Akamai

WHITE PAPER

Plano de ação para você se proteger contra os riscos à segurança listados como os 10 principais riscos de segurança às APIs do OWASP

Como a Akamai pode ajudar você a lidar com vulnerabilidades e ameaças comuns às APIs

"As 10 principais ameaças de segurança de API OWASP"		A Akamai pode ajudar?
API1:2023	Autorização em nível de objeto corrompida	☑
API2:2023	Autenticação corrompida	☑
API3:2023	Autorização em nível de propriedade de objeto corrompida	☑
API4:2023	Consumo irrestrito de recursos	☑
API5:2023	Autorização em nível de função corrompida	☑
API6:2023	Acesso irrestrito a fluxos comerciais confidenciais	☑
API7:2023	Falsificação de solicitação do lado do servidor	☑
API8:2023	Configuração incorreta de segurança	☑
API9:2023	Gerenciamento inadequado de inventário	☑
API10:2023	Consumo inseguro de APIs	☑

As APIs estão no centro dos produtos digitais, serviços e ambientes de nuvem de uma empresa. Elas também são o padrão para criar e conectar aplicativos à medida que as organizações passam adotar, cada vez mais, a arquitetura baseada em microsserviços para o desenvolvimento de aplicativos. No entanto, o acesso constante das APIs a dados e sistemas críticos faz com que elas sejam tanto um gerador de receita quanto um risco operacional.

APIs expostas ou mal configuradas são predominantes e fáceis de comprometer e, muitas vezes, estão desprotegidas. E a violação de apenas uma API pode resultar no furto de milhões de registros.

A proteção de APIs deve ser prioridade, pois 78% das organizações relatam ter experimentado incidentes de segurança de APIs em um ano. No entanto, a rapidez com que a superfície de ataque de API evoluiu como alvo de escolha é muito maior do que a velocidade que as maioria das empresas conseguiu obter na compreensão de:

Riscos de APIs

Métodos de ataques a APIs

Controles e recursos de segurança de APIs

O que a superfície de ataque da API compreende? A resposta é: ela é muito mais ampla do que muitas organizações imaginam. A compreensão tradicional das APIs, por exemplo, APIs de terceiros ou entre computadores, pode e deve ser expandida para incluir serviços de aplicativos móveis e da Web como parte da arquitetura baseada em microsserviços. Em outras palavras, uma solicitação da Web dentro da arquitetura de microsserviços é uma API que atua como uma entre várias chamadas para vários microsserviços.

78%

das organizações relatam que experimentaram incidentes de segurança de API em um ano. É claro que a proteção das APIs deve ser uma prioridade.

Em 5 de junho de 2023, o Open Worldwide Application Security Project (OWASP) publicou a primeira grande atualização de sua lista inicial dos 10 principais riscos de segurança de APIs, lançada em 2019. A lista atualizada aborda a maneira pela qual cada uma dessas chamadas de API potencialmente abre falhas de segurança e cria riscos de privacidade, inclusive:

Validação de dados deficiente

Erros de configuração

Falhas de implementação

Lacunas de integração entre componentes de segurança

Continue lendo para saber mais sobre os principais riscos identificados pelo OWASP e como você pode usar as soluções de segurança de APIs da Akamai para mitigá-los.

É importante ressaltar que até mesmo as organizações que afirmam ter um inventário completo de suas APIs deparam-se com uma lacuna séria:

Apenas **4 entre 10** sabem quais das suas APIs retornam dados confidenciais quando chamadas.

API1:2023 – Autorização em nível de objeto corrompida

Vulnerabilidades de autorização em nível de objeto corrompida (BOLA) podem ocorrer quando a autorização de um cliente não é validada adequadamente para acessar IDs de objetos específicos. Essa vulnerabilidade pode fornecer uma abertura para que invasores acessem recursos diretamente, ignorando o fluxo de trabalho previsto do aplicativo e obtendo acesso não autorizado a dados confidenciais. As organizações podem reduzir esse risco ao evitar a dependência exclusiva de IDs de objetos que os clientes passam em suas solicitações. Em vez disso, elas podem usar IDs aleatórias e indecifráveis para os objetos a fim de garantir uma validação robusta para cada um. Quando apropriado, mascarar a verdadeira identificação dos objetos pode fornecer uma camada adicional de segurança.

Como a Akamai pode ajudar

Os cautelosos sistemas de vigilância da Akamai rastreiam ameaças e geram alertas para tentativas de exploração do BOLA, garantindo atenção e ação imediatas.

A Akamai mitiga riscos ao:

- Identificar tentativas de exploração do BOLA
- Classificar pontos de extremidade da API suscetíveis à exploração do BOLA com base em entradas recebidas, por exemplo, parâmetros enumeráveis, bem como nos relacionamentos entre objetos e propriedades da API
- Gerar alertas sobre tentativas de exploração ou exploração do BOLA bem-sucedida

API2:2023 – Autenticação corrompida

Autenticação corrompida se refere a amplas vulnerabilidades no processo de autenticação, expondo o sistema a invasores que podem explorar esses pontos fracos e comprometer a proteção de objetos da API. Normalmente os invasores que aproveitam as vulnerabilidades da autenticação corrompida manipulam brechas no sistema, como senhas fracas ou repetição de sessão. Para se proteger contra vulnerabilidades de autenticação corrompida, as organizações podem estabelecer mecanismos de autenticação robustos, como políticas de senha fortes, rotação de chaves, assinaturas de token fortes e chaves de criptografia. A aplicação dessas políticas rigorosas em toda a organização pode reduzir significativamente os riscos.

Como a Akamai pode ajudar

A Akamai fortalece a segurança de API identificando e retificando pontos de autenticação fracos, impedindo ataques automatizados e alertando proativamente sobre tentativas de exploração.

A Akamai mitiga este risco ao:

- Identificar pontos de extremidade de API que não exigem autenticação ou não seguem as práticas recomendadas de autenticação, como assinaturas de token ou chaves de criptografia fracas e a aceitação de tokens de autenticação expirados
- Proteger contra ataques automatizados de dicionário ou de preenchimento de credenciais por meio de nossos recursos de gerenciamento de bots
- Manipular a autorização de tokens da Web JSON usando assinaturas de token fortes por meio dos nossos recursos de API Gateway
- Gerar alertas sobre tentativas de exploração do BUA

API3:2023 – Autorização em nível de propriedade de objeto corrompida

Autorização em nível de propriedade de objeto corrompida (BOPLA) é uma falha de segurança em que um ponto de extremidade da API expõe desnecessariamente mais propriedades de dados do que as que são exigidas para sua função, negligenciando o princípio de menor privilégio.

Essa falha pode fornecer inadvertidamente aos invasores dados excessivos que podem ser usados para descobrir mais vulnerabilidades ou extrair dados confidenciais. Isso inclui cenários em que propriedades exclusivas para acesso de administrador podem ser manipuladas por usuários não autorizados, comprometendo ainda mais a integridade do sistema. Para garantir a segurança e evitar que os invasores obtenham ou manipulem informações excedentes, é fundamental fornecer níveis de acesso e exposição de dados adequados, impedindo que os possíveis invasores explorem esses descuidos.

Como a Akamai pode ajudar

Aproveitando as táticas abrangentes da Akamai, as empresas conseguem mitigar os riscos do BOPLA identificando e catalogando pontos de extremidade de API e suas propriedades associadas.

A Akamai mitiga este risco ao:

- Identificar e rotular todos os pontos de extremidade e as propriedades da API que eles expõem, como informações de identificação pessoal (PII)
- Identificar pontos de extremidade, objetos e propriedades de API "sombra" ou não documentados, bem como propriedades anormais
- Aplicar políticas de segurança em parâmetros e propriedades aceitáveis e definidos para garantir a limpeza de dados
- Aplicar políticas de segurança baseadas na especificação OpenAPI/Swagger completa e permitir que apenas pontos de extremidade e métodos de API bem definidos acessem objetos e propriedades da API
- Gerar alertas sobre tentativas de exploração do BOPLA

API4:2023 – Consumo irrestrito de recursos

O consumo irrestrito de recursos, às vezes chamado de "esgotamento de recursos de API", é um tipo de vulnerabilidade em que as APIs não limitam o número de solicitações ou o volume de dados que atendem em um determinado período. Este descuido pode abrir a porta para invasores que desejam realizar ataques de negação de serviço (DoS), o que pode tornar o sistema indisponível para usuários legítimos. Tais explorações podem ter sérias implicações comerciais, resultando em perdas de disponibilidade de serviço, insatisfação do cliente e potenciais perdas de receitas, dependendo da duração e do alcance da interrupção. É fundamental implementar medidas que limitem a taxa de solicitações de API e o tamanho dos dados retornados para evitar a perda de serviço.

Como a Akamai pode ajudar

A Akamai protege suas APIs contra ameaças de consumo irrestrito de recursos ao:

- Identificar pontos de extremidade em risco e fornecer alertas em tempo real sobre tentativas de ataques volumétricos
- Detectar excesso de erros, tentativas de login ou comportamento atípico indicando risco

A Akamai mitiga este risco ao:

- Identificar pontos de extremidade de API que não têm limites de taxa ou estão sob ataque por meio de grandes dicionários volumétricos ou ataques de preenchimento de credenciais
- Iniciar fluxos de trabalho para diminuir ou bloquear ataques volumétricos
- Gerar alertas sobre tentativas de ataques volumétricos

API5:2023 – Autorização em nível de função corrompida

A autorização em nível de função corrompida (BFLA) pode ocorrer quando modelos de controle de acesso para pontos de extremidade de API são implementados incorretamente. Métodos de controle de acesso incorretos ou desatualizados podem não conseguir restringir adequadamente o acesso não autorizado, permitindo que invasores acessem informações confidenciais ou o sistema como um todo. Para mitigar este risco, as organizações podem adotar o princípio do menor privilégio, garantindo que todas as funções, especialmente as administrativas, sejam acessíveis apenas a usuários com permissões apropriadas.

Como a Akamai pode ajudar

Ao rastrear cronogramas comportamentais, aplicar políticas de segurança a funções confidenciais, gerenciar rotação e revogação de chaves e alertar imediatamente sobre quaisquer tentativas suspeitas, a Akamai pode ajudar a fortalecer a estratégia de prevenção e resposta de BFLA das organizações.

A Akamai mitiga este risco ao:

- Identificar cronogramas comportamentais no acesso ao ponto de extremidade da API por meio da captura de usuário, chaves de API, tokens de acesso, IDs de sessão etc.
- Aplicar rotação ou revogação de chaves expostas por meio de recursos do Akamai API Gateway
- Gerar alertas sobre tentativas suspeitas de acesso às funções administrativas

API6:2023 – Acesso irrestrito a fluxos comerciais confidenciais

O acesso irrestrito a fluxos comerciais confidenciais surge quando uma API expõe operações críticas, como lógica de negócios, sem controle de acesso suficiente. Isso pode levar ao acesso e à exploração não autorizados, causando danos significativos a uma organização. A exploração normalmente envolve a compreensão do modelo de negócios apoiado pela API, a identificação de fluxos de negócios confidenciais e a exploração de brechas nesses fluxos. Isso pode levar a impactos como impedir que usuários legítimos comprem um produto.

Como a Akamai pode ajudar

Proteja seus negócios com as soluções abrangentes de proteção de API da Akamai, que oferecem identificação de pontos de extremidade confidenciais, alertas de exploração em tempo real e consultoria especializada para proteger seus dados e operações críticas.

A Akamai mitiga este risco ao:

- Identificar pontos de extremidade de API confidenciais, como fluxos de pagamento ou pontos de extremidade que lidam com PII
- Gerar alertas sobre uma variedade de explorações potenciais que variam desde a exfiltração até a manipulação de dados e as tentativas suspeitas nesses pontos de extremidade de API confidenciais

API7:2023 – Falsificação de solicitação do lado do servidor

A Falsificação de solicitação no lado do servidor (SSRF) permite que um invasor induza o aplicativo do servidor a fazer solicitações HTTPS para um domínio arbitrário de sua escolha. Em um ataque SSRF típico, o invasor engana o servidor para que ele faça uma solicitação a recursos internos, contornando firewalls e obtendo acesso a serviços internos, o que pode levar à exposição de dados ou à execução remota de código. Para mitigar esse risco, é crucial validar, filtrar ou higienizar a entrada do usuário e limitar as conexões de saída que seu servidor pode fazer, garantindo que ele se comunique apenas com serviços críticos.

Como a Akamai pode ajudar

Fortalecendo sua postura de segurança com a Akamai, fornecendo detecção de anomalias em conexões API confiáveis, gerenciamento eficaz de chaves e notificações imediatas sobre tentativas de exploração de SSRF.

A Akamai mitiga este risco ao:

- Aplicar proteção por meio de políticas de proteção de aplicativos da Web e API, tendo em vista ataques SSRF
- Aplicar rotação ou revogação de chaves expostas por meio de recursos do API Gateway

API8:2023 | Configuração incorreta de segurança

A configuração incorreta de segurança refere-se à configuração inadequada de controles de segurança, que pode deixar um sistema vulnerável a ataques. Isso pode incluir configurações padrão inseguras, configurações incompletas ou ad hoc, armazenamento em nuvem aberto, cabeçalhos HTTP(S) configurados incorretamente e mensagens de erro detalhadas contendo informações confidenciais. Para mitigar os riscos, é vital que as organizações garantam que configuraram corretamente os seus controles de segurança em todos os aspectos de seus aplicativos e APIs. Isso envolve atualizações regulares, testes completos e monitoramento contínuo para identificar e corrigir prontamente quaisquer configurações incorretas.

Como a Akamai pode ajudar

Aprimorando seus insights à medida que ajuda você a identificar APIs "sombra", "rogue" ou "zumbis" com detecção de ponto de extremidade, alinhar-se às práticas recomendadas de segurança, obter uma implementação robusta de HTTPS e receber alertas instantâneos sobre configurações incorretas de segurança.

A Akamai mitiga este risco ao:

- Identificar pontos de extremidade de API "sombra" que podem expor ambientes de baixo nível, como ambientes de teste e preparação
- Identificar e fazer a correspondência de pontos de extremidade, objetos e propriedades de API às melhores práticas e padrões de configuração de segurança
- Aplicar políticas de segurança por meio de práticas recomendadas de segurança de API, como solicitações e respostas HTTPS bem formadas, configurar ou remover cabeçalhos HTTP corretos, bem como controlar totalmente o compartilhamento de recursos de origem cruzada (CORS) e cabeçalhos de controle de cache
- Aplicar implementação HTTPS adequada por meio de SSL/TLS, incluindo conjuntos de criptografia corretos e seguros
- Gerar alertas de configuração incorreta ou falta de conformidade com as práticas recomendadas e padrões de segurança de API

API9:2023 – Gerenciamento inadequado de inventário

O gerenciamento inadequado de inventário é um desafio para todas as organizações que lidam com APIs. As soluções de segurança de API podem proteger as APIs conhecidas, mas as desconhecidas, inclusive as APIs "sombra", podem ficar sem patches e vulneráveis a ataques. Isso pode levar a componentes desatualizados, páginas ou APIs não utilizadas e exposição desnecessária de informações confidenciais. O gerenciamento de serviços sem manutenção pode tornar os sistemas vulneráveis a ameaças, e os invasores podem obter acesso a dados confidenciais ou até mesmo ao servidor por meio de APIs desconhecidas conectadas ao mesmo banco de dados. Os controles de acesso e as auditorias regulares são essenciais para evitar os componentes em constante mudança dos serviços de uma organização.

Como a Akamai pode ajudar

A Akamai supervisiona constantemente o tráfego de API para descobrir pontos de extremidade de API ocultos e APIs com classificação de risco para fornecer armazenamento seguro de dados, análise avançada de ameaças e alertas imediatos sobre possíveis explorações.

A Akamai mitiga este risco ao:

- Monitorar continuamente o tráfego de API exposto que flui por meio de seus ambientes, incluindo pontos de extremidade de API do norte ao sul visando APIs publicamente acessíveis e pontos de extremidade internos de API do leste ao oeste
- Identificar pontos de extremidade de API "sombra" que podem expor ambientes de baixo nível, como ambientes de teste e preparação, ou versões de API não documentadas e/ou obsoletas
- Criar um inventário de API atualizado com base na pontuação de risco e classificação de dados
- Gerar alertas sobre uma variedade de explorações potenciais que variam desde a exfiltração até a manipulação de dados e as tentativas suspeitas nesses pontos de extremidade de API confidenciais

API10:2023 – Consumo inseguro de APIs

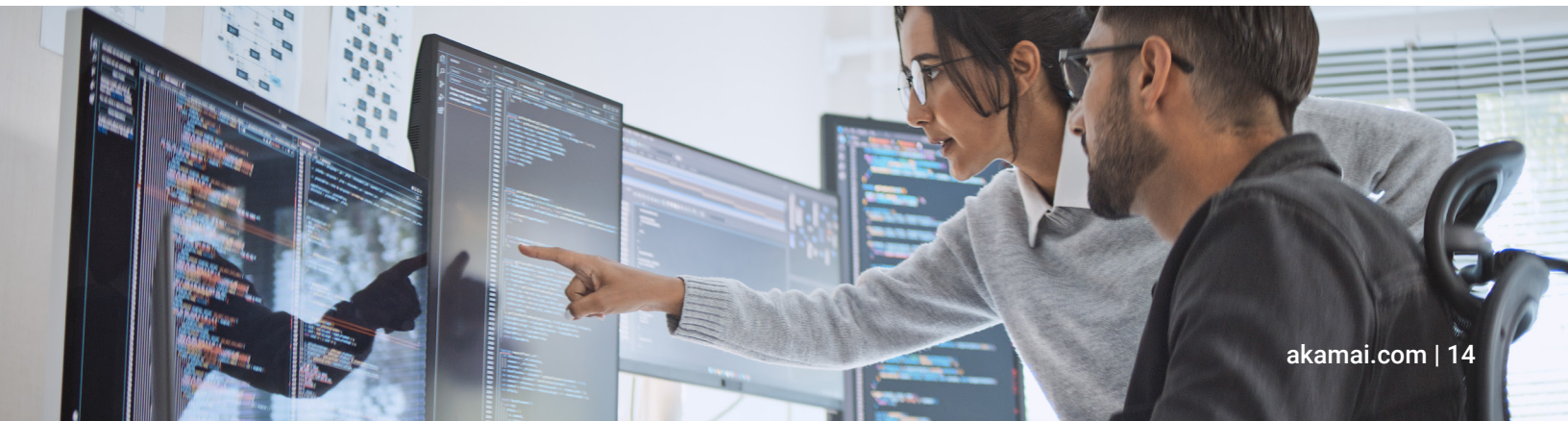
O consumo inseguro de APIs refere-se aos riscos associados ao uso de APIs de terceiros sem que medidas de segurança adequadas estejam em vigor. As organizações dependem cada vez mais de APIs de terceiros para ampliar serviços e funcionalidades, portanto, essas APIs costumam ser confiáveis por padrão. Isso pode levar a vulnerabilidades de segurança significativas. A não implementação adequada de criptografia, validação de dados, sanitização e limites de consumo de recursos pode expor as organizações a vulnerabilidades significativas. Para mitigar esses riscos, as organizações podem implementar criptografia para todos os dados transmitidos pela rede, validar e higienizar todas as entradas de dados e definir limites razoáveis para o consumo de recursos.

Como a Akamai pode ajudar

Proteja continuamente seus sistemas monitorando e validando seus serviços para garantir a segurança com os serviços de monitoramento, alertas e consultoria da Akamai.

A Akamai mitiga este risco ao:

- Monitorar continuamente todo o tráfego de API exposto, que flui por meio de seus ambientes, incluindo APIs do leste ao oeste e de saída, que facilitam integrações B2B (Business-to-business) e/ou de terceiros
- Gerar alertas sobre uma variedade de explorações potenciais que variam desde a exfiltração até a manipulação de dados e as tentativas suspeitas nesses pontos de extremidade de API confidenciais
- Aplicar segurança por meio de políticas de proteção de API e aplicativos da Web, que visam uma variedade de ataques de API coletados em grupos de ataque



Riscos de segurança adicionais do OWASP

A edição da lista Top 10 API Security Risks de 2023 do OWASP foi a primeira grande atualização da organização sem fins lucrativos para sua lista desde 2019. Vale a pena voltar atrás e revisar a lista original, que aborda outros riscos de segurança, como ataques de injeção, que ainda são relevantes no cenário atual.

A Akamai pode ajudar com essa ameaça de segurança ao:

- Identificar pontos de extremidade vulneráveis à injeção de API e tentativas de injeção combinando assinaturas e detectando anomalias
- Aplicar políticas de segurança por meio de inspeção JSON e XML de solicitações de API e verificação de uma variedade de ataques de injeção, como SQLi, XSS, CMDi, RFI (inclusão de arquivo remoto) e LFI
- Gerar alertas sobre exploração de injeção

O OWASP também divulgou listas de outras 10 principais ameaças de segurança, como as 10 principais ameaças de segurança de aplicativos da Web do OWASP. O portfólio de segurança da Akamai também pode ajudar a mitigar essas ameaças de segurança.

Estamos aqui para ajudar!

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

A Akamai fornece soluções de segurança líderes do setor, especialistas altamente experientes e uma plataforma que coleta insights de milhões de ataques a aplicativos da Web e API, bilhões de solicitações de bots e até trilhões de solicitações de API todos os dias.

As soluções de segurança de aplicativos da Web e APIs da Akamai ajudarão a proteger sua organização contra as formas mais avançadas de ataques de DDoS, com base em API e a aplicativos da Web. Além disso, o Akamai Managed Security Service oferece monitoramento 24 horas por dia, 7 dias por semana, gerenciamento de segurança e mitigação de ameaças.

Para saber mais sobre o portfólio de segurança da Akamai, consulte as informações detalhadas em nosso website. Se você quiser discutir e explorar com mais detalhes como podemos fazer parceria para criar a melhor proteção para sua empresa, entre em contato com seu representante de vendas da Akamai hoje mesmo.

As soluções de segurança da Akamai protegem os aplicativos que impulsionam seus negócios em cada ponto de interação, sem comprometer o desempenho ou a experiência do cliente. Ao aproveitar a escala de nossa plataforma global e sua visibilidade de ameaças, trabalhamos com você para evitar, detectar e mitigar ameaças, permitindo que você construa a confiança na sua marca e opere de acordo com a sua visão. Saiba mais sobre as soluções de computação em nuvem, segurança e entrega de conteúdo da Akamai em akamai.com e akamai.com/blog, ou siga a Akamai Technologies no X, antigo Twitter, e LinkedIn. Publicado em 09/24.