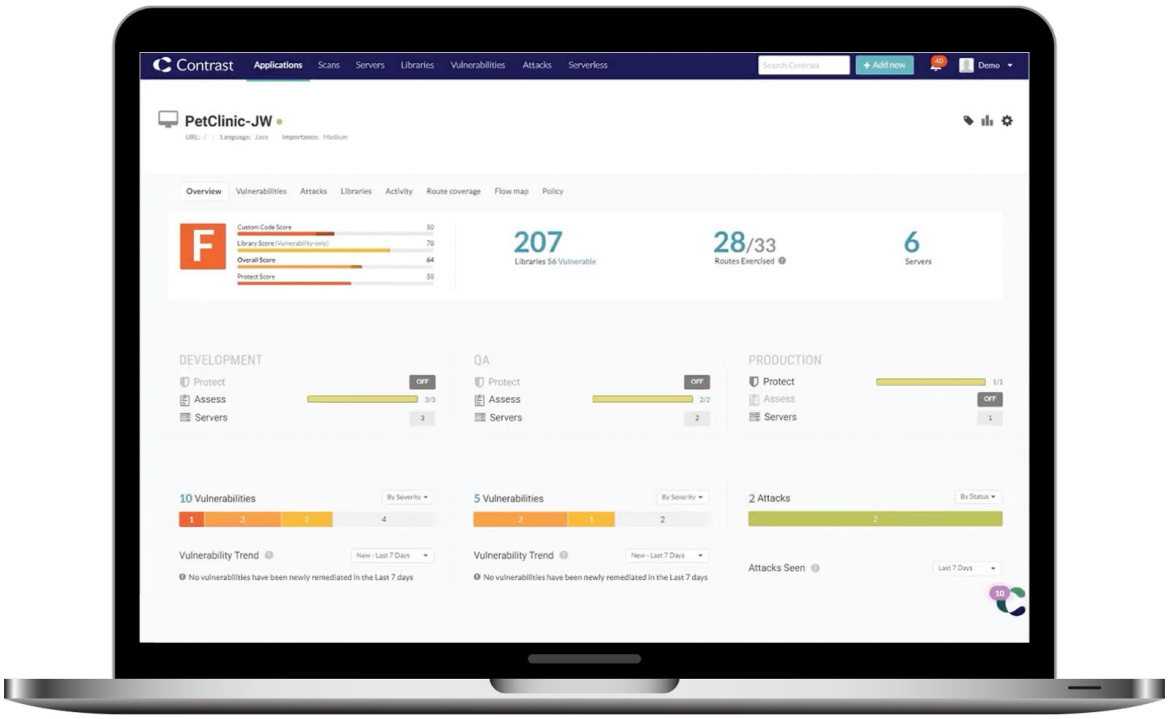
Pour illustrer la puissance et l'efficacité de Contrast Assess, observons l'outil en action sur une application Spring Boot typique : Spring Pet Clinic.

La première étape consiste à ajouter l'agent Contrast à la pile applicative, ce qui ne prend que quelques secondes. Une fois l'agent Contrast ajouté, l'application est exécutée selon son mode habituel et l'outil commence à la surveiller en arrière-plan.

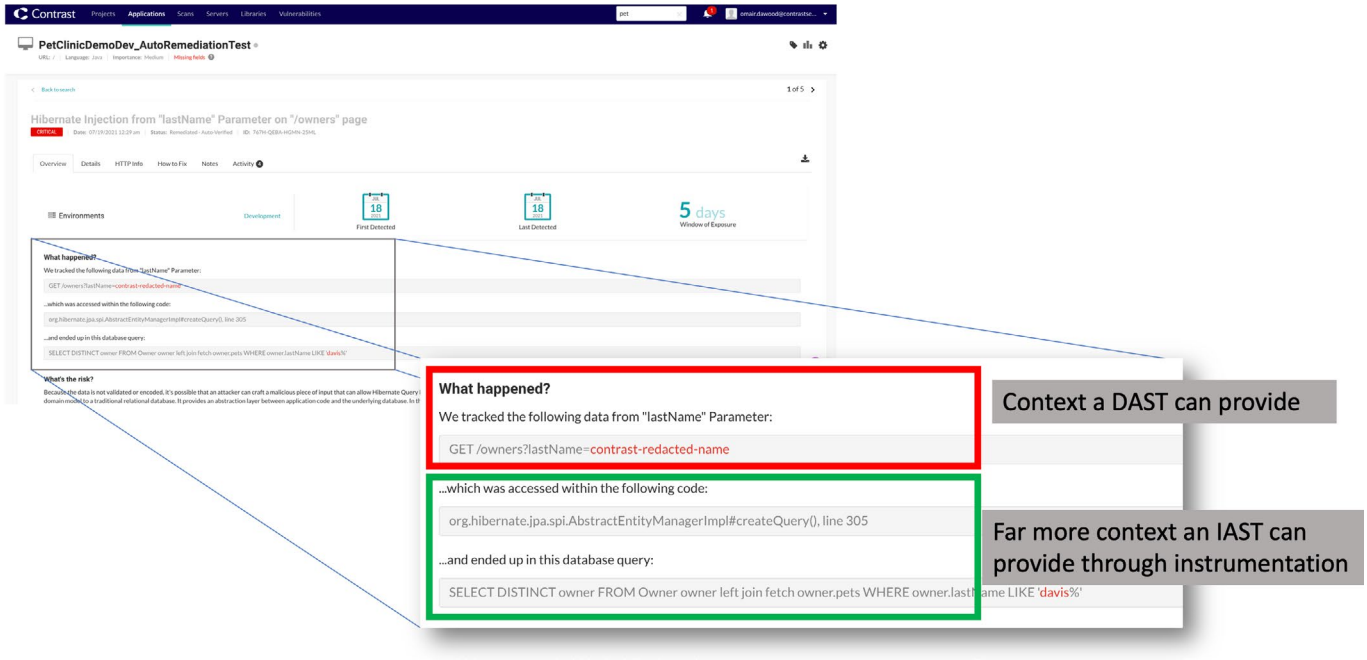
Lorsque vous utilisez l'application, Contrast analyse chaque demande passant par le code en cours d'exécution. Il détecte les vulnérabilités et les signale sur le tableau de bord Contrast.



Le tableau de bord présente une vue d'ensemble de toutes les applications surveillées et fournit des informations sur les bibliothèques utilisées, les chemins empruntés et les serveurs sur lesquels les applications sont exécutées.



Lorsqu'une vulnérabilité est détectée, Contrast fournit une analyse détaillée. Il montre les données suivies de la requête HTTP, leur aboutissement et la manière dont elles ont été utilisées dans une requête sans échappement ni paramétrage appropriés. Les lignes de code et l'historique complet des flux de données sont détaillés, pour permettre aux développeurs de comprendre et corriger plus facilement la vulnérabilité.



La capacité de Contrast Assess à analyser simultanément chaque entrée d'une requête HTTP réduit considérablement le temps nécessaire aux tests de sécurité. En intégrant l'IAST au DAST, Contrast Assess comble efficacement le fossé entre le DAST traditionnel et la nouvelle génération d'outils d'AppSec et marque de ce fait un changement significatif dans la méthodologie DAST. Sa grande précision, le retour d'information immédiat et la possibilité de tester simultanément plusieurs moyens d'attaque font de Contrast Assess un outil puissant de sécurité applicative.

Intégration de Contrast Assess aux outils d'assurance qualité existants

Contrast Assess est conçu pour s'intégrer facilement aux outils QA existants afin d'améliorer encore leurs capacités. Cette intégration permet de tirer parti des avantages des tests de sécurité basés sur l'instrumentation, parallèlement aux fonctionnalités standard de ces outils d'assurance qualité.

Un exemple de cette intégration peut être observé avec Cypress, un outil populaire pour les tests end-to-end. L'ensemble de l'application peut être testé rapidement et efficacement en exécutant les tests Cypress avec Contrast Assess en arrière-plan. Tous les points d'extrémité de l'application peuvent être touchés simultanément, ce qui réduit considérablement le temps nécessaire aux tests de sécurité.

Contrast Assess ne se contente pas de signaler les vulnérabilités, il fournit également le contexte et les détails nécessaires pour les comprendre. Il localise l'emplacement exact du problème dans le code, capture l'état complet et la trace d'appels depuis la méthode et fournit toutes les données sur les requêtes HTTP. Ce niveau de détail améliore considérablement l'efficacité du processus de test, en accélérant l'identification et la correction des failles de sécurité.

La plupart des organisations ont simplement besoin de DAST. Contrast peut facilement répondre à cette exigence, en produisant de meilleurs résultats plus rapidement. Toutefois, il est possible que vous soyez confronté à une demande de DAST strictement traditionnel. Dans ce cas, nous vous suggérons d'utiliser un outil simple et bien connu comme Burp Suite, mais d'ajouter Contrast à l'application. Burp Suite offre de solides fonctionnalités pour explorer, sonder et auditer les applications web. Contrast peut s'intégrer aux applications telles que Burp Suite avec un contexte détaillé de la surface d'attaque, et Burp Suite peut à son tour fournir une télémétrie des vulnérabilités à l'analyse.

En adoptant cette approche, vous pouvez tirer parti des avantages combinés de l'IAST et du DAST traditionnel. Cela garantit l'exhaustivité des tests de sécurité, qui allient la précision des IAST à l'analyse approfondie du code web offerte par les outils tels que Burp Suite. Il en résulte un processus de test de sécurité applicative rationalisé, plus efficace et performant, et à un coût minimum, tout en garantissant des mesures de sécurité fiables.

Conclusion

Face à l'avenir des tests de sécurité applicative, nous vous recommandons vivement d'opter pour un outil DAST de type IAST, tel que Contrast Assess, car cette approche présente tous les avantages du DAST et les surpasse. Il fournit une vue globale de l'application, en mettant en évidence les vulnérabilités depuis l'intérieur et en offrant une précision et une contextualisation supérieures. En conclusion, l'IAST peut efficacement remplacer le DAST traditionnel, et en éliminant le besoin d'implémenter les deux méthodes, il permet de simplifier le processus et de réduire les coûts.

Contrast Security fournit les applications les plus modernes et complètes du secteur
Security Platform élimine les obstacles à la sécurité et donne aux entreprises les moyens d'écrire et de publier plus rapidement des codes d'application sécurisés. Intégrant l'analyse du code et la prévention des attaques directement dans le logiciel grâce à l'instrumentation, la plateforme Contrast détecte automatiquement les vulnérabilités pendant l'écriture du code, élimine les faux positifs et fournit des conseils adaptés au contexte, pour une réparation facile et rapide des vulnérabilités. Les équipes des applications et du développement collaborent ainsi plus efficacement et innovent plus rapidement, tandis que la transformation numérique s'accélère. Voilà pourquoi les grandes entreprises privées et publiques du monde entier sont de plus en plus nombreuses à faire confiance à Contrast pour sécuriser leurs applications en cours de développement et étendre la protection en production.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333

Contrast SECURITY

contrastsecurity.com