LISTA DE VERIFICAÇÃO DA AKAMAI

Os 10 principais riscos de segurança de API do OWASP

As APIs se tornaram o padrão para desenvolver e conectar aplicações modernas, especialmente com a crescente mudança para arquiteturas baseadas em microsserviços. É por isso que é importante proteger sua organização contra os riscos de segurança de API mais comuns identificados pelo OWASP (Open Worldwide Application Security Project). Vamos analisar a lista atual de 2023 para você saber mais durante a sua jornada para proteger suas APIs.

Cobertura da Akamai dos 10 principais riscos de segurança de API do OWASP

- **API1:2023 – Autorização em nível de objeto corrompida (BOLA):** essas vulnerabilidades ocorrem quando a autorização de um cliente não é validada corretamente para acessar os IDs específicos de objeto.
- **API2:2023 – Autenticação corrompida:** refere-se a amplas vulnerabilidades no processo de autenticação, expondo o sistema a invasores que podem explorar esses pontos fracos e comprometer a proteção de objetos de API.
- **API3:2023 – Autorização em nível da propriedade de objeto corrompida:** é uma falha de segurança em que um ponto de extremidade de API expõe desnecessariamente mais propriedades de dados do que as necessárias para sua função, negligenciando o princípio de menor privilégio.
- **API4:2023 – Consumo irrestrito de recursos:** esse é um tipo de vulnerabilidade, às vezes chamada de esgotamento de recursos de API, em que as APIs não limitam o número de solicitações ou o volume de dados que elas fornecem em um determinado momento.
- **API5:2023 – Autorização em nível de função corrompida (BFLA):** pode ocorrer quando os modelos de controle de acesso para pontos de extremidade de API são implementados incorretamente.
- **API6:2023 – Acesso irrestrito a fluxos comerciais confidenciais:** esse risco surge quando uma API expõe operações críticas, como lógica de negócios, sem controle de acesso suficiente.
- **API7:2023 – Falsificação de solicitação do lado do servidor:** permite que um invasor induza a aplicação do lado do servidor a realizar solicitações HTTPS para um domínio arbitrário escolhido pelo invasor.
- **API8:2023 – Configuração incorreta de segurança:** refere-se à configuração inadequada dos controles de segurança, que podem deixar um sistema vulnerável a ataques.
- **API9:2023 – Gerenciamento inadequado de inventário:** esse é um desafio para todas as organizações que gerenciam APIs. As soluções de segurança de API podem proteger as APIs conhecidas, mas as APIs desconhecidas (incluindo APIs preteridas, preexistentes e/ou desatualizadas) podem ficar sem patches e vulneráveis a ataques.
- **API10:2023 – Consumo inseguro de APIs:** refere-se aos riscos associados ao uso de APIs de terceiros sem aplicar as medidas de segurança adequadas.

Quer entender a diferença entre a lista dos 10 principais riscos de segurança de API do OWASP de 2019 e a de 2023? Confira a publicação no blog.

Trabalhe conosco

As organizações e seus fornecedores de segurança devem trabalhar em conjunto, alinhando pessoas, processos e tecnologias para instituir uma defesa sólida contra os riscos de segurança descritos em “Os 10 principais riscos de segurança de API do OWASP”.

Sobre a Akamai

A Akamai oferece soluções de segurança líderes do setor, especialistas altamente experientes e a Akamai Connected Cloud, que obtém insights de milhões de ataques a aplicações Web, bilhões de solicitações de bot e trilhões de solicitações de API todos os dias. As soluções de segurança de aplicações Web e APIs da Akamai ajudarão a proteger sua organização contra as formas mais avançadas de ataques a aplicações Web, de negação de serviço distribuída (DDoS) e baseados em API.

 | Suporte | | Publicado em 08/23