I

Introdução

Bem-vindos

Bem-vindos ao OWASP Top 10! Esta nova versão acrescenta duas novas categorias de vulnerabilidades pela primeira vez: (1) Deficiente Detecção e Prevenção de Ataques e (2) APIs Desprotegidas. Encontramos espaço para estas duas novas categorias através da junção das duas categorias de controlo de acessos (2013-A4 e 2013-A7) na categoria Quebra de Controlo de Acessos (que era a designação original que existia no OWASP Top 10 - 2004), e da remoção da 2013-A10: Reencaminhamentos e Redirecionamentos Não Validados, que havia sido acrescentada no Top 10 em 2010.

O OWASP Top 10 de 2017 baseia-se principalmente em 11 volumosas fontes de dados de empresas que são especializadas em segurança aplicacional, incluindo 8 empresas de consultoria e 3 vendedores de produtos. Estes dados incluem vulnerabilidades recolhidas de centenas de organizações e de mais de 50.000 aplicações e APIs reais. Os itens do Top 10 foram selecionados e ordenados de acordo com estes dados, devidamente combinados com métricas estimadas de exploração, detecção e impacto.

O objectivo principal do OWASP Top 10 é o de educar programadores, desenhadores, arquitectos, gestores e organizações sobre as consequências das mais importantes fraquezas de segurança das aplicações web. O Top 10 oferece técnicas básicas de protecção contra estas áreas problemáticas de risco elevado - e oferece igualmente informação complementar sobre as mesmas.

Avisos

Não fique por estes 10. Existem centenas de outros problemas que podem afetar a segurança de uma aplicação web tais como os que são discutidos no Guia de Programadores do OWASP e na série de guiões do Cheat Sheets do OWASP. Estes dois são de leitura obrigatória para alguém que desenvolva aplicações web e APIs. Orientações sobre como encontrar vulnerabilidades de forma eficiente em aplicações Web e APIs podem ser encontradas no Guia de Testes do OWASP e no Guia de Revisão de Código do OWASP.

Alteração contínua. Este Top 10 vai continuar a mudar. Mesmo sem alterar uma única linha de código da sua aplicação, pode ficar vulnerável uma vez que novas falhas são descobertas e métodos de ataque são refinados. Por favor, verifiquem o conselho no final do Top 10 na secção “O que existe mais para Programadores, Verificadores de Qualidade e Organizações” para mais informação.

Pense positivo. Quando estiver pronto para parar de perseguir vulnerabilidades e focar-se em estabelecer controlos fortes de segurança aplicacional, o OWASP mantém e promove o Standard de Verificação de Segurança Aplicacional (Application Security Verification Standard - ASVS) como um guia para as organizações e revisores aplicacionais sobre o que os mesmos devem verificar.

Use as ferramentas de forma inteligente. As vulnerabilidades de segurança podem ser bastante complexas e estarem enterradas em montanhas de código. Em muitos casos, a abordagem mais eficiente para encontrar e eliminar estas fraquezas é através de seres humanos armados com boas ferramentas.

Empurrar para a esquerda, para a direita, e para todo o lado. Foque-se em fazer da segurança uma parte integral da cultura de desenvolvimento por toda a organização. Pode encontrar mais informação sobre isto no Modelo de Maturidade de Segurança do OWASP (Software Assurance Maturity Model -SAMM) e no “Rugged Handbook”.

Créditos

Gostaríamos de agradecer à Aspect Security for ter iniciado, liderado e atualizado o Top 10 do OWASP desde o seu nascimento em 2003, e aos seus autores principais: Jeff Williams e Dave Wichers.

Desejamos igualmente agradecer às muitas organizações que contribuíram com os seus dados relativos a vulnerabilidades prevalentes e que suportam a actualização de 2017, incluindo as seguintes:

Aspect Security

AsTech Consulting

Aspect Security, AsTech Consulting

Branding Brand Contrast Security Branding Brand, Contrast Security,

EEddgegeScSacnan, iBLISS iBLISS

MMinindeddedSeSceucruitryit,yPaladion NPeatwlaodrioksn, Networks

Softtek

Softtek Vantage Point

Vantage Point, Veracode Veracode

Pela primeira vez, todos os dados que contribuiram para uma versão do Top 10, e a lista completa de contribuidores, está publicamente disponível.

Gostaríamos de agradecer antecipadamente a todos os que contribuíram significativamente com comentários construtivos e tempo nesta revisão do Top 10:

Neil Smithline – por ter produzido produzido a versão wiki desta versão do Top 10, como o havia realizado anteriormente.

Finalmente, gostaríamos ainda de agradecer a todos os tradutores que irão traduzir esta versão do Top 10 em diversas línguas, ajudando a tornar o Top 10 da OWASP mais acessível em todo o planeta.