Fernando Silva Follow

Sep 27, 2021 · 5 min read

OWASP Top 10–2021: O que mudou?

Fonte: https://www.owasptopten.org/the-release-of-the-owasp-top-10-2021

> *A equipe de líderes da OWASP anunciou o lançamento do OWASP Top 10: 2021 em 24 de setembro de 2021*

Introdução

O OWASP Top 10 é um documento padrão de conscientização para desenvolvedores e segurança de aplicações web. Ele representa um amplo consenso sobre os riscos de segurança mais críticos para aplicações web.

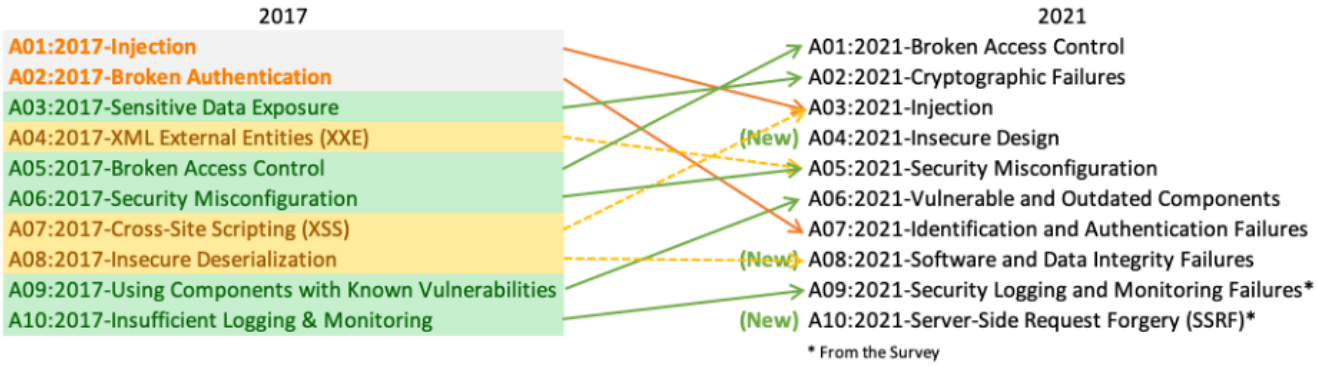
Recentemente, o OWASP publicou uma nova lista das 10 principais vulnerabilidades comuns de aplicações web:

Fonte: https://www.owasptopten.org/the-release-of-the-owasp-top-10-2021

Esta lista é bastante diferente da lista de 2017, com algumas novas adições e algumas categorias foram mescladas em uma categoria maior para refletir a causa raiz em vez de sintomas. Considerando, por exemplo, a exposição de dados confidenciais, sendo um sintoma, enquanto as falhas criptográficas são a causa raiz.

O que mudou no Top 10 2021?

Existem três novas categorias, quatro categorias com alterações de nomenclatura, escopo e algumas consolidações entre as 10 principais vulnerabilidades para 2021. Algumas nomenclaturas também foram alteradas para focar na causa raiz em vez do sintoma.



Fonte: https://owasp.org/Top10/

A01: 2021 — Broken Access Control passou da quinta posição para a categoria com o risco de segurança de aplicações web mais séria. Os dados indicam que, em

ocorrências em aplicações do que qualquer outra categoria.

A02: 2021 — Cryptographic Failures subiu uma posição, foi para a 2ª posição, anteriormente conhecida como **A3: 2017-Sensitive Data Exposure**, que era um sintoma amplo, e não uma causa raiz. O foco aqui está nas falhas relacionadas à criptografia, que geralmente levam à exposição de dados confidenciais ou comprometimento do sistema.

A03: 2021 — Injection foi para a 3ª posição. Conforme os relatórios da OWASP, 94% das aplicações foram testadas para alguma forma de injeção com uma taxa de incidência máxima de 19%, uma taxa de incidência média de 3,37% e os 33 CWEs mapeados nesta categoria têm o segundo maior número de ocorrências em aplicações, com 274 mil ocorrências . Cross-site Scripting agora faz parte desta categoria nesta edição.

A04: 2021 — Insecure Design é uma nova categoria para 2021, com foco em riscos relacionados a falhas de projeto. Se quisermos genuinamente "*move left*", precisamos de mais modelagem de ameaças, padrões e princípios de design seguros e arquiteturas de referência. Um design inseguro não pode ser corrigido por uma implementação perfeita, pois, por definição, os controles de segurança necessários nunca foram criados para a defesa contra ataques específicos.

A05: 2021 — Security Misconfiguration passou da 6ª posição na edição anterior para 5ª posição. Conforme os relatórios da OWASP 90% dos aplicativos foram testados para algum tipo de configuração incorreta, com uma taxa de incidência média de 4,5% e mais de 208 mil ocorrências de CWEs mapeados para esta categoria. Com mais mudanças em software altamente configurável, não é surpreendente ver essa categoria subir. A antiga categoria de **A4: 2017-XML External Entities (XXE)** agora faz parte desta categoria.

A06: 2021 — Vulnerable and Outdated Components era anteriormente intitulado Using Components with Known Vulnerabilities e era o número 2 na pesquisa com a comunidade, mas também tinha dados suficientes para chegar ao Top 10 por meio de análise de dados. Esta categoria passou da 9ª posição em 2017 para 6ª posição e é um problema conhecido que temos dificuldade em testar e avaliar o risco. É a

A07: 2021 — Identification and Authentication Failures (Falhas de identificação e autenticação) anteriormente Broken Authentication, e agora inclui CWEs que estão mais relacionados a falhas de identificação. Essa categoria ainda é parte integrante do Top 10, mas a maior disponibilidade de estruturas padronizadas parece estar ajudando.

A08: 2021 — Software and Data Integrity Failures é uma nova categoria para 2021, com foco em fazer suposições relacionadas a atualizações de software, dados críticos e pipelines de CI/CD sem verificar a integridade. Um dos maiores impactos ponderados dos dados CVE/CVSS mapeados para os 10 CWEs nesta categoria. A **A8:2017-Insecure Deserialization** agora faz parte dessa categoria maior.

A09: 2021 — Security Logging and Monitoring Failures era anteriormente **A10:2017-Insufficient Logging & Monitoring** e foi adicionado a partir da pesquisa com a comunidade (nº 3), passando do nº 10 anterior. Esta categoria foi expandida para incluir mais tipos de falhas, é um desafio para testar e não está bem representada nos dados CVE/CVSS. No entanto, as falhas nesta categoria podem impactar diretamente a visibilidade, o alerta de incidentes e a perícia.

A10: 2021 — Server-Side Request Forgery adicionado da pesquisa com a comunidade (nº 1). Os dados mostram uma taxa de incidência relativamente baixa com cobertura de teste acima da média, junto com classificações acima da média para potencial de exploração e impacto. Essa categoria representa o cenário em que os membros da comunidade de segurança estão dizendo que isso é importante, embora não esteja ilustrado nos dados neste momento.

Conclusão

O cenário de ameaças está mudando rapidamente, com grupos de atores patrocinados pelo estado e hackers profissionais trabalhando em conjunto para explorar os sistemas. O processo de reflexão por trás do novo relatório do OWASP Top 10 2021 é um ótimo passo em direção a um cenário de segurança em constante evolução, onde o foco muda da identificação (e subsequente mitigação) para a prevenção de falhas de segurança através de um design de produto forte e seguro com um foco para alinhar as atividades de AppSec e Secure Development no design

da OWASP Top 10.

Dúvidas e sugestões, fiquem a vontade!