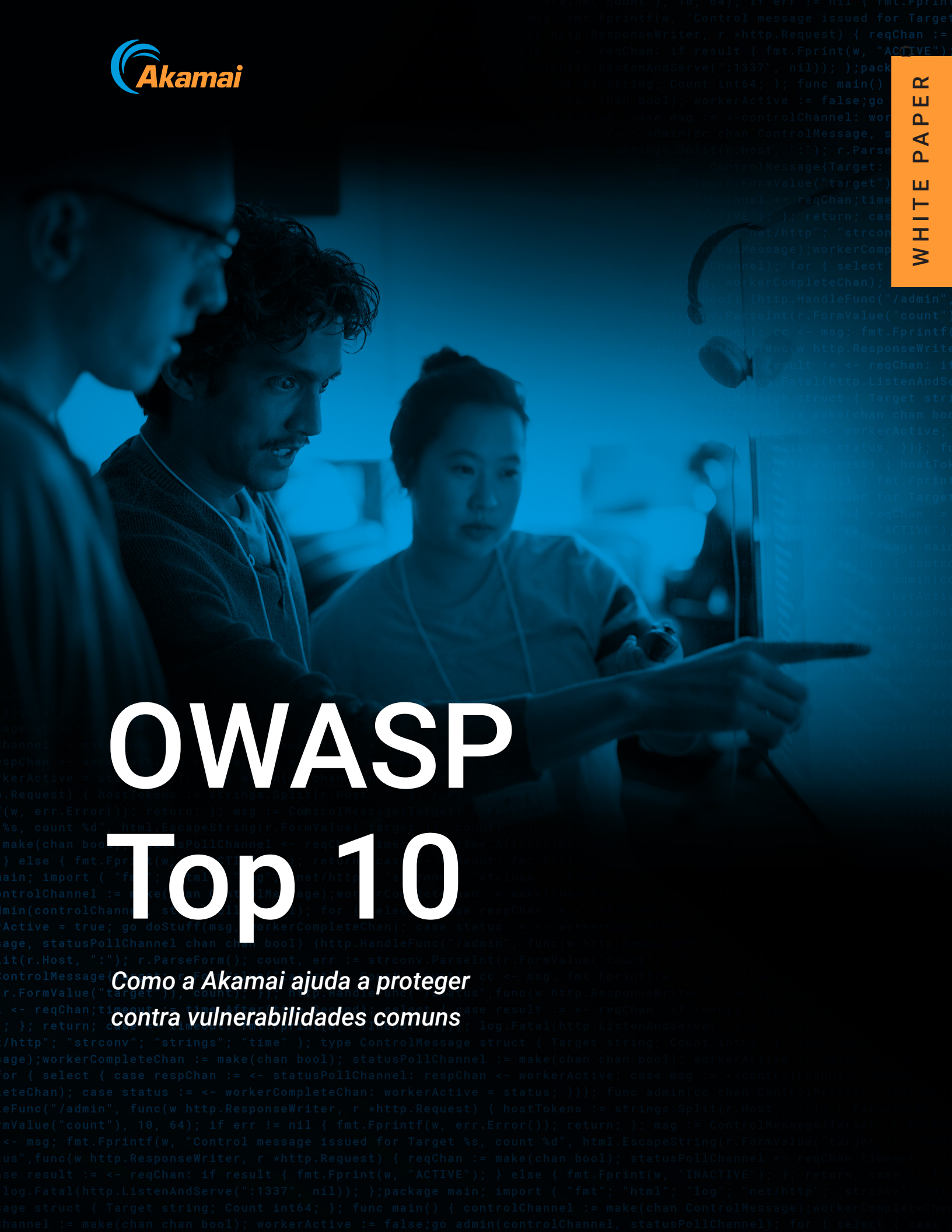
Akamai

WHITE PAPER



OWASP Top 10

Como a Akamai ajuda a proteger contra vulnerabilidades comuns

Introdução

O documento OWASP (Open Web Application Security Project, Projeto Aberto de Segurança em Aplicações Web) Top 10 abrange as vulnerabilidades mais comuns vistas em aplicações da Web, aumentando a conscientização das organizações. Aproveitar ao máximo o documento OWASP Top 10 requer a compreensão de onde, como e quanto os fornecedores de segurança podem ajudar a aumentar as melhorias em suas próprias práticas de desenvolvimento. O detalhamento a seguir das 10 principais vulnerabilidades do OWASP descreve cada uma delas e explica como a Akamai pode ajudar as organizações com soluções de segurança de edge, serviços gerenciados e a maior plataforma de edge inteligente do mundo.

Produtos Akamai

OWASP Top 10		Account Protector	Akamai Guardicore Segmentation	App & API Protector	Bot Manager	Enterprise Application Access	Enterprise Threat Protector	Identity Cloud	Managed Security Services	Akamai MFA	Page Integrity Manager
Controle de acesso interrompido	A01			✓	✓	✓		✓		✓	
Falhas criptográficas	A02			✓		✓	✓				✓
Injeção	A03			✓							
Projeto vulnerável	A04			✓		✓					
Má configuração de segurança	A05		✓	✓	✓						
Componentes vulneráveis e desatualizados	A06		✓	✓							✓
Falhas de identificação e autenticação	A07	✓		✓	✓	✓		✓		✓	
Falhas de integridade de software e dados	A08		✓	✓			✓				✓
Falhas no registro de segurança e monitoramento	A09		✓	✓		✓	✓		✓		
Falsificação de solicitação do lado do servidor	A10		✓	✓							

O OWASP Top 10 lista as principais categorias de riscos, não riscos individuais. As soluções da Akamai abordam essas categorias de risco de várias maneiras. Leia o white paper para saber mais.

A01: Controle de acesso interrompido

> "O controle de acesso aplica a política de modo que os usuários não possam agir fora de suas permissões pretendidas. Falhas geralmente levam à divulgação não autorizada de informações, modificação ou destruição de todos os dados ou à realização de uma função de negócios fora dos limites do usuário."
>
> — Fonte: owasp.org

Como a Akamai ajuda

Embora as organizações precisem corrigir seu modelo de controle de acesso para resolver totalmente a vulnerabilidade de Controle de Acesso interrompido, a experiência da Akamai em WAAP pode ajudá-lo a detectar e proteger contra alguns dos vetores de ataque que tentam explorá-la:

- O **Enterprise Application Access** possibilita um modelo de acesso com menos privilégios para usuários corporativos, permitindo apenas visibilidade e acesso para aplicações autorizadas por usuários autenticados, o que suporta um modelo de segurança Zero Trust.
- O **Akamai MFA** fornece serviços de autenticação sólidos com base em padrões de tecnologia FIDO2 resistentes a phishing.
- O **App & API Protector**, a solução WAAP da Akamai, pode ajudar a bloquear ataques contundentes ao navegador, verificando o cabeçalho "Referer" e reforçando a autenticação de APIs para fortalecer o controle de acesso com o Akamai API Gateway.
- O **Identity Cloud** fornece controles de acesso granulares aos dados do usuário final, permitindo acesso com menos privilégios por usuário interno ou sistema.
- O **Bot Manager** impede ataques automatizados de ferramentas e de login.

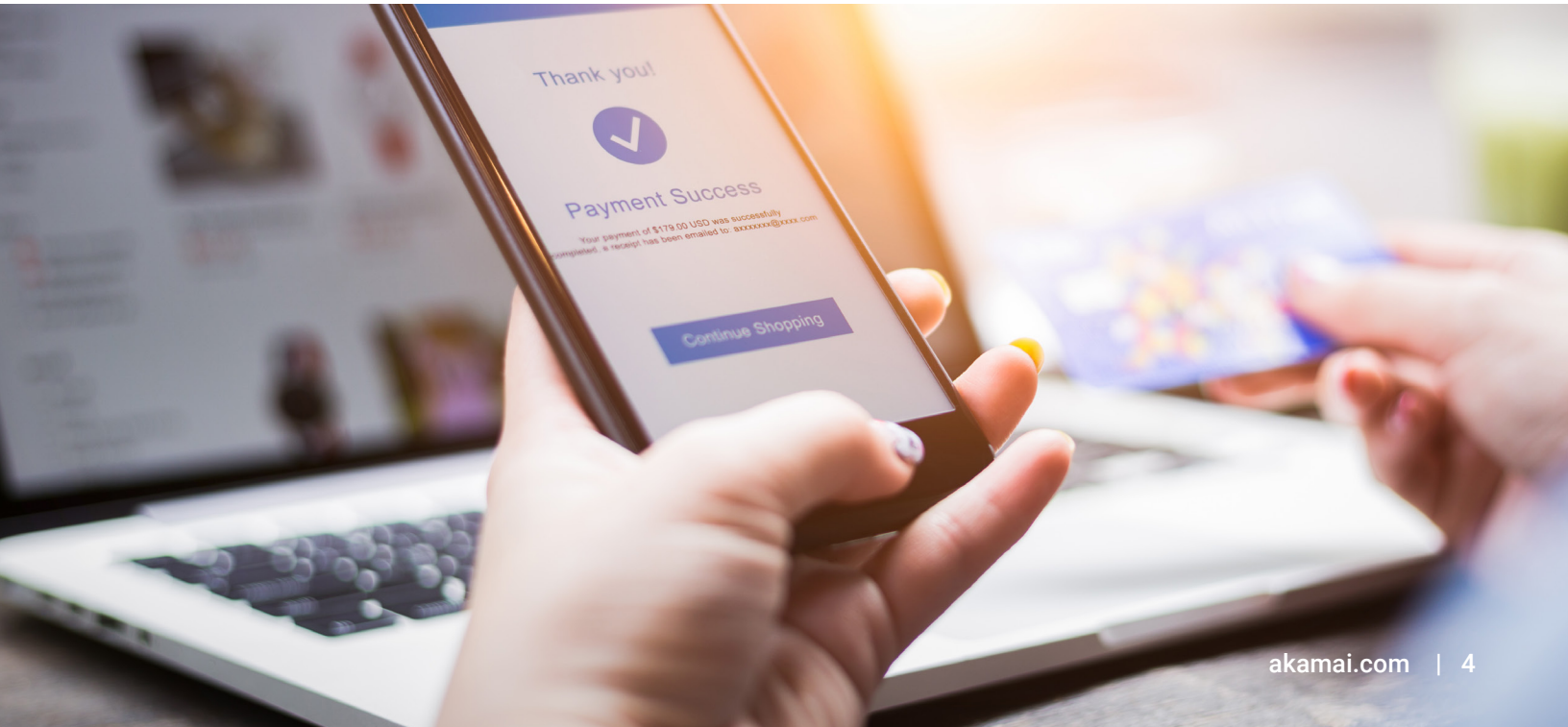
A02: Falhas criptográficas

> "O foco está em falhas relacionadas à criptografia (ou falta dela). Que geralmente levam à exposição de dados confidenciais. … Por exemplo, senhas, números de cartão de crédito, prontuários médicos, informações pessoais e segredos comerciais exigem proteção extra, principalmente se esses dados estiverem sob as leis de privacidade."
>
> — Fonte: owasp.org

Como a Akamai ajuda

As organizações não podem se proteger totalmente contra falhas criptográficas usando uma única solução de segurança. No entanto, a combinação de várias soluções pode ajudar a resolver alguns aspectos dessa vulnerabilidade. Por exemplo, a Akamai oferece:

- O **App & API Protector**, que criptografa e protege dados confidenciais em trânsito com as versões mais recentes de TLS e cifras fortes. Também ajuda a:
  - Manter a conformidade com PCI servindo exclusivamente de uma CDN segura, que suporta todos os certificados TLS de marca e protege as chaves particulares de um cliente.
  - Oferecer uma CDN protegida por segurança operacional e física, como racks em gaiolas e detectores de movimento, que garantam que apenas pessoal autorizado possa acessar os servidores.
  - Localizar e evitar vazamentos de dados confidenciais com o aprendizado de PII da API.
- O **Enterprise Application Access** pode proteger o acesso remoto criptografando a comunicação e ocultando dados confidenciais de olhares curiosos na rede.
- O **Enterprise Threat Protector** pode ajudar a evitar a exposição de dados confidenciais.
- O **Page Integrity Manager** também pode detectar vazamentos de dados PII por meio do uso indevido de código JavaScript que poderia ter resultado de falhas criptográficas.



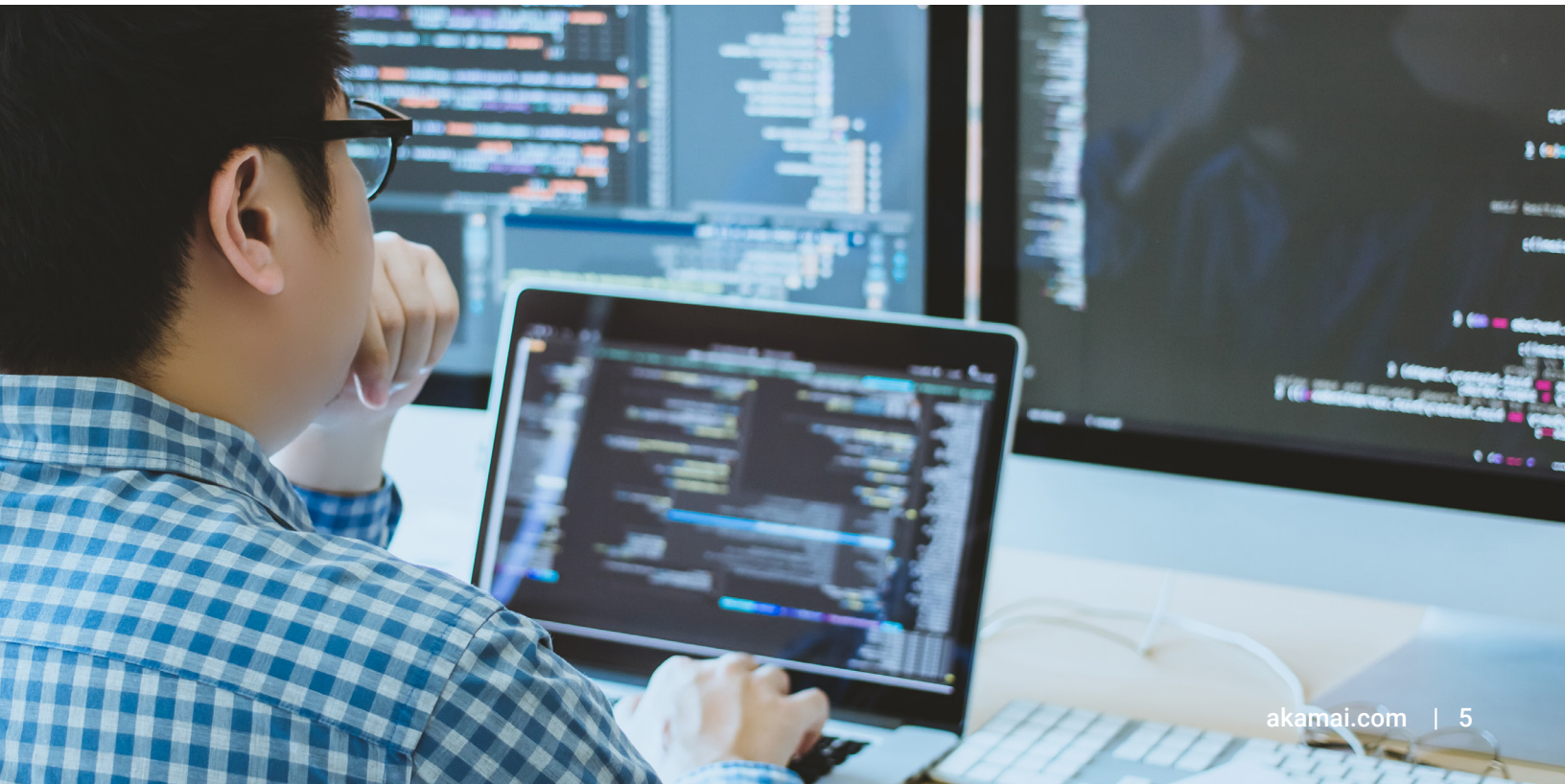
A03: Injeção

> "Falhas de injeção, como injeção de SQL, NoSQL, SO e LDAP, ocorrem quando dados não confiáveis são enviados a um intérprete como parte de um comando ou consulta. Os dados hostis do invasor podem induzir o intérprete a executar comandos não intencionais ou acessar dados sem a devida autorização."
>
> — Fonte: Akamai

Como a Akamai ajuda

Você pode usar o WAAP para reduzir o risco de falhas de aplicação Web e injeção de API. No entanto, as organizações devem sempre corrigir aplicações Web para solucionar quaisquer vulnerabilidades descobertas com base nos respectivos ciclos de vida de desenvolvimento.

- O **App & API Protector** oferece uma solução WAAP líder do setor com um mecanismo de segurança adaptável (ASE), que oferece ampla proteção contra ataques de injeção usando regras existentes e prontas para uso. A caixa de penalidade ASE pode bloquear temporariamente todo o tráfego proveniente de clientes que tentaram recentemente um ataque de injeção usando WAAP.
- A aplicação virtual de patches com regras personalizadas pode ajudar a resolver rapidamente vulnerabilidades de injeção emergentes ou novas vulnerabilidades expostas a partir de alterações de aplicações até que a aplicação possa ser corrigida. As organizações de segurança também podem automatizar a aplicação de patches virtuais e integrá-la aos processos do DevSecOps aproveitando os recursos de API da Akamai.
- O **Client Reputation** pode ajudar a identificar e bloquear ataques baseados em injeção e fornece uma pontuação de risco para clientes mal-intencionados altamente ativos na categoria de invasores da Web.



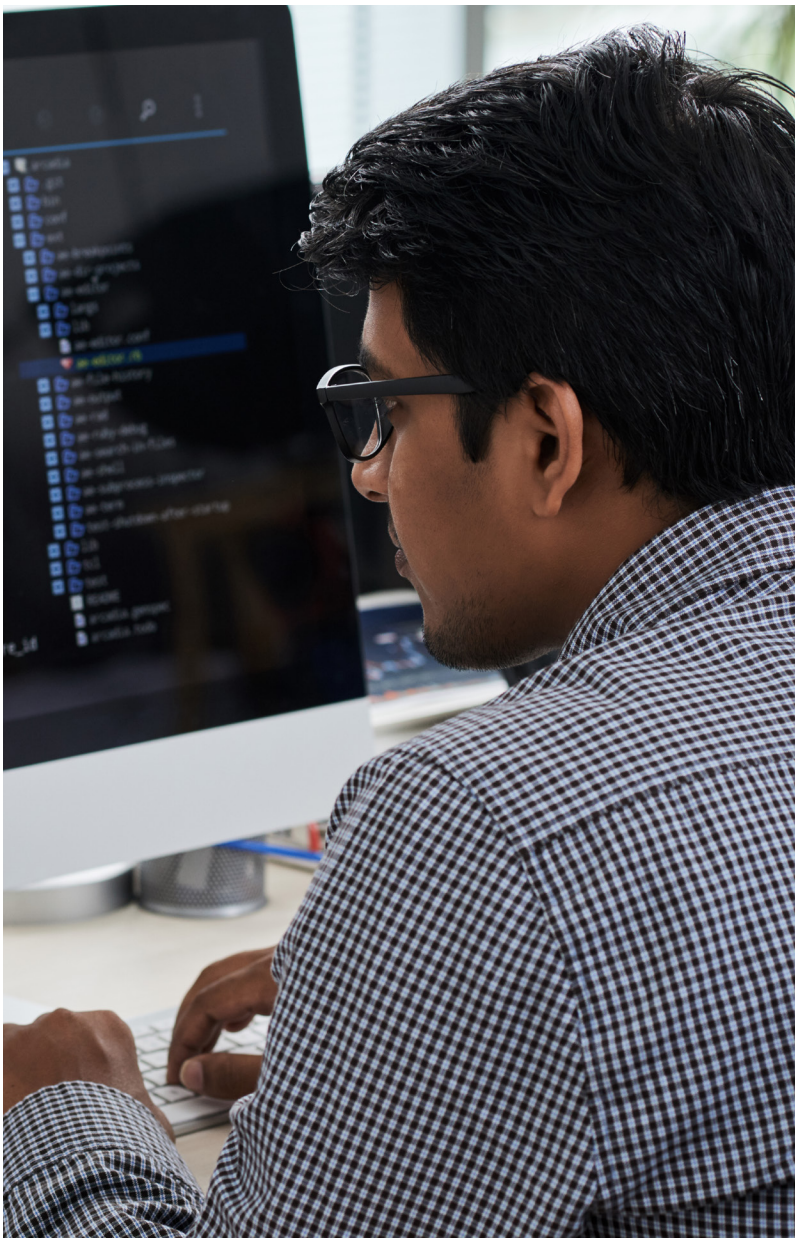
A04: Projeto vulnerável

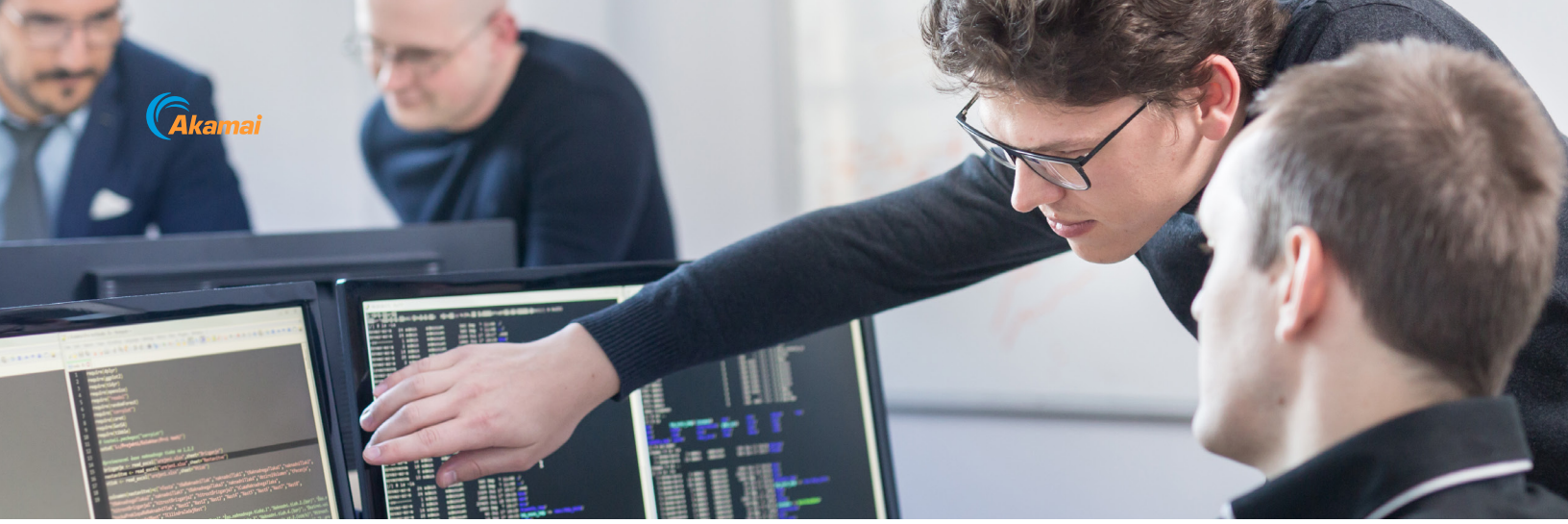
> "O projeto vulnerável é uma categoria ampla que representa diferentes pontos fracos, expressos como 'projeto de controle simples ou ineficaz'. Há uma diferença entre o projeto vulnerável e a implementação vulnerável. Um projeto seguro ainda pode ter defeitos de implementação que levam a vulnerabilidades que podem ser exploradas. Um projeto vulnerável não pode ser corrigido por uma implementação perfeita, pois, por definição, os controles de segurança necessários nunca foram criados para se defender contra ataques específicos."
>
> — Fonte: owasp.org

Como a Akamai ajuda

As organizações devem integrar a segurança desde os primeiros estágios do projeto. No entanto, as equipes de desenvolvimento podem ter dificuldades para realizar isso se a segurança for difícil de incorporar. Os produtos da Akamai ajudam as organizações a se deslocarem mais rápido para evitar que as inseguranças de projeto comprometam suas aplicações e APIs.

- O **App & API Protector**, que compreende nossa solução WAAP e ASE, também pode detectar e corrigir algumas falhas de projeto que chegam à produção. Ele também aproveita a automação para descarregar e simplificar tarefas de rotina, deixando aquelas que exigem análise humana para humanos. Essa automação inclui atualizações automáticas, autoajuste, descoberta de API, programabilidade simplificada e experiência do usuário.
- O **Enterprise Application Access** garante que somente usuários autorizados possam acessar aplicações. Essa abordagem de menos privilégios impede a movimentação lateral para outras aplicações, o que pode acontecer facilmente com soluções de acesso à rede, como VPNs.





A05: Má configuração de segurança

> "[Desde] a edição anterior, 90% das aplicações foram testadas para alguma forma de configuração incorreta, com uma taxa de incidência média de 4% e mais de 208 mil ocorrências de uma Enumeração de fraqueza comum (CWE) nesta categoria de risco. Sem um processo de configuração de segurança de aplicações coordenado e repetível, os sistemas estão em maior risco."
>
> — Fonte: owasp.org

Como a Akamai ajuda

Por definição, a configuração incorreta de segurança abrange vários aspectos da segurança de aplicações. Ela também exige que as organizações configurem corretamente os controles de segurança. Os produtos da Akamai ajudam das seguintes maneiras:

- Embora não substitua a configuração adequada, o **App & API Protector** pode ajudar ao:
  1. Usar grupos de ataque de anomalia de saída para detectar vazamento de informações, como códigos de erro, bem como código-fonte resultante de configurações incorretas de segurança que já existem.
  2. Implementar regras que podem detectar e interromper ataques XXE antes que o analisador XML processe a entidade externa perigosa.
  3. Implementar regras para detectar o acesso a arquivos confidenciais conhecidos deixados por desenvolvedores nos servidores de produção.
- O **Akamai Guardicore Segmentation** ajuda a proteger contra vazamento de dados devido a configurações incorretas, fornecendo visibilidade e controle granular sobre qualquer comunicação não autorizada ou não planejada entre seus aplicativos e a Internet.
- A aplicação virtual de patches com regras personalizadas pode ajudar a resolver rapidamente o vazamento de dados detectado até que sua equipe possa corrigir a aplicação.
- Com o **App & API Protector** e o **Bot Manager**, os ataques de força bruta usando credenciais padrão podem ser protegidos com controles de taxa.
- A configuração de segurança fraca da Política de segurança de conteúdo e outros cabeçalhos HTTP relevantes para a segurança podem ser reforçadas na plataforma Akamai.
- Com a descoberta automática de API no **App & API Protector**, você pode descobrir e criar o perfil de suas APIs de forma automática e contínua, incluindo ponto de extremidade, definições e características de recursos e tráfego.

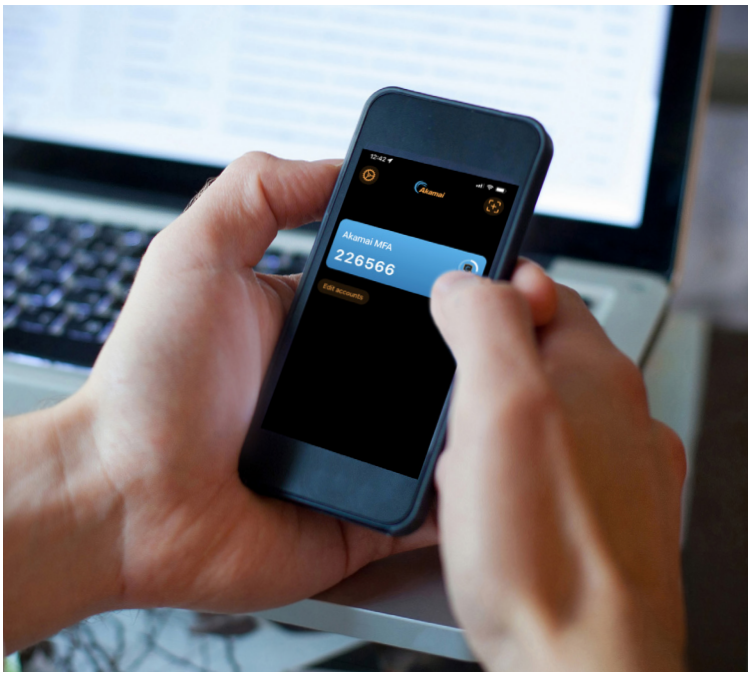
A06: Componentes vulneráveis e desatualizados

> "Componentes como bibliotecas, estruturas e outros módulos de software são executados com os mesmos privilégios da aplicação. Além disso, os scripts agem como recursos de aplicações confiáveis com acesso total aos dados das aplicações. Se um componente vulnerável for explorado, este ataque poderá facilitar uma perda grave de dados ou a tomada de controle do servidor."
>
> — Fonte: Akamai

Como a Akamai ajuda

As organizações geralmente perdem o controle, e as equipes de segurança muitas vezes desconhecem completamente quais componentes de terceiros estão em uso em suas aplicações. Além disso, as organizações não têm controle sobre a rapidez com que o terceiro abordará as vulnerabilidades recém-descobertas. A atenuação dessa falta de visibilidade e segurança requer o uso de uma solução de segurança, como WAAP e proteção de script, como:

- O **App & API Protector** inclui várias regras projetadas para lidar com vulnerabilidades conhecidas, seja especificamente em suas aplicações ou em componentes de terceiros. Ele também fornece recursos de proteção de API, que protegem as APIs mesmo quando componentes de terceiros incorporados à API abrem a API para abuso.



- O módulo de insights **Akamai Guardicore Segmentation** permite consultar quaisquer ativos em sua rede que possam estar vulneráveis. A aplicação granular incluída permite que você delimite qualquer ativo afetado até que um patch seja aplicado.
- A aplicação de patches virtuais com regras personalizadas pode ajudar a resolver rapidamente as vulnerabilidades emergentes ou novas vulnerabilidades expostas por alterações na aplicação até que a aplicação possa ser corrigida.
- O **Client Reputation** fornece uma classificação de risco para clientes mal-intencionados na categoria de verificação na web para ajudar a proteger contra a exploração de novas vulnerabilidades.
- O **Page Integrity Manager** analisa constantemente o comportamento da execução de scripts, em sessões de usuário reais, para identificar comportamentos mal-intencionados suspeitos ou incertos. Ele também bloqueia a exfiltração de dados de scripts primários e de terceiros para URLs com vulnerabilidades conhecidas usando um banco de dados Common Vulnerabilities and Exposures (CVE) constantemente atualizado.

A07: Falhas de identificação e autenticação

> "As funções de aplicações relacionadas à autenticação e ao gerenciamento de sessão geralmente são implementadas incorretamente, permitindo que invasores comprometam senhas, chaves ou tokens de sessão, ou explorem outras falhas de implementação para assumir as identidades de outros usuários de forma temporária ou permanente."
>
> — Fonte: Akamai

Como a Akamai ajuda

As organizações devem corrigir lapsos para resolver totalmente essa vulnerabilidade. No entanto, as soluções da Akamai listadas abaixo podem ajudar a detectar e proteger contra muitos dos vetores de ataque que tentam explorar falhas de identificação e autenticação:

- O **Bot Manager** pode detectar e mitigar ataques automatizados, como os usados em ataques de preenchimento de credenciais.
- O **Account Protector** atenua as tentativas de controle de contas em que os impostores tentam obter acesso não autorizado a contas de usuários.
- O **Enterprise Application Access** pode proporcionar acesso por proxy às aplicações por meio de um "modelo de acesso com privilégios mínimos", reduzindo a superfície de ataque da aplicação e aprimorando o acesso.
- O **Akamai MFA** fornece autenticação sólida usando a tecnologia FIDO2 resistente a phishing.
- O **App & API Protector** fornece um recurso de controle de taxa, que pode lidar com ataques de força bruta.
- O **Identity Cloud** oferece gerenciamento seguro de credenciais de usuário final e informações de perfil protegidas por autenticação de dois fatores e recursos de autenticação baseada em risco.

A08: Falhas de integridade de software e dados

> "As falhas de integridade de software e dados estão relacionadas ao código e à infraestrutura que não protege contra violações de integridade. Um exemplo disso é quando uma aplicação depende de plug-ins, bibliotecas ou módulos de fontes não confiáveis, repositórios e CDNs (Content Delivery Networks, redes de entrega de conteúdo). Um pipeline de CI/CD vulnerável pode introduzir o potencial de acesso não autorizado, código mal-intencionado ou comprometimento do sistema."
>
> — Fonte: owasp.org

Como a Akamai ajuda

As organizações podem usar o WAAP para proteger aplicações da Web e APIs contra falhas de integridade de software e dados. No entanto, as organizações devem sempre corrigir aplicações Web para solucionar quaisquer vulnerabilidades descobertas com base no ciclo de vida de desenvolvimento.

- **App & API Protector**
  - Oferece proteção sólida contra ataques de desserialização.
  - Impede ataques MITM (machine-in-the-middle) que podem resultar em problemas de integridade de dados por meio da implementação das versões mais recentes de TLS e cifras fortes.
  - Garante a autenticação da origem dos dados e a proteção da integridade dos dados dos registros DNS implementando DNSSEC com o Edge DNS. Isso impede a adulteração de registros DNS que podem direcionar os usuários a fontes não confiáveis.
- O módulo de insights no **Akamai Guardicore Segmentation** permite que você consulte quaisquer ativos em sua rede que tenham recebido a atualização corrompida. A aplicação granular incluída permite que você delimite esses ativos afetados até que uma correção seja criada.
- O **Enterprise Threat Protector** detecta ataques de phishing, que podem atrair administradores e superusuários das aplicações para ambientes hostis ou fontes não confiáveis.
- A aplicação de patches virtuais com regras personalizadas pode ajudar a resolver rapidamente novas falhas de desserialização até que a aplicação possa ser corrigida.
- O **Page Integrity Manager** detecta scripts de terceiros, monitora-os quanto a alterações e, em seguida, executa ações em scripts que foram comprometidos.

A09: Falhas no registro de segurança e monitoramento

"Registro, detecção, monitoramento e resposta ativa insuficientes ocorrem a qualquer momento:

- Eventos auditáveis, como logins, logins com falha e transações de alto valor, não são registrados.
- Avisos e erros não geram mensagens de log ou geram mensagens inadequadas ou pouco claras.
- Os registros de aplicações e APIs não são monitorados quanto a atividades suspeitas.
- Os registros são armazenados apenas localmente.
- Os limites de alerta apropriados e os processos de escalação de resposta não estão em vigor ou não são eficazes.
- Testes de penetração e varreduras por ferramentas de teste dinâmico de segurança de aplicações (DAST) não acionam alertas.

A aplicação não pode detectar, escalar ou alertar sobre ataques em tempo real ou quase em tempo real."

— Fonte: owasp.org

Como a Akamai ajuda

As falhas no registro de segurança e monitoramento apresentam uma lacuna na capacidade de uma organização de resolver vulnerabilidades e tentativas de explorá-las. A Akamai oferece vários recursos para fornecer às organizações maior visibilidade dos ataques, incluindo:

- A Akamai fornece painéis e ferramentas de geração de relatórios na interface gráfica do usuário do Akamai Control Center.
- Os produtos de segurança de aplicações da Akamai se integram à infraestrutura SIEM existente de uma organização para correlacionar eventos detectados pela Akamai com os de outros fornecedores de segurança.
- O **Managed Security Service** fornece recursos de análise e resposta 24 horas por dia, 7 dias por semana.
- O **App & API Protector** inclui um recurso de caixa de penalidade que permite o aumento do registro de IPs que mostraram atividades maliciosas ou suspeitas para análises mais detalhadas.
- O **Enterprise Application Access** fornece uma solução integrada de gerenciamento de identidade para autenticar e controlar o acesso a todas as aplicações corporativas. Quando combinada ao recurso de Proxy com reconhecimento de identidade, as organizações podem obter visibilidade detalhada das ações do usuário, incluindo a visibilidade de todas as ações GET/POST.
- O **Enterprise Threat Protector** permite total visibilidade de todas as solicitações de DNS externas de uma empresa, mal-intencionadas e benignas.
- O **Akamai Guardicore Segmentation** fornece visibilidade profunda dos fluxos de comunicação em sua rede, para que os alertas possam ser acionados quando ocorrer uma comunicação não autorizada ou inesperada, e as políticas de segurança possam ser aplicadas no processo individual ou no nível de serviço para restringir essa comunicação. Com o módulo de detecção de violação adicionado, ameaças em potencial podem ser detectadas e corrigidas rapidamente.

A10: Falsificação de solicitação do lado do servidor

> "Falhas de SSRF ocorrem sempre que uma aplicação da Web está buscando um recurso remoto sem validar o URL fornecido pelo usuário. Ele permite que um invasor faça com que a aplicação envie uma solicitação criada a um destino inesperado, mesmo quando protegido por um firewall, VPN ou outro tipo de lista de controle de acesso à rede (ACL)."
>
> — Fonte: owasp.org

Como a Akamai ajuda

O WAAP da Akamai inclui regras que podem procurar a injeção de URLs. Esse recurso pode impedir que os invasores induzam o servidor a ir para outro lugar e enviar uma solicitação, ou seja, fazer com que pareça uma solicitação válida para seus analistas de segurança.

- As regras do **App & API Protector** ajudam a impedir que essas solicitações de exploração cheguem ao servidor vulnerável em primeiro lugar.
- O **Akamai Guardicore Segmentation** pode monitorar e bloquear tráfego de saída inesperado no nível do servidor.

Conclusão

Criar a melhor defesa contra as 10 principais vulnerabilidades do OWASP requer que as organizações e seus fornecedores de segurança trabalhem juntos para eliminar vulnerabilidades o mais rápido possível e implementar soluções para atenuá-las. Saiba mais sobre o portfólio de segurança de edge da Akamai. Se você quiser discutir e explorar como podemos estabelecer uma parceria para criar a melhor proteção para sua empresa, entre em contato com seu representante de vendas da Akamai.

A Akamai potencializa e protege a vida online. As principais empresas do mundo escolhem a Akamai para criar, entregar e proteger suas experiências digitais, ajudando bilhões de pessoas a viver, trabalhar e jogar todos os dias. Com a plataforma de computação mais distribuída do mundo, da nuvem à edge, nós facilitamos o desenvolvimento e a execução de aplicações para os nossos clientes, enquanto mantemos as experiências mais próximas dos usuários e as ameaças ainda mais distantes. Saiba mais sobre as soluções de segurança, computação e entrega da Akamai em akamai.com e akamai.com/blog ou Akamai Technologies no Twitter e LinkedIn. Publicado em 10/22.