Akamai

LIVRE BLANC

Top 10 de l'OWASP

Comment Akamai aide à se protéger contre les vulnérabilités courantes

Introduction

La liste Top 10 de l'OWASP (Open Web Application Security Project) couvre les vulnérabilités les plus courantes constatées dans les applications Web afin d'y sensibiliser les organisations. Afin de tirer pleinement profit du Top 10 de l'OWASP, il faut bien comprendre où, comment et dans quelle mesure les fournisseurs de sécurité peuvent accroître l'amélioration de vos propres pratiques de développement. La ventilation suivante des 10 principales vulnérabilités de l'OWASP décrit chacune d'entre elles et explique comment Akamai peut aider les entreprises grâce à des solutions de sécurité en bordure de l'Internet, des services gérés et la plus grande plateforme de périphérie intelligente au monde.

Produits Akamai

Top 10 de l'OWASP		Account Protector	Akamai Guardicore Segmentation	App & API Protector	Bot Manager	Enterprise Application Access	Enterprise Threat Protector	Identity Cloud	Services de sécurité gérés	Akamai MFA	Page Integrity Manager
Contrôles d'accès défaillants	A01			✓	✓	✓		✓		✓	
Défaillances cryptographiques	A02			✓		✓	✓				✓
Injection	A03			✓							
Conception non sécurisée	A04			✓		✓					
Mauvaise configuration de sécurité	A05		✓	✓	✓						
Composants vulnérables et obsolètes	A06		✓	✓							✓
Identification et authentification de mauvaise qualité	A07	✓		✓	✓	✓		✓		✓	
Manque d'intégrité des données et du logiciel	A08		✓	✓			✓				✓
Carences des systèmes de contrôle et de journalisation	A09		✓	✓		✓	✓		✓		
Falsification de requête côté serveur	A10		✓	✓							

Le Top 10 de l'OWASP représente des catégories de risques, et non des risques isolés. Les solutions d'Akamai répondent à ces catégories de risques de multiples façons. Consultez le livre blanc pour en savoir plus.

A01 : contrôles d'accès défaillants

> « Le contrôle d'accès applique une règle en vertu de laquelle les utilisateurs ne peuvent pas agir en dehors des autorisations prévues. Les défaillances conduisent généralement à la divulgation non autorisée d'informations, à la modification ou à la destruction de toutes les données ou à l'exécution d'une fonction commerciale en dehors des limites de l'utilisateur. »
>
> — Source : owasp.org

Comment Akamai vous aide

Les organisations doivent réparer leur modèle de contrôle d'accès pour traiter intégralement la vulnérabilité liée à la violation du contrôle d'accès, et l'expertise d'Akamai dans le domaine de la WAAP peut les aider à détecter et à se protéger contre certains vecteurs d'attaque qui tentent de l'exploiter :

- **Enterprise Application Access** met à disposition des utilisateurs en entreprise un modèle d'accès de moindre privilège grâce auquel seuls les utilisateurs authentifiés peuvent accéder aux applications autorisées, favorisant ainsi un modèle de sécurité de type Zero Trust.
- **Akamai MFA** fournit des services d'authentification forte sur la base des normes de la technologie FIDO2, résistante à l'hameçonnage.
- **App & API Protector** (la solution WAAP d'Akamai) peut aider à bloquer les attaques en force sur le navigateur en vérifiant l'en-tête « referer » et appliquer l'authentification pour les API afin de renforcer le contrôle d'accès avec API Gateway d'Akamai.
- **Identity Cloud** fournit des contrôles d'accès granulaires aux données de l'utilisateur final, permettant un accès de moindre privilège par utilisateur ou système interne.
- **Bot Manager** empêche les attaques par outils automatisés et les attaques par connexion.

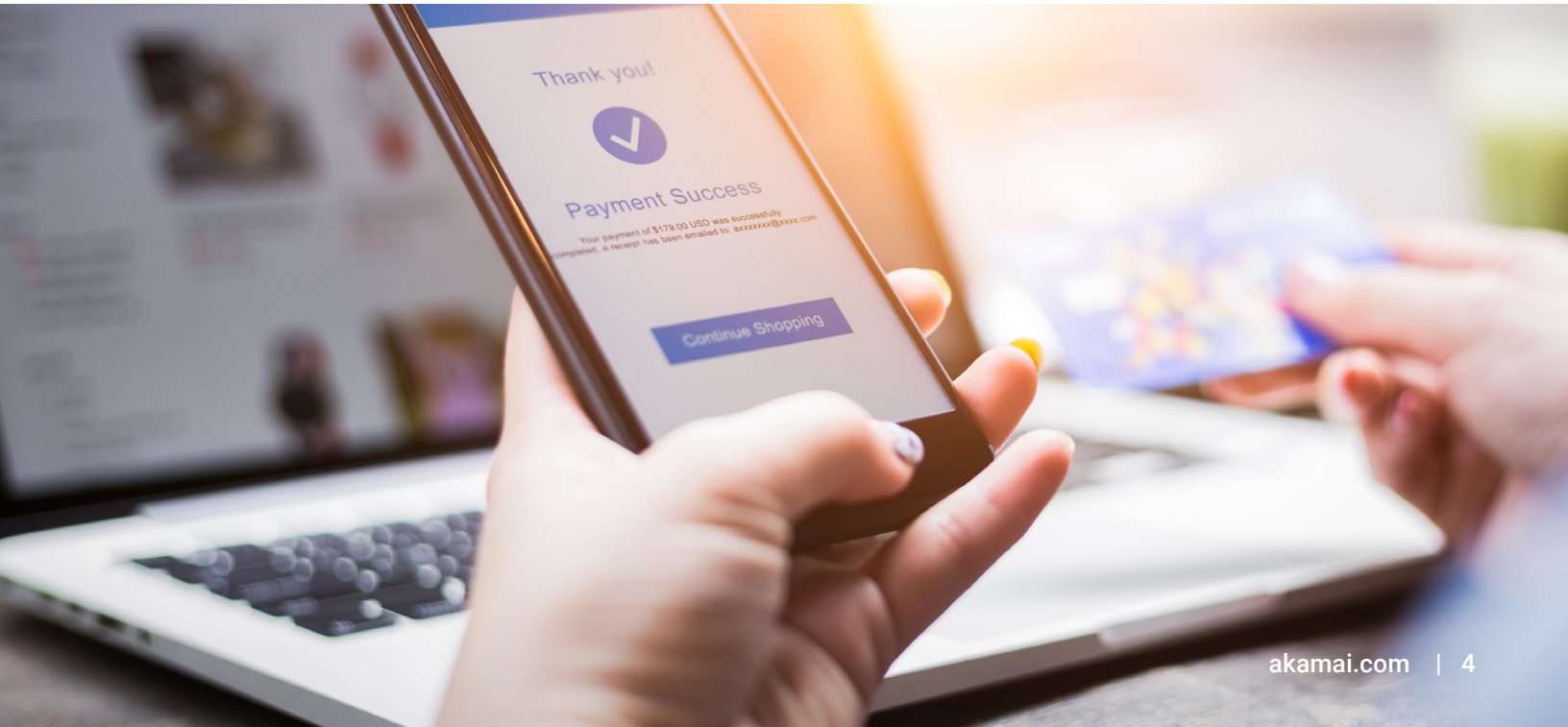
A02 : Défaillances cryptographiques

> « L'accent est mis sur les défaillances liées à la cryptographie (ou à son absence), qui conduisent souvent à l'exposition de données sensibles. ... Par exemple, les mots de passe, les numéros de carte de crédit, les dossiers médicaux, les informations personnelles et les secrets d'entreprise nécessitent une protection supplémentaire, principalement si ces données relèvent des lois sur la protection de la vie privée. »
>
> — Source : owasp.org

Comment Akamai vous aide

Les organisations ne peuvent pas se protéger complètement contre les défaillances cryptographiques en utilisant une seule solution de sécurité. Néanmoins, combiner plusieurs solutions peut permettre de traiter différents aspects de cette vulnérabilité. Par exemple, les solutions suivantes d'Akamai :

- **App & API Protector** crypte et protège les données sensibles en transit à l'aide des dernières versions de TLS et de chiffrements forts. Il contribue également à :
  - Assurer la conformité PCI en utilisant exclusivement un réseau de diffusion de contenu (CDN) sécurisé, qui prend en charge tous les certificats TLS de marque et protège les clés privées du client.
  - Proposer un CDN protégé par une sécurité opérationnelle et physique (comme des racks enfermés et des détecteurs de mouvement) qui garantit que seul le personnel autorisé peut accéder aux serveurs.
  - Localiser et prévenir les fuites de données sensibles grâce à l'apprentissage API des données personnelles identifiables.
- **Enterprise Application Access** peut protéger l'accès distant en chiffrant les communications et en masquant les données confidentielles sur le réseau.
- **Enterprise Threat Protector** peut aider à prévenir l'exposition de données sensibles.
- **Page Integrity Manager** peut également détecter les fuites de données personnelles identifiables via une mauvaise utilisation du code JavaScript qui pourrait résulter de défaillances cryptographiques.



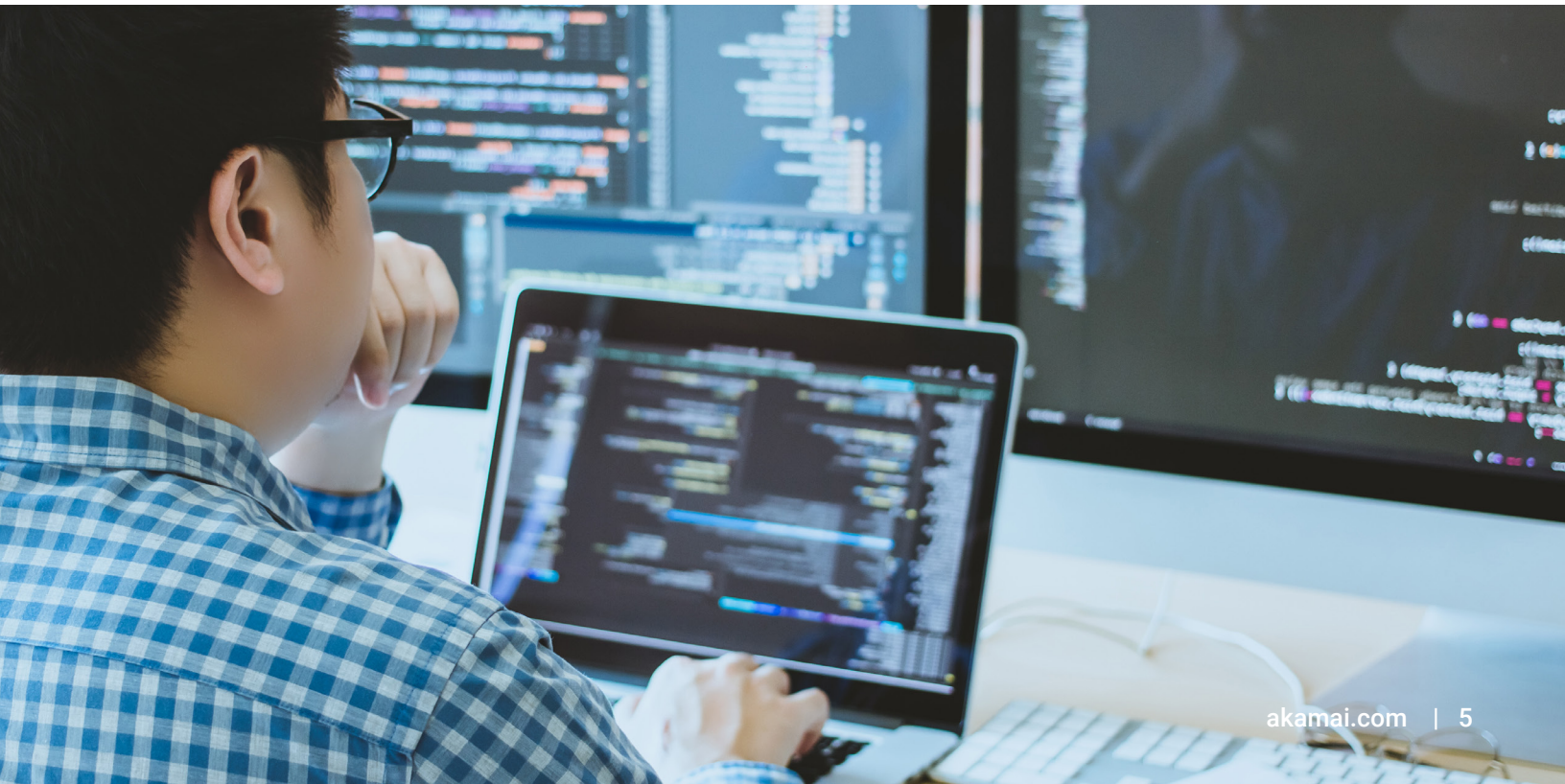
A03 : injection

> « Les failles d'injection (injection SQL, NoSQL, OS et LDAP) surviennent lorsque des données non fiables sont envoyées à un interprète dans le cadre d'une commande ou d'une demande. Les données malveillantes du cybercriminel peuvent leurrer l'interprète, de sorte à ce qu'il exécute des commandes imprévues ou accède à des données sans l'autorisation adéquate. »
>
> — Source : Akamai

Comment Akamai vous aide

Vous pouvez utiliser WAAP pour atténuer les risques liés aux failles d'injection dans les applications Web et les API. Toutefois, les organisations doivent toujours appliquer des correctifs aux applications Web pour traiter les vulnérabilités identifiées en fonction de leur cycle de vie de développement respectif.

- **App & API Protector** offre une solution WAAP de pointe avec un moteur de sécurité adaptatif (ASE), qui fournit une protection étendue contre les attaques par injection en utilisant des règles existantes, prêtes à l'emploi. La case de pénalité de l'ASE peut bloquer temporairement tout le trafic provenant de clients qui ont récemment tenté une attaque par injection en utilisant WAAP.
- En attendant qu'une application puisse être corrigée, des correctifs virtuels avec des règles personnalisées peuvent répondre rapidement aux vulnérabilités liées à l'injection ou aux nouvelles vulnérabilités dues à un changement d'application. Les organisations de sécurité peuvent également automatiser des correctifs virtuels et les intégrer aux processus DevSecOps à l'aide des fonctions dédiées aux API d'Akamai.
- **Client Reputation** peut aider à identifier et à bloquer des attaques par injection en fournissant un score de risque pour les clients malveillants très actifs dans la catégorie Cybercriminels.



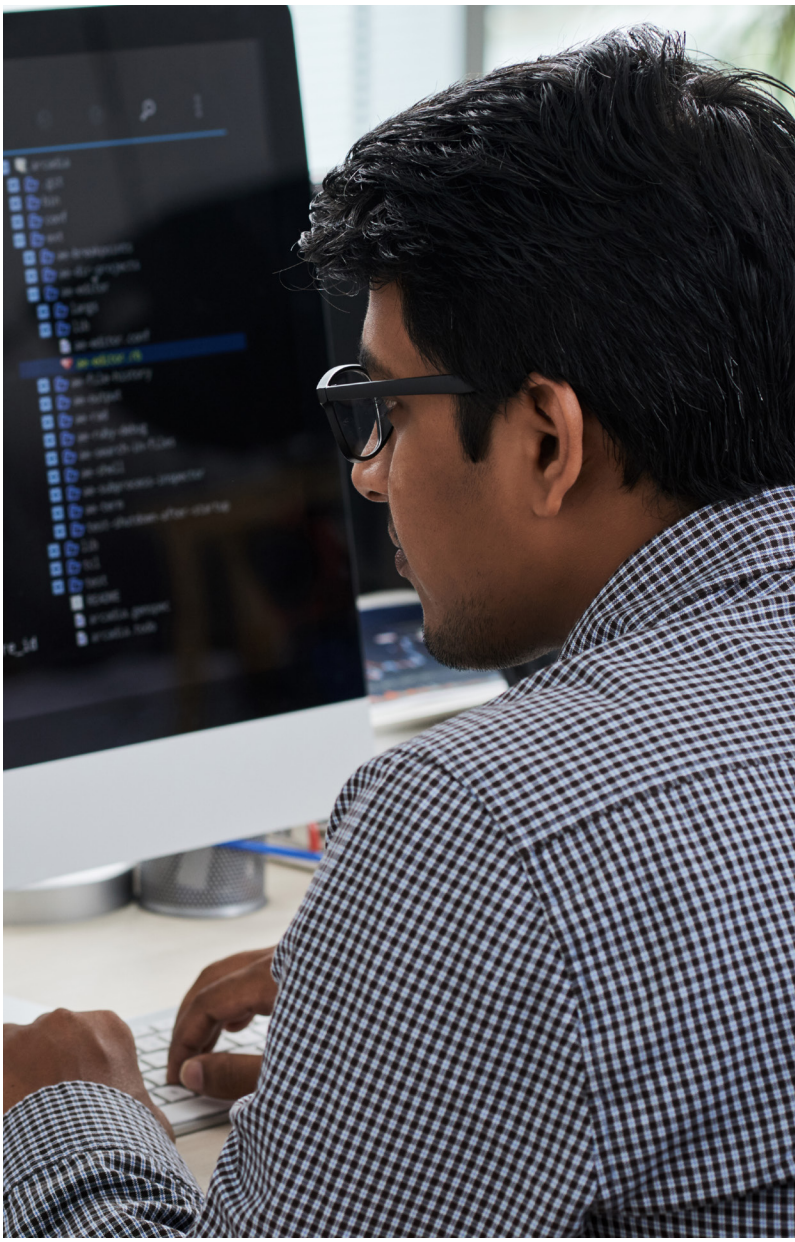
A04 : Conception non sécurisée

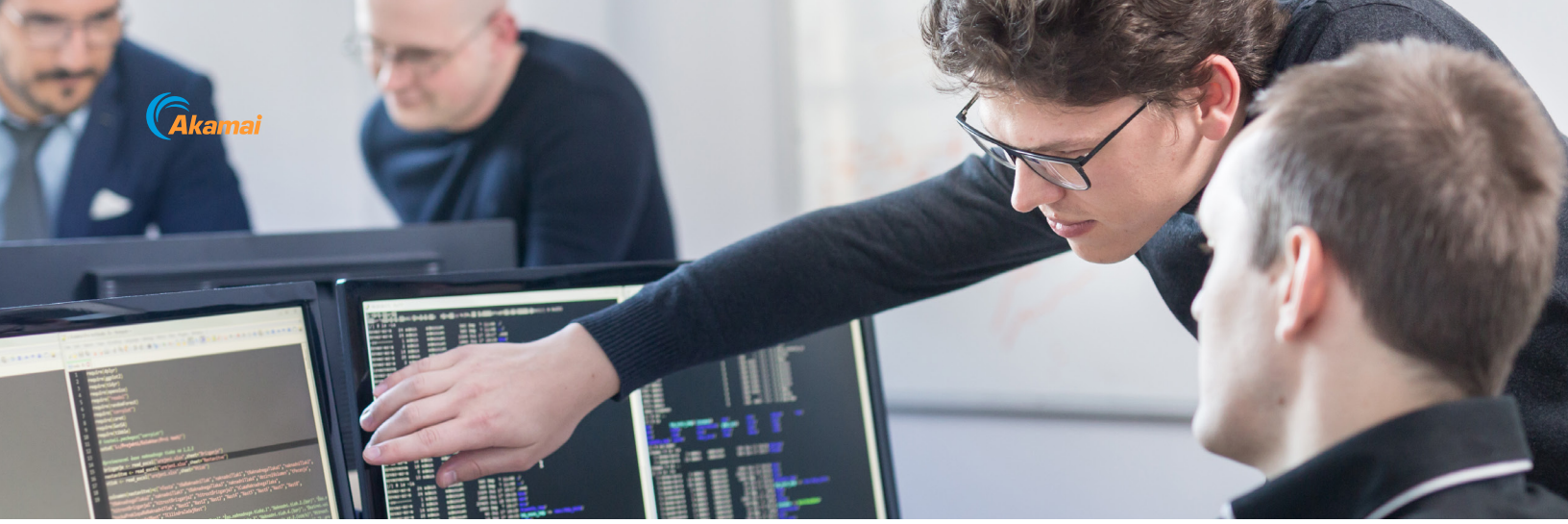
> « La conception non sécurisée est une vaste catégorie représentant différentes faiblesses, exprimée comme une "conception de contrôle manquante ou inefficace". Il y a une différence entre une conception non sécurisée et une mise en œuvre non sécurisée. Une conception sécurisée peut présenter des défauts de mise en œuvre conduisant à des vulnérabilités susceptibles d'être exploitées. Une conception non sécurisée ne peut être corrigée par une mise en œuvre parfaite puisque, par définition, les contrôles de sécurité nécessaires n'ont jamais été créés pour se défendre contre des attaques spécifiques. »
>
> — Source : owasp.org

Comment Akamai vous aide

Les entreprises doivent intégrer la sécurité dès les premières étapes de la conception. Toutefois, les équipes de développement peuvent avoir du mal à y parvenir si la sécurité est difficile à intégrer. Les produits d'Akamai aident les entreprises à adopter plus rapidement une approche « shift left » pour éviter que les insécurités liées à la conception ne compromettent leurs applications et API.

- **App & API Protector** (qui comprend notre solution WAAP et l'ASE) peut également détecter et corriger certains défauts de conception qui atteignent la production. Il s'appuie également sur l'automatisation pour délester et simplifier les tâches de routine, en laissant aux humains le soin d'effectuer celles qui nécessitent une analyse humaine. Cette automatisation comprend les mises à jour automatiques, le réglage automatique, la découverte des API, la programmabilité simplifiée et l'expérience utilisateur.
- **Enterprise Application Access** garantit que seuls les utilisateurs autorisés peuvent accéder aux applications. Cette approche de moindre privilège empêche le déplacement latéral vers d'autres applications, ce qui peut se produire facilement avec des solutions d'accès au réseau telles que les VPN.





A05 : mauvaise configuration de sécurité

> « [Depuis] l'édition précédente, 90 % des applications ont été testées pour une forme ou une autre de mauvaise configuration, avec un taux d'incidence moyen de 4 % et plus de 208 000 occurrences d'une Common Weakness Enumeration (CWE) dans cette catégorie de risque. Sans un processus concerté et reproductible de configuration de la sécurité des applications, les systèmes courent un risque plus élevé. »
>
> — Source : owasp.org

Comment Akamai vous aide

Par définition, une mauvaise configuration de sécurité affecte de multiples aspects de la sécurité des applications. Les entreprises doivent donc configurer correctement leurs contrôles de sécurité. Les produits d'Akamai peuvent vous aider comme suit :

- Sans toutefois remplacer une configuration appropriée, **App & API Protector** peut vous aider en :
  1. Utilisant des groupes d'attaque contre les anomalies sortantes pour repérer les fuites de données telles que les codes d'erreur ainsi que le code source résultant de configurations inadéquates de la sécurité prête à l'emploi.
  2. Mettant en œuvre des règles capables de détecter et d'arrêter les attaques XXE avant que l'analyseur XML traite l'entité externe dangereuse.
  3. Mettant en place des règles permettant de détecter l'accès aux fichiers sensibles connus laissés par les développeurs sur les serveurs de production.
- **Akamai Guardicore Segmentation** contribue à la protection contre les fuites de données dues à des erreurs de configuration en offrant une visibilité et un contrôle granulaire de toute communication non autorisée ou non planifiée entre vos applications et l'Internet.
- En attendant que votre équipe puisse corriger l'application, les correctifs virtuels dotés de règles personnalisées peuvent vous aider à traiter rapidement les fuites de données détectées.
- Avec **App & API Protector** et **Bot Manager**, vous pouvez vous protéger des attaques en force utilisant des identifiants par défaut grâce aux contrôles de débit.
- Une configuration trop faible de la politique de sécurité du contenu et d'autres en-têtes HTTP relatifs à la sécurité peut être renforcée sur la plateforme Akamai.
- Avec l'identification automatique des API dans **App & API Protector**, vous pouvez découvrir et profiler vos API de manière automatique et continue, y compris les points de terminaison, les définitions et les caractéristiques des ressources et du trafic.

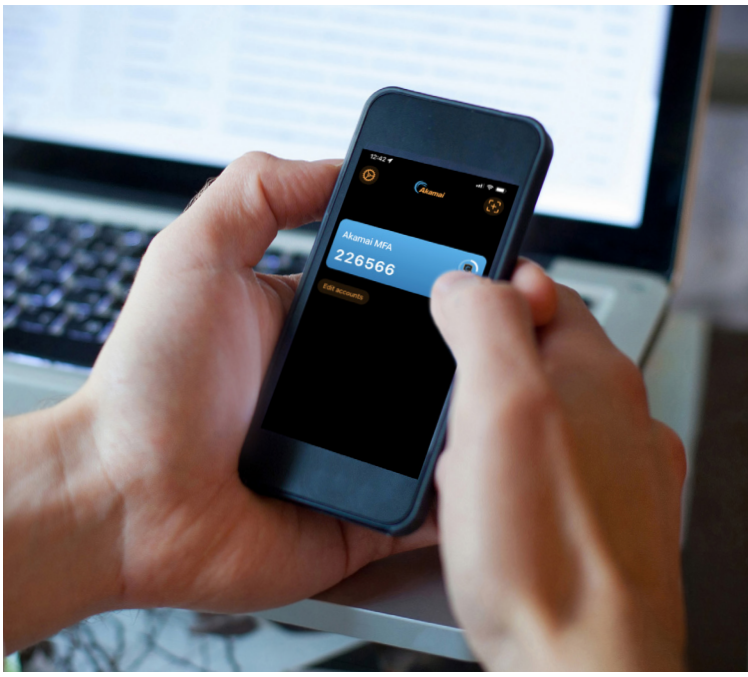
A06 : Composants vulnérables et obsolètes

> « Les composants tels que les bibliothèques, les cadres et autres modules logiciels s'exécutent avec les mêmes privilèges que l'application. De plus, les scripts agissent comme des ressources d'application de confiance avec un accès complet aux données de l'application. Si un composant vulnérable est exploité, une telle attaque peut entraîner une grave perte de données ou une prise de contrôle du serveur. »
>
> — Source : Akamai

Comment Akamai vous aide

Bien souvent, les organisations ne savent plus quels composants existent dans leurs applications et les équipes de sécurité n'ont pas conscience du problème. En outre, les organisations n'ont aucun contrôle sur la vitesse à laquelle l'entité tierce traite les nouvelles vulnérabilités identifiées, le cas échéant. Pour pallier ce manque de visibilité et de certitude, il est nécessaire d'utiliser une solution de sécurité telle que WAAP, ainsi qu'une protection par script, telles que l'une des suivantes :

- **App & API Protector** inclut plusieurs règles conçues pour répondre aux vulnérabilités connues, soit spécifiquement dans vos applications, soit dans les composants tiers. Il fournit également des capacités de protection des API, qui protègent les API même lorsque des composants tiers incorporés dans l'API les exposent aux abus.



- La fonctionnalité d'aperçu d'**Akamai Guardicore Segmentation** vous permet de rechercher tous les actifs de votre réseau qui pourraient être vulnérables. L'application granulaire incluse vous permet en outre d'isoler les ressources affectées jusqu'à ce qu'un correctif ait été appliqué.
- En attendant qu'une application puisse être corrigée, les correctifs virtuels dotés de règles personnalisées répondent rapidement aux vulnérabilités émergentes ou aux nouvelles vulnérabilités dues à un changement d'application.
- **Client Reputation** fournit un score de risque pour les clients malveillants dans la catégorie Analyse Web pour aider à la protection contre l'exploitation des nouvelles vulnérabilités.
- **Page Integrity Manager** utilise des sessions utilisateur réelles pour surveiller le comportement des scripts en temps réel, afin d'identifier les comportements suspects ou tout bonnement malveillants. Il bloque également les extractions de données depuis les scripts internes ou tiers vers des URL avec des vulnérabilités connues grâce à une base de données des vulnérabilités et des failles courantes (CVE).

A07 : identification et authentification de mauvaise qualité

> « Les fonctions d'application liées à l'authentification et à la gestion de session sont souvent mises en œuvre de manière incorrecte, ce qui permet aux cybercriminels de compromettre les mots de passe, les clés ou les jetons de session, ou encore d'exploiter d'autres failles de mise en œuvre pour usurper temporairement ou définitivement l'identité d'autres utilisateurs. »
>
> — Source : Akamai

Comment Akamai vous aide

Les entreprises doivent corriger leurs défaillances afin de répondre pleinement à cette vulnérabilité.

Néanmoins, les solutions d'Akamai énumérées ci-dessous peuvent les aider à détecter les vecteurs d'attaque qui tentent d'exploiter les identifications et authentifications de mauvaise qualité, et à s'en protéger :

- **Bot Manager** peut détecter et réduire l'impact des attaques automatisées telles que celles utilisées dans les attaques par credential stuffing.
- **Account Protector** atténue les tentatives de prise de contrôle de compte où des imposteurs tentent d'obtenir un accès non autorisé aux comptes des utilisateurs.
- **Enterprise Application Access** peut fournir un accès proxy aux applications par le biais d'un « modèle d'accès de moindre privilège » afin de réduire la surface d'attaque de l'application et d'améliorer l'accès.
- **Akamai MFA** est doté d'une fonction de contrôle de débit capable de gérer des attaques en force.
- **App & API Protector** est doté d'une fonction de contrôle de débit capable de gérer des attaques en force.
- **Identity Cloud** fournit une gestion sécurisée des identifiants et du profil de l'utilisateur final, protégée par des capacités d'authentification à deux facteurs et basée sur les risques.

A08 : manque d'intégrité des données et du logiciel

> « Le manque d'intégrité des données et du logiciel est lié au code et à l'infrastructure qui ne protègent pas contre les violations de l'intégrité. C'est le cas, par exemple, lorsqu'une application s'appuie sur des plug-ins, des bibliothèques ou des modules provenant de sources, de référentiels et de réseaux de diffusion de contenu (CDN) non fiables. Un pipeline CI/CD non sécurisé peut introduire un risque d'accès non autorisé, de code malveillant ou de compromission du système. »
>
> — Source : owasp.org

Comment Akamai vous aide

Les entreprises peuvent utiliser WAAP pour protéger les applications Web et les API contre le manque d'intégrité des données et du logiciel. Toutefois, les organisations doivent toujours appliquer des correctifs aux applications Web pour traiter les vulnérabilités identifiées en fonction de leur cycle de vie de développement.

- **App & API Protector**
  - Fournit une protection forte contre les attaques de désérialisation.
  - Empêche les attaques de type « machine-in-the-middle » qui peuvent entraîner des problèmes d'intégrité des données grâce à la mise en œuvre des dernières versions de TLS et de chiffrements forts.
  - Assure l'authentification de l'origine des données et la protection de l'intégrité des données des enregistrements DNS en mettant en œuvre le DNSSEC avec Edge DNS. Cela empêche l'altération d'enregistrements DNS en vue de rediriger les utilisateurs vers des sources non fiables.
- La fonctionnalité d'aperçu d'**Akamai Guardicore Segmentation** vous permet de rechercher toutes les ressources de votre réseau qui ont reçu la mise à jour corrompue. L'application granulaire incluse vous permet en outre d'isoler les ressources concernées jusqu'à ce qu'un correctif ait été créé.
- **Enterprise Threat Protector** détecte les attaques par hameçonnage, qui peuvent attirer les administrateurs et les super-utilisateurs des applications vers des environnements hostiles ou des sources non fiables.
- En attendant qu'une application puisse être corrigée, des correctifs virtuels avec des règles personnalisées peuvent vous aider à traiter rapidement les nouvelles failles de désérialisation.
- **Page Integrity Manager** détecte les scripts tiers, surveille leurs modifications et prend des mesures à l'égard des scripts compromis.

A09 : carences des systèmes de contrôle et de journalisation

« L'insuffisance de la journalisation, de la détection, de la surveillance et de la réponse active peut se produire à tout moment :

- Les événements vérifiables, tels que les connexions, les échecs de connexion et les transactions de grande valeur, ne sont pas enregistrés.
- Les avertissements et les erreurs ne génèrent pas de messages de journalisation, ou en génèrent des inadéquats ou peu clairs.
- Les journaux des applications et des API ne sont pas surveillés pour détecter toute activité suspecte.
- Les journaux ne sont stockés que localement.
- Les seuils d'alerte appropriés et les processus d'escalade des réponses ne sont pas en place ou efficaces.
- Les tests de pénétration et les analyses effectuées par les outils de test de sécurité des applications dynamiques (DAST) ne déclenchent pas d'alertes.

L'application n'est pas en mesure de détecter, de faire remonter ou de signaler les attaques actives en temps réel ou presque. »

— Source : owasp.org

Comment Akamai vous aide

Les carences des systèmes de contrôle et de journalisation représentent une lacune dans la capacité d'une entreprise à traiter les vulnérabilités et les tentatives d'exploitation de celles-ci. Akamai propose de nombreuses fonctionnalités pour fournir aux organisations une meilleure visibilité contre les attaques, y compris :

- Akamai fournit des tableaux de bord et des outils de création de rapport dans l'interface utilisateur graphique du Control Center d'Akamai.
- Les produits de sécurité d'applications d'Akamai intègrent l'infrastructure SIEM existante d'une organisation pour mettre en corrélation les événements détectés par Akamai avec ceux des autres fournisseurs de sécurité.
- **Managed Security Service** assure une analyse et des capacités de réponse 24 h/24, 7 j/7.
- **App & API Protector** comprend une case de pénalité qui permet d'enregistrer davantage d'adresses IP ayant fait preuve d'activités malveillantes ou suspectes en vue d'une analyse approfondie.
- **Enterprise Application Access** intègre une solution de gestion des identités pour authentifier et contrôler l'accès à toutes les applications d'entreprise. En l'associant avec sa fonctionnalité d'Identity Aware Proxy, les organisations peuvent améliorer leur visibilité sur les actions des utilisateurs, en particulier sur les actions GET/POST.
- **Enterprise Threat Protector** assure une visibilité totale sur toutes les requêtes DNS externes à l'entreprise, qu'elles soient malveillantes ou non.
- **Akamai Guardicore Segmentation** offre une visibilité approfondie sur les flux de communication au sein de votre réseau, de sorte que des alertes peuvent être déclenchées en cas de communication non autorisée ou inattendue, et que des politiques de sécurité peuvent être appliquées jusqu'au niveau du processus ou du service individuel pour restreindre cette communication. Grâce au module supplémentaire de détection des violations, les menaces potentielles peuvent être rapidement détectées et corrigées.

A10 : Falsification de requête côté serveur

> « Les failles SSRF se produisent lorsqu'une application Web récupère une ressource distante sans valider l'URL fournie par l'utilisateur. Cela permet à un pirate de contraindre l'application à envoyer une requête élaborée vers une destination inattendue, même lorsqu'elle est protégée par un pare-feu, un VPN ou un autre type de liste de contrôle d'accès au réseau (ACL). »
>
> — Source : owasp.org

Comment Akamai vous aide

La WAAP d'Akamai inclut des règles qui peuvent rechercher des injections d'URL. Cette fonctionnalité peut empêcher les pirates d'inciter le serveur à soumettre une requête ailleurs, par exemple pour la faire passer pour une requête valide pour vos analystes de sécurité.

- Les règles d'**App & API Protector** permettent d'éviter que ces demandes d'exploitation n'atteignent le serveur vulnérable en premier lieu.
- **Akamai Guardicore Segmentation** peut surveiller et bloquer le trafic sortant inattendu au niveau du serveur.

Conclusion

Afin de se défendre au mieux contre les 10 principales vulnérabilités de l'OWASP, les entreprises et leurs fournisseurs de solutions de sécurité doivent travailler ensemble pour identifier les vulnérabilités dès que possible et mettre en œuvre des solutions pour les prévenir. En savoir plus sur l'offre de solutions de sécurité en bordure de l'Internet d'Akamai Si vous souhaitez discuter des solutions que nous proposons pour mettre sur pied la protection la mieux adaptée à votre entreprise, contactez votre représentant commercial Akamai.